



## **Cisco Unified Real-Time Monitoring Tool Administration Guide リリース 11.0(1)**

初版：2015年06月08日

### **シスコシステムズ合同会社**

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

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

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

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

**【注意】** シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. 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、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、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、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned 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. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.



## 目次

### はじめに **xxi**

このマニュアルについて **xxi**

対象読者 **xxii**

関連資料 **xxii**

表記法 **xxii**

マニュアルの入手方法およびテクニカル サポート **xxiv**

    シスコ製品のセキュリティ **xxiv**

Organization **xxiv**

### 管理の概要 **1**

Cisco Unified Real-Time Monitoring Tool **1**

オペレーティング システムのサポート **2**

### 使用する前に **5**

Unified RTMT のインストールおよび設定 **5**

    Unified RTMT のインストール **5**

    RTMT のアップグレード **7**

    Unified RTMT の起動 **8**

    管理者として実行 **10**

    Unified RTMT の複数インストール **11**

### 管理ツール **12**

    システム インターフェイス **12**

    パフォーマンス モニタリング **13**

        システム概要の状態 **14**

        サーバステータスのモニタリング **14**

        パフォーマンス カウンタ インターフェイス **16**

        [カテゴリ (Category) ] タブ **16**

        サンプル レート **17**

perfmon カウンタの拡大表示	17
チャートとグラフの強調表示	18
カウンタ プロパティ	19
カウンタのアラート通知	19
Trace and Log Central	20
トレース ファイルの収集、スロットリング、および圧縮	20
設定プロファイル	22
カテゴリ	22
アラート (Alerts)	23
アラート オプション	23
アラート フィールド	24
アラート ログ	28
Log Partition Monitoring Tool	28
Cisco Unified Analysis Manager	30
サービス、サブレット、サービス パラメータ	31
設定できないコンポーネント	33
Unified RTMT のアンインストール	35
システム パフォーマンスのモニタリング	37
事前定義済みのシステム オブジェクト	37
音声およびビデオのモニタリング	41
Cisco Unified Communications Manager の事前定義済みオブジェクト	41
Cisco Unified Communications Manager の [サマリー (Summary)] ビュー	46
コール処理アクティビティのモニタリング	46
コール処理ログ	48
セッション トレースの実行	49
リアルタイム データのモニタリング	50
ローカル ディスクからセッション トレース データのモニタリング	51
コールのトレース	52
サービスのモニタリング	56
サービス ログ	57
デバイス ログ	58
デバイスのモニタリング	59
デバイスのモニタリング	59

モニタする特定デバイスの検索	60
電話情報の表示	62
デバイスプロパティの表示	63
デバイスおよび perfmon カウンタのポーリング レートのセットアップ	63
CTI アプリケーション、デバイス、および回線のモニタリング	64
CTI Manager 情報の表示	64
モニタする CTI アプリケーションの検索	65
モニタする CTI デバイスの検索	66
モニタする CTI 回線の検索	67
アプリケーション情報の表示	68
コール制御検出の学習パターンと SAF フォワーダ レポートへのアクセス	68
着信側トレース レポートへのアクセス	72
Intercompany Media Service	73
IME サービスのモニタリング	73
IME システム パフォーマンスのモニタリング	74
Intercompany Media Service のモニタリング	75
IM and Presence モニタリング	76
IM and Presence および Cisco Jabber サマリーのモニタリング	76
Cisco XCP カウンタ	77
接続されている XMPP クライアントの数	77
接続されている CAXL クライアントの数	77
アクティブな送信 SIP サブスクリプションの数	77
アクティブな着信 SIP サブスクリプションの数	77
IM セッションの数	78
IM パケットの合計	78
直前の 60 秒の IM	79
ユーザごととセッションごとのカウンタ	79
1 セッションごとに送信される IM パケット	80
1 セッションあたりに受信した IM パケット	80
テキスト会議室の合計	80
アドホック グループ チャット ルームの合計	80
永続的なチャット ルームの合計	81

Per-chat room カウンタ	81
ルームごとに受信した IM パケット	81
1 つの会議室あたりの占有者数	81
SIP プロキシのカウンタ	82
アイドル状態の SIP プロキシワーカープロセスの数	82
Cisco Unity Connection のモニタリング	82
ポート モニタ	82
Cisco Unity Connection ポート モニタのポーリングの開始	83
<b>Cisco Unified Analysis Manager</b>	<b>85</b>
Cisco Unified Analysis Manager のプリファレンス	85
FTP サーバのセットアップ	85
FTP サーバ オプションへのアクセス	86
FTP サーバの追加または編集	86
メール サーバのセットアップ	87
メール サーバの追加または編集	88
トレース収集ディレクトリの設定	88
Cisco Unified Analysis Manager の制限事項	89
Cisco Unified Analysis Manager のセットアップ	90
デバイスとグループの設定のインポート	90
スケジュールされた trace and log collection ジョブのステータス表示	90
FTP サーバへのファイルのアップロードと転送	91
Cisco Unified Analysis Manager ツール	92
Analyze Call Path ツール	92
Analyze Call Path ツールのセットアップに関する考慮事項	93
Cisco Unified Communications Manager	94
Cisco Unified Contact Center Express	95
Cisco Unified Intelligent Contact Management Enterprise および Cisco Unified Contact Center Enterprise	96
Cisco Unified Customer Voice Portal	97
Cisco Access Control Server および Cisco IOS Gateway	98
ノード	100
ノード管理	100
ノードのサマリーの表示	100

ノードの追加または編集	101
グループ管理	102
グループの追加または編集	103
トレース ファイル リポジトリの管理	103
トレース ファイル リポジトリの追加または編集	104
コール レコード リポジトリの管理	105
コール レコード リポジトリの追加または編集	105
トレース テンプレートの定義	106
テンプレートの追加または編集	106
コール定義	107
トレース収集	108
今すぐトレースを収集	108
トレース収集のスケジュール	109
トレースの設定と収集のスケジュール	110
トレース レベルの設定	111
設定の表示	113
Cisco Unified Analysis Manager のトラブルシューティング	113
プロファイルとカテゴリ	117
プロファイル	117
設定プロファイルの追加	117
設定プロファイルの復元	118
設定プロファイルの削除	118
カテゴリ	118
カテゴリの追加	118
カテゴリ名の変更	119
カテゴリの削除	120
パフォーマンス カウンタ (Performance Counters)	121
カウンタ	121
パフォーマンス クエリーを使用したカウンタの追加	121
[パフォーマンスの監視 (Performance Monitoring) ] ペインからのカウンタの削除	123
カウンタ インスタンスの追加	123
カウンタ アラート通知のセットアップ	123

カウンタの説明の表示	125
perfmon カウンタ データのローカル ログिंग	125
perfmon カウンタ ログिंगの開始	125
perfmon カウンタ ログिंगの停止	126
データ サンプルの設定	126
カウンタ データの表示	127
Perfmon ログ ビューアおよび Microsoft パフォーマンス ツールのログ ファイル	128
Perfmon ログ ビューアでのログ ファイルの表示	129
パフォーマンス ログ ビューアの拡大と縮小	130
Microsoft パフォーマンス ツールを使用した Perfmon ログ ファイルの表示	131
トラブルシューティング	132
perfmon データ ログのトラブルシューティング	132
Perfmon データ ログिंगのトラブルシューティング	139
アラート (Alerts)	143
Alert Central の表示	143
システム アラート	143
自動トレース ダウンロードのアクティベーション	144
音声およびビデオ アラート	145
IM and Presence Service アラート	147
Cisco Unity Connection アラート	149
アラート アクションのセットアップ	150
Alert Central へのアクセスとアラートのセットアップ	151
アラート プロパティの設定	152
アラートの一時停止	156
コア ダンプのアラートのセットアップと関連ログの収集	156
電子メール アラートの有効化	157
ログの収集	157
トレースとログ	159
Trace and Log Central	159
準備 (Preparation)	159
証明書のインポート	159
トレースのサポートの種類	160



Trace & Log Central におけるディスク I/O と CPU 制御	160
トレース圧縮サポート	160
[Trace & Log Central] オプションの表示	161
ファイルの収集	162
トレース ファイルの収集	162
クエリー ウィザード	166
クエリーの開始	166
クエリーの実行	169
Cisco Unified Communications Manager のトレース収集のスケジュール	171
Cisco Unity Connection のトレース収集のスケジュール	175
スケジュールの開始	178
スケジュールの実行	181
トレース収集ステータスの表示	182
リアルタイム トレース	183
リアルタイム データの表示	183
ユーザ イベントのモニタリング	184
Cisco Unified Communications Manager のクラッシュ ダンプの収集	187
Cisco Unity Connection のクラッシュ ダンプの収集	190
インストール ログの収集	193
監査ログの収集	193
監査ログの参照	193
監査ログのダウンロード	195
監査ログのダウンロードのスケジュール	197
ローカル ブラウズを使用したダウンロード済みトレース ファイルの表示	198
Cisco Unified Communications Manager でのトレース ファイルの表示とダウンロード	199
Cisco Unity Connection でのトレース ファイルの表示とダウンロード	203
トレース収集属性の設定	206
トレース結果の表示	209
レポート情報の表示	211
ログの圧縮	212
トレース設定の編集	213

ログビューア	213
AuditLog ビューア内のメッセージ	213
AuditApp ログの表示	214
Cisco Unified OS ログの表示	215
SysLog ビューアでのメッセージの表示	215
プラグイン	217
アプリケーションプラグインのダウンロードとインストール	217
アプリケーションプラグインの起動	217
パフォーマンス カウンタとアラート	219
システム カウンタ	219
Cisco Tomcat Connector	219
Cisco Tomcat JVM	220
Cisco Tomcat Web Application	221
Database Change Notification Client	222
Database Change Notification Server	223
Database Change Notification Subscription	224
Database Local DSN	224
DB User Host Information カウンタ	224
Enterprise Replication DBSpace Monitors	224
Enterprise Replication Perfmon Counters	225
IP	225
メモリ (Memory)	227
ネットワーク インターフェイス (Network Interface)	229
Number of Replicates Created and State of Replication	231
パーティション	232
プロセス (Process)	233
プロセッサ	235
システム (System)	236
[TCP]	238
Thread	239
AXL Web Service	239
Ramfs	240
音声およびビデオ カウンタ	241
Cisco Analog Access	241

Cisco Annunciator Device	241
Cisco Call Restriction	242
Cisco CallManager	243
Cisco CallManager System Performance	256
Cisco CTIManager	260
Cisco Dual-Mode Mobility	260
Cisco エクステンション モビリティ	262
Cisco Gatekeeper	263
Cisco H.323	264
Cisco Hunt Lists	265
Cisco HW Conference Bridge Device	266
Cisco IP Manager Assistant	267
Cisco LBM service	268
Cisco Lines	268
Cisco Locations LBM	269
Cisco Locations RSVP	271
Cisco Media Streaming Application	271
Cisco Messaging Interface	277
Cisco MGCP BRI Device	278
Cisco MGCP FXO Device	279
Cisco MGCP FXS Device	280
Cisco MGCP Gateways	280
Cisco MGCP PRI Device	281
Cisco MGCP T1 CAS Device	282
Cisco Mobility Manager	283
Cisco Music On Hold (MoH) Device	285
Cisco MTP Device	287
Cisco Phones	288
Cisco Presence の機能	288
Cisco QSIG Feature	289
Cisco Signaling Performance	289
Cisco SIP	290
Cisco SIP Line Normalization	290
Cisco SIP Normalization	301
Cisco SIP Stack	313

Cisco SIP Station	328
Cisco SW Conf Bridge Device	330
Cisco Telepresence MCU Conference Bridge Device	331
Cisco TFTP Server	331
Cisco Transcode Device	337
Cisco Video Conference Bridge	337
Cisco Web Dialer	338
Cisco WSM Connector	339
IME Client	340
IME Client Instance	342
SAML シングル サインオン	342
Cisco IVR デバイス	343
IM and Presence Service カウンタ	344
Cisco Client Profile Agent	344
Cisco Presence Engine	344
Cisco Server Recovery Manager	351
Cisco SIP Proxy	351
Cisco Sync Agent	356
Cisco XCP 認証コンポーネント	356
Cisco XCP CM	357
Cisco XCP コンポーネント スタンザ トラフィック	357
Cisco XCP JDS	359
Cisco XCP JSM	359
Cisco XCP JSM IQ ネームスペース	361
Cisco XCP JSM セッション	361
Cisco XCP MA の基本	362
Cisco XCP マネージド ファイル転送	363
Cisco XCP Router	363
Cisco XCP SIP S2S	364
Cisco XCP S2S	365
Cisco XCP TC	365
Cisco XCP TC ルーム	366
Cisco XCP WebCM	367
Cisco Unity Connection カウンタ	368

CUC Data Store	368
CUC Data Store: Databases	368
CUC Digital Notifications	369
CUC Directory Services	370
CUC Feeder	370
CUC メールボックス同期	370
CUC Message Store	372
CUC Message Store: Databases	375
CUC Personal Call Transfer Rules	375
CUC Phone System	376
CUC Phone System: Ports	379
CUC Replication	379
CUC Replicator: Remote Connection Locations	380
CUC Sessions: Calendar Access	381
CUC Sessions: E-mail Access	381
CUC Sessions: IMAP Server	382
CUC Sessions: RSS	384
CUC Sessions: SMTP サーバ	384
CUC Sessions: SpeechView Processor	385
CUC Sessions: TRaP	385
CUC Sessions: TTS	386
CUC Sessions: Unified Client	386
CUC Sessions: Video	386
CUC Sessions: Voice	389
CUC Sessions: VUI	392
CUC Sessions: Web	392
CUC Sessions: Web E-mail Access	393
CUC System Agent	394
システム アラート	395
AuthenticationFailed	395
CiscoDRFFailure	395
CoreDumpFileFound	396
CpuPegging	397
CriticalServiceDown	398
DBChangeNotifyFailure	399

DBReplicationFailure	399
DBReplicationTableOutOfSync	400
HardwareFailure	401
LogFileSearchStringFound	402
LogPartitionHighWaterMarkExceeded	403
LogPartitionLowWaterMarkExceeded	403
LowActivePartitionAvailableDiskSpace	404
LowAvailableVirtualMemory	405
LowInactivePartitionAvailableDiskSpace	406
LowSwapPartitionAvailableDiskSpace	407
ServerDown	408
SparePartitionHighWaterMarkExceeded	408
SparePartitionLowWaterMarkExceeded	409
SyslogSeverityMatchFound	410
SyslogStringMatchFound	411
SystemVersionMismatched	412
TotalProcessesAndThreadsExceededThreshold	412
音声およびビデオ アラート	413
BeginThrottlingCallListBLFSubscriptions	413
CallAttemptBlockedByPolicy	414
CallProcessingNodeCpuPegging	415
CARSchedulerJobFailed	416
CARIDSEngineCritical	417
CARIDSEngineFailure	417
CDRAgentSendFileFailed	418
CDRFileDeliveryFailed	419
CDRHighWaterMarkExceeded	419
CDRMaximumDiskSpaceExceeded	420
CiscoElmNotConnected	421
CiscoGraceTimeLeft	422
CiscoNoProvisionTimeout	422
CiscoSystemInDemo	423
CiscoSystemInOverage	424
CiscoSystemSecurityMismatch	425
CodeYellow	425

DDRBlockPrevention	426
DDRDown	427
EMCCFailedInLocalCluster	428
EMCCFailedInRemoteCluster	429
ExcessiveVoiceQualityReports	429
ILSHubClusterUnreachable	430
ILSPwdAuthenticationFailed	431
ILSTLSAuthenticationFailed	432
IMEDistributedCacheInactive	432
IMEOverQuota	433
IMEQualityAlert	434
InsufficientFallbackIdentifiers	435
IMEServiceStatus	436
InvalidCredentials	437
LocationOutOfResource	438
MaliciousCallTrace	439
MediaListExhausted	440
MgcpDChannelOutOfService	440
NumberOfRegisteredDevicesExceeded	441
NumberOfRegisteredGatewaysDecreased	442
NumberOfRegisteredGatewaysIncreased	443
NumberOfRegisteredMediaDevicesDecreased	443
NumberOfRegisteredMediaDevicesIncreased	444
NumberOfRegisteredPhonesDropped	445
RecordingCallSetupFail	446
RecordingGatewayRegistrationRejected	446
RecordingGatewayRegistrationTimeout	447
RecordingGatewaySessionFailed	448
RecordingResourcesNotAvailable	449
RecordingSessionTerminatedUnexpectedly	449
RTMTSessionsExceedsThreshold	450
RouteListExhausted	451
SDLLinkOutOfService	452
TCPSetupToIMEFailed	452
TLSConnectionToIMEFailed	453

UserInputFailure	454
IM and Presence Service アラート	455
CTIGWUserNotLicenced	455
CTIGWQBEMFailedRequest	455
CTIGWModuleNotEnabled	455
CTIGWSystemError	456
CTIGWUserNotAuthorized	456
CTIGWProviderFailedToOpen	456
DuplicateDirectoryURI	457
DuplicateUserid	457
ESPSError	458
ESPCreateLockFailed	458
ESPConfigError	458
ESPSharedMemAllocFailed	459
ESPSharedMemSetPermFailed	459
EspConfigAgentHighCPUUtilization	459
ESPMallocFailure	460
ESPRegistryError	460
EspConfigAgentSharedMemoryStaticRouteError	460
ESPStatsLogFileOpenFailed	461
ESPLoginError	461
EspConfigAgentProxyDomainNotConfigured	461
EspConfigAgentNetworkRestored	462
EspConfigAgentLocalDBAccessError	462
ESPConfigNotFound	462
EspConfigAgentRemoteDBAccessError	463
ESPPassedParamInvalid	463
ESPSharedMemCreateFailed	463
EspConfigAgentHighMemoryUtilization	464
ESPAPTRInvalidRecord	464
ESPWrongIPAddress	464
EspConfigAgentNetworkOutage	465
EspConfigAgentMemAllocError	465
EspConfigAgentFileWriteError	465
ESPVirtualProxyError	466



ESPStopped	466
ESPWrongHostName	466
ESPRoutingError	467
InterclusterSyncAgentAXLConnectionFailed	467
InterclusterSyncAgentPeerDuplicate	467
ICSACertificateFingerPrintMismatch	468
ICSACertificateCASignedTrustCertFound	468
ICSACertificateValidationFailure	468
InvalidDirectoryURI	469
LegacyCUPCLogin	469
NotInCucmServerListError	469
PEStateLocked	470
PWSAboveCPULimit	470
PWSRequestLimitReached	470
PEIDSQueryError	471
PEStateDisabled	471
PELoadHighWaterMark	471
PWSAboveSipSubscriptionLimit	472
PEMemoryHighCondition	472
PEsipSocketBindFailure	472
PEIDStoIMDBDatabaseSyncError	473
PEIDSSubscribeError	473
PWSSCBFindFailed	474
PEDatabaseError	474
PWSSCBInitFailed	474
PEWebDAVInitializationFailure	475
PEPeerNodeFailure	475
PEAutoRecoveryFailed	475
SRMFailover	476
SRMFailed	476
UASCBFindFailed	476
UASCBGetFailed	477
XcpMFTDBConnectError	477
XcpMFTextFsMountError	477
XcpMFTextFsFreeSpaceWarn	478

XcpDBConnectError	478
XcpCmStartupError	478
XcpSIPFedCmComponentConnectError	479
XcpTxtConfGearError	479
XCPCConfigMgrConfigurationFailure	479
XcpWebCmComponentConnectError	480
XcpXMPPFedCmStartupError	480
XcpXMPPFedCmComponentConnectError	480
XcpSIPFedCmStartupError	480
XcpCmXmppdError	481
XcpCmPauseSockets	481
XcpThirdPartyComplianceConnectError	481
XCPCConfigMgrJabberRestartRequired	482
XcpTxtConfDBConnectError	482
XcpMdnsStartError	483
XCPCConfigMgrR2RPasswordEncryptionFailed	483
XcpCmComponentConnectError	483
XcpWebCmStartupError	484
XCPCConfigMgrR2RRequestTimedOut	484
XcpWebCmHttpdError	484
XCPCConfigMgrHostNameResolutionFailed	485
XcpSIPGWStackResourceError	485
Intercompany Media Engine アラート	485
BannedFromNetwork	485
IMEDistributedCacheCertificateExpiring	486
IMEDistributedCacheFailure	487
IMESdlLinkOutOfService	488
InvalidCertificate	489
InvalidCredentials	490
MessageOfTheDay	491
SWUpdateRequired	491
TicketPasswordChanged	492
ValidationsPendingExceeded	493
Cisco Unity Connection アラート	494
NoConnectionToPeer	494

<a href="#">AutoFailoverSucceeded</a>	495
<a href="#">AutoFailoverFailed</a>	496
<a href="#">AutoFailbackSucceeded</a>	496
<a href="#">AutoFailbackFailed</a>	497
<a href="#">SbrFailed (スプリット ブレイン解決の失敗)</a>	498
<a href="#">DiskConsumptionCloseToCapacityThreshold</a>	499
<a href="#">DiskConsumptionExceedsCapacityThreshold</a>	500
<a href="#">LicenseExpirationWarning</a>	501
<a href="#">LicenseExpired</a>	501





## はじめに



(注) このマニュアルに記載された内容は、利用可能な最新のシスコ製品に関する情報とは異なる場合があります。最新のマニュアルは、次の URL にあるシスコ製品のマニュアル ページで入手できます。

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html)

- このマニュアルについて, [xxi ページ](#)
- 対象読者, [xxii ページ](#)
- 関連資料, [xxii ページ](#)
- 表記法, [xxii ページ](#)
- マニュアルの入手方法およびテクニカル サポート, [xxiv ページ](#)
- [Organization](#), [xxiv ページ](#)

## このマニュアルについて

『Cisco Unified Real-Time Monitoring Tool アドミニストレーション ガイド』では、Cisco Unified Real-Time Monitoring Tool に関する情報を提供します。

このガイドは、設定に関する次のマニュアルと併せて使用してください。

Cisco Unified Communications Manager	『System Configuration Guide for Cisco Unified Communications Manager』、『Administration Guide for Cisco Unified Communications Manager』、『Cisco Unified Serviceability Administration Guide』、『CDR Analysis and Reporting Administration Guide』、および『Cisco Unified Communications Manager Call Detail Records Administration Guide』
--------------------------------------	--

Cisco Unified Communications Manager IM and Presence Service	『 <i>Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager</i> 』 および 『 <i>Cisco Unified Serviceability Administration Guide</i> 』
Cisco Unity Connection	『 <i>Cisco Unity Connection System Administration Guide</i> 』 および 『 <i>Cisco Unity Connection Serviceability Administration Guide</i> 』

これらのマニュアルは、次の情報が含まれます。

- Cisco Unified Communications Manager、Cisco Unified Communications Manager IM and Presence Service、および Cisco Unity Connection の管理に関する説明。
- 管理インターフェイスを使用して実行できる手順のタスクの説明。

## 対象読者

『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』は、Cisco Unified Communications Manager、Cisco Unified Communications Manager IM and Presence Service、および Cisco Unity Connection の管理とサポートを担当するネットワーク管理者に対して情報を提供します。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使用して、リモートサービス機能の概要とその管理方法を学習できます。このマニュアルを使用するには、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。

## 関連資料

Cisco Unified Communications Manager および Cisco Unified Communications Manager IM and Presence Service に関する追加ドキュメントについては、『*Cisco Unified Communications Manager Documentation Guide*』を参照してください。

Cisco Unity Connection に関する追加ドキュメントについては、『*Cisco Unity Connection Documentation Guide*』を参照してください。

## 表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
[ ]	コマンドおよびキーワードは <b>太字</b> 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、イタリック体で表記されています。
[ ]	角カッコの中の要素は、省略可能です。

表記法	説明
{ 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。
string	引用符を付けない一組の文字。string 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 string 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。
^	^ 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

「時間の節約に役立つ操作」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

役立つ「ヒント」の意味です。

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。

## マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool (BST) の使用、サービス要求の送信、追加情報の収集の詳細については、『*What's New in Cisco Product Documentation*』を参照してください。このドキュメントは、<http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html> から入手できます。

『*What's New in Cisco Product Documentation*』では、シスコの新規および改訂版の技術マニュアルの一覧を、RSS フィードとして購読できます。また、リーダー アプリケーションを使用して、コンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。

## シスコ製品のセキュリティ

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。

米国の輸出規制の詳細については、[http://www.access.gpo.gov/bis/ear/ear\\_data.html](http://www.access.gpo.gov/bis/ear/ear_data.html) で参照できます。

## Organization

### 管理の概要

ブラウザのサポートを含む Unified RTMT の概要です。

### はじめに

Unified RTMT クライアントのインストール、アクセスおよび使用方法について説明します。

### システム パフォーマンスのモニタリング

RTMT でのシステム パフォーマンス モニタリングの概要です。Cisco Unified Communications Manager、Cisco Intercompany Media Engine、Cisco Unified Communications Manager IM and Presence Service、および Cisco Unity Connection システムで事前定義されたオブジェクトを管理する方法を含みます。



## Cisco Unified Analysis Manager

Unified Analysis Manager をインストールおよび設定する手順、Unified Analysis Manager で診断可能なノードを追加する手順、デバイスの管理手順、およびトラブルシューティングに関する情報を含む、Cisco Unified Analysis Manager に関する情報を提供します。

## プロファイルとカテゴリ

プロファイルおよびカテゴリを管理する方法について説明します。

## パフォーマンス カウンタ

パフォーマンスカウンタおよびカウンタの説明の表示、およびperfmom ログなど、Performance Monitor の使用手順を示します。

## アラート (Alerts)

アラートの使用手順を示します。

## Trace and Log Central

オンデマンドのトレース収集とシステム サービスでのクラッシュ ダンプ ファイルの設定方法、および該当ビューアでのトレース ファイルの表示方法について説明します。

## (付録) パフォーマンス カウンタとアラート

システムの各コンポーネントのパフォーマンス オブジェクトとその関連カウンタの全リストを示します。





## 第 1 章

# 管理の概要

---

- [Cisco Unified Real-Time Monitoring Tool, 1 ページ](#)
- [オペレーティング システムのサポート, 2 ページ](#)

## Cisco Unified Real-Time Monitoring Tool

Cisco Unified Real-Time Monitoring Tool はクライアント側アプリケーションとして実行し、システムコンポーネントの動作をリアルタイムで監視します。Unified RTMT は Hypertext Transfer Protocol Secure (HTTPS) および Transmission Control Protocol (TCP) を使用し、次の項目を監視します。

- システムのパフォーマンス
- デバイスのステータス
- デバイスの検出
- コンピュータ テレフォニー インテグレーション (CTI) アプリケーション

Unified RTMT は、HTTPS を使用してデバイスに直接接続し、システムの問題をトラブルシューティングできます。



(注) Unified RTMT がデスクトップ上のアプリケーションとして動作していない場合でも、アラームやパフォーマンス モニタリングの更新などのタスクは、サーバ上でバックグラウンド処理として続行されます。

Unified RTMT を使用すると、次の作業を実行できます。

- システムの健全性をモニタするための、事前に定義された管理オブジェクトをモニタする。
- 値がユーザ設定のしきい値を超えるか下回ったときに、オブジェクトのさまざまなアラートを電子メール メッセージ形式で生成する。
- トレースを収集し、Unified RTMT に備わっているさまざまなデフォルト ビューアで表示する。

- SysLog ビューアで syslog メッセージを表示する。
- パフォーマンス モニタリング カウンタと連動する。
- Cisco Unified Communications Manager のみ：Q931 メッセージを変換する。

コンピュータにインストールされている Unified RTMT の 1 つのコピーを使用すると、複数のサーバまたは複数のクラスタを同時に監視することができます。たとえば、次のエンティティをすべてモニタできます。

- 1 台のサーバ上の Cisco Unified Communications Manager 製品。
- 1 台のサーバ上の Cisco Intercompany Media Engine (Cisco IME) 製品。
- 1 台のサーバ上の Cisco Unified Communications Manager IM and Presence Service (IM and Presence Service) 製品。
- クラスタ上のサーバ (クラスタの健全性をモニタするため)。

異なるサーバ上の製品を監視するには、Unified RTMT の新しいインスタンスを使用する必要があります。

## オペレーティング システムのサポート

RTMT は、次のオペレーティング システムのいずれかを実行しているコンピュータにインストールできます。

- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- KDE や GNOME クライアントを搭載した Linux



(注) Windows 7 以降の場合は、Unified RTMT を [管理者として実行] モードで起動する必要があります。そうしない場合、ユーザアクセスコントロール (UAC) 権限が無効です。

Unified RTMT をインストールする場合は、次のことを考慮してください。

- Windows OS プラットフォームで Unified RTMT を実行するには、少なくとも 128 MB のメモリが必要です。
- Windows OS プラットフォームで Unified RTMT を実行するには、少なくとも 300 MB のメモリが必要です。
- Windows Vista または Windows 7 プラットフォームに Unified RTMT をインストールする場合は、「認識できないプログラムがこのコンピュータへのアクセスを要求しています」という

ユーザー アカウント コントロール ポップアップ“”メッセージが表示されます。[許可] をクリックして、Unified RTMT のインストール作業を続行します。

- Unified RTMT は、32 ビットおよび 64 ビット Windows プラットフォーム上で動作します。





## 第 2 章

# 使用する前に

---

- [Unified RTMT のインストールおよび設定, 5 ページ](#)
- [管理ツール, 12 ページ](#)
- [Unified RTMT のアンインストール, 35 ページ](#)

## Unified RTMT のインストールおよび設定

### Unified RTMT のインストール

#### はじめる前に

- Unified RTMT を Windows OS プラットフォームで実行するには、少なくとも 128 MB のメモリが必要です。Windows/Linux OS プラットフォームでツールを実行するには、少なくとも 300 MB のディスク領域が必要です。



---

(注) Linux Unified RTMT プラグイン CcmServRtmtPlugin は、RHEL 5、RHEL 6 以上の Linux マシンにインストールできます。RHEL 4 マシンにインストールする場合は、glibc (OS ライブラリ) のバージョンが 2.4.x 以上であることを確認してください。glibc バージョンが 2.3.x 以前の場合、基盤となる JRE のインストールが失敗します。

---

- 現在の Unified RTMT download は、Cisco Unified Communications Manager または Cisco Unity Connection の以前のリリースをサポートします。Unified Communications Manager の一部のリリースをコンピュータにインストールするには、Unified RTMT の複数のバージョンが必要になることがあります (1 つの Unified Communications Manager のリリースごとに 1 バージョン)。インストールする Unified RTMT バージョンが、モニタ対象の製品と互換性があるこ

とを確認します。使用している Unified RTMT バージョンがモニタ対象のサーバと互換性がない場合、互換性のあるバージョンをダウンロードするように求められます。

- コンピュータでは、実行する Unified RTMT の最後のインスタンスに基づいて、IP アドレスや Unified RTMT フレーム サイズなどのユーザ設定を保存します。



(注) 標準監査ユーザと Standard CCM Super Users の権限を持つ管理者だけが Unified RTMT 機能にアクセスできます。これらの権限のないアプリケーションユーザが Unified RTMT にログインした場合、コール制御検出 (CCD) や Service Advertisement Framework (SAF) などの機能の一部は期待どおりに機能しません。



(注) Linux ワークステーションでは、ルートアクセスを使用して RTMT を実行します。そうしない場合、最初に RTMT をインストールするときに、アプリケーションが起動しません。

## 手順

**ステップ 1** 設定の管理インターフェイスの [プラグイン (Plug-ins)] ウィンドウに移動します。

インターフェイス (Interface)	アクセス方法
<b>Cisco Unified Communications Manager</b>	Cisco Unified Communications Manager Administration から、[アプリケーション (Application)] > [プラグイン (Plugins)] の順に選択します。
<b>Cisco Unified Communications Manager IM and Presence Service</b>	Cisco Unified Communications Manager IM and Presence Administration から、[アプリケーション (Application)] > [プラグイン (Plugins)] の順に選択します。
<b>Cisco Unity Connection</b>	Cisco Unity Connection Administration から、[システム設定 (System Settings)] > [プラグイン (Plugins)] の順に選択します。

**ステップ 2** [検索 (Find)] 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クライアントで Unified RTMT をインストールするには、[Real-Time Monitoring Tool - Windows] の [ダウンロード (Download)] 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クライアントで Unified RTMT をインストールするには、[Real-Time Monitoring Tool - Linux] の [ダウンロード (Download)] リンクをクリックします。



- ヒント Windows 7以降で Unified RTMT をインストールするときは、管理者としてインストールを実行してください。
- ステップ 4** クライアント上の優先ロケーションに実行可能ファイルをダウンロードします。
- ステップ 5** Windows バージョンをインストールするには、デスクトップ上に表示される Unified RTMT アイコンをダブルクリックするか、ファイルをダウンロードしたディレクトリを見つけて Unified 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** Linux バージョンをインストールするには、ファイルに実行権限があることを確認します。たとえば、コマンド `chmod +x CcmServRtmtPlugin.bin` (大文字と小文字を区別) を入力します。
- ステップ 7** Unified RTMT のようこそウィンドウが表示されたら、[次へ (Next)] をクリックします。
- ステップ 8** ライセンス契約書を承認するには、[使用許諾契約書の条項に同意します (I accept the terms of the license agreement)] をクリックし、[次へ (Next)] をクリックします。
- ステップ 9** Unified RTMT をインストールする場所を選択します。デフォルトの場所を使用しない場合は、[参照 (Browse)] をクリックして別の場所に移動します。[次へ (Next)] をクリックします。
- ステップ 10** インストールを開始するには、[次へ (Next)] をクリックします。  
[セットアップ ステータス (Setup Status)] ウィンドウが表示されます。
- ステップ 11** インストールを完了するには、[完了 (Finish)] をクリックします。

## RTMT のアップグレード



**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で Cisco Unified Communications Manager のアップグレードを行ってから RTMT をアップグレードすることを推奨します。

RTMT は、ユーザ設定とダウンロードされたモジュール jar ファイルをクライアントマシンのローカルに保存します。システムはユーザが作成したプロファイルをデータベースに保存するため、これらのアイテムにはツールのアップグレード後に Unified RTMT でアクセスできます。

### はじめる前に

RTMT の新しいバージョンにアップグレードする前に、以前のバージョンをアンインストールすることを推奨します。

### 手順

- ステップ 1** Cisco Unified CM の管理から、[アプリケーション (Application)] > [プラグイン (Plugins)] の順に選択します。
- ステップ 2** [検索 (Find)] 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。

- 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ツールをインストールするには、[Cisco Unified Real-Time Monitoring Tool - Windows] の [ダウンロード (Download) ] 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ツールをインストールするには、[Cisco Unified Real-Time Monitoring Tool - Linux] の [ダウンロード (Download) ] リンクをクリックします。

- ステップ 4** 優先ロケーションにインストール ファイルをダウンロードします。
- ステップ 5** インストール ファイルを特定して実行します。  
抽出プロセスが開始されます。
- ステップ 6** RTMT のようこそウィンドウで、[次へ (Next) ] をクリックします。
- ステップ 7** アップグレードのインストール場所は変更できないため、[次へ (Next) ] をクリックします。  
[セットアップ ステータス (Setup Status) ] ウィンドウが表示されます。[キャンセル (Cancel) ] をクリックしないでください。
- ステップ 8** [メンテナンス完了 (Maintenance Complete) ] ウィンドウで、[完了 (Finish) ] をクリックします。

## Unified RTMT の起動

### はじめる前に

Windows XP、Vista、または 7 のシングル サインオンのため、Unified RTMT を管理者として実行します。

### 手順

- ステップ 1** プラグインをインストールしたら、Unified RTMT を開きます。  
Windows XP、Vista、または 7 クライアントがあり、シングルサインオン機能を使用する場合は、デスクトップまたはスタートメニューの Unified RTMT のショートカットを右クリックして [管理者として実行 (Run as Administrator) ] をクリックします。
- 重要** Windows 7 または Vista で RTMT を起動する前に、ユーザアカウント制御 (UAC) 機能が無効になっていることを確認します。UAC 機能の詳細については、  
<http://msdn.microsoft.com/en-us/library/aa511445.aspx> を参照してください。
- ステップ 2** [ホスト IP アドレス (Host IP Address) ] フィールドに、ノードまたはクラスタ内のノード (該当する場合) の IP アドレスまたはホスト名を入力します。
- ステップ 3** ノードをリスンするためにアプリケーションが使用するポートを入力します。  
(注) セキュアな接続のデフォルト設定は 8443 です。ファイアウォールが無効な場合、443 としてポートを指定します。

- (注) Unified RTMT の Trace and Log Central ツールは、指定したポート番号を使用して、クラスタ内のすべてのノードと通信します。システムでポートマッピングを使用し、すべてのノードが同じポート番号にマップされていない場合、一部の Unified RTMT ツールはそれらのノードに接続できません。接続できないツールは、Trace and Log Central、Job Status、SyslogViewer、Perfmon Log Viewer、FTP/SFTP Configuration などです。
- ステップ 4** [セキュアな接続 (Secure Connection) ] チェックボックスをオンにします。
- (注) [セキュアな接続 (Secure Connection) ] チェックボックスをオフにする場合、ポートを 80 に手動で変更する必要があります。
- ステップ 5** [OK] をクリックします。
- シングルサインオン機能が有効になっている場合、Unified RTMT はユーザ名とパスワードを要求しないため、ステップ 8 に進みます。
  - シングルサインオンが有効になっていない場合、Unified RTMT はユーザ名とパスワードを求める別のウィンドウを表示します。以下のステップに示すように詳細を入力します。
- ステップ 6** [ユーザ名 (User Name) ] フィールドに、アプリケーションの管理者ユーザ名を入力します。
- ステップ 7** [パスワード (Password) ] フィールドに、ユーザ名に対して設定した管理者ユーザパスワードを入力します。
- (注) 認証が失敗した場合、またはノードにアクセスできない場合、ノードおよび認証の詳細を再入力するよう要求するプロンプトがツールで表示されます。[キャンセル (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。認証に成功すると、Unified RTMT はローカルキャッシュから、またはバックエンドのバージョンに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はリモートノードから、モニタリングモジュールを起動します。
- ステップ 8** プロンプトが表示されたら、[はい (Yes) ] をクリックして証明書ストアを追加します。Unified RTMT が起動します。

- (注) シングルサインオン機能を使用してサインインした場合、次のメニューのいずれかをクリックすると、Unified RTMT は一度だけユーザ名とパスワードの入力を要求します。
- [システム (System)] > [パフォーマンス (Performance)] > [パフォーマンス ログビューア (Performance log viewer)]
  - [システム (System)] > [ツール (Tools)] > [Trace and Log Central]
  - [システム (System)] > [ツール (Tools)] > [ジョブのステータス (Job status)]
  - [システム (System)] > [ツール (Tools)] > [Syslog ビューア (Syslog Viewer)]
  - [音声/ビデオ (Voice/Video)] > [CallProcess] > [セッショントレース (Session Trace)]
  - [音声/ビデオ (Voice/Video)] > [CallProcess] > [着信側トレース (Called Party Tracing)]
  - [音声/ビデオ (Voice/Video)] > [レポート (Report)] > [学習パターン (Learned Pattern)]
  - [音声/ビデオ (Voice/Video)] > [レポート (Report)] > [SAF フォワーダ (SAF forwarders)]
  - Analysis Manager

### 次の作業

Unified RTMT の使用だけに限定されたプロファイルを持つユーザを作成できます。ユーザは Unified RTMT にフルアクセスできますが、ノードを管理する権限がありません。

Unified RTMT ユーザを作成するには、新しいアプリケーションユーザを管理インターフェイスに追加し、そのユーザを事前定義済みの Standard RealtimeAndTraceCollection グループに追加します。

ユーザとユーザグループの追加方法の詳細な手順については、『*Administration Guide for Cisco Unified Communications Manager*』および『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

### 関連トピック

[管理者として実行, \(10 ページ\)](#)

## 管理者として実行

Windows XP、Vista、または 7 の管理者としてプログラムを実行するには、次の手順に従ってください。



- (注) 上記の Windows クライアントのシングルサインオン機能を使用するには、Unified RTMT を管理者として実行します。

## 手順

- ステップ 1** プログラムのショートカットを見つけます。
- ステップ 2** ショートカットを右クリックします。
- ステップ 3** 次のいずれかの操作を実行します。
- ショートカットを右クリックして [管理者として実行 (Run as administrator) ] を選択します。
  - **1** ショートカットを右クリックします。
  - **2** [プロパティ (Properties) ] を選択します。
  - **3** ショートカット タブで、[詳細設定 (Advanced) ] をクリックします。
  - **4** [管理者として実行 (Run as administrator) ] チェックボックスをオンにします。

## Unified RTMT の複数インストール

コンピュータにインストールされている Unified RTMT の 1 つのコピーを使用すると、複数のサーバまたは複数のクラスタを同時に監視することができます。たとえば、次のエンティティをすべてモニタできます。

- 1 台のノード上の Cisco Unified Communications Manager 製品。
- 1 台のノード上の Intercompany Media Engine (IME) 製品。
- 1 台のノード上の IM and Presence Service。
- クラスタの健全性をモニタするクラスタ内のノード。

別のノードから製品を監視するには、インストールされている Unified RTMT の新しいインスタンスを使用する必要があります。

コンピュータに複数のコピーの Unified RTMT をインストールすると、別のノードにインストールされた複数の IM and Presence Service を同時にモニタできます。

1 台のコンピュータに複数の Unified RTMT をインストールするときは、別々のフォルダに Unified RTMT をインストールする必要があります。コンピュータにインストールする Unified RTMT は、4 つまでにすることを推奨します。

Unified RTMT の別のコピーをインストールしてショートカットを上書きするため、次のタスクを完了する必要があります。

- 1** 以前のインストールのフォルダに `jrtmt.exe` のショートカットを作成して、別のアイコンを作成します。
- 2** アイコンの名前を適宜変更します。

インストール時に選択したフォルダ内に別のバージョンが検出されると、メッセージが表示されます。インストールを続行するには、別のフォルダにバージョンをインストールします。



(注) コンピュータは、最後に終了した Unified RTMT クライアントから IP アドレスや Unified RTMT フレーム サイズなどのユーザ設定を保存します。

## 管理ツール

### システム インターフェイス

Unified RTMT インターフェイスは、次のコンポーネントで構成されています。

- **メニューバー**：メニューバーは、設定に応じて、次のオプションの一部またはすべてを含みます。

#### ファイル

既存の RTMT プロファイルの保存、復元、削除、Java ヒープ メモリ使用量のモニタリング、Cisco Unified Serviceability の [サービスアビリティ レポートのアーカイブ (Serviceability Report Archive) ] ウィンドウへの移動、および RTMT からのログオフまたは終了を可能にします。



(注) RTMT メニュー オプションの [ファイル (File) ] > [Cisco Unified Reporting] では、RTMT から Cisco Unified Reporting にアクセスできます。検査やトラブルシューティングのためにスナップショット クラスタ データに Cisco Unified Reporting アプリケーションを使用できます。詳細については、『Cisco Unified Reporting Administration Guide』を参照してください。

#### システム (System)

システム概要のモニタリング、サーバリソースのモニタリング、パフォーマンスカウンタの使用、アラートの使用、トレースの収集、および syslog メッセージの表示が可能です。

#### Voice/Video

サーバの Cisco Unified Communications Manager 概要情報の表示、呼処理情報のモニタリング、およびデバイスの表示と検索、サービスおよび CTI のモニタリングが可能です。

#### [IM and Presence]

IM and Presence Service の表示とサーバの Cisco Jabber サマリー情報の表示が可能です。

### Cisco Unity Connection

ポート モニタ ツールを表示できます。

### IME サービス

Cisco Intercompany Media Engine サーバのサーバおよびネットワーク アクティビティをモニタリングできます。

### 編集 (Edit)

カテゴリの設定 (表形式用)、デバイスとパフォーマンス モニタリング カウンタに対するポーリング レートの設定、クリック起動チャネルの非表示化、および RTMT のトレース設定の編集を可能にします。

### ウィンドウ

単一の RTMT ウィンドウまたはすべての RTMT ウィンドウを閉じます。

### Application

設定によって、管理インターフェイス、Cisco Unified Serviceability、および Cisco Unity Connection Serviceability の該当する Web ページを参照できます。

### ヘルプ

RTMT オンライン ヘルプにアクセスし、RTMT のバージョンを確認できます。

- クイック起動チャネル：サーバに関する情報やアプリケーションに関する情報を表示するペイン。タブにはユーザがクリックできるアイコンのグループが含まれ、さまざまなオブジェクトをモニタリングできます。
- [モニタ (Monitor) ] ペイン：モニタリング結果が表示されるペイン。

## パフォーマンス モニタリング

Cisco Unified Communications Manager、Cisco Unified Communications Manager IM and Presence Service、および Cisco Unity Connection は直接パフォーマンス カウンタ (perfmon カウンタと呼ばれます) を更新します。カウンタには、登録されている電話機の数、アクティブ コールの数、使用可能な会議ブリッジリソースの数、ボイスメッセージングポートの使用状況など、システムとシステム上のデバイスについての簡単で便利な情報が含まれています。

Cisco Unified Real-Time Monitoring Tool を使用して任意のオブジェクトのカウンタを選択することで、システムのコンポーネントとシステム上のアプリケーションのコンポーネントのパフォーマンスをモニタできます。各オブジェクトのカウンタは、フォルダを展開すると表示されます。

コンピュータで perfmon カウンタをローカルに記録し、Unified RTMT でパフォーマンス ログビューアを使用して、収集した perfmon CSV ログ ファイルまたは Real-time Information Server Data Collection (RISDC) の perfmon ログを表示することができます。

RTMT は、パフォーマンスのモニタリング用の既存のソフトウェアと統合します。

- RTMT では、管理およびサービスアビリティのソフトウェアと統合します。
- RTMT は、すべてのシステム コンポーネントのパフォーマンス情報を表示します。

RTMT はパフォーマンスのトラブルシューティングを実行するためにアラート通知を行います。また、パフォーマンス カウンタを定期的にポーリングして、そのカウンタのデータを表示します。グラフまたは表形式の perfmon カウンタを表示できます。

パフォーマンスをモニタすることにより、次のタスクを実行することができます。

- すべての Unified Communications Manager、IM and Presence Service、および Cisco Unity Connection サーバからパフォーマンス カウンタをモニタする。
- 一連の事前設定されたオブジェクトを継続的にモニタし、電子メールのメッセージ形式で通知を受信する。
- カウンタのしきい値設定をアラート通知に関連付ける。電子メールまたはポップアップメッセージによる通知が管理者に送信されます。
- カスタマイズされたトラブルシューティングタスクのために、モニタされているカウンタ、しきい値設定、アラート通知などの設定を保存して復元する。
- 1 つのパフォーマンス比較図で、最大 6 つの perfmon カウンタを表示する。
- モニタするカウンタを追加するためにパフォーマンス クエリーを使用する。

## システム概要の状態

Real-Time Monitoring Tool は、システムの健全性の監視に役立つ一連のデフォルト モニタリング オブジェクトを提供します。デフォルトのオブジェクトには、システムおよびその他のサポート対象のサービスに関するパフォーマンス カウンタまたは重大イベントのステータスが含まれません。Unified RTMT のシステム概要では、単一のモニタリング ペインで重要な共通情報を監視することができます。システム概要では、次の定義済みオブジェクトの情報を確認できます。

- 仮想メモリの使用率
- CPU 使用率
- 共通パーティションの使用率
- アラート履歴のログ

## サーバステータスのモニタリング

サーバカテゴリでは、サーバ上のさまざまなアプリケーションについて CPU とメモリの使用率、プロセス、ディスク領域の使用率、および重要なサービスがモニタされます。

CPU and Memory Monitor は、各サーバの CPU の使用率と仮想メモリの使用状況に関する情報を示します。サーバの各 CPU の情報には、各プロセッサがさまざまなモードまたは操作 (User、Nice、System、Idle、IRQ、SoftIRQ および IOWait) でプロセスを実行するために費やされた時間の割合が含まれます。CPU の割合は、アイドル時間を除くすべてのモードおよび操作で、動作するため



に費やされた合計時間です。メモリの情報には、キロバイト単位での合計メモリ、使用メモリ、空きメモリ、共有メモリ、バッファメモリ、キャッシュされたメモリ、合計スワップメモリ、使用スワップメモリ、空きスワップメモリが含まれ、使用中の仮想メモリの比率も含まれます。

Process Monitor は、システムで実行されているプロセスについての情報を提供します。RTMT は、各プロセスについて、プロセス ID (PID)、CPU 使用率、ステータス、共有メモリ (KB)、Nice (レベル)、VmRSS (KB)、VmSize (KB)、VmData (KB)、スレッド数、ページフォールト数、およびデータ スタック サイズ (KB) を表示します。

ディスク使用状況のモニタリングカテゴリは、共通パーティションおよびスワップパーティションのディスク使用率を図に示します。このカテゴリはまた、各ホストでの各パーティション (アクティブ、ブート、共通、非アクティブ、スワップ、共有メモリ、スピア) のディスク使用量の比率も表示されます。



(注) 複数の論理ディスク ドライブがシステムで使用可能な場合、システムは最初の論理ディスクの予備パーティションに CTI Manager トレースを、2つ目の論理ディスクに Cisco CallManager トレースを保存します。Unified RTMT は予備パーティションのディスク使用率を [ディスク使用率 (Disk Usage)] ウィンドウでモニタします。

重要なサービスのモニタリングカテゴリでは、重要なサービスの名前、ステータス (サービスが稼働しているか、ダウンしているか、アクティブ化されているか、管理者によって停止されているか、起動中か、停止中か、不明な状態か)、およびシステムでサービスが稼働している間の経過時間を表示します。

各状態の個別の説明については、次の表を参照してください。

表 1: 重要なサービスのステータス

重要なサービスのステータス	説明
起動	現在、サービスが起動モードになっています。[重要なサービス (Critical Services)] ペインおよび Cisco Unified Serviceability の [コントロールセンター (Control Center)] で示されます。
アップ (up)	現在、サービスが動作しています。[重要なサービス (Critical Services)] ペインおよび Cisco Unified Serviceability の [コントロールセンター (Control Center)] で示されます。
停止	現在、サービスが停止しています。[重要なサービス (Critical Services)] ペインおよび Cisco Unified Serviceability の [コントロールセンター (Control Center)] で示されます。

重要なサービスのステータス	説明
down	<p>予期せずに（つまり、サービスを停止するタスクを実行していないのに）サービスが実行を停止しました。 [重要なサービス（Critical Services）] ペインにサービスがダウン状態であることが示されます。</p> <p>CriticalServiceDown アラートは、サービス ステータスがダウンになっているときに生成されます。</p>
stopped by Admin	<p>サービスを意図的に停止するタスクを実行しました。システムをバックアップまたは復元した、アップグレードを実行した、Cisco Unified Serviceability または CLI でサービスを停止したなどの理由によってサービスが停止しました。</p> <p>[重要なサービス（Critical Services）] ペインにこのステータスが示されます。</p>
not activated	<p>現在、サービスは、アクティブにされたステータスになっていません。[重要なサービス（Critical Services）] ペインおよび Cisco Unified Serviceability の [サービスの開始（Service Activation）] で示されます。</p>
unknown state	<p>システムがサービスの状態を判別できないことを示し、[重要なサービス（Critical Services）] ペインに示されます。</p>

## パフォーマンス カウンタ インターフェイス

RTMT には、すぐに表示可能な事前定義されたパフォーマンス カウンタが含まれます。また、パフォーマンス クエリーを使用して、RTMT でモニタするカウンタを選択して追加できます。

RTMT は、パフォーマンス カウンタをチャート形式または表形式で表示します。チャート形式では、小型の情報ウィンドウが表示されます。[perfmon モニタリング（perfmon monitoring）] ペイン内のカウンタをダブルクリックすることで、特定のカウンタを表示できます。

形式やカテゴリなどの事前定義されたパフォーマンス カウンタの属性は固定です。RTMT で設定するカウンタの属性を定義できます。チャート ビューがデフォルトの表示です。カテゴリを作成する際に、表形式で表示するようパフォーマンス カウンタを設定できます。

### [カテゴリ（Category）] タブ

カテゴリは、モニタ対象のパフォーマンス カウンタのグループから構成されます。RTMT モニタリング ペインのタブにはカテゴリ名が含まれます。このタブでモニタされるパフォーマンスカウ

ンタはいずれも 1 つのカテゴリに属します。RTMT は、RTMT セッション中にアクセスされるカテゴリを下のツールバーに表示します。

システムは、タブ内のパフォーマンス カウンタを同じレートでポーリングしますが、各カテゴリには独自のポーリング レートが設定されています。

RTMT モニタリング ペインでカスタム カテゴリを作成し、特定のパフォーマンス、システム、またはデバイスに関する問題のトラブルシューティングに役立つ情報を表示できます。特定のオブジェクトに関するパフォーマンス上の問題が発生している場合は、カスタム カテゴリを作成して、そのオブジェクト内のカウンタのパフォーマンスをモニタできます。特定のデバイスで問題が発生する場合は、システム内のデバイスをモニタするカスタム カテゴリを作成します。また、これらのカスタム カテゴリにカウンタおよびゲートウェイに関するアラート通知を作成できます。カスタム カテゴリを作成するには、新規のカテゴリタブを追加します。タブを作成したら、そのタブ内で特定のパフォーマンス カウンタ、デバイス、およびアラートを指定し、プロファイルを使用してカスタム カテゴリを保存します。

## サンプル レート

アプリケーションがステータス情報を収集するカウンタ、デバイス、ゲートウェイ ポートをポーリングします。

事前に準備された各モニタリングウィンドウのポーリングレートは固定されていて、デフォルト値は 30 秒です。AMC (Alert Manager and Collector) サービス パラメータの収集レートが変化すると、事前に準備されたウィンドウのポーリングレートも更新されます。また、バックエンドサーバの時刻ではなく、RTMT クライアントアプリケーションのローカル時刻が、各チャートのタイムスタンプのベースになります。サービス パラメータの詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』または『*Cisco Unity Connection System Administration Guide*』を参照してください。

RTMT モニタリング ペインで、作成した各カテゴリ タブの該当するパフォーマンス カウンタ、デバイス、およびゲートウェイ ポートに対するポーリング間隔を設定します。



(注) 高頻度のポーリング レートは、サーバのパフォーマンスに影響を与えます。チャート形式でパフォーマンス カウンタをモニタするための最小ポーリング 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ための最小レートは 1 秒です。いずれもデフォルト値は 10 秒です。

## perfmon カウンタの拡大表示

perfmon カウンタがよく見えるようにするには、RTMT で perfmon モニタ カウンタを拡大します。

### 手順

**ステップ 1** カウンタを拡大表示するには、次のいずれかの作業を実行します。

- [システム サマリー (System Summary)] などの定義済みのオブジェクトを拡大表示するには、次のいずれかの操作を実行します。
  - カウンタのプロット領域でマウスをドラッグしてデータを選択し、マウスボタンを放します。カウンタは、チャートを拡大表示します。
  - カウンタをクリックします。カウンタが拡大されます。
- パフォーマンス ペインでカウンタを拡大するには、次のいずれかの操作を実行します（必要に応じてウィンドウ サイズを変更します）。
  - 拡大するカウンタをダブルクリックします。カウンタを含むボックスが強調表示され、[ズーム (Zoom)] ウィンドウが起動します。最小、最大、平均、および最終の各フィールドに、そのカウンタに対するモニタリングが開始されてからの値が表示されます。
  - カウンタをクリックし、拡大するカウンタを選択します。カウンタを含むボックスが強調表示されます。
  - カウンタを右クリックし、[チャートの拡大 (Zoom Chart)] を選択するか、[システム (System)] > [パフォーマンス (Performance)] > [チャートの拡大 (Zoom Chart)] の順に選択します。[ズーム (Zoom)] ウィンドウが起動します。最小、最大、平均、および最終の各フィールドに、そのカウンタに対するモニタリングが開始されてからの値が表示されます。

**ステップ 2** カウンタをズームアウトするには、次のいずれかの作業を実行します。

- [システム サマリー (System Summary)] などの定義済みのオブジェクトをズームアウトするには、アクティブなカウンタで Z を押し、カウンタを元のサイズに戻します。
- パフォーマンス ペインでカウンタをズームアウトするには、[OK] をクリックして [ズーム (Zoom)] ウィンドウを閉じます。

---

## チャートとグラフの強調表示

複数のノードまたはカウンタが色分けされたグラフで表示される場合、強調表示機能はホストとカウンタを区別するのに役立ちます。この機能は、[システム サマリー (System Summary)]、[CPU とメモリ (CPU and Memory)]、[ディスク使用率 (Disk Usage)]、および [パフォーマンス ログ ビューア (Performance Log Viewer)] ウィンドウでアクティブです。

### 手順

---

**ステップ 1** チャートとグラフを強調表示するには、次のいずれかの作業を実行します。

- システム サマリーなどの事前定義済みオブジェクトのグラフとチャートを強調表示するには、プロット領域内を右クリックして最も近いデータ系列またはポイントを強調表示します。
- パフォーマンス ログ ビューアでチャートとグラフを強調表示するには、次のいずれかの作業を実行します。
  - パフォーマンス ログ ビューアでチャートの下にあるテーブル内の任意の色分けを右クリックし、[強調表示 (Highlight)] を選択してそのカウンタのデータ系列を強調表示します。
  - パフォーマンス ログ ビューアでチャートの下にあるテーブル内の任意の色分けを右クリックし、[色の変更 (Change Color)] を選択してカウンタに対して別の色を選択します。

**ステップ 2** パフォーマンスログビューアで強調表示された項目を元の外観に戻すには、強調表示する別の項目を選択します。

---

## カウンタ プロパティ

カウンタプロパティを使用して、パフォーマンス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できます。

[カウンタのプロパティ (Counter Property)] ウィンドウには、カウンタのデータ サンプルを設定するためのオプションがあります。Unified RTMT の [パフォーマンスのモニタリング (performance monitoring)] ペインに表示されるパフォーマンス カウンタには、経時的なデータのサンプルが緑色の点で表示されます。収集するデータ サンプルの数やチャートに表示するデータ点の数は設定することができます。データ サンプルを設定した後は、[すべてのデータを表示 (View All Data)] または [現在のデータを表示 (View Current Data)] メニュー オプションを使用して perfmon カウンタに収集されたデータを表示することで、情報を表示します。

## 関連トピック

[パフォーマンス カウンタとアラート, \(219 ページ\)](#)

## カウンタのアラート通知

アラート通知機能をアクティブにすると、アプリケーションによりシステムの問題が通知されます。システム カウンタのアラート通知をアクティブにするには、次の設定を実行します。

- 1 [RTMT Perfmon モニタリング (RTMT Perfmon Monitoring)] ペインで、システムの perfmon カウンタを選択します。
- 2 アラート通知用に電子メールまたはメッセージのポップアップ ウィンドウを設定します。
- 3 アラートのしきい値を設定します (進行中のコールが 100 コール以上または 50 コール未満というしきい値を超えた場合など)。

- 4 アラート通知の頻度を決定します（アラートが 1 回発生、1 時間ごとに発生など）。
- 5 アラートがアクティブになるスケジュールを決定します（毎日、または 1 日の特定の時刻など）。

## Trace and Log Central

RTMT の Trace and Log Central 機能では、特定の日付範囲や絶対時間でのオンデマンドのトレース収集を設定できます。指定した検索条件が含まれているトレース ファイルを収集し、後で使用するためにそのトレース収集条件を保存したり、繰り返し行う 1 つの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 サーバまたは FTP 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できます。



- (注) Cisco Unified Serviceability から、ノード上のトレースに対する指定済みのトレース設定を編集することもできます。トレース設定を有効にすると、システムのパフォーマンスが低下します。そのため、トラブルシューティングを目的とした場合にだけトレースを有効にします。

ファイルを収集した後、それらのファイルは、リアルタイム モニタリング ツール内の対応するビューアで表示できます。また、リモートブラウズ機能を使用すると、トレースファイルをダウンロードしなくても、ノード上のトレースを表示できます。トレース ファイルは、Unified RTMT に付属する内部ビューアを選択するか、外部ビューアとして適切なプログラムを選択することで、開くことができます。



- (注)
- Trace and Log Central 機能を使用する場合は、Network Access Translation (NAT) なしで RTMT からクラスタ内の該当のノードまたはすべてのノードに直接アクセスできることを確認します。デバイスへのアクセス用に NAT をセットアップしている場合は、ノードを IP アドレスではなくホスト名で設定し、ホスト名（ホストの完全修飾ドメイン名）とそれらに対するルーティング可能な IP アドレスが DNS ノードまたはホスト ファイルに設定されていることを確認します。
  - 暗号化をサポートするデバイスでは、SRTP キー情報はトレース ファイルに出力されません。

### 関連トピック

[Cisco Unified Analysis Manager のセットアップ](#), (90 ページ)

### トレース ファイルの収集、スロットリング、および圧縮

Trace & Log Central の [ファイルの収集 (Collect Files)] オプションは、サーバまたはクラスタ内の 1 台以上のサーバに対してサービス、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。



(注) サービスは、アクティブにされていなくても表示されます。したがって、それらのサービスに対してトレースを収集できます。

### RTMT の Trace and Log Central ディスク I/O と CPU スロットリング

RTMT は、[Trace & Log Central] の重要なオペレーションとジョブの制御をサポートしています。そのオペレーションとジョブがオンデマンドで実行されているのか、スケジュールされているのか、または自動なのかは問いません。I/O 使用率でコール処理に対する要求が多い場合は、スロットリングによってオペレーションを遅くし、コール処理を優先させることができます。

コール処理ノードが高い I/O 条件で実行している場合にオンデマンド操作の要求を行うと、システムは動作を中断する機会を与える警告を表示します。次のサービスパラメータ (Cisco RIS Data Collector サービス内) を使用して警告を表示する条件を制御する I/O レートのしきい値を設定できます。

- TLC Throttling CPU Goal
- TLC Throttling IOWait Goal

システムは、実際のシステム CPU および IOWait 値とこれらのパラメータの値を比較します。目標 (サービスパラメータの値) が実際の値より小さい場合は、警告が表示されます。

### トレース圧縮サポート

この機能により、ROS (Recoverable Outstream) ライブラリでトレースファイルの圧縮された出力をサポートできるようになります。ファイルは生成されるときに圧縮されます。トレースファイル圧縮のメリットは次のとおりです。

- トレースファイルの保存に必要な容量が減少します。
- ディスクヘッドの移動が減少し、結果としてディスク I/O 待機が大幅に改善されます。この機能は、トレースファイルの要求が多い場合に価値があります。

エンタープライズパラメータ Trace Compression を使用して、トレース圧縮の有効化または無効化を行います。このパラメータのデフォルト値は Disabled です。エンタープライズパラメータの値の設定方法については、『*System Configuration Guide for Cisco Unified Communications Manager*』の“Enterprise Parameters Configuration”の章を参照してください。



注意

ファイルの圧縮では、追加の CPU サイクルが追加されます。トレース圧縮のエンタープライズパラメータを有効にすると、コールスループット全体に 10% もの負の影響を与えることがあります。

圧縮ファイルは .gz 拡張子で認識できます (ファイルがまだ書き込まれている場合は .gzo です)。圧縮ファイルを開くには、ファイル名をダブルクリックします。ファイルはログビューアで開きます。

## 設定プロファイル

サーバまたは Cisco Unified Communications Manager クラスタ内の任意のサーバに接続するには、RTMT を使用できます（該当する場合）。サーバにログインしたら、RTMT はローカル キャッシュから、またはバックエンドバージョンに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はリモートサーバから、モニタリングモジュールを起動します。

RTMT には、Default というデフォルト設定が含まれます。RTMT を初めて使用した場合、Default プロファイルを使って [モニタ (Monitor) ] ペインの [システムサマリー (System Summary) ] ページが表示されます。

Unified Communications Manager クラスタのみ : Default プロファイルは、動的にクラスタ内のすべての Unified Communications Manager サーバ用のすべての登録済み電話機をモニタします。クラスタに設定された Unified Communications Manager サーバが 5 台含まれる場合、CM-Default はクラスタ内の各サーバに登録された電話機と、進行中のコール、アクティブなゲートウェイポートおよびチャネルを表示します。

RTMT のモニタ ペインに必要な情報（さまざまな機能に関するさまざまなパフォーマンスカウンタなど）を表示し、プロファイルに設定のフレームワークを保存するように、RTMT を設定することができます。このプロファイルは、同じセッション中、または RTMT への次のログイン時に後で復元できます。複数のプロファイルを作成するとプロファイルごとに固有の情報が表示されるため、プロファイルを切り替えることでそれぞれの情報を迅速に表示することができます。



(注)

Cisco Unified Communications Manager のアップグレード中に RTMT クライアントを実行してパフォーマンスカウンタをモニタしている場合、アップグレード中およびアップグレード後にパフォーマンスカウンタは更新されません。Unified Communications Manager アップグレード完了後にパフォーマンスカウンタを正確にモニタし続けるには、RTMT プロファイルをリロードするか、または RTMT クライアントを再起動する必要があります。

### 関連トピック

[設定プロファイルの追加, \(117 ページ\)](#)

## カテゴリ

カテゴリを使用して、パフォーマンスモニタリング クラスタやデバイスなどの RTMT 内のオブジェクトを整理できます。たとえば、パフォーマンスモニタリング下のデフォルトカテゴリを使用して、RTMT では 6 種類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することができます。さらに多くのカウンタをモニタする場合は、新しいカテゴリを設定し、データを表形式で表示できます。

電話やゲートウェイなど、さまざまなデバイスの検索を実行する場合は、検索ごとにカテゴリを作成し、その結果をカテゴリに保存できます。





- (注) IM and Presence Service のデフォルト プロファイルのプロファイル設定に対して加えた変更は、Unified Communications Manager に転送されません。IM and Presence Service のプロファイルは、プレフィックス “Presence\_” 付きの名前に変更されます。

#### 関連トピック

[カテゴリの追加](#), (118 ページ)

## アラート (Alerts)

アクティブになっているサービスが停止したときなど、事前に定義された条件に達したときに管理者に通知するためのアラート メッセージが生成されます。アラートは、電子メールまたは E ページとして送信することができます。

アラートの定義、設定、表示をサポートする Unified RTMT には、事前に設定されたアラートとユーザ定義のアラートが含まれます。両方のタイプの設定作業を実行できますが、事前設定のアラートは削除できません (ユーザ定義のアラートの追加および削除は可能です)。

### アラート オプション

[アラート (Alert) ] メニュー ([システム (System) ] > [ツール (Tools) ] > [アラート (Alert) ]) は、次のメニュー オプションで構成されます。

- [Alert Central] : このオプションは、システム内のすべてのアラートの履歴と現在のステータスで構成されます。



- (注) システム ドロウの階層ツリーにある [Alert Central] アイコンを選択して [Alert Central] にアクセスすることもできます。

- [アラート/プロパティの設定 (Set Alert/Properties) ] : このメニュー オプションを使用すると、アラートとアラート プロパティを設定できます。
- [アラートの削除 (Remove Alert) ] : このメニュー カテゴリを使用すると、アラートを削除できます。
- [アラートの有効化 (Enable Alert) ] : このメニュー カテゴリを使用すると、アラートを有効にできます。
- [アラートの無効化 (Disable Alert) ] : このカテゴリを使用すると、アラートを無効にできます。
- [クラスタ/ノードのアラートの一時停止 (Suspend cluster/Node Alerts) ] : このメニュー カテゴリを使用すると、特定の IM and Presence ノードまたはクラスタ全体のアラートを一時的に停止できます。

- [アラートのクリア (Clear Alerts)] : このメニューカテゴリを使用すると、アラートをリセットして (アラート項目の色が赤から黒に変わります) 、アラートが処理済みであると示すことができます。アラートが発生すると、Unified RTMT でアラートの色が自動的に変わり、アラートを手動でクリアするまでそのままになります。
- [すべてのアラートをクリア (Clear All Alerts)] : このメニューカテゴリを使用すると、すべてのアラートをクリアできます。
- [すべてのアラートをデフォルト設定にリセット (Reset all Alerts to Default Config)] : このメニューカテゴリを使用すると、すべてのアラートをデフォルト設定にリセットできます。
- [アラートの詳細 (Alert Detail)] : このメニューカテゴリはアラート イベントに関する詳細情報を表示します。
- [電子メールサーバの設定 (Config Email Server)] : このカテゴリでは、電子メールサーバを設定してアラートを有効にできます。
- [アラートアクションの設定 (Config Alert Action)] : このカテゴリを使用すると、特定のアラートに対するアクションの設定、および目的の電子メール受信者にアラートを送信するアクションの設定ができます。

Unified RTMT では、perfmon カウンタのしきい値に対するアラート通知を設定し、そのアラートのアラートプロパティ (しきい値、期間、頻度など) を設定します。

[Alert Central] は、クイック起動の [ツール (Tools)] 階層ツリーの配下にあります。[Alert Central] には、システム内のすべてのアラートの現在のステータスと履歴が表示されます。

## アラート フィールド

Unified RTMT で、事前に設定されたアラートとユーザ定義のアラートの両方を設定できます。また、Unified RTMT で、事前設定のアラートとユーザ定義のアラートの両方を無効にすることもできます。パフォーマンスモニタリングウィンドウではユーザ定義のアラートを追加および削除できます。ただし、事前設定のアラートは削除できません。



(注) syslog エントリの重大度レベルは、すべての Unified RTMT アラートの重大度レベルと一致します。Unified RTMT が重大アラートを発行した場合、対応する syslog エントリも重大になります。

次の表に、各アラートの設定に使用できるフィールドのリストを示します。特に記載がない限り、ユーザは事前に設定されたフィールドを設定できます。

表 2: アラートのカスタマイズ

フィールド	説明	コメント
アラート名 (Alert Name)	RTMT がアラートに関連付けるモニタリング項目の概略的な名前	説明的な名前。事前設定のアラートの場合、このフィールドは変更できません。事前設定されたアラートのリストについては、Alert Central の表示に関連するトピックを参照してください。
説明	アラートの説明	事前設定のアラートの場合、このフィールドは編集できません。事前設定されたアラートのリストについては、Alert Central の表示に関連するトピックを参照してください。
パフォーマンス カウンタ (Performance Counter(s))	パフォーマンスカウンタのソース	このフィールドは変更できません。1つのアラートに関連付けることができるパフォーマンスカウンタは1インスタンスだけです。
しきい値 (Threshold)	アラートの生成条件 (値)	上限<->下限 (#、%、レートより小さい、#、%、レートより大きい) を指定します。このフィールドは、パフォーマンスカウンタをベースとするアラートにのみ適用できます。
次の値で算出 (Value Calculated As)	しきい値条件を確認する方法	評価する値を絶対値、差分 (現在と前回)、または差分比率で指定します。このフィールドは、パフォーマンスカウンタをベースとするアラートにのみ適用できます。
時間 (Duration)	アラートの生成条件 (アラートを生成するまでのしきい値の持続時間)	すぐにアラートを送信させるオプション、またはアラートが指定時間持続した後に送信させるオプションがあります。このフィールドは、パフォーマンスカウンタをベースとするアラートにのみ適用できます。

フィールド	説明	コメント
イベント数のしきい値 (Number of Events Threshold)	設定可能なイベント数が設定可能な時間間隔 (分) を超えた場合にのみアラートを発行します。	ExcessiveVoiceQualityReports のデフォルトのしきい値は 10 ~ 60 分です。RouteListExhausted および MediaListExhausted のデフォルト値は 0 ~ 60 分です。このフィールドは、イベントベースのアラートにのみ適用できます。
ノード ID (Node IDs) (適用対象 : Unified Communications Manager、IM and Presence Service)	監視するサーバのクラスタまたはリスト	Cisco Unified Communications Manager サーバ、Cisco TFTP サーバ、または最初のサーバ。このフィールドは、クラスタ全体のアラート以外のアラートにのみ適用できます。  (注) サーバ上の Cisco CallManager と Cisco TFTP サービスの両方を非アクティブ化すると、現在のモニタリング対象サーバリストからそのサーバが削除されたと見なされます。Cisco CallManager サービスと Cisco TFTP サービスの両方を再アクティブ化すると、そのサーバは再度追加され、設定はデフォルト値に戻ります。
アラートアクション ID (Alert Action ID)	実行するアラートアクションの ID (アラートアクションに関係なく、システムは常にアラートを記録します)。	アラートアクションが最初に定義されます (アラートのカスタマイズの項を参照)。このフィールドが空白の場合は、電子メールが無効であることを意味します。
アラートの有効化 (Enable Alerts)	アラートを有効または無効にします。	オプションは、有効化または無効化です。

フィールド	説明	コメント
アラートのクリア (Clear Alert)	アラートをリセットして (アラート項目の色が赤から黒に変わります)、アラートが解決されたことを示します。	アラートが発生すると、アラートの色が自動的に黒に変わり、アラートを手動でクリアするまでそのままになります。すべてのアラートをクリアするには、[すべてをクリア (Clear All)] を使用します。
アラート詳細 (Alert Details) (適用対象: Unified Communications Manager、IM and Presence Service)	アラートの詳細が表示されます (設定不可)。	ExcessiveVoiceQualityReports、RouteListExhausted、MediaListExhausted については、現在の間隔でアラートが発生した場合、現在のモニタリング間隔で最大 30 まで、現在のイベント詳細が表示されます。それ以外では、前の間隔で前の 30 のイベント詳細が表示されます。DChannel OOS アラートの場合は、アラートが発生した時点で未解決だった OOS デバイスのリストが表示されます。
アラート生成率 (Alert Generation Rate)	アラート条件が持続したときにアラートを生成する頻度	X 分ごとに指定します。(条件が持続した場合には、X 分ごとに 1 回アラートが生成されます)。  X 分ごとに最大 Y 回と指定します。(条件が持続した場合には、X 分ごとに Y 回アラートが生成されます)。
テキスト入力ユーザ (User Provide Text)	定義済みのアラート テキストにテキストを付加する管理者	—
重大度 (Severity)	表示目的のみ (例: Sev.1 のアラートのみ表示)	定義済みのアラート (Error、Warning、Information など) に割り当てられるデフォルトを指定します。

関連トピック

[パフォーマンス カウンタとアラート, \(219 ページ\)](#)

## アラート ログ

アラートは、アラート ログに保存されます。また、メモリにも保存されます。メモリは一定間隔でクリアされ、最後の30分間のデータがメモリに残されます。サービスが開始または再開されると、クラスタ内の特定のサーバまたはすべてのサーバに存在するアラート ログから最後の30分間のアラートデータが読み込まれ、メモリにロードされます。メモリ内のアラートデータは、要求に応じて RTMT クライアントに送信されます。

RTMT の起動時に、Alert Central ログ履歴の最後の30分間に発生したすべてのログが表示されます。アラートログは定期的に更新され、新しいログがログ履歴ウィンドウに挿入されます。ログの数が100に達すると、RTMT は最も古い40個のログを削除します。

アラート ログに対して、次のファイル名形式が適用されます：

AlertLog\_MM\_DD\_YYYY\_hh\_mm.csv。

アラート ログには次の属性が含まれます。

- タイムスタンプ (Time Stamp) : RTMT はデータを記録した時間
- アラート名 (Alert Name) : アラートを説明する名前
- ノード (Node) : RTMT でアラートが発生したサーバ名
- アラートメッセージ (Alert Message) : アラートに関する詳細な説明
- タイプ (Type) : アラートのタイプ
- 説明 (Description) : モニタされるオブジェクトの説明
- 重大度 (Severity) : アラートの重大度
- PollValue : アラート状態が発生したモニタ対象オブジェクトの値
- アクション (Action) : 実行されたアラートアクション
- グループ ID (Group ID) : アラートの原因を識別する

各ログ ファイルの最初の行はヘッダーです。各アラートの詳細は1行に書き込まれ、カンマによって区切られます。

## Log Partition Monitoring Tool

Log Partition Monitoring (LPM) は、システムとともに自動的にインストールされ、設定可能なしきい値を使用して、サーバ上のログパーティションのディスク使用率をモニタします。Cisco Log Partition Monitoring Tool サービスには、システムのインストール後に自動的に起動します。

Log Partition Monitoring は、次の設定済みのしきい値を使用して、サーバ上のログパーティションおよび予備のログパーティションのディスク使用率を5分ごとにモニタします。

- LogPartitionLowWaterMarkExceeded (ディスク領域使用率) : 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 syslog にアラームメッセージを送信し、RTMT Alert Central にアラートを送信します。ログ ファイルを保存してディスク領域を回復するには、RTMT の [Trace & Log Central] オプションを使用します。

- **LogPartitionHighWaterMarkExceeded** (ディスク領域使用率) : 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 syslog にアラーム メッセージを送信し、RTMT Alert Central にアラートを送信します。
- **SparePartitionLowWaterMarkExceeded** (ディスク領域使用率) : 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 syslog にアラーム メッセージを送信し、RTMT Alert Central にアラートを送信します。ログファイルを保存してディスク領域を回復するには、RTMT の [Trace & Log Central] オプションを使用します。
- **SparePartitionHighWaterMarkExceeded** (ディスク領域使用率) : 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 syslog にアラーム メッセージを送信し、RTMT Alert Central にアラートを送信します。

さらに、Cisco Log Partitioning Monitoring Tool サービスは 5 秒ごとにサーバをチェックして、新たに作成されたコア ダンプ ファイルの有無をチェックします。新しいコア ダンプ ファイルが存在した場合、Cisco Log Partitioning Monitoring Tool サービスは、新しい各コア ファイルに関する情報とともに CoreDumpFileFound アラームとアラートを Alert Central に送信します。

ログパーティションモニタを利用するには、ネットワーク サービスである Cisco Log Partitioning Monitoring Tool サービスがそのサーバ上またはクラスタ内の各サーバ上 (該当する場合) の Cisco Unified Serviceability で実行されていることを確認します。サービスを停止すると、機能が失われます。

Log Partition Monitoring サービスは、システム起動時に開始されたときに、現在のディスク領域の使用率をチェックします。ディスク使用率のパーセンテージが下限を上回っていても、上限を下回っている場合には、syslog にアラーム メッセージが送信され、RTMT Alert Central で対応するアラートが生成されます。

Log Partitioning Monitoring を設定するには、Alert Central で LogPartitionLowWaterMarkExceeded アラートと LogPartitionHighWaterMarkExceeded アラートのアラートプロパティを設定します。

ログファイルをオフロードしてサーバのディスク領域を回復するためには、リアルタイムモニタリング ツールを使用して領域を節約する必要があるトレースを収集する必要があります。

ディスク使用率のパーセンテージが設定した上限を上回っている場合は、syslog にアラーム メッセージが送信され、RTMT Alert Central で対応するアラートが生成され、値が下限に達するまでログ ファイルが自動的にページされます。



(注) Log Partition Monitoring は、アクティブなディレクトリと非アクティブなディレクトリを含む共通のパーティションを自動的に識別します。アクティブなディレクトリには、現在インストールされているバージョンのソフトウェア（Cisco Unified Communications Manager または Cisco Unity Connection）のログファイルが含まれ、非アクティブなディレクトリには、以前にインストールしたバージョンのソフトウェアのログファイルが含まれます。必要に応じて、サービスは非アクティブなディレクトリのログ ファイルを先に削除します。次に、すべてのアプリケーションの最も古いログ ファイルから順に、ディスク領域のパーセンテージが設定された下限を下回るまで、アクティブなディレクトリのログ ファイルを削除します。Log Partition Monitoring によってログ ファイルがパージされても、システムは電子メールを送信しません。

システムがディスク使用率を判断し、必要なタスク（アラームの送信、アラートの生成、またはログのパージ）を実行した後は、ログパーティションモニタリングが通常の5分間隔で行われます。

## Cisco Unified Analysis Manager

トラブルシューティング操作を実行するには、Cisco Unified Real-Time Monitoring Tool に含まれているツールの Cisco Unified Analysis Manager を使用します。Unified Analysis Manager は、起動すると、システムからトラブルシューティング情報を収集して、その情報を分析します。この情報を使用して独自のトラブルシューティング操作を実行したり、分析のために Cisco Technical Assistance に情報を送信したりできます。

Unified Analysis Manager アプリケーションは、RTMT ソフトウェアをインストールする際にオプションとしてインストールされます。Unified Analysis Manager インターフェイスには、RTMT のメインメニューおよびクイック起動チャネルからアクセスできます。

このアプリケーションをインストールすると、システム上にあるサポート対象の Unified Communications (UC) 製品およびアプリケーションを識別し、トレースおよびログファイルを収集して、これらの UC アプリケーションでのコール障害をトラブルシューティングできます。

Unified Analysis Manager は、次の製品をサポートします。

- Cisco Unified Communications Manager
- Cisco Unified Contact Center Enterprise (Unified CCE)
- Cisco Unified Contact Center Express (Unified CCX)
- Cisco IOS Voice Gateways (37xx, 28xx, 38xx, 5350XM, 5400XM) IOS リリース PI 11
- Cisco Unity Connection
- IM and Presence Service

Unified Analysis Manager インターフェイスの3つの主要コンポーネントは次のとおりです。



- 管理 (Administration) : 管理コンポーネントでは、外部ファイルからデバイスおよびグループの設定をインポートし、Unified Analysis Manager で実行されるジョブのステータスを指定できます。
- インベントリ (Inventory) : インベントリ コンポーネントは、Unified Analysis Manager によってアクセスおよび分析できるシステム上のすべてのデバイスを識別するために使用します。
- ツール (Tools) : ツールコンポーネントには、Unified Analysis Manager がサポートしているすべての機能が含まれます。トレースの設定、ログの収集、および設定の表示がこれに含まれます。

#### 関連トピック

[\[Trace & Log Central\] オプションの表示, \(161 ページ\)](#)

## サービス、サブレット、サービスパラメータ

Unified RTMT クライアントをサポートするには、サーバ上で多数のサービスがアクティブになり、実行されている必要があります。Unified RTMT では、次のサービスおよびサブレットを使用します。

- Cisco AMC サービス : このサービスはインストール後に自動的に開始され、Unified RTMT がクラスタ内のノードに存在するリアルタイム情報を取得できるようになります。IM and Presence Service は、最初のノードを自動的にプライマリ コレクタとして割り当てます。プライマリコレクタに障害が発生しても、Unified RTMT で引き続き情報を取得できるよう、管理インターフェイスのサービスパラメータで後続ノードをフェールオーバー コレクタとして設定する必要があります。

次のリストは、Unified RTMT に関連付けられたいくつかの Cisco AMC サービスパラメータを示しています。パラメータの最新のリストについては、管理インターフェイスの [システム (System) ] > [サービスパラメータ (Service Parameters) ] の順に選択します。次に、サーバと Cisco AMC サービスを選択します。

- Primary Collector
- Failover Collector
- Data Collection Enabled
- Data Collection Polling Rate
- Server Synchronization Period
- RMI Registry Port Number
- RMI Object Port Number
- Logger Enabled
- Unified Communications Manager: Alarm Enabled
- Unified Communications Manager: AlertMgr Enabled

- Cisco Unity Connection: PerfMon Log Deletion Age
- Cisco Unity Connection: AlertMgr Enabled

これらのサービスパラメータの詳細については、管理インターフェイスの [サービスパラメータ設定 (Service Parameter configuration)] ウィンドウに表示される [?] ボタンを選択してください。

次のリストは、Unified RTMT に関連付けられた servlet およびネットワーク サービスで構成されます。これらのサービスを表示するには、Cisco Unified Serviceability で、[ツール (Tools)] > [コントロールセンター - ネットワーク サービス (Control Center - Network Services)] の順に選択します。

- Cisco CallManager Serviceability RTMT : Unified RTMT をサポートします。このサービスは、インストール後に自動的に起動します。
- Cisco RIS Data Collector : Real-time Information Server (RIS) は、パフォーマンスカウンタ統計、生成された重大アラームなどのリアルタイム情報を保持します。Cisco RIS Data Collector サービスは、Real-Time Monitoring Tool、SOAP アプリケーション、および AlertMgrCollector (AMC) などのアプリケーションに対して、サーバに保存された情報を取得するためのインターフェイスを提供します。
- Cisco Tomcat Stats Servlet : Cisco Tomcat Stats Servlet は Unified RTMT または CLI を使用して、Tomcat perfmon カウンタをモニタすることができます。このサービスが CPU 時間などのリソースを大量に使用していることが疑われる場合を除き、このサービスを停止しないでください。
- Cisco Trace Collection Servlet : Cisco Trace Collection Servlet は、Cisco Trace Collection サービスとともにトレース収集をサポートし、ユーザが Unified RTMT クライアントでトレースを表示できるようにします。サーバ上でこのサービスを停止すると、そのサーバ上のトレースは収集または表示ができなくなります。
- Cisco Trace Collection サービス : Cisco Trace Collection サービスは、Cisco Trace Collection Servlet とともにトレース収集をサポートし、ユーザが Unified RTMT クライアントでトレースを表示できるようにします。サーバ上でこのサービスを停止すると、そのサーバ上のトレースは収集または表示ができなくなります。
- Cisco Log Partition Monitoring Tool : このサービスはインストール後に自動的に開始され、サーバ上のログパーティションのディスク使用量をモニタします。
- Cisco SOAP-Real-Time Service APIs : インストール後に自動的に開始される Cisco SOAP-Real-Time Service APIs は、Unified RTMT がデバイスと CTI アプリケーションに関するリアルタイム情報を収集できるようにします。
- Cisco SOAP-Performance Monitoring APIs : このサービスはインストール後に自動的に開始され、SOAP API を介したさまざまなアプリケーションのパフォーマンスモニタリングカウンタを Unified RTMT で使用できるようにします。
- Cisco RTMT Reporter servlet : このサービスはインストール後に自動的に開始され、Unified RTMT に関するレポートの公開を可能にします。

## 設定できないコンポーネント

アプリケーションと共に自動的にインストールされるコンポーネントである RTMT Collector は、定義済みのモニタリングオブジェクト情報を記録します。一方、同じく自動的にインストールされる Alert Manager は、アラート履歴をログファイルに記録します。定義済みの各オブジェクトは、デバイス、サービス、ノード、コールアクティビティ、および PPR という複数のカテゴリのいずれかに属します。各カテゴリには個別のログファイルがあり、アラートの詳細が個別のファイルに記録されます。

また、重要な perfmon オブジェクト値はパフォーマンス ログファイルに記録されます。



### ヒント

Unified Communications Manager クラスタと IM and Presence Service クラスタのみ：実行が必要な設定タスクはありませんが、RTMT Collector および Alert Manager は冗長性をサポートします。プライマリ コレクタまたはマネージャに何らかの障害が発生した場合でも、プライマリサポートが可能になるまで、セカンダリ コレクタおよびマネージャがタスクを実行します。RTMT Collector、Alert Manager、および RTMT Reporter は、コール処理のための中断を最小限にするために、最初のノードで動作します。

ローカルで書き込まれたログファイルは、`cm/log/amc` でプライマリ コレクタ サーバに表示されます。フェールオーバーやフォールバックのシナリオではプライマリ コレクタが変更されるため、Unified Communications Manager クラスタでログファイルが複数のサーバに存在する可能性があります。

アラート ログファイル以外のログファイルは、Unified RTMT でパフォーマンス ログ ビューアを使用するか、ネイティブの Microsoft Performance ビューアを使用して表示できます。アラート ログファイルは、テキスト エディタを使用して表示できます。

ログファイルをローカルマシンにダウンロードするには、Unified RTMT の Trace and Log Central にある [ファイルの収集 (Collect Files)] オプションを使用できます。

他の方法として、CLI で `file list` コマンドを使用してファイルのリストを表示し、`file get` コマンドを使用して SFTP でファイルをダウンロードできます。CLI コマンドの詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。

ログファイルは CSV 形式です。新しいログファイルは、ローカルシステムで毎日 00:00 に作成されます。Unified Communications Manager クラスタでは、デバイス、サービス、ノード、およびコールの新しいログは、タイムゾーンが変更されたとき、または新しいノードがクラスタに追加されたとき、あるいはフェールオーバー/フォールバックシナリオの間に作成されます。これらのログの最初の列には、タイムゾーンに関する情報と、グリニッジ標準時間 (GMT) を起点とする分数が表示されます。RTMT Reporter は、これらのログファイルをデータソースとして使用して、毎日のサマリーレポートを生成します。デフォルトのモニタリングオブジェクトに基づくこのレポートは、次の情報について、24 時間ごとに生成されます。

- コールアクティビティの状態：各 Unified Communications Manager、各ゲートウェイ、トランク、およびクラスタ全体（該当する場合）について、試行されたコール数および完了したコール数。各ゲートウェイの利用可能なインサービスのチャンネル数。

- デバイスの状態：各ノードおよびクラスタ全体（該当する場合）の登録済みの電話機、ゲートウェイ、およびトランクの数。
- サーバの状態：ノードごとの CPU 負荷率、メモリ使用率、ディスク スペース使用率。
- サービスの状態：（Unified Communications Manager）各 CTI Manager の場合は、オープンデバイスとオープン回線の数。各 TFTP サーバの場合は、試行された要求数と失敗した要求数。
- アラートの状態：ノードあたりのアラートの数。Unified Communications Manager クラスタでは、クラスタの上位 10 位までのアラートなど、クラスタの重大度レベルごとのアラート数。
- パフォーマンス保護レポート：システム全体の状態をトラッキングできるデフォルトのモニタリングオブジェクトに関する傾向分析情報。レポートには、ノードごとに過去 7 日間の情報が記録されます。



ヒント Unified RTMT レポートは英語でのみ表示されます。

サービス パラメータ RTMT Reporter Designated node、RTMT Report Generation Time、および RTMT Report Deletion Age は、Unified RTMT レポートの生成に適用されます。これらのパラメータに関する情報を参照するには、設定に関する次のサービス パラメータ ヘルプに移動します。

Cisco Unified Communications Manager および Cisco Unified Communications Manager IM and Presence Service	Cisco Unified Communications Manager の管理ページにある [サービスパラメータ (Service Parameter)] ウィンドウで、[Cisco Serviceability Reporter] を選択します。
<b>Cisco Business Edition 5000</b>	Cisco Cisco Unified Communications Manager IM and Presence の管理ページにある [サービスパラメータ (Service Parameter)] ウィンドウで、[Cisco Serviceability Reporter] を選択し、[?] ボタンをクリックします。
<b>Cisco Unity Connection</b>	[サービスパラメータ (Service Parameters)] ウィンドウの [サービス (Service)] ドロップダウンリストボックスでサービスをクリックし、[ヘルプ (Help)] > [このページ (This Page)] をクリックします。

Serviceability レポートの詳細については、『Cisco Unified Serviceability Administration Guide』の「“Serviceability Reports”」の章を参照してください。

## Unified RTMT のアンインストール



- (注) Unified RTMT は、ユーザ設定およびモジュール jar ファイル (キャッシュ) をクライアントマシンのローカルに保存します。Unified RTMT をアンインストールするときは、キャッシュを削除するか保存するかを選択します。



- (注) Windows Vista または 7 マシンで Unified RTMT をアンインストールする場合、“未確認のプログラムがコンピュータにアクセスしようとしています (An unidentified program wants to access your computer)” というユーザアカウント制御ポップアップメッセージが表示されます。[許可] をクリックして、Unified RTMT のインストール作業を続行します。

### 手順

- ステップ 1** Unified RTMT のアクティブセッションをすべて終了します。
- ステップ 2** Unified RTMT をアンインストールするには、次のいずれかの操作を実行します。
- a) Windows クライアントの場合、[スタート (Start)] > [設定 (Settings)] > [コントロールパネル (Control Panel)] > [プログラムの追加と削除 (Add/Remove Programs)] の順に選択します。
  - b) KDE または GNOME クライアントを使用した Red Hat Linux インストールの場合、タスクバーから [スタート (Start)] > [アクセサリ (Accessories)] > [リアルタイムモニタリングツールのアンインストール (Uninstall Real-time Monitoring tool)] の順に選択します。
- ステップ 3** プラグインのアンインストールを終了します。





## 第 3 章

# システムパフォーマンスのモニタリング

- [事前定義済みのシステム オブジェクト](#), 37 ページ
- [音声およびビデオのモニタリング](#), 41 ページ
- [Intercompany Media Service](#), 73 ページ
- [IM and Presence モニタリング](#), 76 ページ
- [Cisco Unity Connection のモニタリング](#), 82 ページ

## 事前定義済みのシステム オブジェクト

Unified RTMT はモニタリング ペインに事前定義済みシステム オブジェクトの情報を表示します。



ヒント

事前に準備された各モニタリング ウィンドウのポーリング レートは固定されていて、デフォルト値は 30 秒です。AMC (Alert Manager and Collector) サービス パラメータの収集レートが変化すると、事前に準備されたウィンドウのポーリング レートも更新されます。また、バックエンド サーバの時刻ではなく、RTMT クライアント アプリケーションのローカル時刻が、各チャートのタイムスタンプのベースになります。

サービス パラメータについては、管理ページのオンライン ヘルプを参照してください。



ヒント

事前に定義されたオブジェクトのモニタを拡大するには、対象となるチャートの領域上でマウスの左ボタンをクリックし、ドラッグします。必要な領域を選択してから、マウスの左ボタンを放します。RTMT は、モニタ対象のビューを更新します。モニタを縮小して、初期のデフォルト ビューにリセットするには、R キーを押します。

次の表に、RTMT がモニタする事前定義済みオブジェクトに関する情報を示します。

表 3: システム カテゴリ

カテゴリ (Category)	説明
システム概要 (System Summary)	仮想メモリの使用状況、CPU 使用率、共通パーティションの使用、およびアラート履歴ログに関する情報を表示します。 事前定義システム オブジェクトに関する情報を表示するには、[システム (System) ]>[システム概要 (System Summary) ] を選択します。



カテゴリ (Category)	説明
サーバ	

カテゴリ (Category)	説明
	<ul style="list-style-type: none"> <li>• CPU とメモリ (CPU and Memory) : サーバの CPU 使用率と仮想メモリの使用率に関する情報を表示します。 CPU、仮想メモリの使用状況に関する情報を表示するには、[システム (System)] &gt; [サーバ (Server)] &gt; [CPU およびメモリ (CPU and Memory)] を選択します。特定のサーバの CPU とメモリの使用率を監視するには、[ホスト (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。</li> <li>• プロセス (Process) : サーバ上で実行中のプロセスに関する情報を表示します。 システムで実行されているプロセスに関する情報を表示するには、[システム (System)] &gt; [サーバ (Server)] &gt; [プロセス (Process)] を選択します。特定のサーバのプロセスの使用率をモニタするには、[ホスト (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。</li> <li>• [ディスク使用率 (Disk Usage)] : サーバ上のディスク使用率に関する情報を表示します。 システムのディスク使用状況情報を表示するには、[システム (System)] &gt; [サーバ (Server)] &gt; [ディスク使用率 (Disk Usage)] を選択します。特定のサーバのディスク使用率をモニタするには、[ホスト (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。</li> <li>• 重要なサービス (Critical Services) : 重要なサービスの名前、ステータス (サービスが起動しているか、ダウンしているか、管理者によってアクティブ化されたか、停止されたか、開始しているか、停止しているか、または不明な状態か)、およびサーバまたは (該当する場合は) クラスタ内の特定のサーバのサービスが特定の状態にある間に経過した時間を表示します。 重要なサービスの情報を表示するには、[システム (System)] &gt; [サーバ (Server)] &gt; [重要なサービス (Critical Services)] を選択し、適切なタブをクリックしてください。 <ul style="list-style-type: none"> <li>◦ システムの重要なサービスを表示するには、[システム (System)] タブを選択します。</li> <li>◦ Cisco Unified Communications Manager の重要なサービスを表示するには、[音声/ビデオ (Voice/Video)] タブをクリックします。 (注) [音声/ビデオ (Voice/Video)] タブは、[ホスト (Host)] ドロップダウン リスト ボックスで [Unified Communications Manager] サーバを選択している場合のみ表示されます。</li> <li>◦ IM and Presence Service の重要なサービスを表示するには、[IM and Presence] タブをクリックします。</li> </ul> </li> </ul>

カテゴリ (Category)	説明
	<p>(注) [IM and Presence] タブは、[ホスト (Host) ] ドロップダウンリスト ボックスで [IM and Presence] サーバを選択している場合のみ表示されます。</p> <ul style="list-style-type: none"> <li>° Cisco Unity Connection の重要なサービスを表示するには、[Cisco Unity Connection] タブをクリックします。</li> <li>° タブで特定のサーバの重要なサービスをモニタするには、[ホスト (Host) ] ドロップダウンリスト ボックスからサーバを選択し、関心のある重大なサービスのタブをクリックします。</li> </ul> <p>管理者がサービスを停止したことを重要なサービスの状態が示している場合は、管理者は意図的にサービスを停止するタスクを実行した（たとえば、Cisco Unified Communications Manager をバックアップまたはリストアした、アップグレードを実行した、あるいは、Cisco Unified Serviceability または CLI でサービスを停止した）ことを意味します。</p> <p>(注) 重要なサービスの状態が不明な状態として表示される場合は、システムがサービスの状態を決定できないことを意味します。</p>

## 音声およびビデオのモニタリング

### Cisco Unified Communications Manager の事前定義済みオブジェクト

Unified RTMT では、クイック起動チャネルで音声/ビデオを選択すると、事前定義された Cisco Unified Communications Manager オブジェクトについての情報がモニタリング ペインに表示されます。クラスタ内のすべてのサーバの事前定義済みオブジェクトが、必要に応じて、ツールによりモニタされます。



## ヒント

事前に準備された各モニタリング ウィンドウのポーリング レートは固定されていて、デフォルト値は 30 秒です。AMC (Alert Manager and Collector) サービス パラメータの収集レートが変化すると、事前に準備されたウィンドウのポーリング レートも更新されます。また、バックエンドサーバの時刻ではなく、Unified RTMT クライアント アプリケーションのローカル時刻が、各チャートのタイムスタンプのベースになります。

サービス パラメータの詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』または『*Cisco Unity Connection System Administration Guide*』を参照してください。



## ヒント

事前に定義されたオブジェクトのモニタを拡大するには、対象となるチャートの領域上でマウスの左ボタンをクリックし、ドラッグします。必要な領域を選択してから、マウスの左ボタンを放します。Unified RTMT は、モニタ対象のビューを更新します。モニタを縮小して、初期のデフォルト ビューにリセットするには、R キーを押します。

次の表に、Unified RTMT がモニタする事前定義済みオブジェクトに関する情報を示します。

表 4 : Cisco Unified Communications Manager のカテゴリ

カテゴリ (Category)	説明
音声およびビデオの概要 (Voice and Video Summary)	登録済みの電話機、進行中のコール、およびアクティブな MGCP ポートとチャンネルを表示します。 事前定義済みの Cisco Unified Communications Manager オブジェクトに関する情報を表示するには、[音声/ビデオ (Voice/Video)] > [音声およびビデオの概要 (Voice and Video Summary)] を選択します。

カテゴリ (Category)	説明
コール処理 (Call Process)	<ul style="list-style-type: none"> <li>• コール アクティビティ : Cisco Unified Communications Manager の、完了したコール、試行されたコール、進行中のコール、論理パーティション合計エラー数などのコールアクティビティを表示します。該当する場合、これはクラスタ内のすべてのサーバが含まれます。 コールアクティビティに関する情報を表示するには、[音声/ビデオ (Voice/Video) ]&gt;[コール処理 (Call Process) ]&gt;[コールアクティビティ (Call Activity) ]を選択します。</li> <li>• ゲートウェイ アクティビティ (Gateway Activity) : アクティブポート、サービス中のポート、完了したコールを含む Cisco Unified Communications Manager のゲートウェイアクティビティを表示します。該当する場合、これはクラスタ内のすべてのサーバが含まれます。 ゲートウェイアクティビティに関する情報を表示するには、[音声/ビデオ (Voice/Video) ]&gt;[コール処理 (Call Process) ]&gt;[ゲートウェイアクティビティ (Gateway Activity) ]を選択します。[ゲートウェイタイプ (Gateway Type) ]ドロップダウンリストから、ゲートウェイインターフェイスのタイプを選択します。</li> <li>• トランクアクティビティ (Trunk Activity) : 進行中のコールおよび完了したコールを含む Cisco Unified Communications Manager 上のトランクアクティビティを表示します。該当する場合、これはクラスタ内のすべてのサーバが含まれます。 トランクアクティビティに関する情報を表示するには、[音声/ビデオ (Voice/Video) ]&gt;[コール処理 (Call Process) ]&gt;[トランクアクティビティ (Trunk Activity) ]を選択します。[トランクタイプ (Trunk Type) ]ドロップダウンボックスでトランクタイプを選択します。</li> <li>• SDL キュー (SDL Queue) : キューに格納されている信号の数や処理済みの信号の数などの SDL キュー情報が表示されます。 SDL キューに関する情報を表示するには、[音声/ビデオ (Voice/Video) ]&gt;[コール処理 (Call Process) ]&gt;[SDL キュー (SDL Queue) ]を選択します。[SDL キュータイプ (SDL Queue Type) ]ドロップダウンリストボックスからタイプを選択します。</li> <li>• SIP アクティビティ (SIP Activity) : Cisco Unified Communications Manager 上の概要要求、概要応答、着信失敗応答の概要、発信失敗応答の概要、発信再試行要求、発信再試行応答などの SIP アクティビティを表示します。該当する場合、これはクラスタ内のすべてのサーバが含まれます。 SIP アクティビティに関する情報を表示するには、[音声/ビデオ (Voice/Video) ]&gt;[コール処理 (Call Process) ]&gt;[SIP アクティビティ (SIP Activity) ]を選択します。</li> </ul>

カテゴリ (Category)	説明
セッショントレース (Session Trace)	<p>すべての SIP メッセージのアクティビティ、特に着信コールと発信コールおよび Cisco Unified Communications Manager を通過するセッションを表示します。各 SIP トランザクションに対して関連付けられたコールフローダイアグラムを提供します。</p> <p>セッショントレースに関する情報を表示するには、[音声/ビデオ (Voice/Video)] &gt; [コール処理 (Call Process)] &gt; [セッショントレース (Session Trace)] を選択します。</p>
Device	<p>[デバイス概要 (Device Summary)] には、登録済み電話機デバイス、登録済みゲートウェイデバイス、他の登録済み端末デバイス、登録済みメディアリソースデバイスなど、Cisco Unified Communications Manager サーバに関する情報を表示します。該当する場合、これはクラスタ内のすべてのサーバが含まれます。</p> <p>[デバイスの検索 (Device Search)] には、クラスタ名とデバイスタイプがツリー階層に表示され、電話機やデバイスに関する情報を問い合わせることができます。</p> <p>[電話機概要 (Phone Summary)] には、登録済み電話機の数、登録済み SIP 電話機の数、登録済み SCCP 電話機の数、一部登録済み電話機の数、および登録試行の失敗回数など、Cisco Unified Communications Manager のサーバに関する情報を表示します。該当する場合、これはクラスタ内のすべてのサーバが含まれます。</p> <p>Cisco Unified Communications Manager 上にある登録済み電話機、ゲートウェイ、およびメディアリソースデバイスの数に関する情報を表示するには、[音声/ビデオ (Voice/Video)] &gt; [デバイス (Device)] &gt; [デバイス概要 (Device Summary)] を選択します。</p> <p><b>ヒント</b> 他のデバイスを監視するには、追加の設定手順を実行します。</p>

カテゴリ (Category)	説明
サービス	<ul style="list-style-type: none"> <li>• Cisco TFTP : 合計 TFTP 要求数、および異常終了した合計 TFTP 要求数など、Cisco Unified Communications Manager サーバの Cisco TFTP のステータスを表示します。該当する場合、これはクラスタ内のすべてのサーバが含まれます。 Cisco TFTP サービスに関する情報を表示するには、[音声/ビデオ (Voice/Video)] &gt; [サービス (Service)] &gt; [Cisco TFTP] を選択します。</li> <li>• ハートビート (Heartbeat) : Cisco Unified Communications Manager、Cisco TFTP サービスのハートビート情報を表示します。 Cisco Unified Communications Manager サーバ、Cisco TFTP サーバのハートビートの状態を表示するには、[音声/ビデオ (Voice/Video)] &gt; [サービス (Service)] &gt; [ハートビート (Heartbeat)] を選択します。</li> <li>• データベース概要 (Database Summary) : サーバの接続情報を提供します。データベースのキューに格納されている変更通知要求、メモリのキューに格納されている変更通知要求、アクティブなクライアント接続の総数、作成された複製の数、複製のステータスなどの情報です。 データベースに関する情報を表示するには、[音声/ビデオ (Voice/Video)] &gt; [サービス (Service)] &gt; [データベース概要 (Database Summary)] を選択します。</li> </ul>
[CTI]	<p>CTI Manager とインターフェイスするデバイスおよびアプリケーションに関する情報を表示します。</p> <p>CTI アプリケーションに関する情報を表示するには、[音声/ビデオ (Voice/Video)] &gt; [CTI] &gt; [CTI Manager] を選択します。</p> <p>特定の CTI タイプをモニタするには、追加の設定手順を実行する必要があります。CTI アプリケーション、デバイス、および回線のモニタについてのトピックを参照してください。</p>

カテゴリ (Category)	説明
Intercompany Media Service	<ul style="list-style-type: none"> <li>ルーティング (Routing) : Cisco Unified Communications Manager によって管理される Cisco Intercompany Media Engine ルートの合計数を表示します。 コール アクティビティに関する情報を表示するには、[音声/ビデオ (Voice/Video)] &gt; [Intercompany Media Service] &gt; [ルーティング (Routing)] を選択します。</li> <li>コール アクティビティ (Call Activities) : 受け入れられたコール、ビジョ コール、無応答のコール、失敗したコールの数など、Cisco Intercompany Media Engine コール アクティビティを表示します。 コール アクティビティに関する情報を表示するには、[音声/ビデオ (Voice/Video)] &gt; [Intercompany Media Service] &gt; [コール アクティビティ (Call Activities)] を選択します。</li> </ul>

## Cisco Unified Communications Manager の [サマリー (Summary)] ビュー

単一のモニタリング ペインで、Cisco Unified Communications Manager サーバに関する情報またはクラスタ内のすべてのサーバに関する情報 (該当する場合) を Unified RTMT によりモニタできます。CallManager の [サマリー (Summary)] ウィンドウで、次の事前定義されたオブジェクトに関する情報を確認できます。

- 登録済みの電話機 (Registered Phones)
- 進行中のコール (Calls in Progress)
- アクティブなゲートウェイ、ポート、およびチャネル (Active Gateway, Ports, and Channels)

## コール処理アクティビティのモニタリング

[コール処理 (Call Process)] のモニタリング カテゴリは次の項目をモニタします。

- コールアクティビティ (Call Activity) : 特定のサーバまたはクラスタ全体 (該当する場合) について、試行されたコール数、完了したコール数、進行中のコール数、および論理パーティションの失敗の合計数をモニタできます。
- ゲートウェイ アクティビティ (Gateway Activity) : 各ゲートウェイ タイプについて、ゲートウェイ アクティビティをモニタできます。ゲートウェイ アクティビティのモニタリングには、特定のサーバまたはクラスタ全体 (該当する場合) についての、ゲートウェイ タイプごとのアクティブ ポート数、サービス中のポート数、および完了したコール数が含まれます。



- **トランクアクティビティ (Trunk Activity)** : システムは、特定のサーバ、またはクラスタ全体 (該当する場合) について、トランクタイプ別にトランクアクティビティをモニタします。トランクアクティビティのモニタリングには、特定のトランクタイプについての、進行中のコール数と完了したコール数が含まれます。
- **SDLキュー (SDL Queue)** : SDLキューのモニタリングでは、特定の信号分配レイヤ (SDL) キュータイプについて、SDLキュー内の信号数と処理された信号数をモニタします。SDLキューのタイプは、高、標準、低、最低のキューから構成されます。特定のサーバまたはクラスタ全体 (該当する場合) のSDLキューを監視できます。
- **SIPアクティビティ (SIP Activity)** : システムにより、SIP要求、SIP応答、失敗した着信応答数の合計 (4xx、5xx、および6xx)、失敗した発信応答数の合計 (4xx、5xx、および6xx)、再試行要求数、および再試行応答数の要約が表示されます。
- **セッショントレース (Session Trace)** : コールの検索またはトレースの条件として、発信者番号/URI、着信者番号/URI、開始時刻、および通話時間を用えます。RTMTでは、開始時刻および期間を含むコールログファイルをダウンロードし、一致するコールを検索し、一致するコールレコードをリストし、コールフロー図を表示します。

次の表に、RTMTでモニタするコール処理オブジェクト、アラート、しきい値、およびデフォルトに関する情報を示します。コールアクティビティの日報の詳細については、『*Cisco Unified Serviceability Administration Guide*』を参照してください

表 5: コール処理のカテゴリ

監視対象オブジェクト (表示)	アラート/しきい値/デフォルト
各サーバおよびクラスタ (該当する場合) について、CallsAttempted、CallsCompleted、CallsInProgress、および Logical Partition Failures Total。	—
各サーバおよびクラスタ (該当する場合) について、MGCP FXS/FXO/PRI/T1CAS/H.323 ゲートウェイ、ならびに SIP および H.323 トランクの各タイプの CallsAttempted、CallsCompleted、および CallsInProgress。	—
各 MGCP FXS/FXO/PRI/T1CAS ゲートウェイの Channel/Port Status。	—
各サーバの SDL Queue アクティビティ。	—
MGCP FXS ゲートウェイ: 各サーバおよびクラスタ (該当する場合) のサービス中およびアクティブなポートの数。	ルートリストが使い果たされました (Route-List exhausted)

監視対象オブジェクト (表示)	アラート/しきい値/デフォルト
MGCP FXO ゲートウェイ：各サーバおよびクラスタ (該当する場合) のサービス中およびアクティブなポートの数。	ルートリストが使い果たされました (Route-List exhausted)
MGCP PRI Gateway：各サーバおよびクラスタ (該当する場合) のサービス中およびアクティブなチャネルの数。	<ul style="list-style-type: none"> <li>• D チャネルがアウト オブ サービスです (Channel out of service)</li> <li>• ルート リストが使い果たされました (Route List exhausted)</li> </ul>
MGCP T1CAS Gateway：各サーバおよびクラスタ (該当する場合) のサービス中およびアクティブなポートの数。	ルート リストが使い果たされました (Route List exhausted)

## コール処理ログ

Unified RTMT により LogCall API が呼び出されると常に、コール処理データがメモリに蓄積されます。5 分ごとに、Unified RTMT はデータを単一のレコードとしてファイルに記録し、メモリを消去します。

次のカウンタについて、それぞれの計算に基づき、5 分ごとにデータが記録されます。

- cmCallsAttempted：累積 (過去 5 分間で、最後に収集された値と最初に収集された値の差分)
- cmCallsCompleted：累積 (過去 5 分間で、最後に収集された値と最初に収集された値の差分)
- cmCallsInProgress：過去 5 分間に収集されたすべての値の平均
- gwMGCP\_FXS\_CallsCompleted：累積 (過去 5 分間で、最後に収集された値と最初に収集された値の差分)
- gwMGCP\_FXO\_CallsCompleted：累積 (過去 5 分間で、最後に収集された値と最初に収集された値の差分)
- gwMGCP\_PRI\_CallsCompleted：累積 (過去 5 分間で、最後に収集された値と最初に収集された値の差分)
- gwMGCP\_T1\_CAS\_CallsCompleted：累積 (過去 5 分間で、最後に収集された値と最初に収集された値の差分)
- gwH323\_CallsAttempted：累積 (過去 5 分間で、最後に収集された値と最初に収集された値の差分)
- gwH323\_CallsInProgress：過去 5 分間に収集されたすべての値の平均

- gwH323\_CallsCompleted : 累積 (過去 5 分間で、最後に収集された値と最初に収集された値の差分)
- trunkH323\_CallsAttempted : 累積 (過去 5 分間で、最後に収集された値と最初に収集された値の差分)
- trunkH323\_CallsInProgress : 過去 5 分間に収集されたすべての値の平均
- trunkH323\_CallsCompleted : 累積 (過去 5 分間で、最後に収集された値と最初に収集された値の差分)
- trunkSIP\_CallsAttempted : 累積 (過去 5 分間で、最後に収集された値と最初に収集された値の差分)
- trunkSIP\_CallsInProgress : 過去 5 分間に収集されたすべての値の平均
- trunkSIP\_CallsCompleted : 累積 (過去 5 分間で、最後に収集された値と最初に収集された値の差分)
- gwMGCP\_FXS\_PortsInService : 過去 5 分間に収集されたすべての値の平均
- gwMGCP\_FXO\_PortsInService : 過去 5 分間に収集されたすべての値の平均
- gwMGCP\_PRI\_SpansInService : 過去 5 分間に収集されたすべての値の平均
- gwMGCP\_T1\_CAS\_SpansInService : 過去 5 分間に収集されたすべての値の平均
- gwMGCP\_FXS\_ActivePorts : 過去 5 分間に収集されたすべての値の平均
- gwMGCP\_FXO\_ActivePorts : 過去 5 分間に収集されたすべての値の平均
- gwMGCP\_PRI\_ActiveChannels : 過去 5 分間に収集されたすべての値の平均
- gwMGCP\_T1\_CAS\_ActiveChannels : 過去 5 分間に収集されたすべての値の平均

AMC サービスは、Windows パフォーマンス ツールと互換性のある CSV 形式でコールデータを記録します。ログのヘッダーは、タイムゾーン情報と、サーバの以前にリストされたカウンタを含む列のセットで構成されます。該当する場合、これら一連のカラムが、クラスタ内のすべてのサーバに対して繰り返されます。

コールログのファイル名には、CallLog\_MM\_DD\_YYYY\_hh\_mm.csv という形式が適用されます。各ログファイルの最初の行はヘッダーです。

## セッショントレースの実行

Cisco Unified Communications Manager は、通過する着信および発信のコールまたはセッションを構成する SIP メッセージのすべてのアクティビティをキャプチャしてログに記録します。Unified Communications Manager は、メッセージをトランザクションごとに新しいコールログファイルに格納します。このファイルは、後処理作業のために RTMT でダウンロードできます。

RTMT を使用すると、次の基準に基づいてコールを検索したりトレースしたりすることができます。

- 発信者番号/URI
- 着信者番号/URI
- 開始時刻
- 時間 (Duration)

RTMT では、開始時刻と通話時間を含むコールログファイルがダウンロードされます。一致するコールが検索され、一致するコールレコードがリストに示され、SIP メッセージのコールフロー図が表示されます。

ローカルシステムにもコールログを保存できます。保存されているコールログに基づいて、RTMT は一致するコールを検索し、一致するレコードを表示し、SIP メッセージのコールフロー図を提供できます。

### はじめる前に

次の作業を実行します。

- コールトレースを有効または無効にするには、エンタープライズパラメータ [コールトレースログの有効化 (Enable Call Trace Log)] を使用します。エンタープライズパラメータの設定の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。
- コールトレースログファイルの最大数のデフォルト値を 2000 に設定し、コールトレースログファイルの最大サイズのデフォルト値を 2 MB に設定します。

## リアルタイムデータのモニタリング

RTMT を使用してリアルタイムデータをモニタするには、次の手順に従ってください。



- (注) コールの検索条件として使用できるのは、発信者番号/URI、着信者番号/URI、開始時刻、および通話時間です。検索は、ローカルノードだけでなく Unified Communications Manager クラスタ全体に適用されます。トレースファイルを収集できないノードがある場合は、下のパネルにエラーメッセージが表示され、メッセージプロンプトがポップアップされます。



- (注) 発信者番号/URI と着信者番号/URI では、任意の数の文字に一致するワイルド文字「\*」を使用できます。たとえば、123\* を検索すると、123、1234、123456 などの数値が検索されます。  
“\*”を含む数値を検索するには、“\\*”を使用します。たとえば、12\*45 という Called Number を検索するには、検索ボックスに 12\\*45 と入力します。

## 手順

- ステップ 1** セッショントレースに関する情報を表示するには、RTMT メニューから、[音声/ビデオ (Voice/Video)] > [コール処理 (Call Process)] > [セッショントレース ログ表示 (Session Trace Log View)] > [リアルタイム データ (Real Time Data)] の順に選択します。  
[リアルタイム データ (Real Time Data)] 画面が表示されます。
- ステップ 2** 検索条件を入力し、[実行 (Run)] をクリックします。  
エラーを無視して入力に基づくテーブルを生成する場合は、[Yes] をクリックします。
- 一致するコールが見つかった場合は、[一致するコール (Matching Call)] ペインに、[開始時刻 (Start Time)]、[発信 DN (Calling DN)]、[元の着信 DN (Original Called DN)]、[最終着信 DN (Final Called DN)]、[発信側デバイス名 (Calling Device Name)]、[着信側デバイス名 (Called Device Name)]、および [終了原因コード (Termination Cause Code)] が表示されます。
- (注) 着信側のトレース機能により、[発信側デバイス名 (Calling Device Name)] フィールドと [着信側デバイス名 (Called Device Name)] フィールドが追加されます。
- 発信側デバイス名と着信側デバイス名は、到達不能な宛先に対して発信されたコールなど、失敗したコールには使用できません。
  - [終了原因コード (Termination Cause Code)] を使用して失敗したコールを特定できます。また、コールが失敗した理由も示されます。[Termination Cause Code] はカッコ内に表示され、その後に説明が続きます。
  - コールが実行中の場合、またはコールの後にコールトレースログ機能がオフにされた場合、[Termination Cause Code] 列は空白になります。
- コールレコードが [一致するコール (Matching Calls)] ペインに表示されると、コールをトレースできます。
- (注) 原因コードの説明が表示されない場合、または終了原因コードの詳細を確認する必要がある場合は、『Cisco Unified Call Details Records Administration Guide』の「CDR cause codes」を参照してください。

## ローカル ディスクからセッショントレース データのモニタリング

ローカル ディスクに保存されるログからセッショントレース データをモニタするには、次の手順に従ってください。

## 手順

- ステップ 1** RTMT メニューから、[音声/ビデオ (Voice/Video)] > [コール処理 (Call Process)] > [セッショントレース ログ表示 (Session Trace Log View)] > [ローカル ディスクから開く (Open from Local Disk)] の順に選択します。

[ローカルディスクから開く (Open from Local Disk) ] 画面が表示されます。

- ステップ 2** [ファイルの場所 (File Location) ] フィールドに、ローカルディスク上のコールログファイルが保存されるディレクトリを指定します。[参照 (Browse) ] をクリックしてディレクトリパスを指定することもできます。
- ステップ 3** 特定の期間のコールレコードを表示するには、[時間による検索を有効にする (Enable Time Based Search) ] チェックボックスをオンにします。このチェックボックスをオンにすると、[期間 (Duration) ] フィールドで期間を指定できます。このチェックボックスをオンにしない場合、期間を指定できなくなります。このような場合、保存されたログファイル内にある指定された開始時刻からのすべてのコールが表示されます。
- ステップ 4** 検索条件を入力し、[実行 (Run) ] をクリックします。
- (注) 発信者番号/URIと着信者番号/URIでは、任意の数の文字に一致するワイルド文字「\*」を使用できます。たとえば、123\*を検索すると、123、1234、123456などの数値が検索されます。
- 「\*」を含む数値を検索するには、「\\*」を使用します。たとえば、12\*45 という Called Number を検索するには、検索ボックスに 12\\*45 と入力します。
- 一致するコールが見つかった場合は、[一致するコール (Matching Call) ] ペインに、[開始時刻 (Start Time) ]、[発信 DN (Calling DN) ]、[元の着信 DN (Original Called DN) ]、[最終着信 DN (Final Called DN) ]、[発信側デバイス名 (Calling Device Name) ]、[着信側デバイス名 (Called Device Name) ]、および [終了原因コード (Termination Cause Code) ] が表示されます。
- (注) 着信側のトレース機能により、[発信側デバイス名 (Calling Device Name) ] フィールドと [着信側デバイス名 (Called Device Name) ] フィールドが追加されます。
- a) 発信側デバイス名と着信側デバイス名は、到達不能な宛先に対して発信されたコールなど、失敗したコールには使用できません。
- b) [終了原因コード (Termination Cause Code) ] を使用して失敗したコールを特定できます。また、コールが失敗した理由も示されます。終了原因コードはカッコ内に表示され、その後に説明が続きます。
- c) コールが実行中の場合、またはコールの後にコールトレースログ機能がオフにされた場合、[Termination Cause Code] 列は空白になります。
- (注) 原因コードの説明が表示されない場合、または終了原因コードの詳細を確認する必要がある場合は、『Cisco Unified Call Details Records Administration Guide』の「CDR cause codes」を参照してください。

## コールのトレース

指定した検索条件によって表示されるコールレコードをトレースするには、次の手順に従います。



(注) この手順は、“リアルタイムデータのモニタリング”と“ローカルディスクからセッショントレースデータのモニタリング”とともに使用します。

## 手順

- ステップ 1** トレースするコール（行）を選択します。  
デフォルトでは、[SIP メッセージを含める (Include SIP Message)] チェックボックスはオンで、関連する SIP プロトコル メッセージまたはコール トランザクションが表示されます。
- ステップ 2** SIP メッセージコールフロー図を生成するには、[Trace Call] をクリックします。セッション情報の生成を停止する場合は、進捗ウィンドウで [Cancel] をクリックします。  
[コール図の分析 (Analyze Call Diagram)] ウィンドウに、コールフロー図の対応する SIP メッセージが表示されます。
- ステップ 3** 表示するタブをクリックします。次のタブを使用できます。
- コールフロー図 (Call Flow Diagram) : コールフロー図の対応する SIP メッセージが表示されます。
  - ログファイル (Log File) : ログファイル全体が表示されます。
  - SIP メッセージ (SIP Message) : [SIP メッセージを含める (Include SIP Message)] チェックボックスがオンになっている場合にだけ表示されます。SDI ログファイルに記録された実際の SIP メッセージが表示されます。
- ステップ 4** コールフロー図の SIP メッセージにマウスをポイントします。表示される詳細を次の表に示します。

フィールド	説明
Sender	起点のコールの IP アドレスを表示します。
GUID	SIP コール ID を表示します。
Message Label	ポイントした対応する SIP メッセージのメッセージタイプ（「200 OK」、「180 呼び出し中 (180 Ringing)」など）を表示します。
レシーバ	宛先のコールの IP アドレスを表示します。
MAC_ADDRESS	デバイス名を表示します。
Message Tag	SDI トレース ファイルの実際のメッセージと一致するシーケンス番号を表示します。
MSG_TYPE	メッセージのタイプを表示します。
相関 ID (Correlation ID)	相関 ID を表示します。

フィールド	説明
Timestamp	コール操作（コールセットアップ、スプリット、参加、解放）が行われるサーバ時刻を表示します。

詳細な SIP メッセージ (Detailed SIP Message) : [SIP メッセージを含める (Include SIP Message)] チェックボックスがオンになっている場合にだけ表示されます。SDL ログファイルに記録された実際の SIP メッセージが表示されます。

ログファイルのメッセージ (Message in Log File) : メッセージを含むログファイルを表示します。

SDL ログファイルに記録された SIP メッセージを表示するには、次の操作を実行します。

- Cisco Unified Serviceability ([トレース (Trace)] > [設定 (Configuration)] の [トレース設定 (Trace Configuration)] ウィンドウで [SIP 呼処理のトレースの有効化 (Enable SIP Call Processing Trace)] チェックボックスをオンにします。詳細については、『Cisco Unified Serviceability Administration Guide』を参照してください。
- トレースレベルを、[状態遷移 (State Transition)]、[重大 (Significant)]、[任意 (Arbitrary)] または [詳細 (Detailed)] のいずれかに設定します。

(注) ローカルディスクに保存されたログからセッショントレースデータをモニタする場合は、SDL/SDI ログがコールログの親ディレクトリに存在する場合にだけ、詳細な SIP メッセージが使用できます。

**ステップ 5** [保存 (Save)] をクリックします。

リアルタイムデータをモニタする場合、SIP メッセージを含む SDL ファイルとともに、コールフロー図が指定したフォルダに index.html として保存されます。ファイルはテクニカルアシスタンスセンター (TAC) に電子メールで送信できます。リアルタイムデータのモニタリングの詳細については、“リアルタイムデータのモニタリング”を参照してください。保存したコールフロー図の SIP メッセージは、ハイパーリンクとして表示されます。SIP メッセージをクリックすると、次の詳細情報とともに詳細な SIP メッセージが新しいウィンドウに表示されます。

フィールド	説明
Sender	起点のコールの IP アドレスを表示します。
GUID	SIP コール ID を表示します。
Message Label	ポイントした対応する SIP メッセージのメッセージタイプ（「200 OK」、「180 呼び出し中 (180 Ringing)」など）を表示します。
レシーバ	宛先のコールの IP アドレスを表示します。
MAC_ADDRESS	デバイス名を表示します。



フィールド	説明
Message Tag	SDI トレース ファイルの実際のメッセージと一致するシーケンス番号を表示します。
MSG_TYPE	メッセージのタイプを表示します。
相関 ID (Correlation ID)	相関 ID を表示します。
Timestamp	コール操作 (コールセットアップ、スプリット、参加、解放) が行われるサーバ時刻を表示します。

[ローカルディスクから開く (Open from Local Disk)] オプションを使って Cisco Unified Communications Manager 8.5(1) または 8.6(1) のログを開き、ラダー図を保存した場合、SIP メッセージ、SIP メッセージを含んでいる SDI ログ ファイル、およびコールを開始する 5 分前からコールを開始してから 5 分経つまでの期間の SDL ログ ファイルが保存されます。Cisco Unified Communications Manager 9.0(1) 以降からログを保存すると、コールの詳細を含む SDL ログ ファイルは index.html と SIP メッセージとともに保存されます。ローカルディスクに保存したログからのセッショントレースデータのモニタリングの詳細については、“ローカルディスクからセッショントレースデータのモニタリング”を参照してください。

(注) ファイルを zip 形式にしている場合は、zip ファイルをローカルフォルダに解凍し、それらのファイルを開いてイメージを表示します。

次の操作を実行できます。

- オンライン ヘルプを表示するには、[Help] をクリックします。
- [Analyze Call Diagram] 画面を終了するには、[Close] をクリックします。
- 前のページに戻るには、[Previous Messages] をクリックします。
- 次のページに進むには、[Next Messages] をクリックします。

(注) [前のメッセージ (Previous Messages)] または [次のメッセージ (Next Messages)] は、メッセージのサイズがしきい値を超えた場合にのみ有効になります。

Session Manager では、新しいログファイルにコールデータが記録されます。これらの新しいログファイルは、/var/log/active/cm/trace/ccm/calllogs/ フォルダにあります。

コール ログ名のファイル名パターンは、calllogs\_ddd.txt.gz です。

詳細な SIP メッセージは、SDI トレースに記録されます。

コール ログには、次の種類のメッセージが含まれます。

- コール制御：コールセットアップ、スプリット、参加およびリリースでコール情報が書き込まれます。

```
Timestamp|MessageType (CC)|Operation (SETUP/SPLI/JOIN/RELEASE)|CI for one leg (aCI)|CI for other leg (bCI)|calling DN|Orig Called DN|Final Called DN
```

- デバイスレイヤ：デバイスとやりとりされるメッセージに関連するメタデータ情報が書き込まれます。

```
Timestamp|MessageType (SIPL/SIPT)|My leg CI|Protocol(tcp/ucp)|Direction (IN/OUT)|local
ip|local port|device name|device ip|device port|Correlation id|Message Tag|SIP Call
ID|SIP method
```

次の制限は、コールフロー図が生成された場合に適用されます。

- 検索では、不完全なコールは表示されません。

例：

ユーザがハンドセットを取り上げ、完全な DN にダイヤルせずにコールを終了した場合、そのコールは検索結果にリストされません。

- 次のシナリオでは、コールフロー図に一部の SIP メッセージが表示されないことがあります。

- 電話会議の参加者が 3 人以上いる場合。
- コールレグを使用して、機能を単独で呼び出した場合。

例：

電話機 B と電話機 C は同じピックアップグループ内にあります。

- 1 ユーザ A が電話機 B に電話します。
- 2 ユーザ C が電話機 C のハンドセットを取り上げます。
- 3 ユーザ C は [ピック (PickUp) ] ソフトキーを押してコールをピックアップします。

手順 2 で交換された SIP メッセージは、コールフロー図に表示されません。

このような場合、RELEASE メッセージはコールログに記録されますが、対応する SETUP メッセージは記録されません。

## サービスのモニタリング

サービスモニタリングカテゴリは、サーバまたはクラスタ内の異なるサーバ上の Cisco TFTP 要求、データベースアクティビティおよびハートビートのアクティビティをモニタします（該当する場合）。

Cisco TFTP サービスは、File Transfer Protocol (FTP) の簡易バージョンである Trivial File Transfer Protocol と整合性のあるファイルを構築して提供します。Cisco TFTP は、コンフィギュレーションファイルを作成し、埋め込みコンポーネント実行ファイル、リンガーファイル、デバイスコンフィギュレーションファイルを提供します。Cisco TFTP 要求の合計、見つからない要求、および中止された要求を表示できます。

Unified RTMT は、Cisco Unified Communications Manager と、サーバまたはクラスタ内の異なるサーバ（該当する場合）用の Cisco TFTP サービスのハートビートをモニタします。ハートビートはモニタ対象の期間のインジケータとして機能します。ハートビートが失われると、RTMT ウィンドウの右下隅に点滅するアイコンが表示されます。ハートビートの損失がいつ検出されたのかを確認するには、点滅するアイコンをクリックします。システムを設定した場合は、電子メールでハートビートの損失を通知できます。

データベース サマリーは、データベースにキューイングされる変更通知要求、メモリにキューイングされる変更通知要求、アクティブなクライアント接続の合計数、デバイスリセットでキューイングされるデバイスの数、作成されたレプリケート、複製ステータスなど、サーバまたはクラスタ内の各サーバに関する接続情報を提供します。

CTI と Cisco TFTP 使用状況の統計情報に関する日次レポートについては、『Cisco Unified Serviceability Administration Guide』を参照してください。

次の表に、RTMT がモニタするサービス オブジェクト、アラート、しきい値とそのデフォルト値に関する情報を提供します。

表 6: サービス カテゴリ

監視対象オブジェクト（表示）	アラート/しきい値/デフォルト
各 CTI Manager のオープン デバイス、回線、CTI 接続、およびアクティブな Cisco Unified Communications Manager リンクの数。	該当なし
各 Cisco TFTP サーバの TotalTftpRequests および TotalTftpRequestsAborted。	該当なし
各ディレクトリ サーバの接続と複製のステータス。	<ul style="list-style-type: none"> <li>• 接続に失敗しました。</li> <li>• 複製に失敗しました。</li> </ul>
Cisco CallManager、Cisco TFTP サービスのハートビート率。	<ul style="list-style-type: none"> <li>• Cisco Unified Communications Manager のハートビート率は &lt;0.x を指定します。デフォルトは 0.5 です。</li> <li>• Cisco TFTP のハートビート率は &lt;0.x を指定します。デフォルトは 0.5 です。</li> </ul>

## サービス ログ

RTMT が LogService API を呼び出すたびにサービスデータはメモリに蓄積されます。5 分ごとに、RTMT はデータを単一のレコードとしてファイルに記録し、メモリを消去します。

次に示すカウンタのデータが、それぞれの計算に基づいて 5 分ごとに記録されます。

- ctiOpenDevices : 最後の 5 分間に収集されたすべての値の平均
- ctiLines : 最後の 5 分間に収集されたすべての値の平均
- ctiConnections : 最後の 5 分間に収集されたすべての値の平均
- ctiActiveCMLinks : 最後の 5 分間に収集されたすべての値の平均
- tftpRequests : 累積 (最後に収集された値と最後の 5 分間の最初に収集された値の差)
- tftpAbortedRequests : 累積 (最後に収集された値と最後の 5 分間の最初に収集された値の差)

AMC サービスは、サービス データを CSV 形式で記録します。ログのヘッダーは、タイムゾーン情報と、サーバに関して以前にリストされた前のカウンタを含むカラムのセットで構成されます。該当する場合、これら一連のカラムが、クラスタ内のすべてのサーバに対して繰り返されます。

サービス ログのファイル名には、ServiceLog\_MM\_DD\_YYYY\_hh\_mm.csv という形式が適用されます。

各ログの最初の行はヘッダーです。

## デバイス ログ

RTMT から LogDevice API がコールされるたびに、デバイス データがメモリに蓄積されます。5 分ごとに、RTMT はデータを単一のレコードとしてファイルに記録し、メモリを消去します。

次に示すカウンタのデータが、それぞれの計算に基づいて 5 分ごとに記録されます。

- gatewayDevicesFXS : 過去 5 分間に収集されたすべての値の平均
- gatewayDevicesFXO : 過去 5 分間に収集されたすべての値の平均
- gatewayDevicesPRI : 過去 5 分間に収集されたすべての値の平均
- gatewayDevicesT1 : 過去 5 分間に収集されたすべての値の平均
- gatewayDevicesH323 : 過去 5 分間に収集されたすべての値の平均

AMC サービスは、デバイス データを CSV 形式で記録します。ログのヘッダーは、時間帯情報とサーバの前回リストしたカウンタを含む列のセットで構成されます。該当する場合、これら一連のカラムが、クラスタ内のすべてのサーバに対して繰り返されます。

デバイス ログのファイル名には、DeviceLog\_MM\_DD\_YYYY\_hh\_mm.csv という形式が適用されます。

各ログ ファイルの最初の行はヘッダーです。

## デバイスのモニタリング

### デバイスのモニタリング

デバイスのモニタリング カテゴリは、デバイスの概要、デバイス検索機能、および電話機の概要を提供します。

登録されたデバイスの日次レポートの詳細については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

次の表に、Unified RTMT がモニタするオブジェクト、アラート、しきい値、デフォルト、およびこれらのデバイスに対して RTMT が生成するレポートの種類に関する情報を示します。

表 7: デバイスのカテゴリ

監視対象オブジェクト (表示)	アラート/しきい値/デフォルト
サーバごと、またはクラスタ内のすべてのサーバ (該当する場合) に登録された電話機の数。	登録される電話機の合計数は、連続したポーリング中は X% 下がります。デフォルトは 10% です。
サーバごと、またはクラスタ内のすべてのサーバ (該当する場合) に登録されたゲートウェイの数。	<p>Cisco Unified Communications Manager の場合 :</p> <ul style="list-style-type: none"> <li>• (警告) 登録されるゲートウェイのクラスタ全体での合計数は、連続したポーリング中は減少します。</li> <li>• (情報) 登録されるゲートウェイのクラスタ全体での合計数は、連続したポーリング中は増加します。</li> </ul>
サーバごと、またはクラスタ内のすべてのサーバ (該当する場合) に登録されたメディア デバイスの数。	<p>Unified Communications Manager の場合 :</p> <ul style="list-style-type: none"> <li>• (警告) 登録されるメディアデバイスのクラスタ全体での合計数は、連続したポーリング中は減少します。</li> <li>• (情報) 登録されるメディアデバイスのクラスタ全体での合計数は、連続したポーリング中は減少します。</li> <li>• メディア リストが使い果たされました。</li> </ul>

[デバイス検索 (Device search) ]メニューを構成する検索可能な項目は、電話、ゲートウェイデバイス、H.323 デバイス、CTI デバイス、ボイス メッセージ デバイス、メディア リソース、ハンドリスト、および SIP トランクです。

Unified Communications Manager システム内のすべてのデバイスを検索でき、登録済みデバイス、未登録デバイス、拒否されたデバイス、すべての状態のデバイス、およびデータベースで設定されただけのデバイスなどのデバイスの状態を選択できます。また、任意のモデルまたは特定のデバイスモデルで検索したり、複数の異なる属性を含む条件を設定できます。電話検索では、電話プロトコルに基づいて検索することもできます。

Unified RTMT では、一致するデバイスを見つけるために RIS の問い合わせを行います。結果は、一致した各デバイスを行に、指定された各属性を列に含む表で表示されます。オープンまたはクローズされたデバイスのタイムスタンプ、およびデバイスメディアを制御するアプリケーションも表示されます。

Unified Communications Manager クラスタがあり、[任意のステータス (Any Status)] オプションを選択してデバイスを検索する場合、RTMT では一致したデバイスタイプのスナップショットを表示しませんが、一定期間のすべての指定された Unified Communications Manager サーバの RIS データベースからそのデバイスタイプのデータを表示します。その結果、Unified RTMT 内で複数のステータス（登録済み、未登録など）であるデバイスについて複数のエントリが表示される場合があります。

1 つのデバイスに複数のエントリが表示される場合は、そのデバイスの現在のステータスは最新のタイムスタンプを持つエントリに反映されています。System Configuration Guide for Cisco Unified Communications Manager にある Cisco RIS Data Collector サービスに対する RIS Unused Cisco CallManager Device Store Period サービスパラメータを設定すると、登録解除されたかまたは拒否されたデバイスの情報を RIS データベースが維持する期間を設定できます。サービスパラメータの設定の詳細については、『System Configuration Guide for Cisco Unified Communications Manager』を参照してください。



#### ヒント

一致する項目を Unified RTMT で検索するには、[サービスのアクティブ化 (Service Activation)] ウィンドウで Cisco RIS Data Collector サービスをアクティブにする必要があります。

結果は、一致した各デバイスを行に、指定された各属性を列に含む表で表示されます。オープンまたはクローズされたデバイスのタイムスタンプ、およびデバイスメディアを制御するアプリケーションも表示されます。

電話機の概要では、登録済みの電話機の数、SIP を実行中の電話機、SCCP を実行中の電話機、部分的に登録された電話機、および登録の試行に失敗した回数に関する情報を提供します。

## モニタする特定デバイスの検索

次のデバイスタイプのデータをモニタするには、次の手順に従ってください。

- 電話機
- ゲートウェイ デバイス
- H.323 デバイス
- CTI デバイス
- ボイスメール デバイス

- メディア リソース
- ハント リスト
- SIP トランク

## 手順

- ステップ 1** 次のいずれかの作業を実行します。
- a) クイック起動チャンネルで、次の手順を実行します。
- 1 [音声/ビデオ (Voice/Video) ] ボタンをクリックします。
  - 2 ツリー階層で [デバイス (Device) ] をダブルクリックします。
  - 3 [デバイス検索 (Device Search) ] アイコンをクリックします。
- b) [音声/ビデオ (Voice/Video) ] > [デバイス (Device) ] > [デバイス検索 (Device Search) ] > [デバイス検索を開く (Open Device Search) ] の順に選択し、デバイス タイプ (電話機、ゲートウェイ、ハントリストなど) を選択します。検索条件を入力するデバイス検索ウィンドウが表示されます。
- [デバイス検索 (Device Search) ] ウィンドウに、クラスタ名 (該当する場合) および、モニタできるすべてのデバイス タイプを一覧表示するツリー階層が表示されます。
- ヒント [デバイス検索 (Device Search) ] または [CTI 検索 (CTI Search) ] ペインが表示されたら、デバイス タイプを右クリックし、[CCMAdmin] を選択して Cisco Unified Communications Manager Administration に進むことができます。
- ステップ 2** すべてのデバイスを検索するか、または選択できるデバイス モデルの完全なリストを表示するには、クラスタ名を右クリックし、[モニタ (Monitor) ] を選択します。
- ステップ 3** 特定のデバイス タイプをモニタするには、ツリー階層でデバイス タイプを右クリックするか、ダブルクリックします。
- (注) デバイス タイプを右クリックする場合、デバイス 選択ウィンドウが表示されるように、[モニタ (Monitor) ] を選択する必要があります。
- ステップ 4** [ステータスでデバイスを選択 (Select device with status) ] ウィンドウで、適用するオプション ボタンをクリックします。
- ステップ 5** クリックしたオプション ボタンの横にあるドロップダウン リスト ボックスで、[すべての CallManager (Any CallManager) ] を選択するか、デバイス情報を表示する特定の Cisco Unified Communications Manager サーバを選択します。
- ヒント 残りの手順では、[戻る (< Back) ]、[次へ (> Next) ]、[終了 (Finish) ]、または [キャンセル (Cancel) ] ボタンを選択できます。
- ステップ 6** [次へ (> Next) ] ボタンをクリックします。
- ステップ 7** [ダウンロード ステータスでデバイスを選択 (Select Device with Download Status) ] ペインで、適用するオプション ボタンをクリックし、[次へ (Next) ] をクリックします。
- ステップ 8** [デバイス モデルで検索 (Search by device model) ] ペインで、適用するオプション ボタンをクリックします。

ヒント [デバイス モデル (Device Model)] を選択した場合、デバイス情報を表示するデバイスタイプを選択します。

ステップ 9 [次へ (Next)] をクリックします。

ステップ 10 [名前検索 (Search with name)] ペインで、適用するオプション ボタンをクリックし、必要に応じて対応するフィールドに適切な情報を入力します。

(注) IPv6 アドレスを入力すると、IP サブネットは適用されません。

ステップ 11 [次へ (Next)] をクリックします。

ステップ 12 [次の属性をモニタ (Monitor following attributes)] ペインで、検索する属性を 1 つまたはすべてにします。

ステップ 13 [終了 (Finish)] をクリックします。

(注) デバイスの中には、すべての検索条件に対して情報を提供しないものがあります。たとえば、アクティブ ロード、非アクティブ ロード、ダウンロード ステータス、またはダウンロード理由に対して電話機をモニタするように選択した場合、ダウンロードステータスの結果は、この情報を提供できない電話機モデルに対して Unknown と表示します。

## 電話情報の表示

RTMT デバイス モニタリング ペインに表示する電話に関する情報を表示できます。この項では、電話情報の表示方法について説明します。

### 手順

ステップ 1 RTMT デバイス モニタリング ペインで、電話を検索して表示します。

ステップ 2 次のいずれかの作業を実行します。

a) 情報を表示する電話を右クリックし、[開く (Open)] を選択します。

b) 電話をクリックし、[デバイス (Device)] > [開く (Open)] の順に選択します。  
[デバイス情報 (Device Information)] ウィンドウが表示されます。

ステップ 3 [ステータスでデバイスを選択 (Select device with status)] ペインで、適用するオプション ボタンをクリックします。

ステップ 4 クリックしたオプション ボタンの横にあるドロップダウン リスト ボックスで、[すべての CallManager (Any CallManager)] を選択するか、デバイス情報を表示する特定の Cisco Unified Communications Manager サーバを選択します。

ステップ 5 [デバイス モデルごとに検索 (Search By Device Model)] ペインで、表示する電話プロトコルを選択します。

ステップ 6 [すべてのモデルまたはデバイスモデル (Any Model or Device Model)] オプション ボタンをクリックします。

[デバイス モデル (Device Model)] オプション ボタンをクリックした場合、表示する電話モデルを選択します。



- ステップ 7** [次へ (Next) ] をクリックします。
- ステップ 8** [名前を検索 (Search With Name) ] ペインで適用するオプション ボタンをクリックし、対応するフィールドに適切な情報を入力します。
- ステップ 9** [次の属性をモニタ (Monitor following attributes) ] ペインで、検索する属性を 1 つまたはすべてオンにします。
- ステップ 10** [終了 (Finish) ] をクリックします。  
[デバイス情報 (Device Information) ] ウィンドウが表示されます。デバイスの詳細については、ウィンドウの左側のペインに表示されている任意のフィールドを選択します。

## デバイス プロパティの表示

RTMT デバイス モニタリング ペインに表示されるデバイスのプロパティを表示できます。デバイスのプロパティを表示するには、次の手順に従います。

### 手順

- ステップ 1** RTMT デバイス モニタリング ペインで、デバイスを検索して表示します。
- ステップ 2** 次のいずれかの作業を実行します。
- プロパティ情報が必要なデバイスを右クリックし、[プロパティ (Properties) ] を選択します。
  - プロパティ情報が必要なデバイスをクリックし、[デバイス (Device) ] > [プロパティ (Properties) ] の順に選択します。
- ステップ 3** デバイスの説明情報を表示するには、[説明 (Description) ] タブをクリックします。
- ステップ 4** 他のデバイス情報を表示するには、[その他の情報 (Other Info) ] タブをクリックします。

## デバイスおよび perfmon カウンタのポーリング レートのセットアップ

Cisco Unified Communications Manager は、ステータス情報を収集するために、カウンタ、デバイス、およびゲートウェイポートをポーリングします。RTMT モニタリング ペインで、パフォーマンス モニタリング カウンタとデバイスのポーリング間隔を設定します。



- (注) 頻度の高いポーリング レートを設定すると、Cisco Unified Communications Manager のパフォーマンスが低下する場合があります。チャート形式でパフォーマンス カウンタをモニタするための最小ポーリング 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ための最小レートは 1 秒です。いずれもデフォルト値は 10 秒です。



(注) デバイスに対するデフォルト値は 10 分です。

ポーリング レートを更新するには、次の手順に従ってください。

#### 手順

- ステップ 1 RTMT モニタリング ペインにデバイスまたはパフォーマンス 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、[編集 (Edit)] > [ポーリング レート (Polling Rate)] の順に選択します。
- ステップ 3 [ポーリング間隔 (Polling Interval)] ペインで、使用する時間を指定します。
- ステップ 4 [OK] をクリックします。

## CTI アプリケーション、デバイス、および回線のモニタリング

CTI カテゴリは、CTI Manager アクティビティをモニタし、CTI 検索機能を提供します。CTI Manager によって、オープンしているデバイスの数、回線の数、および CTI 接続の数をモニタできます。

CTI アプリケーション、デバイス、および回線についての基準 (CTI の状況、デバイス名、アプリケーション パターン、属性など) を指定できます。



ヒント 一致する項目を RTMT で検索するには、Cisco Unified Serviceability の [サービスのアクティブ化 (Service Activation)] ウィンドウで Cisco RIS Data Collector サービスをアクティブにする必要があります。

結果は、一致した各デバイスを行に、指定された各属性を列に含む表で表示されます。オープンまたはクローズされたデバイスのタイム スタンプ、およびデバイス メディアを制御するアプリケーションも表示されます。

### CTI Manager 情報の表示

各サーバまたは (該当する場合は) クラスタ内の各サーバに対して開いているデバイス、回線、および CTI 接続のチャートを表示するには、次の手順に従います。

## 手順

- 
- ステップ 1** クイック起動チャンネルの [音声/ビデオ (Voice/Video) ] をクリックします。
  - ステップ 2** [CTI] をダブルクリックします。
  - ステップ 3** [CTI Manager] アイコンをクリックします。
- 

## モニタする CTI アプリケーションの検索

モニタする特定の CTI アプリケーションを検索するには、次の手順を実行します。

## 手順

- 
- ステップ 1** 次のいずれかの作業を実行します。
    - クイック起動チャンネルで、次の手順を実行します。
      - 1** [音声/ビデオ (Voice/Video) ] ボタンをクリックします。
      - 2** ツリー階層で [CTI] をダブルクリックします。
      - 3** [CTI 検索 (CTI Search) ] アイコンをクリックします。
    - [音声/ビデオ (Voice/Video) ] > [CTI] > [CTI 検索 (CTI Search) ] > [CTI アプリケーション (CTI Applications) ] の順に選択します。検索条件を入力できる選択ウィンドウが表示されます。
  - ステップ 2** [CTI Manager] ドロップダウン リスト ボックスから、モニタする CTI Manager を選択します。
  - ステップ 3** [アプリケーションのステータス (Applications Status) ] ドロップダウン リスト ボックスから、アプリケーションのステータスを選択します。
  - ステップ 4** [次へ (Next) ] をクリックします。
  - ステップ 5** [アプリケーション パターン (Application Pattern) ] ペインで、適用するオプション ボタンをクリックします。
  - ステップ 6** クリックしたオプション ボタンのフィールドに情報を入力します。たとえば [IP サブネット (IP Subnet) ] オプション ボタンをクリックした場合、フィールドに IP アドレスとサブネット マスクを入力します。

(注) IPv6 アドレスを入力すると、IP サブネットは適用されません。
  - ステップ 7** [次へ (Next) ] をクリックします。
  - ステップ 8** [次の属性をモニタ (Monitor following attributes) ] ウィンドウで、モニタする属性のチェックボックスを 1 つまたはすべてオンにします。
  - ステップ 9** [終了 (Finish) ] をクリックします。

アプリケーション モニタリング ペインでは、選択した情報を表示します。

---

## モニタする CTI デバイスの検索

モニタする特定の CTI デバイスを検索するには、次の手順に従います。

### 手順

---

**ステップ 1** 次のいずれかの作業を実行します。

- クイック起動チャンネルで、次の手順を実行します。
  - 1 [音声/ビデオ (Voice/Video) ] ボタンをクリックします。
  - 2 ツリー階層で [CTI] をダブルクリックします。
  - 3 [CTI 検索 (CTI Search) ] アイコンをクリックします。
- [音声/ビデオ (Voice/Video) ] > [CTI] > [CTI 検索 (CTI Search) ] > [CTI デバイス (CTI Devices) ] の順に選択します。検索条件を入力できる選択ウィンドウが表示されます。

**ヒント** オプションを右クリックする場合、[モニタ (Monitor) ] を選択します。

**ステップ 2** [CTI Manager] ドロップダウン リスト ボックスから、モニタする CTI Manager を選択します。

**ステップ 3** [デバイスのステータス (Devices Status) ] ドロップダウン リスト ボックスから、デバイスのステータスを選択します。

**ステップ 4** [デバイス (Devices) ] ペインで、適用するオプション ボタンをクリックします。

**ヒント** [デバイス名 (Device Name) ] を選択した場合、フィールドにデバイス名を入力します。

**ステップ 5** [次へ (Next) ] をクリックします。

**ステップ 6** [アプリケーションパターン (Application Pattern) ] ウィンドウで、適用するオプション ボタンをクリックします。

**ステップ 7** クリックしたオプション ボタンのフィールドに情報を入力します。たとえば [IP サブネット (IP Subnet) ] をクリックした場合、フィールドに IP アドレスとサブネット マスクを入力します。  
(注) IPv6 アドレスを入力すると、IP サブネットは適用されません。

**ステップ 8** [次へ (Next) ] をクリックします。

**ステップ 9** [次の属性をモニタ (Monitor following attributes) ] ウィンドウで、モニタする属性のチェックボックスを 1 つまたはすべてオンにします。

**ステップ 10** [終了 (Finish) ] をクリックします。  
デバイスのモニタリング ペインでは、選択した情報を表示します。

---

## モニタする CTI 回線の検索

モニタする特定の CTI 回線を検索するには、次の手順に従います。

### 手順

**ステップ 1** 次のいずれかの作業を実行します。

- クイック起動チャンネルで、次の手順を実行します。
  - 1 [音声/ビデオ (Voice/Video) ] ボタンをクリックします。
  - 2 ツリー階層で [CTI] をダブルクリックします。
  - 3 [CTI 検索 (CTI Search) ] アイコンをクリックします。
- [音声/ビデオ (Voice/Video) ] > [CTI] > [CTI 検索 (CTI Search) ] > [CTI 回線 (CTI Lines) ] の順に選択します。検索条件を入力できる選択ウィンドウが表示されます。

**ヒント** オプションを右クリックする場合、[モニタ (Monitor) ] を選択します。

**ステップ 2** [CTI Manager & ステータス (CTI Manager & Status) ] ドロップダウンリスト ボックスから、モニタする CTI Manager を選択します。

**ステップ 3** [回線ステータス (Lines Status) ] ドロップダウンリスト ボックスから、ステータスを選択します。

**ステップ 4** [デバイス (Devices) ] ペインで、適用するオプション ボタンをクリックします。

**ヒント** [デバイス名 (Device Name) ] を選択した場合、フィールドにデバイス名を入力します。

**ステップ 5** [回線 (Lines) ] ペインで、適用するオプション ボタンをクリックします。

(注) [電話番号 (Directory Number) ] を選択した場合、フィールドに電話番号を入力します。

**ステップ 6** [次へ (Next) ] をクリックします。

**ステップ 7** [アプリケーション パターン (Application Pattern) ] ペインで、適用するオプション ボタンをクリックします。

**ステップ 8** クリックしたオプション ボタンのフィールドに情報を入力します。たとえば [IP サブネット (IP Subnet) ] をクリックした場合、フィールドに IP アドレスとサブネット マスクを入力します。

(注) IPv6 アドレスを入力すると、IP サブネットは適用されません。

**ステップ 9** [次へ (Next) ] をクリックします。

**ステップ 10** [次の属性をモニタ (Monitor following attributes) ] ウィンドウで、モニタする属性のチェックボックスを 1 つまたはすべてオンにします。

**ステップ 11** [終了 (Finish) ] をクリックします。

回線のモニタリング ペインでは、選択した情報を表示します。

## アプリケーション情報の表示

Cisco Unified IP Phone、CTI ポート、CTI ルート ポイントなど、選択したデバイスのアプリケーション情報を表示できます。アプリケーション情報を表示するには、次の手順に従ってください。

### 手順

**ステップ 1** RTMT モニタリング ペインで、デバイスを検索して表示します。

**ステップ 2** 次のいずれかの作業を実行します。

- CTI など、アプリケーション情報が必要なデバイスを右クリックして、[アプリ情報 (App Info)] を選択します。
- アプリケーション情報が必要なデバイスをクリックし、[デバイス (Device)] > [アプリ情報 (App Info)] の順に選択します。

[アプリケーション情報 (Application Information)] ウィンドウに CTI Manager Server の名前、アプリケーション ID、ユーザ ID、アプリケーション IP アドレス、アプリケーション ステータス、アプリケーションのタイムスタンプ、デバイスのタイムスタンプ、デバイス名、および CTI デバイスのオープン ステータスが表示されます。

**ステップ 3** 更新された情報を表示するには、[更新 (Refresh)] をクリックします。ウィンドウを閉じるには、[OK] をクリックします。

## コール制御検出の学習パターンと SAF フォワーダ レポートへのアクセス

学習パターン レポートと Service Advertisement Framework (SAF) フォワーダ レポートは、コール制御検出機能をサポートします。コール制御ディスカバリ機能を設定すると、Cisco Unified Communications Manager は、SAF ネットワークを使用する他のリモート コール制御エンティティにそれ自身とホストされた DN パターンをアドバタイズします。同様に、これらのリモート コール制御エンティティは、ホストされた DN パターンをアドバタイズします。Cisco Unified Communications Manager は、それらを学習して、番号分析に挿入できます。コール制御検出機能の詳細については、『*Feature Configuration Guide for Cisco Unified Communications Manager*』の“Call Control Discovery”を参照してください。



(注) 学習パターンは異なるソースから送信されている場合があるので、学習パターンがレポートで繰り返されることがあります。たとえば、別の IP アドレスから送信される可能性があります。

学習パターンレポートには、学習パターン名、タイムスタンプ、およびパターンの到達可能性ステータスなどが含まれます。次の表を参照してください。

表 8: 学習パターンレポートのデータ

カラム (Column)	説明
パターン	リモートコール制御エンティティからの学習パターンの名前が表示されます。
TimeStamp	ローカル Unified Communications Manager がパターンを学習パターンとしてマークした日時を表示します。
ステータス (Status)	学習パターンが到達可能だったか、到達不能だったかを示します。
プロトコル	学習パターンへの発信コールに使用した SAF 対応トランクのプロトコルが表示されます。リモートコール制御エンティティに SAF 対応トランクの QSIG トンネリングが設定されている場合は、データは、QSIG トンネリングが使用されていたことを示します。たとえば、このカラムに H.323 とともに EMCA が表示されます。
AgentID	学習パターンをアドバタイズしたリモートコール制御エンティティの名前が表示されます。
IP アドレス (IP Address)	学習パターンをアドバタイズしたコール制御エンティティの IP アドレスが表示されます。また、コール制御エンティティがコールの待機に使用するポート番号を表示します。
ToDID	学習パターンの PSTN フェールオーバー設定を表示します。
CUCMNodeId	ローカル Unified Communications Manager ノードの ID を表示します。

SAF フォワーダレポートは、SAF フォワーダの認証ステータスおよび登録ステータスなどの情報を表示します。次の表を参照してください。

表 9: SAF フォワーダ レポートのデータ

カラム (Column)	説明
名前 (Name)	Cisco Unified Communications Manager Administration の [SAF フォワーダの設定 (SAF Forwarder Configuration) ] ウィンドウで設定した SAF フォワーダの名前が表示されます。
説明	Cisco Unified Communications Manager Administration の [SAF フォワーダの設定 (SAF Forwarder Configuration) ] ウィンドウで設定した SAF フォワーダの説明が表示されます。SAF フォワーダの説明を入力していない場合は、何も表示されません。
IP アドレス (IP Address)	Cisco Unified Communications Manager Administration の [SAF フォワーダの設定 (SAF Forwarder Configuration) ] ウィンドウで設定した SAF フォワーダの IP アドレスが表示されます。
ポート (Port)	Cisco Unified Communications Manager が SAF フォワーダに接続するために使用するポート番号を示します。デフォルトでは、Unified Communications Manager は 5050 を使用します。
タイプ (Type)	SAF フォワーダがプライマリ SAF フォワーダか、またはバックアップ SAF フォワーダに分類されているかを示します。
接続状況	Unified Communications Manager が SAF フォワーダに接続できるかどうかを示します。
認証タイプ (Authentication Type)	Cisco Unified Communications Manager がダイジェスト認証を使用して SAF フォワーダに接続したことを示します。
登録ステータス	Cisco Unified Communications Manager が SAF フォワーダに登録されているかどうかを示します。
最後に登録された時間 (Time Last Registered)	Unified Communications Manager が SAF フォワーダに最後に登録された日時が表示されます。



カラム (Column)	説明
登録されたアプリケーション数 (No of Registered Applications)	SAF フォワーダに登録されたサービスをアドバタイズおよび要求する CCD の総数を表示します。
接続の再試行数 (No of Connection Re-Attempts)	コール制御エンティティ (この場合は、Unified Communications Manager) が SAF フォワーダに接続しようとした回数を表示します。

RTMT を使用すると、さまざまな条件に基づいて検索できます。たとえば、リモート コール制御エンティティの検索を指定すると、リモート コール制御エンティティのすべての学習パターンが表示されます。

RTMT で学習パターン レポートまたは SAF フォワーダ レポート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** レポートにアクセスするには、次のいずれかのアクションを実行します。
- 学習パターンの場合：RTMT のメニューから、[音声/ビデオ (Voice/Video)] > [レポート (Report)] > [学習パターン (Learned Pattern)] の順に選択します。または、[音声/ビデオ (Voice/Video)] タブをクリックし、[学習パターン (Learned Pattern)] をクリックします。
  - SAF フォワーダの場合：RTMT のメニューから、[音声/ビデオ (Voice/Video)] > [レポート (Report)] > [SAF フォワーダ (SAF Forwarders)] の順に選択します。または、[音声/ビデオ (Voice/Video)] タブをクリックし、[SAF フォワーダ (SAF Forwarders)] をクリックします。
- ステップ 2** [ノードの選択 (Select a Node)] ドロップダウンリスト ボックスからノードを選択します。学習パターン レポートでは、Cisco CallManager サービスを実行しているが、そのノード上で CCD 要求サービスを実行していない場合は、ノードを選択したら、CCD Report Service が動作していないというメッセージが報告されます。CCD 要求サービスが選択したノードでアクティブでない場合、レポートは空として表示されます。
- ステップ 3** レポート内のデータを確認します。レポートされた項目の説明については、[学習パターン レポート (Learned Pattern Report)] テーブルのデータおよび [SAF フォワーダ レポート (SAF Forwarder Report)] テーブルのデータを参照します。

- ステップ 4** データの表示後に、特定の条件に基づいて結果をフィルタ処理する場合は、[フィルタ (Filter)] ボタンをクリックし、検索する条件を指定し、[適用 (Apply)] をクリックし、次に[OK]をクリックします。
- ステップ 5** 最新の結果を表示するには、[更新 (Refresh)] をクリックします。
- ステップ 6** データの特定の文字列を検索する場合は、[検索 (Find)] ボタンをクリックして、文字列を入力したら、[次を検索 (Find Next)] をクリックします。
- ステップ 7** 結果を保存する場合は、[保存 (Save)] をクリックし、結果をどのように保存するかに応じて [XML] または [テキスト (Text)] を選択します。データを保存する場所を参照し、保存するファイルに名前を付け、[保存 (Save)] をクリックします。

## 着信側トレースレポートへのアクセス

着信側トレースでは、トレースする電話番号または電話番号のリストを設定することができます。セッショントレースツールを使用してコールのオンデマンドトレースを要求できます。

着信側トレース機能は、ノード内の着信者番号に加えて、その発信者番号についての情報を提供します。各ノードの情報を使用して、発信元へのコールバックをトレースできます。



- (注) ユーザは、電話番号のログにアクセスする権限を持つ管理者である必要があります。MLA を使用して特定のロールに許可を付与するには、“着信側トレース”のリソースはロールに対して読み取りアクセス許可を有効にする必要があります。

Real-Time Monitoring Tool で着信側トレースレポートにアクセスするには、以下のステップに従います。

### 手順

- ステップ 1** [RTMT] メニューから、[音声/ビデオ (Voice/Video)] > [Callprocess] > [着信側トレース (Called Party Trace)] の順に選択します。または、[音声/ビデオ (Voice/Video)] タブをクリックし、次に、[着信側トレース (Called Party Trace)] をクリックします。
- ステップ 2** ドロップダウンボックスを使用して、レポートの開始時刻を選択します。  
(注) 開始時間は、現在の日付から 5 年前より古く設定できません。
- ステップ 3** このレポートには、次の情報が表示されます。
- 開始時刻
  - 発信側電話番号
  - 元の送信先電話番号
  - 着信側電話番号

- 発信側デバイス名
- 着信側デバイス名

(注) 5 MB のトレース ファイル エントリが、RTMT によってアクセスされるログ ファイルに書き込まれている場合、新しいトレース エントリが記録されると最も古いログ情報が上書きされます。RTMT は、与えられた検索に対して最大で 500 エントリしか一覧表示できません。

## Intercompany Media Service

### IME サービスのモニタリング

IME サービス カテゴリでは、次の項目がモニタされます。

- ネットワーク アクティビティ (Network Activity) : Cisco Intercompany Media Engine に関連する、Cisco Unified Communications Manager 上のアクティビティが表示されます。Network Activity オブジェクトにより、次のグラフが表示されます。
    - IME 分散キャッシュの状態 (IME Distributed Cache Health) : IME サーバ パフォーマンス オブジェクトの IMEDistributedCacheHealth カウンタに基づき、IME 分散キャッシュの状態を表示します。
    - IME 分散ノード数 (IME Distributed Node Count) : IME サーバ パフォーマンス オブジェクトの IMEDistributedCacheNodeCount カウンタの値に基づき、IME 分散キャッシュ内のノードの概数を表示します。Cisco Intercompany Media Engine の各物理サーバには複数のノードが含まれるため、グラフに表示される数は、IME 分散キャッシュに参加している Cisco Intercompany Media Engine の物理サーバの数を示しません。
    - 受信インターネット帯域幅 (Internet BW Received) : Cisco IME サービスで着信インターネットトラフィックのために使用される帯域幅量をキロビット/秒単位で表示します。IME サーバ パフォーマンス オブジェクトの InternetBandwidthRecv カウンタを表します。
    - 送信インターネット帯域幅 (Internet BW Send) : Cisco IME サービスで発信インターネットトラフィックのために使用される帯域幅量をキロビット/秒単位で表示します。IME サーバ パフォーマンス オブジェクトの InternetBandwidthSend カウンタを表します。
    - IME 分散キャッシュに保存されたデータ レコード (IME Distributed Cache Stored Data Records) : Cisco Intercompany Media Engine サーバが保存した IME 分散キャッシュ レコードの数を表示します。IME サーバ パフォーマンス オブジェクトの IMEDistributedCacheStoredData カウンタを表します。
- ネットワーク アクティビティに関する情報を表示するには、[Cisco IME サービス (Cisco IME Service)] > [ネットワーク アクティビティ (Network Activity)] を選択します。

- サーバアクティビティ (Server Activity) : Cisco Intercompany Media Engine サーバ上のアクティビティをモニタできます。Server Activity オブジェクトにより、次のグラフが表示されます。
  - 登録済みクライアントの数 (Number of Registered Clients) : Cisco IME サービスに接続しているクライアントの現在の数を表します。IME サーバパフォーマンス オブジェクトの ClientsRegistered カウンタの値を表します。
  - IME 分散キャッシュ クォータ (IME Distributed Cache Quota) : この IME サーバに接続されている Cisco Cisco Unified Communications Manager が IME 分散キャッシュに書き込むことのできる個別の DID の数を表します。この数は、IME 分散キャッシュの全体的な設定と IME サーバにインストールされている IME ライセンスによって決まります。
  - IME 分散キャッシュ クォータの使用 (IME Distributed Cache Quota Used) : この IME サーバに現在接続されている Cisco Cisco Unified Communications Manager が、登録されたパターンで Intercompany Media Service にパブリッシュされるように設定した固有の DID 番号の総数を表します。
  - 着信側コール VCR (Terminating VCRs) : コールの着信側の Cisco IME サーバに保存された IME 音声コール レコードの合計数を示します。これらのレコードは、学習ルートの検証に使用できます。
  - 保留中の検証 (Validations Pending) : Cisco IME サービスの保留中の検証の数および検証のしきい値を表示します。このグラフは、Cisco IME サーバパフォーマンス オブジェクトの ValidationsPending カウンタを表します。

サーバアクティビティに関する情報を表示するには、[Cisco IME サービス (Cisco IME Service)] > [サーバアクティビティ (Server Activity)] を選択します。

## IME システムパフォーマンスのモニタリング

IME システムパフォーマンス モニタリング カテゴリは、SDL キュー内の信号の数および特定の Signal Distribution Layer (SDL) キュータイプとして処理された信号の数をモニタする SDL キュー オブジェクトを提供します。SDL キューのタイプは、高、標準、低、最低のキューから構成されます。特定のサーバまたはクラスタ全体 (該当する場合) の SDL キューを監視できます。

SDL キューに関する情報を表示するには、[Cisco IME サービス (Cisco IME Service)] > [SDL キュー (SDL Queue)] を選択します。[SDL キュータイプ (SDL Queue Type)] ドロップダウンリスト ボックスからタイプを選択します。

## Intercompany Media Service のモニタリング



**ヒント** 事前に準備された各モニタリング ウィンドウのポーリング レートは固定されていて、デフォルト値は 30 秒です。AMC (Alert Manager and Collector) サービス パラメータの収集レートが変化すると、事前に準備されたウィンドウのポーリング レートも更新されます。また、バックエンドサーバの時刻ではなく、RTMT クライアント アプリケーションのローカル時刻が、各チャートのタイム スタンプのベースになります。



**ヒント** 事前に定義されたオブジェクトのモニタを拡大するには、対象となるチャートの領域上でマウスの左ボタンをクリックし、ドラッグします。必要な領域を選択してから、マウスの左ボタンを放します。RTMT は、モニタ対象のビューを更新します。モニタを縮小して、初期のデフォルト ビューにリセットするには、R キーを押します。

[Intercompany Media Services] モニタリング カテゴリでは、次の項目がモニタされます。

- ルーティング (Routing) : Cisco Unified Communications Manager が保持する Cisco Intercompany Media Engine ルートの合計数が表示されます。この合計数には、次のルートが含まれます。
  - Cisco Intercompany Media Engine クライアントが学習し、Cisco Unified Communications Manager のルーティング テーブル内に存在する電話番号を表す学習ルート
  - Cisco Intercompany Media Engine ルートが存在するピア企業の固有ドメイン
  - すべての Cisco Intercompany Media Engine サービス間の IME 分散ハッシュ テーブルに正常に発行されたダイヤルイン方式 (DID) の番号を表す発行済みルート
  - 管理者がブロックしたために拒否される学習ルートの番号を表す拒否ルート。

これらのチャートは、Cisco IME Client パフォーマンス オブジェクトの次のパフォーマンス カウンタを示します: RoutesLearned、DomainsUnique、RoutesPublished、および RoutesRejected。

ルーティングに関する情報を表示するには、[音声/ビデオ (Voice/Video)] > [Cisco IME クライアント (Cisco IME Client)] > [ルーティング (Routing)] の順に選択します。

- コール アクティビティ (Call Activities) : Cisco Intercompany Media Engine コールの総数をモニタできます。この合計値には、次のタイプのコールが含まれます。
  - 試行されたコール (受け入れられたコール、話し中のコール、応答のないコール、および失敗したコールが含まれます)
  - 受信されたコール
  - セットアップされたコール (つまり、Cisco Unified Communications Manager が実行し、リモート側が受け入れたコール)

- 受け入れられたコール（Cisco Unified Communications Manager が受信し、着信側が応答したコール）
- PSTN へのフォールバックが完了したコール
- PSTN に正常にフォールバックされなかったコール。

これらのチャートは、Cisco IME Client パフォーマンス オブジェクトの次のパフォーマンス カウンタを示します：CallsAttempted、CallAccepted、CallsReceived、CallsSetup、IMESetupsFailed、および FallbackCallsFailed。

コール アクティビティ 情報を表示するには、[音声/ビデオ (Voice/Video)] > [Cisco IME クライアント (Cisco IME Client)] > [コール アクティビティ (Call Activities)] の順に選択します。

## IM and Presence モニタリング

### IM and Presence および Cisco Jabber サマリーのモニタリング

Real-Time Monitoring Tool は、IM and Presence service および Cisco Jabber の全体的なパフォーマンスのモニタリングをサポートする一連の重要なパフォーマンス カウンタを提供します。RTMT の IM and Presence および Cisco Jabber のサマリーでは、1つのモニタリング ペインで重要な共通情報を監視することができます。

IM and Presence および Cisco Jabber の全体的なパフォーマンスを反映する重要なパフォーマンス カウンタに情報を表示するには、[IM and Presence] > [IM and Presence のサマリー (IM and Presence Summary)] または [IM and Presence] > [Cisco Jabber][サマリー (Summary)] の順に選択します。

IM and Presence のサマリーで、次の情報を確認します。

- PE 実行中 JSM セッション
- XCP JSM IM セッション (XCP JSM IM Sessions)
- 処理された IM の合計 (Total IMs Handled)
- 現在接続されている XMPP クライアント (Current XMPP Clients Connected)
- アドホック チャットルームの合計 (Total Ad hoc Chat Rooms)
- 永続的なチャットルームの合計 (Total Persistent Chat Rooms)

Cisco Jabber サマリーで、次の情報を確認します。

- クライアントの SOAP インターフェイス
- SIP クライアントの登録ユーザ
- SIP クライアントの登録ユーザの失敗
- SIP クライアントの IM メッセージ

## Cisco XCP カウンタ

### 接続されている XMPP クライアントの数

#### Cisco XCP CM : CmConnectedSockets

個々の IM and Presence サーバの Cisco XCP Connection Manager に接続されている XMPP クライアントの現在の数を表示します。この数値は、展開の使用パターンに基づいて上下動します。この数値が予想されるユーザベースよりも高い場合、詳細な調査が必要になることがあります。

### 接続されている CAXL クライアントの数

#### Cisco XCP Web CM : WebConnectedSockets

個々の IM and Presence サーバの Cisco XCP Web Connection Manager に接続されている CAXL Web クライアントの現在の数を表示します。この数値は、展開の使用パターンに基づいて上下動します。この数値が予想されるユーザベースよりも高い場合、詳細な調査が必要になることがあります。

### アクティブな送信 SIP サブスクリプションの数

#### Cisco XCP SIP S2S : SIPS2SSubscriptionsOut

IM and Presence サーバの Cisco XCP SIP Federation Connection Manager サービスで管理されているアクティブな送信 SIP サブスクリプションの現在の数を表示します。IM and Presence サーバが SIP ドメイン間フェデレーションまたは SIP ドメイン内フェデレーションに対して設定されている場合、このカウンタを監視します。



(注) SIPS2SSubscriptionsOut と SIPS2SSubscriptionsIn を組み合わせた合計数は、単一の IM and Presence サーバ上で 260,000 を超えることはできません。

### アクティブな着信 SIP サブスクリプションの数

#### Cisco XCP SIP S2S : SIPS2SSubscriptionsIn

IM and Presence サーバの Cisco XCP SIP Federation Connection Manager サービスによって維持されているアクティブな着信 SIP サブスクリプションの現在の数を表示します。IM and Presence サーバが SIP ドメイン間フェデレーションまたは SIP ドメイン内フェデレーションに対して設定されている場合、このカウンタを監視します。



(注) SIPS2SSubscriptionsOut と SIPS2SSubscriptionsIn を組み合わせた合計数は、単一の IM and Presence サーバ上で 260,000 を超えることはできません。

## IM セッションの数

### Cisco XCP JSM : JsmIMSessions

このカウンタは、すべてのユーザ間の IM and Presence ノードで IM セッションの総数を示します。Cisco Presence Engine (PE) は、プレゼンス構成サービスと、豊富な機能を持つ常時のネットワークプレゼンスを提供し、PE の起動時にすべてのユーザに代わって IM セッションを作成します。これは、ユーザが IM クライアントにログインしていなくても、Cisco Unified Communications Manager の Telephony Presence や Exchange Calendar の通知などのネットワークプレゼンスイベントがユーザのプレゼンスに反映されるために必要です。

IM and Presence ノードでライセンスを取得したすべてのユーザには、ログインしているクライアント用の 1 つの IM セッションに加えて、Presence Engine の高度なプレゼンス機能用の 1 つの IM セッションがあります。

### 例

IM and Presence ノードに次のような 100 人のライセンス取得済みユーザがいるとします。

- 50 人のユーザがログインしていません。
- 40 人のユーザが 1 つの IM クライアントにログインしています。
- 10 人のユーザが 2 つの IM クライアントにログインしています。

これにより、合計 160 の IM セッションが次のように構成されます。

- 高度な Presence Engine セッションは 100 x 1。
- 1 つのクライアントにログインしているユーザは 40 x 1。
- 2 つのクライアントにログインしているユーザは 10 x 2。

## IM パケットの合計

### Cisco XCP JSM : JsmTotalMessagePackets

このカウンタには、すべてのユーザにまたがる IM and Presence ノードによって処理される IM セッション総数が表示されます。

ユーザ Alice がユーザ Bob に IM パケットを送信し、両方のユーザが同じ IM and Presence ノードに割り当てられている場合、この IM パケットは 2 回カウントされます。これは、XCP ルータと Jabber Session Manager が 2 人のユーザを別々に扱うためです。たとえば、Alice のプライベート



ルールは IM パケットが Bob に配信される前にその IM パケットに適用され、Bob のプライバシールールは IM パケットが Bob のクライアントに配信される前にその IM パケットに適用されます。IM and Presence が IM パケットを処理するときは必ず、そのパケットは発信元と端末で 1 回ずつカウントされます。

Alice と Bob が別々の IM and Presence ノードに割り当てられ、Alice が Bob に IM パケットを送信する場合、その IM パケットは Alice のノードと Bob のノードで 1 回ずつカウントされます。

## 直前の 60 秒の IM

### Cisco XCP JSM : JsmMsgsInLastSlice

このカウンタは、直前の 60 秒のすべてのユーザ間で IM and Presence ノードによって処理される IM パケットの総数を示します。このカウンタは、60 秒ごとにゼロにリセットされます。JsmTotalMessagePackets と同じ IM パケットをカウントするためのルールが適用されます。このカウンタを監視すると、組織内のビジネスマン IM 時間を識別できるようになります。

## ユーザごととセッションごとのカウンタ

### Cisco XCP JSM セッションカウンタ

セッションカウンタごとにこれらは IM セッションまたはユーザ ログイン期間だけに表示されません。これらのカウンタは Presence Engine ネットワーク プレゼンスセッションごとに 1 つ存在し、クライアント ログインセッションごとに 1 つ存在します。IMSessions カウンタに関する上記の例では、160 個の異なる Cisco XCP JSM セッションカウンタがあります。ユーザがログアウトするか、Cisco Presence Engine が停止すると、関連付けられた Cisco XCP JSM セッションカウンタのインスタンスが削除されます。

Cisco XCP JSM セッションカウンタを使用すると、現在ログインしているすべてのユーザのスナップショットを取得できます。これらのカウンタは、次のコマンドを使って、CLI からアクセスできます。

#### **admin: show perf list instances "Cisco XCP JSM Session Counters"**

システムにログインしている IM and Presence ノードに割り当てられたすべてのユーザは、現在ログインしているクライアントセッションと、Presence Engine ネットワークセッションの JSM セッションカウンタのセットを持ちます。5000 人のユーザがログインしている IM and Presence ノードでは、この結果、少なくとも 10,000 セットの JSM セッションカウンタが発生します。これらの値が変化すると新しい値でこれらのカウンタを更新することは、システムにストレスを与えることとなります。これに対処するため、JSM セッションカウンタ値がシステムによってローカルにキャッシュ、RTMT に 30 分ごとに更新されます。

## 1 セッションごとに送信される IM パケット

### Cisco XCP JSM セッション カウンタ : JsmSessionMessagesIn

これは、IM クライアントまたはセッションのユーザによって送信された IM パケットの総数をカウントします。JsmSessionMessagesIn という用語は IM and Presence サーバの観点で使用されていることに注意してください。クライアントによって送信される IM パケットは、IM and Presence に着信する IM パケットです。

## 1 セッションあたりに受信した IM パケット

### Cisco XCP JSM セッション カウンタ : JsmSessionMessagesOut

これは、IM クライアントまたはセッションのユーザに送信された IM パケットの総数をカウントします。SessionMessagesOut という用語は IM and Presence サーバの観点で使用されていることに注意してください。IM パケットはクライアントに送信され、IM and Presence から送信される IM パケットです。



(注) JsmTotalMessagePackets、JsmMsgsInLastSlice、JsmSessionMessagesIn、および JsmSessionMessagesOut は、それぞれ IM and Presence に送信されるインスタントメッセージパケットを表し、システムのインスタントメッセージの正確な数字ではありません。IM ごとの IM and Presence に送信される IM パケットの量は、使用中のクライアントによって異なる場合があります。

## テキスト会議室の合計

### Cisco XCP TC : TcTotalRooms

このカウンタは、ノードでホストされるテキスト会議室の合計を表します。これは、アドホック会議室と常設チャットルームの両方を含みます。

## アドホック グループチャットルームの合計

### Cisco XCP TC : TcAdHocRooms

このカウンタは、ノードで現在ホストされているアドホックチャットルームの合計を表します。アドホックチャットルームは、すべてのユーザがグループを離れると自動的に破棄されます。そのため、このカウンタの値は定期的に増減します。

## 永続的なチャット ルームの合計

### Cisco XCP TC : TcPersistentRooms

このカウンタは、ノードでホストされる永続的なチャット ルームの合計を表します。常設チャット ルームは、そのチャット ルームのオーナーが明示的に破棄する必要があります。このカウンタを監視すると、常設チャット ルームの合計が非常に多いかどうかを識別したり、いくつかの常設チャット ルームが定期的には使用されなくなっているかどうかを識別したりできます。

## Per-chat room カウンタ

### Cisco XCP TC ルーム カウンタ

pre-chatroom カウンタは、チャット ルームのライフタイムだけに表示されます。アドホック チャット ルームでは、これらのカウンタ インスタンスは、アドホック チャット ルームが破棄されたときに削除されます。常設チャット ルームの場合、カウンタ インスタンスは常設チャット ルームが破棄されるときに破棄されますが、常設チャット ルームは長期間存続するので、破棄されることがほとんどありません。

per-chat room カウンタを使用すると、常設（およびアドホック）チャット ルームの使用率と参加者を監視し、ほとんど使用されなくなった常設チャット ルームの識別に役立ちます。

Cisco XCP TC ルーム カウンタを使用すると、ノードで現在ホストされているすべてのルームのスナップショットを取得できます。これらのカウンタには、次のコマンドを使用して CLI からアクセスできます。

```
admin:show perf list instances "Cisco XCP TC Room Counters"
```

## ルームごとに受信した IM パケット

### Cisco XCP TC ルーム カウンタ : TCRoomMsgPacketsRecv

このカウンタは、ルームごとに受信した IM パケット数を表します。

## 1つの会議室あたりの占有者数

### Cisco XCP TC ルーム カウンタ : TCRoomNumOccupants

このカウンタは、チャット ルームの現在の占有者数を提供します。チャット ルームの使用状況の傾向を把握するために、常設チャット ルームでこのカウンタを監視します。

1つの IM and Presence ノードで、最大 16,500 のテキスト会議室を持つことができます。これらの会議室のそれぞれに、1 チャット ルームあたりの独自のカウンタのセットがあります。JSM セッションカウンタと同じように、これらの値が変化すると同時に新しい値でこれらを更新することは、システムにストレスを与えることとなります。これに対処するため、1 チャット ルームあた

りのカウンタの値はシステムによってローカルにキャッシュされ、30分ごとにのみ RTMT に更新されます。

## SIP プロキシのカウンタ

### アイドル状態の SIP プロキシ ワーカー プロセスの数

#### SIP プロキシ : NumIdleSipWorkers

IM and Presence の SIP プロキシでアイドル状態またはフリーな状態の SIP ワーカー プロセスの現在の数を表示します。このカウンタは、それぞれの IM and Presence サーバの SIP プロキシに適用される負荷の良い指標となります。IM and Presence サーバが SIP ドメイン間フェデレーションまたは SIP ドメイン内フェデレーションに対して設定されている場合、このカウンタを監視します。

アイドル状態のプロセスの数はゼロになる場合がありますが、心配する必要はありません。ただし、アイドルプロセスの数が常に 5 プロセスより少なくなる場合は、IM and Presence サーバの負荷が増えており、調査が必要なことを示します。

## Cisco Unity Connection のモニタリング

### ポート モニタ

ポート モニタでは、各 Cisco Unity Connection ボイス メッセージング ポートのアクティビティをリアルタイムにモニタすることができます。この情報は、システムのポート数が多すぎるかまたは不十分かを判断するために役立ちます。

ポート モニタでは、各 Cisco Unity Connection ボイス メッセージング ポートに関する情報をリアルタイムに提供します。この情報は、ポートごとのアクティビティを判断してシステムのポート数が多すぎるかまたは不十分かを判断するために役立ちます。ポート モニタは、次の表に説明するような各ポートの情報を表示します。

表 10: ポート モニタのフィールドと説明

フィールド	説明
[ポート名 (Port Name) ]	Cisco Unity Connection Administration でのポートの表示名。
発信者 (Caller)	着信コールの場合、発信者の電話番号。
着信者 (Called)	着信コールの場合、電話がかかっている電話番号。
理由 (Reason)	該当する場合、コールがリダイレクトされた理由。

フィールド	説明
リダイレクト (Redir)	コールがリダイレクトされた内線番号。コールが複数の内線番号にリダイレクトされている場合、このフィールドには最後の内線番号の1つ前の内線番号が表示されます。
最後のリダイレクト (Last Redir)	コールがリダイレクトされた最後の内線番号。
アプリケーションのステータス (Application Status)	Cisco Unity Connection が発信者に行っているカンパセーションの名称。ポートでコールの処理が行われていない場合、ステータスは [アイドル (Idle) ] と表示されます。
画面のステータス	カンパセーションが現在実行中のアクション。ポートでコールの処理が行われていない場合、ステータスは [アイドル (Idle) ] と表示されます。
カンパセーションのステータス (Conversation Status)	カンパセーションが実行中のアクションに関する特定の詳細。ポートでコールの処理が行われていない場合、ステータスは [アイドル (Idle) ] と表示されます。
ポートの内線番号 (Port Ext)	ポートの内線番号。
接続先 (Connected To)	Cisco Unified Communications Manager SCCP 統合に対しては、ポートが登録されている Cisco Unified Communications Manager サーバの IP アドレスおよびポート。



(注) 電話システム統合によって提供される情報およびコールの状態によって、一部のフィールドは空白のままになります。

## Cisco Unity Connection ポート モニタのポーリングの開始

ポート モニタを使用するには、次の手順を実行します。



(注) 低いポーリング レートを設定すると、システム 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** Real Time Monitoring Tool では、Unity Connection にアクセスし、[ポート モニタ (Port Monitor) ] をクリックします。[ポート モニタ (Port Monitor) ] ウィンドウが表示されます。
- ステップ 2** [ノード (Node) ] ドロップダウン ボックスで、Cisco Unity Connection サーバを選択します。
- ステップ 3** [ポーリング レート (Polling Rate) ] フィールドでデフォルト値を承認するか、[ポート モニタ (Port Monitor) ] タブでデータの更新間隔の秒数を入力し、[ポーリング レートの設定 (Set Polling Rate) ] をクリックします。
- ステップ 4** [ポーリングの開始 (Start Polling) ] をクリックします。[ポート モニタ (Port Monitor) ] ウィンドウに、Cisco Unity Connection のすべてのボイス メッセージング ポートのステータスが表示されます。
-



## 第 4 章

# Cisco Unified Analysis Manager

- [Cisco Unified Analysis Manager のプリファレンス](#), 85 ページ
- [Cisco Unified Analysis Manager の制限事項](#), 89 ページ
- [Cisco Unified Analysis Manager のセットアップ](#), 90 ページ
- [Cisco Unified Analysis Manager ツール](#), 92 ページ
- [Cisco Unified Analysis Manager のトラブルシューティング](#), 113 ページ

## Cisco Unified Analysis Manager のプリファレンス

Unified Analysis Manager のドロップダウンメニューを使用して、次のプリファレンスを設定します。

### FTP サーバのセットアップ

この機能により、FTPサーバを設定し、これを使用して情報をエクスポートできます。Cisco TAC FTPサーバをこのサーバとして指定できます。この情報には、ログ、トレースファイル、およびシステム コールのトレース情報などを含めることができます。

デフォルトで、Cisco TAC FTPサーバは事前入力されています。デフォルトのFTPサーバでこの設定を変更できます。

[FTPサーバ (FTP Server)] オプションにより、設定済みのサーバを管理することができます。次の操作を実行できます。

- 新しいFTPサーバの追加
- 既存のFTPサーバの編集
- FTPサーバの削除
- FTPサーバとの接続のテスト

Cisco TAC には、ファイルのエクスポート用に設定できる次の 2 つの FTP サーバがあります。

- ftp-rtp.cisco.com
- ftp-sj.cisco.com



(注) どちらのサーバでも、ファイルは **/incoming** ディレクトリにアップロードする必要があります。

## FTP サーバオプションへのアクセス

次の手順では、FTP サーバ オプションにアクセスする方法について説明します。

### 手順

- ステップ 1** [Unified Analysis Manager] ドロップダウンメニューから、[AnalysisManager]>[設定 (Preferences)] の順に選択します。  
[設定 (Preferences)] ウィンドウが表示されます。[FTP サーバ (FTP Server)] をクリックします。
- ステップ 2** [FTP サーバ (FTP Servers)] 画面が表示され、設定済みサーバの一覧と、サーバの追加、編集、削除を行うボタンが併せて表示されます。[接続のテスト (Test Connection)] ボタンは、サーバへの接続をテストすることができます。
- ステップ 3** ボタンを使用して目的のオプションを選択します。

## FTP サーバの追加または編集

FTP サーバを追加するか、既存の設定を編集するには、次の手順に従ってください。



## 手順

- 
- ステップ 1** [Unified Analysis Manager] ドロップダウンメニューから、[AnalysisManager]>[設定 (Preferences)] の順に選択します。[設定 (Preferences)] ウィンドウが表示されます。[FTPサーバ (FTP Server)] をクリックします。
- ステップ 2** [FTPサーバ (FTP Servers)] 画面が表示され、設定済みサーバの一覧と、サーバの追加、編集、削除を行うボタンが併せて表示されます。[接続のテスト (Test Connection)] ボタンは、サーバへの接続をテストすることができます。
- ステップ 3** [追加 (Add)] ボタンをクリックしてサーバを追加するか、[編集 (Edit)] ボタンをクリックして既存の設定を編集します。[FTPサーバの追加 (Add FTP Server)] 画面が表示されます。
- ステップ 4** [名前/IP アドレス (Name/IP Address)] フィールドに、追加する FTP サーバの名前または IP アドレスを入力します。
- ステップ 5** [プロトコル (Protocol)] フィールドでは、接続しているサーバのタイプによって FTP または SFTP プロトコルを選択します。Cisco TAC サーバに接続している場合は SFTP を使用します。
- ステップ 6** [ユーザ名 (User Name)] フィールドと [パスワード (Password)] フィールドに、サーバへのアクセスを提供するユーザ名とパスワードを入力します。
- ステップ 7** [ポート (Port)] フィールドに、使用するサーバのポート番号を入力します。
- ステップ 8** [宛先ディレクトリ (Destination Directory)] フィールドに、ファイルをエクスポートするディレクトリのパスを入力します。Cisco TAC サーバを追加している場合は、/incoming ディレクトリを使用します。
- ステップ 9** [OK] ボタンをクリックすると、サーバが追加されます。[キャンセル (Cancel)] ボタンを使って、FTP サーバを追加せずに操作を終了できます。
- 

## メールサーバのセットアップ

このオプションを使用すると、トレースおよびログの収集やファイル転送など、Unified Analysis Manager の操作に関する状態を、ユーザが設定した一連の受信者に通知するように、メールサーバを設定できます。

通知を送信するには、少なくとも 1 台のメールサーバを設定する必要があります。



(注)

- 最大 2 台のメールサーバを設定できます。
  - Unified Analysis Manager 通知には、このオプションを使って設定したメールサーバしか使用できません。RTMT 通知については、別のメールサーバを設定する必要があります。
-

## メール サーバの追加または編集

次の手順では、メールサーバを追加するか、または既存の設定を編集する方法について説明します。

### 手順

- 
- ステップ 1** [Unified Analysis Manager] ドロップダウンメニューから、[AnalysisManager]>[設定 (Preferences)] の順に選択します。  
[設定 (Preferences)] ウィンドウが表示されます。[メールサーバ (Mail Server)] をクリックします。
  - ステップ 2** [メールサーバ (Mail Servers)] 画面が表示され、設定済みサーバの一覧と、サーバの追加、編集、削除を行うボタンが併せて表示されます。[接続のテスト (Test Connectivity)] ボタンは、サーバへの接続をテストすることができます。[更新 (Refresh)] ボタンを使用するとサーバをリロードできます。
  - ステップ 3** [追加 (Add)] ボタンをクリックしてサーバを追加するか、[編集 (Edit)] ボタンをクリックして既存の設定を編集します。[追加 (Add)] ボタンをクリックすると、[メールサーバの追加 (Add Mail Server)] 画面が表示されます。
  - ステップ 4** [名前/IP アドレス (Name/IP Address)] フィールドに、追加するメールサーバの名前または IP アドレスを入力します。
  - ステップ 5** [ポート番号 (Port No.)] フィールドに、使用するサーバのポート番号を入力します。
  - ステップ 6** [保存 (Save)] ボタンをクリックして設定を保存するか、[キャンセル (Cancel)] ボタンをクリックしてメールサーバを追加せずに操作を終了します。[接続のテスト (Test Connection)] ボタンは、サーバへの接続をテストすることができます。
- 

## トレース収集ディレクトリの設定

次の手順では、トレースログのディレクトリを設定するために、[設定 (Preferences)] でトレース収集オプションを使用する方法について説明します。

### 手順

- 
- ステップ 1** [Unified Analysis Manager] ドロップダウンメニューから、[AnalysisManager]>[設定 (Preferences)] の順に選択します。  
[設定 (Preferences)] ウィンドウが表示されます。[トレース収集 (Trace Collection)] をクリックします。
  - ステップ 2** [トレース収集 (Trace Collection)] 画面が表示されます。トレースログに使用するディレクトリを [ダウンロードディレクトリ (Download Directory)] ボックスに入力するか、[参照 (Browse)]

ボタンを使用してディレクトリを特定します。オプションで、[デフォルト (Default)] ボタンをクリックして、デフォルトディレクトリを選択できます。

**ステップ 3** [保存 (Save)] をクリックします。

## Cisco Unified Analysis Manager の制限事項

Unified Analysis Manager を使用する場合、次の制限事項を考慮してください。

- Call Search Report で表示可能なコール レコードの最大数は 500 です。
- Call Track Report で表示可能なコール レコードの最大数は 100 です。
- 使用するグローバルに一意的な callID がいないため、Unified Analysis Manager はコールをトレースするためにリンク単位のアプローチを使用します。コールパス中の製品の 1 台でコールのコールレコードが欠落している場合、リンクの残りの連鎖は壊れている可能性があり、トラッキングが完全ではない可能性があります。
- コールレコードは、データベースに保存される際、いずれの特定の列に基づく順序にも従いません。Call Search Report を実行する際、返されるレコード数は 500 に制限されます。取得された 500 レコードは、指定された時間範囲の（発生時間、接続時間、または切断時間に基づいた）最新のものではない可能性があります。指定した時間範囲内のすべてのコールレコードを確実に取得するには、返されるレコード数が 500 未満になるまで時間範囲を短くする必要があります。
- Cisco Unity Connection または IM and Presence ノードにはコールレコードのデータベースがないため、Unified RTMT がこれらの製品に接続するときに Unified Analysis Manager オプションが表示されません。

Unified RTMT を使用して Cisco Unified Communications Manager ノードに接続する場合、Unified Analysis Manager に Cisco Unity Connection および IM and Presence ノードを含めるようノードを追加することができます。

- コールトラッキングでは、Unified CCE および Unified IME から Cisco IOS ゲートウェイへの SIP Unified Outbound Option コールはサポートされません。
- コールトラッキングでは、Unified CCE から Unified CVP への GED-125 プロトコルを使用したコールパスの直接コールトラッキングはサポートされません。
- Cisco Unified Communications Manager からのコールをトラッキングするには、Cisco Unified Communications Manager がコールパス内にある必要があります。
- コールトラッキングでは、Cisco Unified Communications Manager からの単一分岐トラッキングだけがサポートされます。
- MGCP ゲートウェイはコール制御を実装しておらず、Q.931 がシグナリングのために Cisco Unified Communications Manager にトンネルされるため、MGCP ゲートウェイのコールに対してコール詳細レコード (CDR) は生成されません。CDR は Cisco Unified Communications Manager でのみ使用可能です。

- ACS サーバでは、Unified Analysis Manager はコール トレースにのみ使用され、その後は、トレースデータにゲートウェイの記録や情報を含める場合にのみ使用されます。ACS サーバ、または ACS サーバがサポートするハードウェア/ソフトウェアのバージョンがない場合、導入している Unified Analysis Manager 機能の大部分は引き続き動作しますが、ゲートウェイ情報はコール トレースに含まれません。

## Cisco Unified Analysis Manager のセットアップ

[Unified Analysis Manager] メニューの [管理 (Administration)] オプションを使用して、デバイスおよびグループの設定を .csv ファイルにより Unified Analysis Manager ツールにインポートできます。

### デバイスとグループの設定のインポート

Unified Analysis Manager に .csv ファイルからデバイスおよびグループ設定をインポートするには、次の手順に従ってください。

#### 手順

- 
- ステップ 1 [Unified Analysis Manager] メニューから、[管理 (Administration)] > [インポート (Import)] の順に選択します。
  - ステップ 2 インポートする .csv コンフィギュレーションファイルを選択します。
  - ステップ 3 [インポート (Import)] ボタンをクリックします。  
選択したファイルが表示されます。
- 

### スケジュールされた trace and log collection ジョブのステータス表示

この機能では、スケジュールされたトレース設定のステータスを表示し、収集ジョブを記録できます。ジョブは Unified Analysis Manager ツールを使用してスケジュールできます。デバイスがグループに追加された場合、トレース設定をスケジュールし、デバイスに収集ジョブに記録できません。

スケジューリングされたジョブは設定したマシンにリンクされ、異なるマシンでジョブを実行することはできません。ジョブがスケジュールされたマシンが何らかの理由で使用できない場合は、古いジョブのクローンを作成し、新しいパラメータを使用して新しいジョブとして保存し、新しいマシン上で実行することができます。

デバイスで実行されるジョブの状態は次のいずれかです。

- スケジュール設定済み：ジョブは Unified Analysis Manager 内でスケジュールされていますが、開始されていません

- 実行中：現在トレースを設定しているかログを収集しているジョブ
- 完了：完了したジョブ
- 保留中：ログ収集の実行が 1 回完了し、次の実行を開始するまで待機しているジョブ。
- 中止：予期しないエラーにより異常停止しているジョブ
- キャンセル：ユーザによるキャンセル操作によって停止されているジョブ。

[ジョブのステータス (Job Status)] 画面は、Unified Analysis Manager のすべてのジョブのシステムビューを提供します。複数実行されるジョブの場合、最後の実行のステータスと時間もこのページに表示されます。

次の操作をジョブで実行できます。

- 詳細の表示：ジョブの詳細ビューを入手するには、このオプションを使用します。
- キャンセル：ジョブをキャンセルするには、このオプションを使用します。キャンセル操作は、ジョブが実行中またはスケジュールされているマシンでのみ実行できます。このオプションは、完了/中止/キャンセル状態にあるジョブに使用できません。
- クローン：ジョブを選択し、新しいジョブとして保存するには、このオプションを使用します。どのような状態のジョブもクローンできます。このオプションは、保存する前にジョブの属性を変更することができます。ジョブのクローンはクローンするジョブの属性には影響しません。

## FTP サーバへのファイルのアップロードと転送

このオプションを使用すると、設定済みの FTP サーバにファイルを転送し、関係者に電子メールを送信することができます。またこのオプションを使って、別のユーザが確認できるように、一部のファイルを別のマシンに転送することもできます。

この画面では、転送するファイルとフォルダの指定と、これらのファイルに添付する注釈の指定が実行できます。

次の手順では、FTP サーバにファイルを転送する方法を説明します。

### 手順

- ステップ 1** [Unified Analysis Manager] メニューから、[管理 (Administration)] > [ファイルのアップロード (Upload Files)] の順に選択します。

[ファイルのアップロード (Upload Files) ] 画面が表示されます。

- ステップ 2** [ケース ID (Case ID) ] フィールドに、Cisco TAC がケースに割り当てた番号を入力します。
- ステップ 3** ファイルを送信する FTP サーバを選択するには、[送信先サーバ (Send to Server) ] フィールドのドロップダウンリスト ボックスを使用します。
- ステップ 4** ファイルに関する詳細情報を提供するには、[メモ (Notes) ] ボックスを使用します。
- ステップ 5** ファイルがアップロードされたことを知らせる通知を送信するメールアドレスを追加する場合は、[電子メール通知の送信 (Send Email Notifications) ] チェックボックスを使用します。複数の電子メールアドレスを追加するには、メール ID をカンマで区切って追加します。メールアドレスは <username> だけの場合もあれば、username@domain.com の形式で指定することもできます。
- ステップ 6** 画面の下部にある [アップロードするファイル (Files to upload) ] ボックスで、転送するファイルを選択します。ファイルを選択または選択解除するには、[追加 (Add) ] または [削除 (Remove) ] ボタンを使用します。選択されたファイルはデフォルトで zip 形式で圧縮された後、アップロードされます。zip 形式のファイル名は、<case id>\_uploadedfile.zip という形式になります。
- ステップ 7** [OK] ボタンをクリックすると、ファイルが転送されます。

## Cisco Unified Analysis Manager ツール

ここでは、特定のデバイスおよびデバイスグループに対して管理タスクを実行できるツールセットを提供する Unified Analysis Manager の詳細を説明します。

### Analyze Call Path ツール

Analysis Call Path ツールは複数の Cisco Unified Communications 製品間でコールをトレースすることができます。Analysis Call Path ツールを使用してコールをトレースするには、ノードが Unified Analysis Manager で定義され、ノードがグループに属している必要があります。



- (注) ユーザ定義のすべてのノードは AllNodes グループにデフォルトで割り当てられます。異なるグループにノードを割り当てる場合は、ノードグループ機能を使用します。コールレコードリポジトリの設定に関する詳細については、Analyze Call Path 機能を使用する前に、Analysis Call Path のセットアップに関するトピックを参照してください。

#### 手順

- ステップ 1** [Unified Analysis Manager] メニューから、[ツール (Tools) ] > [Analyze Call Path] の順に選択します。

[Analyze Call Path] 情報ウィンドウが表示されます。

- ステップ 2** [Continue (続行)] ボタンをクリックします。[検索条件 (Search Criteria)] ウィンドウが表示されます。
- ステップ 3** コールの発信元の番号を [発信番号 (Calling Number)] フィールドに入力します。デフォルトはアスタリスク (\*) で、ノードのすべての数値を追跡するワイルドカードです。
- ステップ 4** コールが終端した番号を [着信番号 (Called Number)] フィールドに入力します。デフォルトはアスタリスク (\*) で、ノードのすべての数値を追跡するワイルドカードです。
- ステップ 5** [終了原因 (Termination Cause)] ドロップダウン リスト ボックスを使用してコール終了の原因を選択します。放棄、ドロップ、失敗または 3 つすべてを選択できます。
- ステップ 6** トレースの開始時間を入力するには、[開始時間 (Start Time)] フィールドを使用します。
- ステップ 7** トレースする期間の長さを示すには、[期間 (Duration)] フィールドを使用します。
- ステップ 8** コールをトレースするタイムゾーンを選択するには、[タイムゾーン (Time Zone)] ドロップダウン リスト ボックスを使用します。
- ステップ 9** トレースするノードのグループを選択するには、[グループごとにノードをフィルタ (Filter Nodes by Group)] ドロップダウン リスト ボックスを使用します。
- ステップ 10** トレースするノードの種類を選択するには、[ノードタイプ (Node Type)] ドロップダウン リスト ボックスを使用します。  
グループおよびノードを選択した場合、ノードごとに情報が表示されます。表示された各ノードのチェックボックスを使用すると、ノードを選択または選択解除することができます。
- (注) 一度に選択できるノードの数の制限は 20 です。
- ステップ 11** トレースを開始するには、[実行 (Run)] ボタンをクリックします。トレース結果がウィンドウの下部に表示されます。複数のノードを選択した場合、タブはノードごとに表示されます。タブをクリックすると、そのノードの情報が表示されます。
- ステップ 12** 通話レコード情報が表示されると、[フルパスの表示 (View Full Path)] ボタンをクリックして完全なコールパスを表示できます。コールに関する情報を表示するには、[レコードの詳細の表示 (View Record Details)] ボタンをクリックできます。レポートを保存するには、[結果の保存 (Save Results)] ボタンを使用します。

## Analyze Call Path ツールのセットアップに関する考慮事項



### 注意

コンピュータが英語以外の言語に設定されていると、Analyze Call Path ツールが正しく機能しない場合があります。

Analysis Call Path ツールを使用する場合、Unified Analysis Manager が管理する製品ごとに、設定に関する考慮事項があります。

Analysis Call Path ツールには、Cisco Unity Connection と、IM and Presence サーバの情報は含まれません。

## Cisco Unified Communications Manager

次の情報は、Cisco Unified Communications Manager リリースの分析の通話パスを設定すると適用されます。

- バージョン サポート : Cisco Unified Communications Manager には Unified Analysis Manager サポート リリース 8.0(1) 以上。
- コール レコードのリポジトリ : HTTPS プロトコルおよびデフォルト ポート 8443 のコール レコードのリポジトリとして最初のノード (パブリッシャ) を使用します。
- ユーザ グループおよびアクセス権限 : ユーザは、次のリソースのコール レコードへのアクセスに必要な読み取りと更新の権限を持つロールのユーザグループに属している必要があります。
  - SOAP コール レコード API
  - SOAP コントロール センターに関する API
  - SOAP 診断ポータル データベース サービス
  - SOAP ログ収集 API
  - SOAP パフォーマンス情報に関する API
  - SOAP リアルタイム情報およびコントロール センターに関する API




---

(注) アップグレード時に追加された“SOAP 診断ポータル データベース サービス”と“SOAP コール レコード API”の新しいソースには、既存のユーザに対するセキュリティ上の理由から、デフォルトで読み取りと更新の権限を付与しないでください。作成またはロールをカスタム リソースにコピーし、必要に応じて前述のリソースに対する権限を更新する必要があります。詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

---

- NTP 設定 : ソリューションに搭載されている各製品は、NTP クロック ソースの同じセットをポイントするように設定する必要があります。NTP は SCT 機能のコールを含むすべてのノードで設定する必要があります。Cisco Unified Communications Manager に、NTP を設定するには、**utils ntp config CLI** コマンドを使用します。
- Cisco Unified Communications Manager Administration を記録するコール レコードをイネーブルにして [サービス パラメータ設定 (Service Parameter Configuration) ] ウィンドウに移動し、[Cisco CallManager サービス (Cisco CallManager Service) ] を選択します。[CDR 有効フラグ (CDR Enabled Flag) ] および [接続時間がゼロのコールを CDR に記録するフラグ (CDR Log Calls with Zero Duration Flag) ] をイネーブルにします。すぐに有効に変更通知のために [Cisco CallManager] サービスを再起動します。Cisco Unified Communications Manager リリースのクラスタ内のすべてのノードでこの手順を繰り返して行ってください。





(注) 必要に応じてフラグが `https://<HOSTNAME>:<PORT>/ccmadmin/vendorConfigHelp.do` で設定されていることを確認できます。

- CAR CDR ローダ : CDR Analysis and Reporting (CAR) ローダが [連続ロード 24/7 (Continuous Loading 24/7)] に設定されるようにします。これを確認するには、次の手順を実行します。

- Cisco Unified Serviceability に移動し、[ツール (Tools)] > [CDR Analysis and Reporting (CAR)] ページの順に選択します。CAR ページが新しいブラウザで開きます。
- [システム (System)] > [スケジューラ (Scheduler)] > [CDR ロード (CDR Load)] に移動します。
- ローダと [連続ロード 24/7 (Continuous Loading 24/7)] がイネーブルであることを確認します。これにより、Cisco Unified Communications Manager ノードから生成された CDR レコードは、Cisco Unified Communications Manager の最初のノード (パブリッシャ) に到着するとすぐに CAR データベースにロードされます。

コールレコードが Cisco Unified Communications Manager リリースにない場合、CAR ローダが失敗したり、または最新の CDR レコードがロードされる遅延が発生している可能性があります。この場合、CAR の [システム (System)] > [データベース (Database)] > [手動消去 (Manual Purge)] ページに移動し、[テーブル情報 (Table Information)] ボタンをクリックします。CAR データベースで使用できる最も古い CDR レコードと最も新しい CDR レコードを確認します。レコードが最新の日付に設定されていない場合は、[システム (System)] > [ログ画面 (Log Screens)] > [イベントログ (Event Log)] に移動して [CDR ロード (CDR Load)] を選択し、最近の実行状態と失敗した実行があるかどうかを確認します。CDR ロードにエラーがある場合は、CAR スケジューラのトレースを収集し、トラブルシューティングのためにシスコのサポートに提供します。

- raw コールレコードの詳細 : raw コールレコードに関する情報については、Cisco Unified Communications Manager の場合、『*Cisco Unified Communications Manager Call Detail Records Administration Guide*』を参照してください。

## Cisco Unified Contact Center Express

次の情報は、Analyze Call Path を Unified CCX に対して設定するときに適用されます。

- バージョンサポート : Unified Analysis Manager は Unified CCX バージョン 8.0(1) 以降をサポートします。
- コールレコードリポジトリ : Unified CCX に使用するコールレコードリポジトリは、Unified CCX ノードのいずれか (またはハイ アベイラビリティ システムの場合は両方) です。データベースは両方のノードでアクティブになっており、データが複製されます。JDBC のユーザは `uccxsct` で、パスワードは TFTP パスワードの暗号化バージョンです。パスワードは、通常は Unified CCX 管理者によって設定されます。

- **Unified CCX コールレコードリポジトリを追加するためのデフォルトユーザ**：Unified CCX コールレコードリポジトリを追加するための Informix ユーザは **uccxsct** です。上記ユーザのインストール時のデフォルトパスワードは、Unified CCX Application の [管理 (Administration)] > [ツール (Tools)] > [パスワード管理 (Password Management)] ページでリセットできます。通常、Unified CCX 管理者は必要なパスワードにリセットし、Unified Analysis Manager 管理者にそれを渡します。
- **ユーザグループおよびアクセス権限**：Unified CCX では、コールレコードにアクセスするための追加のユーザグループおよびアクセス権限は必要ありません。uccxsct ユーザのアクセス権限は、特定のテーブルへの読み取りアクセスについて、Unified CCX インストールで設定されています。外部設定は必要ありません。
- **NTP 設定**：Unified CCX に対して NTP を設定するには、[OS の管理 (OS Administration)] > [設定 (Settings)] > [NTP サーバ (NTP Server)] に移動します。
- **コールレコードのロギング**：デフォルトで、Unified CCX は常にコールレコードを生成します。したがって、コールレコードのロギングを有効にするための設定は必要ありません。

## Cisco Unified Intelligent Contact Management Enterprise および Cisco Unified Contact Center Enterprise

次の情報は、Cisco Unified Intelligent Contact Management Enterprise (Unified ICME) および Unified CCE の Analyze Call Path を設定するときに適用されます。

- **バージョンサポート**：Unified Analysis Manager は、Unified ICME および Unified CCE に対し、リリース 8.0(1) をサポートします。
- **コールレコードリポジトリ**：Unified ICME に使用するコールレコードリポジトリは、AW-HDS-DDS または HDS-DDS のいずれかです。Unified CCE に使用されるサーバは、HDS/AW データベース (ポート 1433) です。
- **ユーザグループおよびアクセス権限**：リリース 8.0(1) では、コールレコードにアクセスするために必要な推奨されるユーザグループとアクセス権は SQL Server 用の Windows 認証のみです。これは、設定マネージャから [ユーザリスト (User List)] ツールを使用して、適切なアクセス権限でユーザを作成することで実現できます。
- **NTP 設定**：Unified CCE サーバの時刻同期の設定は、Microsoft Windows タイムサービスに基づいています。Unified CCE ルータコンポーネントを設定する場合、オンになっている [ICM の時刻同期の無効化 (Disable ICM Time Synchronization)] “ ” ボックスのデフォルト設定を保持します。推奨されるデフォルト設定を使用すると、ネットワークを介してコンピュータの内部クロックを自動的に同期する Windows タイムサービスにより、Unified CCE サーバの時刻同期が提供されます。この同期の時刻源は、コンピュータが Active Directory ドメイン内にあるか、またはワークグループ内にあるかによって異なります。Windows タイムサービスの設定の詳細については、『Microsoft Windows Time Service Technical Reference』 ([http://technet.microsoft.com/en-us/library/cc773061\(ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc773061(ws.10).aspx)) を参照してください。
- **コールレコードロギングの有効化**：コールレコードロギングが有効であることを確認するには、まず、Unified CCE の Unified Analysis Manager サービスが有効であることを確認します。Web セットアップを使用するには、管理者およびデータサーバロールにより

AW-HDS-DDS サーバまたは HDS-DDS サーバをインストールする必要があります。Web セットアップを使用してこれらのロールをインストールした後は、デフォルトでコールレコードを使用できます。

- raw コールレコードの詳細 : raw コールレコードの詳細に関するヘルプを検索するには、AW-HDS-DDS サーバまたは HDS-DDS サーバのどちらかにある、Unified CCE Administration Tool グループからアクセスできる Schema Help を参照してください。また、特定のリリースに対する『United CCE Database Schema Handbook』  
([http://www.cisco.com/en/US/products/sw/custcosw/ps1844/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1844/tsd_products_support_series_home.html)) を参照することもできます。



- (注) RTMT を使用して Cisco Unified Contact Center Enterprise をモニタする場合は、ファイル `<RTMT_INSTALLATION_FOLDER_PATH>/conf/rtmt.xml` を開き、ReadTimeout の値を 360 に変更する必要があります。値を変更しない場合、RTMT のデフォルトのタイムアウト値は OPC ログの収集にかかる時間より大きいいため、RTMT で OPC ログを収集できません。

## Cisco Unified Customer Voice Portal

次の情報は、Analyze Call Path を Unified CVP に対して設定するときに適用されます。

- バージョン サポート : Unified Analysis Manager は Unified CVP Release 8.0(1) 以降をサポートします。
- コールレコードリポジトリ : Unified CVP ではコールレコードリポジトリ用に Unified CVP Reporting Server を使用します。
- ユーザグループおよびアクセス権限 : Unified CVP では、コールレコードにアクセスするために必要なユーザグループおよびアクセス権限を設定するために Unified CVP OAMP を使用します。
  - Unified CVP データベースから Unified CVP レコードへのアクセスを試行するすべてのユーザは、Unified CVP OAMP で作成される必要があります。
  - Unified CVP Reporting ユーザは、Unified CVP OAMP で Unified CVP Reporting ロールを付与される必要があります。
  - Unified CVP Reporting Server にセキュリティ強化がインストールされている場合は、ユーザパスワードが期限切れになる場合があります。これが発生した場合、SNMP モニタにアラートが表示されます。
- NTP 設定 : Unified CVP サーバの時刻同期の設定は、Microsoft Windows タイムサービスに基づいています。Windows タイムサービスの設定の詳細については、『Microsoft Windows Time Service Technical Reference』  
([http://technet.microsoft.com/en-us/library/cc773061\(ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc773061(ws.10).aspx)) を参照してください。

- コール レコード ログの有効化：コール レコード ログが有効になっていることを確認するには、次を実行します。
  - Unified CVP Reporting Server はデフォルトではインストールも設定もされていません。顧客およびパートナーは、Unified CVP で Analysis Call Path ツールを使用するには、Unified CVP Reporting Server をインストールする必要があります。
  - Unified CVP データベース スキーマは、Unified CVP\_database\_config.bat ファイルである必要があります。このファイルは、Unified CVP Reporting Server インストール完了後にユーザによって実行される必要があります。
  - Unified CVP Reporting Server をインストールした後は、Unified CVP OAMP を介して設定し、Unified CVP Call Server を Unified CVP Reporting Server に関連付ける必要があります。
  - Unified CVP Reporting Server、Unified CVP VXML Server、および Unified CVP Call Server の設定については、Unified CVP CAG および RPT ガイドラインに従ってください。
  - デフォルトで、Unified CVP のデータは 30 日間保持されます。この値は Unified CVP OAMP によりカスタマイズできます。データベースをバックアップしていないかぎり、データはデータ保持日数の最後に消去されます。バックアップされた Unified CVP データは、データベースにインポートして戻さないかぎりアクセスできません。
  - Unified CVP VXML Server フィルタを、Unified CVP OAMP で設定する必要があります。これらのフィルタの設定については、Unified CVPOAMP のガイドを参照してください。
- raw コール レコードの詳細：raw コール レコードの詳細については、『*Unified CVP Reporting Guide for version 7.0(2)*』を参照してください。

## Cisco Access Control Server および Cisco IOS Gateway

次の情報は、Cisco Access Control (ACS) Server および Cisco IOS Gateway の Analyze Call Path を設定しているときに適用されます。

- バージョンのサポート：Unified Analysis Manager は、ACS リリース 5.1 をサポートします。
- コール レコード リポジトリ：コール レコード リポジトリを割り当てるために、ACS サーバの 1“”つを「コレクタ」ノードとして設定できます。
- ユーザグループおよびアクセス権限：ユーザグループおよびアクセス権限を設定するには、ACS サーバのインストール後、ssh/telnet アクセスで、ユーザ名として `acsadmin`、パスワードとして `default` を入力します。これにより、パスワードの変更を要求されます。
- NTP の設定：ACS サーバ上で NTP サーバを設定するには、`cli: ntp server <NTP server IP/host>` を使用します。
- Web ビューの有効化：Web ビューを有効にするには、CLI コマンド `acs config-web-interface view enable` を実行します。この機能はデフォルトでは無効になっています。
- ACS ネットワーク デバイスまたは AAA クライアントとしての Cisco IOS ゲートウェイ：正しい RADIUS シークレットを持つように ACS ネットワーク デバイスを設定する必要があります。

ます。正しい RADIUS シークレットは、IOS ゲートウェイ上のシークレットと同じものです。

- `acsadmin` から、[ネットワーク デバイス グループ (Network Devices Group) ]>[ネットワーク デバイス (Network Devices) ]および AAA クライアントにアクセスして、ACS ネットワーク デバイスまたは AAA クライアントとして Cisco IOS ゲートウェイを追加します。

- IOS の設定 :

- 次の CLI を使用して NTP サーバを設定します。 `ntp server <NTP server IP/host>`
- Cisco IOS ゲートウェイを ACS サーバの Radius クライアントとして設定します。サンプル CLI は次のとおりです。

```
aaa new-model!  
!  
aaa group server radius acs  
server 172.27.25.110 auth-port 1812 acct-port 1813  
!  
aaa authentication login h323 group acs  
aaa authorization exec h323 group acs  
aaa accounting connection h323 start-stop group acs  
aaa session-id common  
gw-accounting aaa  
radius-server host 172.27.25.110 auth-port 1812 acct-port 1813  
radius-server key cisco  
radius-server vsa send accounting  
radius-server vsa send authentication
```

- Cisco IOS ゲートウェイへのローカル ログイン アクセスが可能であることを確認してください。
- コール レコード ロギングの有効化 : コール レコード ロギングが有効になっていることを確認するには、次を実行します。
  - `aaa accounting connection h323 start-stop group acs`
  - `aaa session-id common`
  - `gw-accounting aaa`
  - `radius-server host 172.27.25.110 auth-port 1812 acct-port 1813`
  - `radius-server key cisco`
  - `radius-server vsa send accounting`

## ノード

### ノード管理

設定後は、サポートされているノードが Unified Analysis Manager データベースに追加され、サポートされる Unified Analysis Manager ノード一覧に表示されます。次の 3 種類の方法のいずれかにより、Unified Analysis Manager ノードを識別できます。

- 設定ファイルからノードおよびグループ設定をインポートする。
- Unified Analysis Manager 画面で手動でノードとグループ情報を入力する。
- シード ノードから Unified Analysis Manager ノードを検出する。シード ノードは、導入時にすべてのノードに関する情報を返すことのできるノードです。検出されると、このノードはノードのインベントリに追加できます。このオプションにより、これらのノードの詳細情報を手動入力する時間を節約できます。

Cisco Unified Communications Manager では、最初のノード（パブリッシャ）はシード ノードです。Cisco Unified Customer Voice Portal（Unified CVP）サーバ、Cisco Unified CVP OAMP サーバはシード ノードです。

このオプションでは、ノードの追加、編集、削除、および検出を実行できます。すべての設定済みの Unified Analysis Manager ノード（手動入力、ファイルからインポート、または検出）がノードの一覧に表示されます。

[ノード (Nodes) ] オプションを使用して、次の機能を実行できます。

- 追加：[追加 (Add) ] ボタンをクリックすると、手動で新しいノードを入力できます。
- 編集：[編集 (Edit) ] ボタンをクリックすると、設定済みのノードを編集することができます。
- 削除：[削除 (Delete) ] ボタンをクリックすると、1つ以上のノードを削除することができます。
- 検出：シード ノードだけに適用される [検出 (Discover) ] オプションを使用できます。[検出 (Discover) ] ボタンを使用してシード ノードにクエリーを送信します。これにより、シード ノードが認識している導入環境内のすべてのノードに関する情報がシード ノードから返されます。検出後、ノードはノード インベントリに自動的に追加されます。
- 接続のテスト：[接続のテスト (Test Connectivity) ] ボタンをクリックすると、設定済みのアクセス情報を使用してノードへの接続をテストすることができます。

### ノードのサマリーの表示

[ノード (Node) ] サマリー画面は、現在 Unified Analysis Manager アプリケーションで設定されているすべてのノードを表示します。ノードのサマリー画面にアクセスするには、次の手順を使用します。

## 手順

- 
- ステップ 1** [Unified Analysis Manager] メニューから、[インベントリ (Inventory)] > [ノード (Node)] の順に選択します。
- ステップ 2** [ノード (Node)] サマリー画面が表示され、設定済みノードの一覧と、追加、編集、削除、検出を行うボタンが併せて表示されます。[接続のテスト (Test Connection)] ボタンは、ノードへの接続をテストすることができます。ノードは[名前 (Name)] と [製品タイプ (Product Type)] ごとにリストされます。
- 

## ノードの追加または編集

次の手順では、ノードを追加するか、または既存の設定を編集する方法について説明します。

## 手順

- 
- ステップ 1** [Unified Analysis Manager] メニューから、[インベントリ (Inventory)] > [ノード (Node)] の順に選択します。  
[ノード (Nodes)] ウィンドウが表示されます。
- ステップ 2** [追加 (Add)] ボタンをクリックしてノードを追加するか、またはリストからノードを選択し、[編集 (Edit)] ボタンをクリックして既存の設定を編集します。[追加 (Add)] または [ノードの編集 (Edit Node)] 画面が表示されます。
- (注) この画面のアスタリスク (\*) の付いたフィールドは必須フィールドです。

- ステップ 3** [製品タイプ (Product Type) ] ドロップダウン リスト ボックスを使用して製品を選択します。
- ステップ 4** [IP/ホスト名 (IP/Host Name) ] フィールドに、追加または編集するノードのホスト名または IP アドレスを入力します。
- ステップ 5** [トランスポートプロトコル (Transport Protocol) ] フィールドで、使用するプロトコルを選択します。このフィールドのオプションは、選択した [製品タイプ (Product Type) ] によって異なります。
- ステップ 6** [ポート番号 (Port Number) ] フィールドに、使用するノードのポート番号を入力します。
- ステップ 7** [ユーザ名 (User Name) ] フィールドと [パスワード (Password) ] フィールドに、ノードへのアクセスを提供するユーザ名とパスワードを入力します。[パスワードの確認 (Confirm Password) ] フィールドにパスワードを再入力します。
- ステップ 8** オプションで、[説明 (Description) ] フィールドに追加するノードの簡単な説明を提供できます。
- ステップ 9** [関連コールレコードリポジトリ (Associated Call Record Repositories) ] および [関連トレースファイルリポジトリ (Associated Trace File Repositories) ] フィールドでは、ドロップダウンリストを使用してノードに使用するそれぞれのサーバを選択します。
- ステップ 10** 既存のグループにノードを追加する場合は、[関連グループ (Associated Group) ] チェックボックスを使用します。
- ステップ 11** NAT またはターミナルサーバ設定がある場合は、[詳細設定 (Advanced) ] ボタンを使用して [ノードの追加 - 詳細設定 (Add Node-Advanced) ] 画面を表示します。[代替 IP/ホスト名 (Alternate IP/Hostname) ] フィールドと [代替ポート (Alternate Port) ] フィールドに、適切な情報を入力します。
- ステップ 12** [保存 (Save) ] ボタンをクリックすると、ノードが追加されます。[キャンセル (Cancel) ] ボタンを使って、ノードを追加せずに操作を終了できます。

## グループ管理

Unified Analysis Manager 内で、グループを作成し、グループにノードを追加できます。グループにノードを追加した後は、ユーザは、グループレベルで一連の機能（トレース収集やトレース設定）を実行できます。1つのノードが複数のグループに属することができます。ネストグループはサポートされません。グループのコピーはサポートされません。



- (注) ノードが Unified Analysis Manager に追加されると、デフォルトで、AllNodes グループが追加されます。Unified Analysis Manager に追加されたすべてのノードは、デフォルトで、AllNodes グループの一部になります。AllNodes グループは編集も削除もできません。



- (注) 設定できるグループの数は 20 までに制限され、グループ (AllNodes グループ以外) に含めるノードの数も 20 に制限されます。

[グループ (Group) ] オプションを使用して、次の機能を実行できます。



- 追加 (Add) : グループを作成するには、[追加 (Add)] ボタンを使用します。グループを作成した後は、そのグループにノードを追加できます。
- 編集 (Edit) : グループ情報を選択して編集するには、[編集 (Edit)] ボタンを使用します。[編集 (Edit)] 機能では、グループのノードメンバーを追加または削除することもできます。グループにノードを追加、またはグループからノードを削除することにより、グループに属するノードを変更できます。
- 削除 (Delete) : グループを削除するには、[削除 (Delete)] ボタンを使用します。この機能により、Unified Analysis Manager からグループが削除されます。ただし、この機能によって、Unified Analysis Manager からグループ内の個別のノードが削除されることはありません。ノードを個々に削除するには、[編集 (Edit)] ボタンを使用する必要があります。

### グループの追加または編集

次の手順では、グループを追加するか、または既存の設定を編集する方法について説明します。

#### 手順

- 
- ステップ 1** [Unified Analysis Manager] メニューから、[インベントリ (Inventory)] > [ノードグループ (Node Groups)] の順に選択します。
  - ステップ 2** [グループ (Groups)] ウィンドウが表示されます。[追加 (Add)] ボタンをクリックしてグループを追加するか、またはリストからグループを選択し、[編集 (Edit)] ボタンをクリックして既存の設定を編集します。[追加 (Add)] または [グループの編集 (Edit Group)] 画面が表示されます。
  - ステップ 3** グループ名を入力するには、[グループ名 (Group Name)] フィールドを使用します。
  - ステップ 4** グループの簡単な説明を入力するには、[グループの説明 (Group Description)] フィールドを使用します。
  - ステップ 5** [ノードの選択 (Select Nodes)] セクションには、設定された各ノードのリストが含まれています。グループにノードを追加するには、リストでノードを強調表示し、[追加 (Add)] ボタンをクリックします。
  - ステップ 6** グループに対するノードの選択が終了したら、[追加 (Add)] ボタンをクリックしてグループを追加するか、または、グループの内容を編集している場合は [更新 (Update)] ボタンをクリックします。[キャンセル (Cancel)] ボタンを使って、グループを追加または編集せずに操作を終了できます。
- 

### トレース ファイル リポジトリの管理

このオプションは、Unified Analysis Manager のトレース ファイル リポジトリの追加/編集/削除操作の実行を可能にします。管理対象ノードは、通常、トレースファイルおよびログファイルに対する負荷を低減するためトレース ファイル リポジトリを使用します。その後、Unified Analysis Manager は、ログとトレースを収集するためにトレース ファイル リポジトリに接続できます。

トレース ファイル リポジトリ オプションを使用して、次の機能を実行できます。

- 追加：[追加 (Add) ] ボタンをクリックすると、手動で新しいサーバを入力できます。
- 編集：[編集 (Edit) ] ボタンをクリックすると、設定済みのサーバを編集できます。
- 削除：[削除 (Delete) ] ボタンをクリックすると、1つ以上のサーバを削除することができます。
- 接続のテスト：[接続のテスト (Test Connectivity) ] ボタンをクリックすると、設定済みのアクセス情報を使用してサーバへの接続をテストすることができます。

## トレース ファイル リポジトリの追加または編集

次の手順では、トレースファイルリポジトリを追加するか、または既存の設定を編集する方法について説明します。

### 手順

- 
- ステップ 1** [Unified Analysis Manager] メニューから、[インベントリ (Inventory) ]>[トレース ファイル リポジトリ (Trace File Repositories) ] の順に選択します。
- ステップ 2** 設定されているサーバのリストを含む [トレース ファイル リポジトリ (Trace File Repositories) ] ウィンドウが表示されます。[追加 (Add) ] ボタンをクリックして新しいサーバを追加するか、またはリストでサーバを強調表示し、[編集 (Edit) ] ボタンをクリックして既存の設定を編集します。
- ステップ 3** [IP/ホスト名 (IP/Host Name) ] フィールドに、追加するサーバのホスト名または IP アドレスを入力します。
- ステップ 4** [トランスポートプロトコル (Transport Protocol) ] フィールドで、ドロップダウン リストボックスを使用して、使用するプロトコルを SFTP または FTP から選択します。
- ステップ 5** [ポート番号 (Port Number) ] フィールドに、使用するサーバのポート番号を入力します。
- ステップ 6** [ユーザ名 (User Name) ] フィールドと [パスワード (Password) ] フィールドに、サーバへのアクセスを提供するユーザ名とパスワードを入力します。[パスワードの確認 (Confirm Password) ] フィールドにパスワードを再入力します。
- ステップ 7** オプションで、[説明 (Description) ] フィールドに追加するサーバの簡単な説明を提供できます。
- ステップ 8** [関連ノード (Associated Nodes) ] フィールドで、チェックボックスを使用してサーバにアクセスできるノードを選択します。
- ステップ 9** NAT またはターミナルサーバ設定がある場合は、[詳細設定 (Advanced) ] ボタンを使用して [トレース ファイル リポジトリの追加 - 詳細設定 (Add Trace File Repository-Advanced) ] 画面を表示します。[代替 IP/ホスト名 (Alternate IP/Hostname) ] フィールドと [代替ポート (Alternate Port) ] フィールドに、適切な情報を入力します。
- ステップ 10** [追加 (Add) ] ボタンをクリックしてサーバを追加するか、[編集 (Edit) ] ボタンをクリックして設定を更新します。[キャンセル (Cancel) ] ボタンを使って、サーバを追加せずに操作を終了できます。
-

## コールレコードリポジトリの管理

このオプションを使用すると、Unified Analysis Manager のコールレコードのリポジトリで Add、Edit、および Delete 操作を実行できます。管理対象ノードは通常、データベースにコールデータを保存するためにコールレコードリポジトリを参照します。その後、Unified Analysis Manager は、コールレコードリポジトリに接続して詳細なコールデータを取得します。

[コールレコードリポジトリ (Call Record Repository) ] オプションを使用して、次の機能を実行できます。

- 追加 (Add) : 手動で新しいサーバを入力できます。
- 編集 (Edit) : 設定済みのサーバを編集できます。
- 削除 (Delete) : 1 つ以上のサーバを削除することができます。
- 接続のテスト (Test Connectivity) : 設定済みのアクセス情報を使用してサーバへの接続をテストすることができます。

### コールレコードリポジトリの追加または編集

コールレコードのリポジトリを追加するか、既存の設定を編集するには、次の手順に従ってください。

#### 手順

- 
- ステップ 1** [Unified Analysis Manager] メニューから、[インベントリ (Inventory) ] > [コールレコードリポジトリ (Call Record Repositories) ] の順に選択します。
- ステップ 2** 設定されているサーバのリストを含む [コールレコードリポジトリ (Call Record Repositories) ] ウィンドウが表示されます。[追加 (Add) ] ボタンをクリックして新しいサーバを追加するか、またはリストでサーバを強調表示し、[編集 (Edit) ] ボタンをクリックして既存の設定を編集します。
- ステップ 3** [リポジトリタイプ (Repository Type) ] ドロップダウンリストを使用して、サーバにアクセスするノードの製品タイプを選択します。
- ステップ 4** [ホスト名 (Hostname) ] フィールドに、追加するサーバの名前を入力します。
- ステップ 5** [JDBC ポート (JDBC Port) ] フィールドに、使用するサーバのポート番号を入力します。
- ステップ 6** [JDBC ユーザ名 (JDBC User Name) ] フィールドと [JDBC パスワード (JDBC Password) ] フィールドに、サーバへのアクセスを提供するユーザ名とパスワードを入力します。[パスワードの確認 (Confirm Password) ] フィールドに、パスワードを再度入力します。
- ステップ 7** オプションで、[説明 (Description) ] フィールドに追加するノードの簡単な説明を提供できます。
- ステップ 8** [関連付けに使用可能なノード (Nodes Available for Association) ] を使用して、サーバにアクセスできるノードを選択します。
- ステップ 9** NAT またはターミナルサーバ設定がある場合は、[詳細設定 (Advanced) ] ボタンを使用して [コールレコードリポジトリの追加 - 詳細設定 (Add Call Record Repository-Advanced) ] 画面を表示し

ます。[代替ホスト名 (Alternate Hostname)] フィールドと [代替ポート (Alternate Port)] フィールドに、適切な情報を入力します。

**ステップ 10** [追加 (Add)] ボタンをクリックしてサーバを追加するか、[編集 (Edit)] ボタンをクリックして設定を更新します。[キャンセル (Cancel)] ボタンを使って、サーバを追加せずに操作を終了できます。

---

## トレース テンプレートの定義

グループ内に多数のノードがある場合、Unified Analysis Manager はトレース レベルを変更するコンポーネントを選択するためのショートカットとしてテンプレートを提供します。テンプレートを使用して、ノードの新しいトレース レベルを確立することもできます。また、ログおよびトレース ファイルの収集にテンプレートを使用できます。

[テンプレート (Templates)] オプションを使用して、次の機能を実行できます。

- **追加** : [追加 (Add)] ボタンで新しいテンプレートを作成できます。テンプレートを追加するときは、実際のノードではなくノードタイプに対して追加していることに注意してください。特定のノードタイプの場合、コンポーネントとサービスの既知の固定セットがあります。
- **編集** : [編集 (Edit)] ボタンで既存のテンプレートを編集することができます。
- **クローン** : [クローン (Clone)] ボタンでは、既存のテンプレートを新しいテンプレートとして保存ことができ、元のテンプレートが置換されません。
- **削除** : [削除 (Delete)] ボタンでは、テンプレートを削除できます。
- **インポート** : フラットファイルから定義済みのテンプレートをインポートするには、[インポート (Import)] ボタンを使用します。
- **エクスポート** : フラットファイルにテンプレートをエクスポートするには、[エクスポート (Export)] ボタンを使用します。

### テンプレートの追加または編集

次の手順では、テンプレートを追加したり、既存の設定を編集する方法について説明します。



(注) Unified Analysis Manager に編集または削除できないデフォルトのテンプレートがあります。

---

## 手順

- ステップ 1** [Unified Analysis Manager] メニューから、[インベントリ (Inventory)] > [テンプレート (Templates)] の順に選択します。
- ステップ 2** [テンプレート (Templates)] ウィンドウが表示されます。[追加 (Add)] ボタンをクリックしてテンプレートを追加するか、またはリストからテンプレートを選択し、[編集 (Edit)] ボタンをクリックして既存の設定を編集します。[追加 (Add)] または [テンプレートの編集 (Edit Template)] 画面が表示されます。
- ステップ 3** テンプレート名を入力するには、[名前 (Name)] フィールドを使用します。
- ステップ 4** グループの簡単な説明を入力するには、[説明 (Description)] フィールドを使用します。
- ステップ 5** [製品タイプ (Product Type)] セクションには、Unified Analysis Manager でサポートされている製品のリストが含まれています。このリストから製品を選択すると、関連するコンポーネントが [コンポーネント名 (Component Name)] フィールドに表示されます。
- ステップ 6** 表示される各コンポーネントに対して、[トレース レベル (Trace Level)] フィールドのドロップダウンリストを使用してトレース レベルを適用できます。  
(注) すべてのコンポーネントが、この画面でトレース レベルを設定できるわけではありません。
- ステップ 7** [収集 (Collect)] フィールドのボックスをオンにすることで、コンポーネントのトレース ログを収集するかどうかを示すことができます。
- ステップ 8** [追加 (Add)] ボタンをクリックしてテンプレートを追加するか、[編集 (Edit)] ボタンをクリックして設定を更新します。[キャンセル (Cancel)] ボタンを使って、サーバを追加せずに操作を終了できます。

## コール定義

次の表に、コール終了のタイプを定義します。

表 11: コール定義

コールタイプ	コール終了の説明
失敗したコール	接続が完了する前に、ユーザによる切断以外の何らかの原因により、コールが接続されない。
放棄されたコール (Abandoned call)	コールを開始した後、ユーザが切断したため、コールが接続されない。
ドロップされたコール	ユーザによる切断以外の何らかの原因で、接続確立後、コールが切断される。

次の表に、失敗したコール、放棄されたコール、およびドロップされたコールをサポートする製品を示します。

表 12: コールタイプに対する製品サポート

コールタイプ	Unified Communications Manager	Unified CCE	Unified CVP	Unified CCX
失敗したコール	サポート対象	サポート対象	サポート対象	サポート対象
放棄されたコール (Abandoned call)	サポート対象	サポート対象	未サポート	サポート対象
ドロップされた コール	サポート対象	サポート対象	未サポート	サポート対象

## トレース収集

Unified Analysis Manager は、サポートされるデバイス サービスからログおよびトレース ファイルの収集を可能にします。ログおよびトレース ファイルを収集する方法は 3 つあります。

- 今すぐトレースを収集 (Collect Traces Now) : [今すぐトレースを収集 (Collect Traces Now) ] オプションを使用すると、過去に発生した任意の期間デバイスまたはデバイスのグループのサービスを選択することに基づいてトレース ファイルを収集できます。
- トレース収集をスケジュール (Schedule Trace Collection) : [トレース収集をスケジュール (Schedule Trace Collection) ] オプションを使用すると、将来の任意の期間デバイスまたはデバイスのグループのサービスを選択することに基づいてトレース ファイルを収集できます。
- トレースの設定および収集をスケジュール (Schedule Trace Settings and Collections) : [トレースの設定および収集をスケジュール (Schedule Trace Settings and Collections) ] オプションを使用すると、現在から将来にトレース ファイルを収集し、スケジュールされた期間内に使用するトレース レベルも指定できます。

### 今すぐトレースを収集

[今すぐトレースを収集 (Collect Traces Now) ] オプションを使用すると、過去に発生した任意の期間デバイスまたはデバイスのグループのサービスを選択することに基づいてトレース ファイルを収集できます。

## 手順

- 
- ステップ 1** [Unified Analysis Manager] メニューから、[ツール (Tools)] > [今すぐトレースを収集 (Collect Traces Now)] の順に選択します。  
[今すぐトレースを収集 (Collect Traces Now)] ウィンドウが表示されます。
- ステップ 2** サポートされているグループのリストを表示するには [グループ (Group)] を、サポートされているデバイスのリストを表示するには [ノード (Node)] を選択します。トレースを収集するグループまたはデバイスを選択します。
- ステップ 3** 使用するトレース レベルを含むテンプレートを選ぶには、[テンプレートの選択 (Select the template to)] ドロップダウン リストを使用します。また、グループまたはデバイスの新しいトレース レベルをカスタマイズする場合は、[カスタマイズ (Customize)] ボタンをクリックします。
- ステップ 4** 収集期間を選択するには、[開始時刻 (Start Time)] フィールドと [終了時刻 (End Time)] フィールドを使用します。
- ステップ 5** 収集期間のタイムゾーンを選択するには、[参照タイムゾーン (Referenced Time Zone)] フィールドを使用します。
- ステップ 6** オプションで [要約の表示 (View Summary)] ボタンをクリックして、[収集のサマリー (Collection Summary)] ウィンドウを表示することもできます。このウィンドウには、ノードに関連するコンポーネントのリストが含まれます。
- ステップ 7** トレースを開始するには、[OK] ボタンをクリックします。トレースを実行した場合、トレースのステータス サマリーおよびステータス詳細がウィンドウに表示されます。ステータス詳細は、ログの送信先ディレクトリへのパスを提供します。
- 

## トレース収集のスケジュール

現在から未来の任意の期間のトレース ファイルを収集する場合は、トレース収集のスケジュール オプションを使用します。

## 手順

- 
- ステップ 1** [Unified Analysis Manager] メニューから、[ツール (Tools)] > [トレース収集のスケジュール (Schedule Trace Collection)] の順に選択します。

[トレース収集のスケジュール (Schedule Trace Collection) ] ウィンドウが表示されます。

- ステップ 2** サポートされているグループのリストを表示するには [グループ (Group) ] を、サポートされているデバイスのリストを表示するには [ノード (Node) ] を選択します。トレースを収集するグループまたはデバイスを選択します。
- ステップ 3** 使用するトレース レベルを含むテンプレートを選ぶには、[テンプレートの選択 (Select the template to) ] ドロップダウンリストを使用します。また、特定のコンポーネントのトレースを収集する場合は、[カスタマイズ (Customize) ] ボタンをクリックできます。
- ステップ 4** 収集期間を選択するには、[開始時刻 (Start Time) ] フィールドと [終了時刻 (End Time) ] フィールドを使用します。
- ステップ 5** 収集期間のタイムゾーンを選択するには、[参照タイムゾーン (Referenced Time Zone) ] フィールドを使用します。
- ステップ 6** 収集の頻度を示すには、[トレースの収集頻度 (Collect Traces Every) ] ドロップダウンフィールドを使用します。
- ステップ 7** オプションで、トレース収集に関する電子メール通知の送信を選択することもできます。そのためには、[電子メール通知の送信 (Send Email Notification to) ] チェックボックスをクリックして、テキスト ボックスに電子メールアドレスを入力します。
- ステップ 8** オプションで [要約の表示 (View Summary) ] ボタンをクリックして、[収集のサマリー (Collection Summary) ] ウィンドウを表示することもできます。このウィンドウには、ノードに関連するコンポーネントのリストが含まれます。
- ステップ 9** トレースを開始するには、[OK] ボタンをクリックします。トレースをスケジュールした場合、トレースのステータス サマリーおよびステータス詳細がウィンドウに表示されます。トレースが完了すると、レポートがログファイルに書き込まれます。電子メール情報が提供された場合、システムにより生成された電子メールが送信されます。

## トレースの設定と収集のスケジュール

現在から将来にかけての任意の期間でトレース ファイルを収集する場合、トレースの設定と収集のスケジュールオプションを使用します。また、スケジュールされた時間に使用するトレースレベルを指定します。このオプションのトレース設定を変更すると、トレースレベルは、収集期間後にデフォルト設定に復元されます。

### 手順

- ステップ 1** [Unified Analysis Manager] メニューから、[ツール (Tools) ] > [トレース収集のスケジュール (Schedule Trace Collection) ] の順に選択します。



[トレース収集のスケジュール (Schedule Trace Collection) ] ウィンドウが表示されます。

- ステップ 2** サポートされているグループのリストを表示するには [グループ (Group) ] を、サポートされているデバイスのリストを表示するには [ノード (Node) ] を選択します。トレースを収集するグループまたはデバイスを選択します。
- ステップ 3** 使用するトレース レベルを含むテンプレートを選ぶには、[テンプレートの選択 (Select the template to) ] ドロップダウン リストを使用します。また、グループまたはデバイスの新しいトレース レベルをカスタマイズする場合は、[カスタマイズ (Customize) ] ボタンをクリックします。このオプションを使用すると、特定のコンポーネントのトレースを収集できます。
- ステップ 4** 収集期間を選択するには、[開始時刻 (Start Time) ] フィールドと [終了時刻 (End Time) ] フィールドを使用します。
- ステップ 5** 収集期間のタイムゾーンを選択するには、[参照タイムゾーン (Referenced Time Zone) ] フィールドを使用します。
- ステップ 6** 収集の頻度を示すには、[トレースの収集頻度 (Collect Traces Every) ] ドロップダウンフィールドを使用します。
- ステップ 7** オプションで、トレース収集に関する電子メール通知の送信を選択することもできます。そのためには、[電子メール通知の送信 (Send Email Notification to) ] チェックボックスをクリックして、テキストボックスに電子メールアドレスを入力します。
- ステップ 8** オプションで [要約の表示 (View Summary) ] ボタンをクリックして、[収集のサマリー (Collection Summary) ] ウィンドウを表示することもできます。このウィンドウには、ノードに関連するコンポーネントのリストが含まれます。
- ステップ 9** トレースを開始するには、[OK] ボタンをクリックします。トレースをスケジュールした場合、トレースのステータス サマリーおよびステータス詳細がウィンドウに表示されます。トレースが完了すると、レポートがログ ファイルに書き込まれます。電子メール情報が提供された場合、システムにより生成された電子メールが送信されます。

## トレース レベルの設定

トレース レベルの設定オプションを使って、デバイスのグループまたは個々のデバイスにトレース レベルを割り当てます。テンプレートを使用してトレース レベルを割り当てることも、トレース レベルをカスタマイズすることもできます。トレース レベルは、次の Cisco Unified Communications コンポーネントに対して設定できます。

- Cisco Unified Communications Manager : Cisco Unified Communications Manager と共通のトレース コンポーネントに対してトレース レベルを設定できます。
- IM and Presence : Unified Presence と共通のトレース コンポーネントに対してトレース レベルを設定できます。
- Cisco Unity Connection : Cisco Unity Connection と共通のトレース コンポーネントに対してトレース レベルを設定できます。

- Cisco Unified Contact Center Express : 共通のトレース コンポーネントに対してのみトレース レベルを設定できます。

次の表では、Unified Analysis Manager によって管理される Cisco Unified Communications コンポーネントに対する一般的なトレース レベル設定について説明します。

表 13 : *Unified Analysis Manager* トレース レベルの設定

トレースレベル	ガイドライン	トレースの予想ボリューム
デフォルト	このレベルは、異常なパスに生成されたすべてのトレースを含める必要があります。このレベルは通常発生してはならないコーディングエラー トレースとエラーのトレースを対象としています。	最小トレース (予想値)
警告	このレベルは、システムレベル操作のトレースを含める必要があります。これは、コンポーネント内の“状態遷移”によって生成されるすべてのトレースを含める必要があります。	コンポーネント使用時に中規模ボリュームのトレース (予想値)
情報 (Informational)	これは、コンポーネントの困難な問題をデバッグする目的で、ラボで使用できるトレースを含める必要があります。	コンポーネント使用時に大規模ボリュームのトレース (予想値)
デバッグ (Debug)	このレベルはデバッグ用に基本的に使用されるメッセージの詳細なデバッグ情報や大量データを含める必要があります。	コンポーネント使用時に非常な大規模ボリュームのトレース (予想値)

## 手順

- 
- ステップ 1** [Unified Analysis Manager] メニューから、[ツール (Tools)] > [トレース レベルの設定 (Set Trace Level)] の順に選択します。  
[トレース レベルの設定 (Set Trace Level)] ウィンドウが表示されます。
- ステップ 2** サポートされているグループのリストを表示するには [グループ (Group)] を、サポートされているデバイスのリストを表示するには [ノード (Node)] を選択します。トレースを収集するグループまたはデバイスを選択します。
- ステップ 3** [テンプレートの選択 (Select the template)] ドロップダウンリストボックスから、使用するトレースレベルを含むテンプレートを選択します。また、グループまたはデバイスのトレースレベルをカスタマイズする場合は、[カスタマイズ (Customize)] ボタンをクリックします。[カスタマイズ (Customize)] オプションを選択する場合、サポートされるデバイスのリストとともに [Design

Preview (設計プレビュー) ] ダイアログが表示されます。対象のデバイスを選択し、[選択済みコンポーネント (Selected Components) ] フィールドを使ってトレース レベルを設定します。

- ステップ 4** ノードのトレース レベルに対する変更を表示するには、[変更の表示 (View Changes) ] をクリックします。[OK] をクリックすると、レベルが設定され、この画面を終了します。

## 設定の表示

ノードに関連する設定情報を表示するには、[設定の表示 (View Configuration) ] オプションを使用します。バージョンおよび設定情報を収集し、ブラウザで表示したり、結果を保存することができます。

### 手順

- ステップ 1** [Unified Analysis Manager] メニューから、[ツール (Tools) ] > [設定の表示 (View Configuration) ] の順に選択します。  
[設定の表示 (View Configuration) ] ウィンドウが表示され、ノードのリストが表示されます。
- ステップ 2** ノードを選択して、[次へ (Next) ] ボタンをクリックすると、[選択済みのコンポーネント (Selected Components) ] 画面が表示されます。この画面は、製品のバージョン、プラットフォーム、ライセンス、およびその他のカテゴリの設定情報を示します。
- ステップ 3** 設定情報を収集するには、[完了 (Finish) ] をクリックします。  
サマリーウィンドウが表示されます。ブラウザで収集した情報を表示したり、[名前を付けて保存 (Save As) ] ボタンを使って収集した設定情報を保存することができます。

## Cisco Unified Analysis Manager のトラブルシューティング

次の表に、Unified Analysis Manager のノードへの接続をテストしているときに発生する可能性のあるエラーと、そのエラーを修正するために推奨されるアクションを示します。

表 14: 接続テストでのエラーと修正アクション

番号	エラー コード (Error Code)	メッセージ	修正処置
1	NOT_AUTHORIZED_CODE	ユーザ名またはパスワードが正しくありません (Username or password is not correct)	正しいユーザ名とパスワードを入力します。

番号	エラーコード (Error Code)	メッセージ	修正処置
2	MISSING_SERVICE_CODE	サービスが見つかりません (Missing Service)	要求された Web サービスが見つかりません。Web サービスがターゲットアプリケーションでダウンしているかどうかを確認します。
3	SERVER_BUSY_CODE	サーバがビジー状態です (Server is busy)	サーバ上に実行中の他のジョブがあるかどうかを確認します。ある場合は、そのジョブが完了するまで待機します。そうでない場合は、数分待ってから、再試行してください。
4	INVALID_PORT_CODE	ポートが無効です (Invalid Port)	指定されたポートは構文的に正しくないか、範囲外の可能性があります。
5	CONNECTION_FAILED_CODE	指定されたノードに接続されていません (Not connected to the specified node)	このノードの正しいアドレスを入力したことを確認します。アドレスが正しい場合は、ノードが起動しており、到達可能であることを確認します。
[6]	NOT_SUPPORTED_CODE	未サポート	指定した製品のこのバージョンは、このリリースではサポートされていません。サポートされるバージョンにこの製品をアップグレードします。

番号	エラーコード (Error Code)	メッセージ	修正処置
7	CERTIFICATE_HANDLING_ERROR_CODE	SSL のハンドシェイクに失敗しました。クライアントとサーバは、必要なレベルのセキュリティをネゴシエートできませんでした (SSL handshake failed. The client and server could not negotiate desired level of security)	サーバからクライアントに送信された証明書を受け入れことを確認します。
8	GENERAL_CONNECTION_ERROR_CODE	内部エラーが発生しました (An internal error has occurred)	最近の Unified Analysis Manager ログファイルを保存し、Unified Analysis Manager サポートに問い合わせてください。





## 第 5 章

# プロフィールとカテゴリ

---

- [プロフィール, 117 ページ](#)
- [カテゴリ, 118 ページ](#)

## プロフィール

### 設定プロフィールの追加

RTMTを使用すると、異なるパフォーマンスカウンタをモニタして、モニタリング ウィンドウをカスタマイズし、独自の設定プロフィールを作成できます。各ウィンドウを再び開くのではなく、それらのモニタリング ウィンドウをワンステップで復元できます。

同一のRTMTセッション中に別のプロフィールに切り替えたり、後続のRTMTセッションで設定プロフィールを使用したりすることができます。

プロフィールを作成するには、次の手順に従ってください。

#### 手順

---

- ステップ 1** [ファイル (File) ]>[プロフィール (Profile) ]の順に選択します。  
[プリファレンス (Preferences) ]ダイアログボックスが表示されます。
- ステップ 2** [保存 (Save) ]をクリックします。  
[現在の設定を保存 (Save Current Configuration) ]ダイアログボックスが表示されます。
- ステップ 3** [設定名 (Configuration name) ]フィールドに、この特定の設定プロフィールの名前を入力します。
- ステップ 4** [設定の説明 (Configuration description) ]フィールドに、この特定の設定プロフィールの説明を入力します。
- (注) プロフィールはクラスタ内のすべてのサーバに適用されますが、プロフィールを別のクラスタに保存し、適用することはできません。

システムが新しい設定プロファイルを作成します。

---

## 設定プロファイルの復元

設定した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 [ファイル (File) ]>[プロファイル (Profile) ]の順に選択します。  
[プリファレンス (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 [復元 (Restore) ]をクリックします。  
復元された設定の事前に準備された設定またはパフォーマンスモニタリングカウンタがあるすべてのウィンドウが開きます。
- 

## 設定プロファイルの削除

ユーザが設定した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 [ファイル (File) ]>[プロファイル (Profile) ]の順に選択します。  
[プリファレンス (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 [削除 (Delete) ]をクリックします。
  - ステップ4 [閉じる (Close) ]をクリックします。
- 

## カテゴリ

### カテゴリの追加

カテゴリを追加するには、次の手順に従ってください。



手順

**ステップ 1** 設定に該当するウィンドウに進みます。

<b>Cisco Unified Communications Manager</b>	[システム (System) ]> [パフォーマンス (Performance) ]> [パフォーマンス監視を開く (Open Performance Monitoring) ] を選択します。
<b>Cisco Unified Communications Manager IM and Presence Service</b>	[システム (System) ]> [パフォーマンス (Performance) ]> [パフォーマンス監視を開く (Open Performance Monitoring) ] を選択します。
<b>Cisco Unity Connection</b>	[システム (System) ]> [パフォーマンス (Performance) ]> [パフォーマンス監視を開く (Open Performance Monitoring) ] を選択します。

**ステップ 2** [編集 (Edit) ]> [新しいカテゴリの追加 (Add New Category) ] の順に選択します。

**ステップ 3** カテゴリの名前を入力し、[OK] をクリックします。  
 カテゴリ タブがウィンドウの下部に表示されます。

## カテゴリ名の変更

カテゴリの名前を変更するには、次の手順を実行します。

手順

**ステップ 1** 次のいずれかの作業を実行します。

- a) 名前を変更するカテゴリ タブを右クリックし、[カテゴリの名前変更 (Rename Category) ] を選択します。
- b) 名前を変更するカテゴリ タブをクリックし、[編集 (Edit) ]> [カテゴリの名前変更 (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名前変更されたカテゴリが表示されます。

## カテゴリの削除

カテゴリを削除するには、次のいずれかの作業を実行します。

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



## 第 6 章

# パフォーマンス カウンタ (Performance Counters)

- [カウンタ](#), 121 ページ
- [perfmon カウンタ データのローカル ロギング](#), 125 ページ
- [Perfmon ログ ビューアおよび Microsoft パフォーマンス ツールのログ ファイル](#), 128 ページ
- [トラブルシューティング](#), 132 ページ

## カウンタ

### パフォーマンス クエリーを使用したカウンタの追加

perfmon カウンタを選択し、表示するためにクエリーを使用できます。機能ベースのカウンタのセットを表示し、1つのカテゴリに保存するように、perfmon カウンタを整理できます。Unified RTMT プロファイルを保存した後は、関心のあるカウンタにすばやくアクセスできます。

Unified RTMT は、perfmon カウンタをチャート形式または表形式で表示します。チャート形式では、perfmon カウンタ情報が折れ線グラフを使用して表示されます。作成した各カテゴリ タブの [Perfmon モニタリング (Perfmon Monitoring)] ペインに最大 6 つのチャートを表示でき、1 つのチャートに最大 3 つのカウンタを表示できます。カテゴリを作成した後で、チャート形式から表形式に、またはその逆に表示を変更することはできません。



ヒント

[Perfmon モニタリング (Perfmon Monitoring)] ペインでは、1つのチャートに最大 3 つのカウンタを表示できます。チャート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 [Perfmon モニタリング (Perfmon Monitoring)] ペインにドラッグします。この操作を繰り返して、最大 3 つまでカウンタを追加します。

デフォルトでは、Unified RTMTはperfmonカウンタをチャート形式で表示します。また、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 [データを表形式で表示する (Present Data in Table View)] チェックボックスをオンにする必要があります。

## 手順

- 
- ステップ 1** [システム (System)] > [パフォーマンス (Performance)] > [パフォーマンス監視を開く (Open Performance Monitoring)] を選択します。
- ステップ 2** モニタするカウンタを追加するサーバの名前をクリックします。ツリー階層が拡大し、すべての perfmon オブジェクトが表示されます。
- ステップ 3** 表形式でカウンタをモニタするには、ステップ 4 に進みます。チャート形式でカウンタをモニタするには、ステップ 9 にスキップします。
- ステップ 4** [編集 (Edit)] > [新規カテゴリ (New Category)] の順に選択します。
- ステップ 5** [名前を入力 (Enter Name)] フィールドに、タブの名前を入力します。
- ステップ 6** perfmon カウンタを表形式で表示するには、[データを表形式で表示する (Present Data in Table View)] チェックボックスをオンにする必要があります。
- ステップ 7** [OK] をクリックします。入力した名前の新しいタブが、ペインの下部に表示されます。
- ステップ 8** 1 つ以上のインスタンスを指定した 1 つ以上のカウンタを選択して、表形式でモニタリングするには、次のいずれかの作業を実行します (この手順の残りのステップをスキップしてください)。
- 単一のカウンタをダブルクリックし、ポップアップウィンドウから単一のインスタンスを選択します。次に、[追加 (Add)] をクリックします。
  - 単一のカウンタをダブルクリックし、ポップアップウィンドウから複数のインスタンスを選択します。次に、[追加 (Add)] 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に、チャート形式で表示するには、カテゴリ タブを右クリックし、[カテゴリの削除 (Remove Category)] を選択します。カウンタはチャート形式で表示されます。
- ステップ 9** チャート形式のカウンタをモニタするには、次のタスクを実行します。
- a) モニタするカウンタを示すオブジェクト名の横の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。
  - b) カウンタ情報を表示するには、カウンタを右クリックし、[カウンタ モニタリング (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、または [Perfmon モニタリング (Perfmon Monitoring)] ペインにカウンタをドラッグアンドドロップします。カウンタ チャートが [Perfmon モニタリング (Perfmon Monitoring)] ペインに表示されます。
-

## [パフォーマンスの監視 (Performance Monitoring) ] ペインからのカウンタの削除

カウンタ チャート (表エントリ) は、メニュー バーの [Perfmon] メニューにある [チャート/表エントリの削除 (Remove Chart/Table Entry) ] メニュー項目を使用して削除できます。

不要になったカウンタは、[RTMT Perfmon モニタリング (RTMT Perfmon Monitoring) ] ペインから削除できます。ペインからカウンタを削除するには、次の手順に従ってください。

### 手順

次のいずれかの作業を実行します。

- 削除するカウンタを右クリックし、[削除 (Remove) ] を選択します。
- 削除するカウンタをクリックし、[Perfmon]>[チャート/表エントリの削除 (Remove Chart/Table Entry) ] の順に選択します。

## 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、次の手順に従ってください。

### 手順

- 
- ステップ 1** パフォーマンス モニタリング カウンタを検索して表示します。
  - ステップ 2** パフォーマンス モニタリングのツリー階層で、パフォーマンス モニタリング カウンタをクリックし、[システム (System) ]>[パフォーマンス (Performance) ]>[カウンタインスタンス (Counter Instances) ] の順に選択します。
  - ステップ 3** [インスタンスの選択 (Select Instance) ] ウィンドウで、インスタンスをクリックし、次に、[追加 (Add) ] をクリックします。  
カウンタが表示されます。
- 

## カウンタ アラート通知のセットアップ

カウンタのアラート通知を設定するには、次の手順に従ってください。



## 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、[アラートの削除 (Remove Alert)] を選択します。オプションは、アラートを削除するとグレー表示されます。

## 手順

- ステップ 1 パフォーマンス カウンタを検索して表示します。
- ステップ 2 カウンタのチャートまたは表から、アラート通知を設定するカウンタを右クリックし、[アラート/プロパティの設定 (Set Alert/Properties)] を選択します。
- ステップ 3 [アラートの有効化 (Enable Alert)] チェックボックスをオンにします。
- ステップ 4 [重大度 (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 [説明 (Description)] ペインで、アラートの説明を入力して [次へ (Next)] をクリックします。
- ステップ 6 [しきい値 (Threshold)]、[次の値で算出 (Value Calculated As)]、[期間 (Duration)]、[頻度 (Frequency)]、および [スケジュール (Schedule)] ペインで設定値を設定します。ウィンドウで設定を入力したら、[次へ (Next)] をクリックして次のペインに進みます。
- ステップ 7 アラートの電子メールメッセージを送信するようにシステムを設定するには、[電子メールの有効化 (Enable Email)] チェックボックスをオンにします。
- ステップ 8 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には、[アラートアクションをトリガー (Trigger Alert Action)] ドロップダウン リスト ボックスから対象のアラートアクションを選択します。
- ステップ 9 アラートの新しいアラートアクションを設定するには、[設定 (Configure)] をクリックします。  
(注) 指定されたアラートがトリガーされたときに、システムはアラートアクションを送信します。  
[アラートアクション (Alert Action)] ダイアログ ボックスが表示されます。
- ステップ 10 新しいアラートアクションを追加するには、[追加 (Add)] をクリックします。  
[アクション設定 (Action Configuration)] ダイアログ ボックスが表示されます。
- ステップ 11 [名前 (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 12 [説明 (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 13 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、[追加 (Add)] をクリックします。  
[入力 (Input)] ダイアログ ボックスが表示されます。
- ステップ 14 アラートアクションの通知を受け取る受信者の電子メールまたは E ページアドレスを入力し、[OK] をクリックします。
- ステップ 15 ユーザー定義の電子メール テキスト ボックスに、電子メールに表示するテキストを入力し、[有効化 (Activate)] をクリックします。

## カウンタの説明の表示

カウンタの説明を取得する方法を次に示します。

### 手順

- 
- ステップ 1** 次のいずれかの作業を実行します。
- a) Perfmon ツリー階層で、プロパティ情報が必要な対象のカウンタを右クリックし、[カウンタの説明 (Counter Description)] を選択します。
  - b) [RTMT パフォーマンス モニタリング (RTMT Performance Monitoring)] ペインで、カウンタをクリックし、メニューバーから [システム (System)] > [パフォーマンス (Performance)] > [カウンタの説明 (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 パラメータを設定できます。  
[カウンタのプロパティ (Counter Property)] ウィンドウには、カウンタの説明が表示されます。この説明には、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、およびカウンタの内容の概要が含まれます。
- ステップ 2** [カウンタのプロパティ (Counter Property)] ウィンドウを閉じるには、[OK] をクリックします。
- 

## perfmon カウンタ データのローカル ロギング

RTMT では、さまざまな perfmon カウンタを選択して、ローカルにロギングすることができます。その perfmon CSV ログのデータは、パフォーマンス ログ ビューアを使用して表示できます。

## perfmon カウンタ ロギングの開始

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

### 手順

- 
- ステップ 1** パフォーマンス モニタリング カウンタを検索して表示します。
- ステップ 2** perfmon カウンタをチャート形式で表示している場合は、データ サンプル情報が必要な対象のグラフを右クリックし、[カウンタ ロギングの開始 (Start Counter(s) Logging)] を選択します。[カウンタ ロギングの設定 (Counter Logging Configuration)] ダイアログ ボックスが表示されます。

- ステップ 3** 画面上のすべてのカウンタを記録するには (チャート形式および表形式のいずれも)、ウィンドウの一番下にあるカテゴリ名タブを右クリックして、[カウンタ ログイングの開始 (Start Counter(s) Logging)] を選択します。  
[カウンタ ログイングの設定 (Counter Logging Configuration)] ダイアログ ボックスが表示されます。
- ステップ 4** ファイルパラメータの最大ファイル サイズおよび最大数を設定します。
- ステップ 5** [ロガー ファイル名 (Logger File Name)] フィールドに、ファイル名を入力して [OK] をクリックします。  
RTMT は、ユーザのホーム ディレクトリにある .jrtmt ディレクトリ内のログ フォルダに CSV ログ ファイルを保存します。たとえば、Windows ではパスが D:\Documents and Settings\userA\.jrtmt\log となり、Linux では /users/home/.jrtmt/log となります。  
ファイルの数とサイズを制限するには、特定サービスのトレース出力設定でファイルパラメータの最大ファイル サイズと最大数を、Cisco Unified Serviceability の [トレース設定 (Trace Configuration)] ウィンドウで設定します。『Cisco Unified Serviceability Administration Guide』を参照してください。
- (注) perfmon カウンタのログイングをすでに開始していて、ファイルの最大ファイル サイズおよび最大数を変更する場合は、最初にカウンタを停止してから最大ファイル サイズとファイル数のパラメータを再設定する必要があります。パラメータをリセットすると、perfmon カウンタのログイングを再開できます。

## perfmon カウンタ ログイングの停止

perfmon カウンタ データのログイングを停止するには、次の手順を実行します。

### 手順

- ステップ 1** パフォーマンス モニタリング カウンタを検索して表示します。
- ステップ 2** perfmon カウンタをチャート形式で表示している場合は、カウンタ ログイングが開始されているグラフを右クリックし、[カウンタ ログイングの停止 (Stop Counter(s) Logging)] を選択します。画面上のすべてのカウンタのログイングを停止するには (チャート形式および表形式のいずれも)、ウィンドウの一番下にあるカテゴリ名タブを右クリックして、[カウンタ ログイングの停止 (Stop Counter(s) Logging)] を選択します。

## データ サンプルの設定

[カウンタのプロパティ (Counter Property)] ウィンドウには、カウンタのデータ サンプルを設定するためのオプションがあります。[RTMT Perfmon モニタリング (RTMT Perfmon Monitoring)] ペインに表示される perfmon カウンタには、経時的なデータのサンプルが緑色の点で表示されます。収集するデータ サンプルの数やチャートに表示するデータ点の数は設定することができま



す。データ サンプルを設定した後は、[すべてのデータを表示/現在のデータを表示 (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できます。

カウンタのために収集するデータ サンプルの数を設定するには、次の手順に従ってください。

### 手順

- 
- ステップ 1** カウンタを検索、表示します。
  - ステップ 2** データ サンプル情報が必要な対象のカウンタをクリックし、[システム (System)] > [パフォーマンス (Performance)] > [モニタリングのプロパティ (Monitoring Properties)] の順に選択します。[カウンタのプロパティ (Counter Property)] ウィンドウには、カウンタの説明のほか、データ サンプルを設定するためのタブが表示されます。この説明には、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、およびカウンタの内容の概要が含まれます。
  - ステップ 3** カウンタのデータ サンプル数を設定するには、[データ サンプル (Data Sample)] タブをクリックします。
  - ステップ 4** [データ サンプルの数 (No. of data samples)] ドロップダウン リストボックスで、サンプル数を選択します (100 ~ 1000)。デフォルトは 100 です。
  - ステップ 5** [チャートに表示するデータ ポイント数 (No. of data points shown on chart)] ドロップダウン リストボックスで、チャートに表示するデータ ポイントの数を選択します (10 ~ 50)。デフォルトは 20 です。
  - ステップ 6** 次のいずれかのパラメータをクリックします。
    - [絶対値 (Absolute)] : 一部のカウンタ値は累積されるため、データの現在のステータスを表示する場合に選択します。
    - [差分 (Delta)] : 現在のカウンタ値と前回のカウンタ値の差分を表示する場合に選択します。
    - [差分比率 (Delta Percentage)] : カウンタ パフォーマンスの変化を比率で表示する場合に選択します。
  - ステップ 7** [カウンタのプロパティ (Counter Property)] ウィンドウを閉じ、[RTMT Perfmon モニタリング (RTMT Perfmon Monitoring)] ペインに戻るには、[OK] をクリックします。
- 

## カウンタ データの表示

パフォーマンス カウンタで収集されたデータを表示するには、次の手順に従ってください。

## 手順

- 
- ステップ 1** [RTMT Perfmon モニタリング (RTMT Perfmon Monitoring) ] ペインで、データ サンプルを表示するカウンタのカウンタ チャートを右クリックします。
- ステップ 2** [すべてのデータを表示 (View All Data) ] を選択します。カウンタ チャートには、サンプリングされたすべてのデータが表示されます。緑色の点は近接して表示されます。
- ステップ 3** 現在表示されているカウンタを右クリックします。
- ステップ 4** [現在のデータを表示 (View Current) ] を選択します。カウンタ チャートには、最後に設定され、収集されたデータ サンプルが表示されます。
- 

## Perfmon ログビューアおよび Microsoft パフォーマンス ツールのログ ファイル

パフォーマンスログビューアには、選択したカウンタのデータを示すチャートが表示されます。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。

次の表では、パフォーマンスログビューアで使用できるさまざまなボタンの機能について説明します。

表 15: パフォーマンス ログビューア

ボタン	機能
カウンタの選択 (Select Counters)	パフォーマンス ログビューアに表示するカウンタの追加を可能にします。カウンタを表示しない場合は、カウンタの横にある [表示 (Display) ] カラムのチェックマークを外します。
Reset View	パフォーマンス ログビューアを初期のデフォルト表示にリセットします。
ダウンロードしたファイルの保存 (Save Downloaded File)	ローカルコンピュータへのログファイルの保存を可能にします。

## Perfmon ログ ビューアでのログ ファイルの表示

パフォーマンス ログ ビューアには、perfmon CSV ログ ファイルからのカウンタのデータがグラフィック形式で表示されます。パフォーマンス ログ ビューアを使用して、収集したローカル perfmon ログのデータを表示することも、Real-time Information Server Data Collection (RISDC) perfmon ログのデータを表示することもできます。

### はじめる前に

ローカル perfmon ログは、コンピュータで選択し、ローカルに保存したカウンタのデータで構成されます。

### 手順

**ステップ 1** [システム (System) ]>[パフォーマンス (Performance) ]>[パフォーマンス ログ ビューアを開く (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。

- RisDC Perfmon ログについては、次の手順を実行します。

- 1 [Perfmon ログの場所の選択 (Select Perfmon Log Location) ]セクションで RisDC Perfmon ログを選択します。
- 2 リスト ボックスからノードを選択します。
- 3 [開く (Open) ]を選択します。
- 4 ファイルを選択し、[ファイルを開く (Open File) ]を選択します。
- 5 表示するカウンタにチェックマークを付けます。
- 6 [OK] を選択します。

- ローカルに保存されたデータについては、次の操作を実行します。

- 1 [ローカル Perfmon ログ (Local Perfmon Logs) ]を選択します。
- 2 [開く (Open) ]を選択します。
- 3 ファイル ディレクトリを参照します。
- 4 表示する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。
- 5 [開く (Open) ]を選択します。
- 6 表示するカウンタにチェックマークを付けます。

7 [OK] を選択します。

**ステップ 3** 表示するカウンタを選択します。

**ステップ 4** [OK] を選択します。

トラブルシューティングのヒント

- Real-Time Monitoring Tool は、ユーザのホーム ディレクトリにある .jrtmt ディレクトリ内のログ フォルダに perfmon CSV ログ ファイルを保存します。Windows ではパスが D:\Documents and Settings\userA\.jrtmt\log となり、Linux では /users/home/.jrtmt/log となります。
- RISDC perfmon ロギングは、Troubleshooting Perfmon データ ロギングとしても知られています。RISDC perfmon ロギングを有効にすると、サーバは問題のトラブルシューティングに使用されるデータを収集します。IM and Presence Service は短期間に大量のデータを収集するので、RISDC perfmon データ ロギング (Troubleshooting perfmon データ ロギング) を有効にする時間を制限するようにしてください。
- カラムの見出しを選択することにより、各カラムを整理できます。カラムの見出しを最初に選択したときは、レコードが昇順で表示されます。上向きの小さい三角形が、昇順を示します。カラムの見出しを再び選択すると、レコードは降順で表示されます。下向きの小さい三角形が、降順を示します。カラムの見出しをもう一度選択すると、レコードのソートは解除されます。

## パフォーマンス ログ ビューアの拡大と縮小

パフォーマンス ログ ビューアには、チャートの一部を拡大および縮小できるズーム機能が備わっています。

### 手順

**ステップ 1** 次のいずれかの操作を実行します。

a) クイック起動チャンネルで次の手順を実行します。

- [システム (System) ] を選択します。
- ツリー階層で、[パフォーマンス (Performance) ] をダブルクリックして、パフォーマンス アイコンを表示します。
- [パフォーマンス (Performance) ] アイコンを選択します。

b) [システム (System) ] > [パフォーマンス (Performance) ] > [パフォーマンス モニタリングを開く (Open Performance Monitoring) ] の順に選択します。

**ステップ 2** カウンタが配置されているサーバの名前を選択します。

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

**ステップ 3** モニタするパフォーマンス カウンタをダブルクリックします。

**ステップ 4** 次のいずれかの操作を実行します。

目的	Action
チャートの一部を拡大する	<ul style="list-style-type: none"> <li>マウスの左ボタンをクリックし、チャート内で関心のあるエリアにドラッグします。</li> <li>必要な領域を選択してから、マウスの左ボタンを放します。</li> </ul>
チャートを初期のデフォルト表示にリセットする	<p>次のいずれかの操作を実行します。</p> <ul style="list-style-type: none"> <li>[ビューのリセット (Reset View)] を選択します。</li> <li>チャートを右クリックし、[リセット (Reset)] を選択します。</li> </ul>

## Microsoft パフォーマンス ツールを使用した Perfmon ログ ファイルの表示



(注) [パフォーマンス (Performance)] にアクセスする方法は、コンピュータにインストールされている Windows のバージョンによって異なります。

### 手順

**ステップ 1** [スタート (Start)] > [設定 (Settings)] > [コントロール パネル (Control Panel)] > [管理ツール (Administrative Tools)] > [パフォーマンス (Performance)] の順に選択します。

**ステップ 2** アプリケーション ウィンドウで次の操作を実行します。

- マウスの右ボタンをクリックします。
- [プロパティ (Properties)] を選択します。

**ステップ 3** [システム モニタのプロパティ (System Monitor Properties)] ダイアログボックスで [ソース (Source)] タブを選択します。

**ステップ 4** perfmon ログ ファイルをダウンロードしたディレクトリを参照し、perfmon csv ファイルを選択します。ログ ファイルに使用される命名規則は

PerfMon\_<node>\_<month>\_<day>\_<year>\_<hour>\_<minute>.csv です。たとえば、PerfMon\_172.19.240.80\_06\_15\_2005\_11\_25.csv となります。

- ステップ 5 [適用 (Apply)] を選択します。
- ステップ 6 [時間の範囲 (Time Range)] を選択します。表示する perfmon ログ ファイルで時間の範囲を指定するには、適切な開始時刻と終了時刻までバーをドラッグします。
- ステップ 7 [カウンタの追加 (Add Counters)] ダイアログボックスを開くには、[データ (Data)] タブを選択し、[追加 (Add)] を選択します。
- ステップ 8 [パフォーマンス オブジェクト (Performance Object)] ドロップダウンリストボックスから perfmon オブジェクトを選択します。オブジェクトに複数のインスタンスがある場合は、[すべてのインスタンス (All instances)] を選択するか、表示するインスタンスだけを選択します。
- ステップ 9 [すべてのカウンタ (All Counters)] を選択することも、表示するカウンタだけを選択することもできます。
- ステップ 10 [追加 (Add)] を選択して、選択したカウンタを追加します。
- ステップ 11 カウンタの選択が終了したら、[閉じる (Close)] を選択します。

## トラブルシューティング

### perfmon データ ログのトラブルシューティング

Troubleshooting perfmon データ ログ機能は、Cisco TAC がシステムの問題を識別する際に役立ちます。Troubleshooting perfmon データ ログ機能を有効にすると、選択したノードでの一連のシステムとオペレーティング システムのパフォーマンス統計情報の収集が開始されます。収集された統計情報には、システム診断に使用できる総合的な情報が含まれます。

Troubleshooting perfmon データ ログ機能は、システムの状態に関する総合的な情報を提供する一連の perfmon カウンタから統計情報を収集するように、自動的に設定されます。Troubleshooting Perfmon データ ログ機能が有効である場合、CPU 使用率の増加は 5 パーセント未満であり、使用されるメモリ量にも目立った増加はなく、毎日約 50 MB の情報がログ ファイルに書き込まれることが推測されます。

Troubleshooting perfmon データ ログ機能を使用して、次の管理タスクを実行できます。

- Troubleshooting perfmon データ ログ機能用のトレース フィルタを有効または無効にする。
- 各サーバで事前定義された一連のシステムとパフォーマンス オブジェクトおよびカウンタをモニタする。
- モニタされたパフォーマンス データをサーバ上のアクティブ ログ パーティションの var/log/active/cm/log/ris/csv ディレクトリに CSV ファイル形式で記録する。ログ ファイルに使用される命名規則は PerfMon\_<node>\_<month>\_<day>\_<year>\_<hour>\_<minute>.csv です。たとえば、PerfMon\_172.19.240.80\_06\_15\_2005\_11\_25.csv となります。ポーリング レートを指定する。このレートは、パフォーマンス データが収集され、ログに記録されるレートを示しま

す。ポーリング レートは 5 秒まで縮めることができます。デフォルトのポーリング レートは 15 秒です。

- Microsoft Windows パフォーマンス ツールを使用するか、Real-Time Monitoring Tool のパフォーマンス ログ ビューアを使用して、ログ ファイルをグラフィック形式で表示する。
- ディスクに保存するログ ファイルの最大数を指定する。この制限を超えると、最も古いログ ファイルが削除される方法でログ ファイルは自動的にページされます。デフォルトは 50 ファイルです。
- メガバイト単位の最大ファイル サイズに基づいて、ログ ファイルのロールオーバー基準を指定する。デフォルト値は 2 MB です。
- Real-Time Monitoring Tool の Trace & Log Central 機能またはコマンドライン インターフェイスを使用して、Cisco RIS Data Collector PerfMonLog ログ ファイルを収集する。

Troubleshooting perfmon データ ログ機能は、次の perfmon オブジェクト内の次のカウンタから情報を収集します。



(注) Cisco Unity Connection カウンタは、troubleshooting perfmon データ ログに記録されません。

- Database Change Notification Server オブジェクト :
  - Clients
  - CNProcessed
  - QueueDelay
  - QueuedRequestsInDB
  - QueuedRequestsInMemory
- Database Local DSN オブジェクト :
  - CcmDbSpace\_Used
  - CcmtempDbSpace\_Used
  - CNDbSpace\_Used
  - LocalDSN
  - RootDbSpace\_Used
  - SharedMemory\_Free
  - SharedMemory\_Used
- Enterprise Replication DBSpace Monitors オブジェクト :
  - ERDbSpace\_Used
  - ERSBDbSpace\_Used

- IP オブジェクト :
  - In Receives
  - In HdrErrors
  - In UnknownProtos
  - In Discards
  - In Delivers
  - Out Requests
  - Out Discards
  - Reasm Reqds
  - Reasm Oks
  - Reasm Fails
  - Frag OKs
  - Frag Fails
  - Frag Creates
  - InOut Requests
  
- Memory オブジェクト :
  - % Page Usage
  - % VM Used
  - % Mem Used
  - Buffers Kbytes
  - Cached KBytes
  - Free KBytes
  - Free Swap KBytes
  - HighFree
  - HighTotal
  - Low Total
  - Low Free
  - Page Faults Per Sec
  - Page Major Faults Per Sec
  - Pages
  - Pages Input
  - Pages Input Per Sec
  - Pages Output



- Pages Output Per Sec
- SlabCache
- SwapCached
- Shared Kbytes
- Total Kbytes
- Total Swap Kbytes
- Total VM Kbytes
- Used Kbytes
- Used Swap Kbytes
- Used VM Kbytes
  
- Network Interface オブジェクト :
  - Rx Bytes
  - Rx Packets
  - Rx Errors
  - Rx Dropped
  - Rx Multicast
  - Tx Bytes
  - Tx Packets
  - Tx Errors
  - Tx Dropped
  - Total Bytes
  - Total Packets
  - Tx QueueLen
  
- Number of Replicates Created and State of Replication オブジェクト :
  - Replicate\_State
  
- Partition オブジェクト :
  - % CPU Time
  - %Used
  - Await Read Time
  - Await Time
  - Await Write Time
  - キューの長さ (Queue Length)

- Read Bytes Per Sec
- Total Mbytes
- Used Mbytes
- Write Bytes Per Sec
  
- Process オブジェクト :
  - % Memory Usage
  - Data Stack Size
  - Nice
  - PID
  - STime
  - % CPU Time
  - Page Fault Count
  - Process Status
  - Shared Memory Size
  - VmData
  - VmRSS
  - VmSize
  - Thread Count
  - Total CPU Time Used
  
- Processor オブジェクト :
  - Irq Percentage
  - Softirq Percentage
  - IOWait Percentage
  - User Percentage
  - Nice Percentage
  - System Percentage
  - Idle Percentage
  - %CPU Time
  
- System オブジェクト :
  - Allocated FDs
  - Freed FDs
  - Being Used FDs

- Max FDs
- Total Processes
- Total Threads
- Total CPU Time
- TCP オブジェクト :
  - Active Opens
  - Passive Opens
  - Attempt Fails
  - Estab Resets
  - Curr Estab
  - In Segs
  - Out Segs
  - Retrans Segs
  - InOut Segs
- Thread オブジェクト (Troubleshooting Perfmon データ ロガーは、Cisco Unified Communications Manager スレッドのみを記録します) :
  - %CPU Time
- Cisco CallManager オブジェクト :
  - CallManagerHeartBeat
  - CallsActive
  - CallsAttempted
  - CallsCompleted
  - InitializationState
  - RegisteredHardwarePhones
  - RegisteredMGCPGateway
- Cisco SIP Stack オブジェクト :
  - CCBsAllocated
  - SCBsAllocated
  - SIPHandlerSDLQueueSignalsPresent
- Cisco CallManager System Performance オブジェクト :
  - AverageExpectedDelay

- CallsRejectedDueToThrottling
  - CodeRedEntryExit
  - CodeYellowEntryExit
  - QueueSignalsPresent 1-High
  - QueueSignalsPresent 2-Normal
  - QueueSignalsPresent 3-Low
  - QueueSignalsPresent 4-Lowest
  - QueueSignalsProcessed 1-High
  - QueueSignalsProcessed 2-Normal
  - QueueSignalsProcessed 3-Low
  - QueueSignalsProcessed 4-Lowest
  - QueueSignalsProcessed Total
  - SkinnyDevicesThrottled
  - ThrottlingSampleActivity
  - TotalCodeYellowEntry
- Cisco TFTP Server オブジェクト :
- BuildAbortCount
  - BuildCount
  - BuildDeviceCount
  - BuildDialruleCount
  - BuildDuration
  - BuildSignCount
  - BuildSoftKeyCount
  - BuildUnitCount
  - ChangeNotifications
  - DeviceChangeNotifications
  - DialruleChangeNotifications
  - EncryptCount
  - GKFoundCount
  - GKNotFoundCount
  - HeartBeat
  - HttpConnectRequests
  - HttpRequests

- HttpRequestsAborted
- HttpRequestsNotFound
- HttpRequestsOverflow
- HttpRequestsProcessed
- HttpServedFromDisk
- LDFoundCount
- LDNotFoundCount
- MaxServingCount
- Requests
- RequestsAborted
- RequestsInProgress
- RequestsNotFound
- RequestsOverflow
- RequestsProcessed
- SegmentsAcknowledged
- SegmentsFromDisk
- SegmentsSent
- SEPFFoundCount
- SEPNotFoundCount
- SIPFoundCount
- SIPNotFoundCount
- SoftkeyChangeNotifications
- UnitChangeNotifications

## Perfmon データ ログのトラブルシューティング

perfmon のデータ ログ機能を使用して perfmon オブジェクト内のカウンタから情報を収集するには、次の手順に従います。

### はじめる前に

- RISDC perfmon ログも Troubleshooting Perfmon データ ログとして知られています。RISDC perfmon ログを有効にすると、サーバは問題のトラブルシューティングに使用されるパフォーマンス データを収集します。

- RIS Data Collector (RISDC) の perfmon ログを有効にすると、Unified Communications Manager および IM and Presence Service は、サーバ上に書き込まれるログのシステムに関する情報を収集します。
- RISDC perfmon ログを有効または無効にするには、管理インターフェイスで、[システム (System)] > [サービスパラメータ (Service Parameter)] の順に選択し、[サービス (Service)] リストボックスから [Cisco RIS Data Collector] サービスを選択します。デフォルトでは、RISDC perfmon ログは有効になります。

## 手順

- ステップ 1** 管理インターフェイスで、[システム (System)] > [サービスパラメータ (Service Parameter)] の順に選択します。
- ステップ 2** [サーバ (Server)] リストボックスで、サーバを選択します。
- ステップ 3** [サービス (Service)] ドロップダウンリストボックスから [Cisco RIS Data Collector] を選択します。
- ステップ 4** 次の表の説明に従って、適切な設定を入力します。

表 16: Perfmon データロギングパラメータのトラブルシューティング

フィールド	説明
Enable Logging	ドロップダウンボックスから [True] を選択すると perfmon データロギングのトラブルシューティングが有効になり、[False] を選択すると無効になります。デフォルト値は False です。
Polling Rate	ポーリングレートの間隔 (秒単位) を入力します。5 (最小) ~ 300 (最大) の値を入力できます。デフォルト値は 15 です。
Maximum No. of Files	<p>ディスクに保存する Troubleshooting Perfmon データロギングファイルの最大数を入力します。1 (最小) ~ 100 (最大) の値を入力できます。デフォルト値は 50 です。</p> <p>[最大ファイル数 (Maximum No. of Files)] パラメータと [最大ファイルサイズ (Maximum File Size)] パラメータを設定する際は、ストレージ容量を考慮してください。[最大ファイル数 (Maximum Number of Files)] の値と [最大ファイルサイズ (Maximum File Size)] の値を掛けたときに、100 MB を超えない値にすることが推奨されます。</p> <p>ファイル数が、このフィールドに指定した最大ファイル数を超えると、タイムスタンプの最も古いログファイルが削除されます。</p> <p><b>注意</b> このパラメータを変更する前に別のコンピュータにログファイルを保存しておかないと、ログファイルが失われるおそれがあります。</p>

フィールド	説明
ファイルの最大サイズ (MB) (Maximum File Size (MB))	<p>新しいファイルが開始される前に、perfmon ログファイルに保存する最大ファイルサイズ (メガバイト単位) を入力します。1 (最小) ~ 500 (最大) の値を入力できます。デフォルト値は 2 MB です。</p> <p>[最大ファイル数 (Maximum No. of Files) ]パラメータと [最大ファイルサイズ (Maximum File Size) ]パラメータを設定する際は、ストレージ容量を考慮してください。[最大ファイル数 (Maximum Number of Files) ]の値と [最大ファイルサイズ (Maximum File Size) ]の値を掛けたときに、100 MB を超えない値にすることが推奨されます。</p>

**ステップ 5** [保存 (Save) ]を選択します。

(注) RTMT を使用してログ ファイルをダウンロードすることにより、サーバ上の Cisco RIS Data Collector サービスに関するログ ファイルを収集できます。CLI を使用してログ ファイルをダウンロードする場合は、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。ログ ファイルを収集した後は、RTMT でパフォーマンス ログ ビューアを使用するか、Microsoft Windows パフォーマンス ツールを使用してログ ファイルを表示できます。







## 第 7 章

# アラート (Alerts)

---

- [Alert Central の表示, 143 ページ](#)
- [アラートアクションのセットアップ, 150 ページ](#)
- [コア ダンプのアラートのセットアップと関連ログの収集, 156 ページ](#)

## Alert Central の表示

Unified RTMT は、事前設定されたアラートとカスタム アラートの両方を Alert Central に表示します。Unified RTMT は、該当するタブ ([システム (System) ]、[音声/ビデオ (Voice/Video) ]、[IM and Presence サービス (IM and Presence Service) ]、[Cisco Unity Connection]、[カスタム (Custom) ]) でアラートを整理します。

[Alert Central] で事前設定のアラートとカスタムアラートを有効または無効にできます。ただし、事前設定のアラートは削除できません。

## システム アラート

次に、設定済みのシステム アラートを示します。

- AuthenticationFailed
- CiscoDRFFailure
- CoreDumpFileFound
- CpuPegging
- CriticalServiceDown
- DBChangeNotifyFailure
- DBReplicationFailure
- DBReplicationTableOutOfSync
- HardwareFailure

- LogFileSearchStringFound
- LogPartitionHighWaterMarkExceeded
- LogPartitionLowWaterMarkExceeded
- LowActivePartitionAvailableDiskSpace
- LowAvailableVirtualMemory
- LowInactivePartitionAvailableDiskSpace
- LowSwapPartitionAvailableDiskSpace
- ServerDown (Unified Communications Manager クラスタに適用)
- SparePartitionHighWaterMarkExceeded
- SparePartitionLowWaterMarkExceeded
- SyslogSeverityMatchFound
- SyslogStringMatchFound
- SystemVersionMismatched
- TotalProcessesAndThreadsExceededThreshold

#### 関連トピック

[システム アラート, \(395 ページ\)](#)

## 自動トレース ダウンロードのアクティベーション

事前に設定されたアラートの中には、イベントが発生するとトレース ダウンロードを開始できるアラートがあります。次のアラートで [アラート/プロパティの設定 (Set Alert/Properties)] の [トレース ダウンロードの有効化 (Enable Trace Download)] チェックボックスをオンにすると、特定のイベントが発生したときに、トレースを自動的に取り込みます。

- **CriticalServiceDown** : CriticalServiceDown アラートは、いずれかのサービスが停止すると生成されます。CriticalServiceDown アラートは、RTMT の [重要なサービス (Critical Services)] リストに含まれるサービスだけをモニタします。




---

(注) Unified RTMT バックエンドサービスは、(デフォルトで) 30 秒ごとにステータスを検査します。サービスが停止し、その期間中に復帰した場合、CriticalServiceDown アラートは生成されない場合があります。

---

- **CodeYellow** : このアラームは、コール処理中の許容できない大幅な遅延が原因で、Cisco Unified Communications Manager がコール制御を開始したことを意味します。
- **CoreDumpFileFound** : CoreDumpFileFound アラートは、Unified RTMT バックエンド サービスが新しいコア ダンプ ファイルを検出すると生成されます。



(注) CriticalServiceDown と CoreDumpFileFound の両方のアラートを設定して、トラブルシューティング目的で、対応するトレース ファイルをダウンロードすることができます。この設定は、クラッシュしたときにトレース ファイルを維持するために役立ちます。



注意 トレース ダウンロードを有効にすると、ノードのサービスに影響を与える場合があります。多数のダウンロードを設定すると、ノードの QoS に悪影響が生じます。

## 音声およびビデオ アラート

次に、事前設定された音声およびビデオ アラートを示します。

- BeginThrottlingCallListBLFSubscriptions
- CallAttemptBlockedByPolicy
- CallProcessingNodeCpuPegging
- CARIDSEngineCritical
- CARIDSEngineFailure
- CARSchedulerJobFailed
- CDRAgentSendFileFailed
- CDRFileDeliveryFailed
- CDRHighWaterMarkExceeded
- CDRMaximumDiskSpaceExceeded
- CiscoElmNotConnected
- CiscoGraceTimeLeft
- CiscoNoProvisionTimeout
- CiscoSystemInDemo
- CiscoSystemInOverage
- CiscoSystemSecurityMismatch
- CodeYellow
- DDRBlockPrevention
- DDRDown
- EMCCFailedInLocalCluster
- EMCCFailedInRemoteCluster
- ExcessiveVoiceQualityReports

- ILSHubClusterUnreachable
- ILSPwdAuthenticationFailed
- ILSTLSAuthenticationFailed
- IMEDistributedCacheInactive
- IMEOverQuota
- IMEQualityAlert
- IMEServiceStatus
- InsufficientFallbackIdentifiers
- InvalidCredentials
- LocationOutOfResource
- MaliciousCallTrace
- MediaListExhausted
- MgepDChannelOutOfService
- NumberOfRegisteredDevicesExceeded
- NumberOfRegisteredGatewaysDecreased
- NumberOfRegisteredGatewaysIncreased
- NumberOfRegisteredMediaDevicesDecreased
- NumberOfRegisteredMediaDevicesIncreased
- NumberOfRegisteredPhonesDropped
- RecordingCallSetupFail
- RecordingGatewayRegistrationRejected
- RecordingGatewayRegistrationTimeout
- RecordingGatewaySessionFailed
- RecordingResourcesNotAvailable
- RecordingSessionTerminatedUnexpectedly
- RouteListExhausted
- RTMTSessionExceedsThreshold
- SDLLinkOutOfService
- TCPSetupToIMEFailed
- TLSConnectionToIMEFailed
- UserInputFailure

#### 関連トピック

[音声およびビデオ アラート, \(413 ページ\)](#)

## IM and Presence Service アラート

事前設定された IM and Presence Service アラートを次に示します。

- CTIGWModuleNotEnabled
- CTIGWProviderDown
- CTIGWUserNotLicenced
- CTIGWUserNotAuthorized
- CTIGWProviderFailedToOpen
- CTIGWQBFailedRequest
- CTIGWSystemError
- EspConfigAgentMemAllocError
- EspConfigAgentFileWriteError
- EspConfigAgentNetworkOutage
- EspConfigAgentNetworkRestored
- EspConfigAgentHighMemoryUtilization
- EspConfigAgentHighCPUUtilization
- EspConfigAgentLocalDBAccessError
- EspConfigAgentProxyDomainNotConfigured
- EspConfigAgentRemoteDBAccessError
- EspConfigAgentSharedMemoryStaticRouteError
- ESPConfigError
- ESPConfigNotFound
- ESPCreateLockFailed
- ESPLoginError
- ESPMallocFailure
- ESPNAPTRInvalidRecord
- ESPPassedParamInvalid
- ESPRegistryError
- ESPRoutingError
- ESPSharedMemCreateFailed
- ESPSharedMemSetPermFailed
- ESPSharedMemAllocFailed
- ESPSocketError

- ESPStopped
- ESPStatsLogFileOpenFailed
- ESPVirtualProxyError
- ESPWrongIPAddress
- ESPWrongHostName
- ICSACertificateCAsignedTrustCertFound
- ICSACertificateFingerPrintMismatch
- ICSACertificateValidationFailure
- InterclusterSyncAgentPeerDuplicate
- LegacyCUPCLogin
- NotInCucmServerListError
- PEAutoRecoveryFailed
- PEDatabaseError
- PEIDSQueryError
- PEIDSSubscribeError
- PEIDStoIMDBDatabaseSyncError
- PELoadHighWaterMark
- PEMemoryHighCondition
- PEPeerNodeFailure
- PESipSocketBindFailure
- PEStateDisabled
- PEStateLocked
- PEWebDAVInitializationFailure
- PWSSCBFindFailed
- PWSSCBInitFailed
- PWSAboveCPULimit
- PWSAboveSipSubscriptionLimit
- PWSRequestLimitReached
- SRMFailed
- SRMFailover
- SyncAgentAXLConnectionFailed
- UASCBFindFailed
- UASCBGetFailed

- XcpCmComponentConnectError
- XcpCmPauseSockets
- XcpCmStartupError
- XcpCmXmppdError
- XcpConfigMgrConfigurationFailure
- XcpConfigMgrHostNameResolutionFailed
- XcpConfigMgrJabberRestartRequired
- XcpConfigMgrR2RPasswordEncryptionFailed
- XcpConfigMgrR2RRequestTimedOut
- XcpDBConnectError
- XcpMdnsStartError
- XcpSIPFedCmComponentConnectError
- XcpSIPFedCmStartupError
- XcpSIPGWStackResourceError
- XcpThirdPartyComplianceConnectError
- XcpTxtConfComponentConfigError
- XcpTxtConfDBConnectError
- XcpTxtConfDBQueueSizeLimitError
- XcpTxtConfGearError
- XcpWebCmComponentConnectError
- XcpWebCmHttpdError
- XcpWebCmStartupError
- XcpXMPPFedCmComponentConnectError
- XcpXMPPFedCmStartupError

#### 関連トピック

[IM and Presence Service アラート](#), (455 ページ)

## Cisco Unity Connection アラート

次のリストに、事前設定された Cisco Unity Connection アラートを示します。

- NoConnectionToPeer
- AutoFailoverSucceeded
- AutoFailoverFailed

- AutoFailbackSucceeded
- AutoFailbackFailed
- SbrFailed (スプリットブレイン解決の失敗)
- DiskConsumptionCloseToCapacityThreshold
- DiskConsumptionExceedsCapacityThreshold
- LicenseExpirationWarning
- LicenseExpired



(注) 最初の 6 つのアラートは、Cisco Unity Connection クラスタ設定にのみ適用されます。

#### 関連トピック

[Cisco Unity Connection アラート](#), (494 ページ)

## アラートアクションのセットアップ

RTMT では、生成されたすべてのアラートに対してアラートアクションを設定し、そのアラートアクションをアラートアクションリストで指定した電子メール受信者に送信することができます。

次の表に、アラートアクションの設定に使用するフィールドのリストを示します。特に記載がない限り、すべてのフィールドを設定できます。

表 17: アラートアクションの設定

フィールド	説明	コメント
アラートアクション ID (Alert Action ID)	実行するアラートアクションの ID	説明的な名前を指定します。
メール受信者 (Mail Recipients)	電子メールアドレスのリスト。リスト内の個別の電子メールを選択的に有効または無効にできます。	—



## Alert Central へのアクセスとアラートのセットアップ

次の手順を使用して、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、または削除、アラートのクリア、またはアラートの詳細の表示などのタスクを実行できます。

### 手順

- ステップ 1** 次のいずれかの作業を実行します。
- クイック起動チャンネルで、次の操作を実行します。
    - [システム (System)] をクリックします。
    - ツリー階層で [ツール (Tools)] をダブルクリックします。
    - [Alert Central] アイコンをクリックします。
  - [システム (System)] > [ツール (Tools)] > [アラート (Alert)] > [Alert Central] の順に選択します。  
[Alert Central モニタリング (Alert Central monitoring)] ウィンドウが表示され、システムで生成されたアラートのアラートステータスおよびアラート履歴を示します。
- ステップ 2** 次のいずれかの作業を実行します。
- アラートプロパティを設定します。
  - アラートを一時停止します。
  - アラート通知の電子メールを設定します。
  - アラートアクションを設定します。
  - [アラートステータス (Alert Status)] ペイン内のアラート情報をソートします。カラムの見出しに表示される上/下矢印をクリックします。  
たとえば、[有効 (Enabled)] または [安全範囲内 (In Safe Range)] カラムに表示される上/下矢印をクリックします。  
[アラート履歴 (Alert History)] ペインでカラムの上/下矢印をクリックして、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、[アラート履歴 (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、次のいずれかのタスクを実行します。
    - [アラートステータス (Alert Status)] ウィンドウで、アラートを右クリックし、目的に応じて [アラートの無効化/有効化 (Disable/Enable Alert)] (オプションが切り替わります) または [アラートの削除 (Remove Alert)] を選択します。
    - [アラートステータス (Alert Status)] ウィンドウでアラートを強調表示し、[システム (System)] > [ツール (Tools)] > [アラート (Alert)] > [アラートの無効化/有効化 (または削除) (Disable/Enable (or Remove) Alert)] の順に選択します。

ヒント RTMT からユーザ定義のアラートだけを削除できます。事前設定のアラートを選択すると、[アラートの削除 (Remove Alert)] オプションはグレー表示されます。

g) アラートが解決された後にそれらを個別にまたはまとめてクリアするには、次のいずれかのタスクを実行します。

- [アラートステータス (Alert Status)] ウィンドウの表示後、アラートを右クリックして [アラートのクリア (Clear Alerts)] (または [すべてのアラートをクリア (Clear All Alerts)]) を選択します。
- [アラートステータス (Alert Status)] ウィンドウでアラートを強調表示し、[システム (System)] > [ツール (Tools)] > [アラート (Alert)] > [アラートのクリア (Clear Alerts)] (または [すべてのアラートをクリア (Clear All Alerts)]) の順に選択します。

アラートをクリアしたら、アラートは赤から黒に変更されます。

h) アラートをデフォルト設定にリセットするには、次のいずれかの手順を実行します。

- [アラートステータス (Alert Status)] ウィンドウの表示後、アラートを右クリックし、[アラートをデフォルト設定にリセット (Reset Alert to Default Config)] を選択して、そのアラートをデフォルト設定にリセットします。
- [システム (System)] > [ツール (Tools)] > [アラート (Alert)] > [すべてのアラートをデフォルト設定にリセット (Reset all Alerts to Default Config)] の順に選択し、すべてのアラートをデフォルト設定にリセットします。

i) アラートの詳細を表示するには、次のいずれかの手順を実行します。

- [アラートステータス (Alert Status)] ウィンドウの表示後、アラートを右クリックして [アラートの詳細 (Alert Details)] を選択します。
- [アラートステータス (Alert Status)] ウィンドウでアラートを強調表示し、[システム (System)] > [ツール (Tools)] > [アラート (Alert)] > [アラートの詳細 (Alert Details)] の順に選択します。

ヒント アラートの詳細の表示が完了したら、[OK] をクリックします。

## アラートプロパティの設定

アプリケーションは、アラート通知機能を使用してシステムの問題を通知します。システムパフォーマンスカウンタのアラート通知をアクティブにするには、次の設定が必要です。

[RTMT Perfmon モニタリング (RTMT Perfmon Monitoring)] ペインで、システムの perfmon カウンタを選択し、次のアクションを実行します。

- アラート通知の電子メールまたはメッセージのポップアップウィンドウをセットアップします。

- アラートのしきい値を設定します。
- アラート通知の頻度を決定します（アラートが1回発生、1時間ごとに発生など）。
- アラートがアクティブになるスケジュールを決定します（毎日、または1日の特定の時刻など）。



## 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、[アラートの削除 (Remove Alert) ]を選択します。オプションは、アラートを削除するとグレー表示されます。

## 手順

**ステップ 1** 次のいずれかの操作を実行します。

目的	Action
パフォーマンスカウンタのアラートプロパティを設定する	<ul style="list-style-type: none"> <li>• パフォーマンスカウンタを表示します。</li> <li>• カウンタのチャートまたは表から、アラート通知を設定するカウンタを右クリックし、[アラート/プロパティの設定 (Set Alert/Properties) ]を選択します。</li> <li>• [アラートの有効化 (Enable Alert) ]チェックボックスをオンにします。</li> </ul>
Alert Central からアラートプロパティを設定する	<ul style="list-style-type: none"> <li>• [Alert Central] にアクセスします。</li> <li>• アラートプロパティを設定するアラートを選択します。次のいずれかの操作を実行します。 <ul style="list-style-type: none"> <li>◦ アラートを右クリックし、[アラート/プロパティの設定 (Set Alert/Properties) ]を選択します。</li> <li>◦ [システム (System) ]&gt;[ツール (Tools) ]&gt;[アラート (Alert) ]&gt;[アラート/プロパティの設定 (Set Alert/Properties) ]の順に選択します。</li> <li>◦ [アラートの有効化 (Enable Alert) ]チェックボックスをオンにします。</li> </ul> </li> </ul>

- ステップ 2** [重大度 (Severity) ] リストチェックボックスで、通知の対象となる重大度レベルを選択します。
- ステップ 3** [説明 (Description) ] ペインにアラートの説明を入力します。
- ステップ 4** [次へ (Next) ] を選択します。
- ステップ 5** [しきい値 (Threshold) ]、[次の値で算出 (Value Calculated As) ]、[期間 (Duration) ]、[頻度 (Frequency) ]、および [スケジュール (Schedule) ] ペインで設定値を設定します。

表 18: カウンタのアラート設定パラメータ

設定	説明
[しきい値 (Threshold) ] ペイン	
次の条件 ([以上 (Over) ]、[以下 (Under) ]) が満たされたときにアラートをトリガーする	<p>オンにして適用する値を入力します。</p> <ul style="list-style-type: none"> <li>• 以上 (Over) : アラート通知がアクティブになる前に一致する必要がある最大しきい値を設定する場合にオンにします。[以上 (Over) ] の値フィールドには、値を入力します。たとえば、進行中のコールの数と等しい値を入力します。</li> <li>• 以下 (Under) : アラート通知がアクティブになる前に一致する必要がある最小しきい値を設定する場合にオンにします。[以下 (Under) ] の値フィールドには、値を入力します。たとえば、進行中のコールの数と等しい値を入力します。</li> </ul> <p><b>ヒント</b> これらのチェックボックスは、[頻度 (Frequency) ] および [スケジュール (Schedule) ] の設定パラメータと組み合わせて使用します。</p>
[次の値で算出 (Value Calculated As) ] ペイン	
[絶対値 (Absolute) ]、[差分 (Delta) ]、[差分比率 (Delta Percentage) ]	<p>適用するオプション ボタンを選択します。</p> <ul style="list-style-type: none"> <li>• 絶対値 (Absolute) : 一部のカウンタ値は累積されるため、データの現在のステータスを表示する場合に選択します。</li> <li>• 差分 (Delta) : 現在のカウンタ値と前回のカウンタ値の差分を表示する場合に選択します。</li> <li>• 差分比率 (Delta Percentage) : カウンタ パフォーマンスの変化を比率で表示する場合に選択します。</li> </ul>
[期限 (Duration) ] ペイン	

設定	説明
<p>[値が常に次の場合にアラートをトリガー (Trigger alert only when value constantly...)]、[アラートをすぐにトリガー (Trigger alert immediately)]</p>	<ul style="list-style-type: none"> <li>• 値が常に次の場合にアラートをトリガー (Trigger alert only when value constantly...) : 指定した秒数にわたって値が常にしきい値の下限または上限を超えた場合に限りアラート通知を送信する場合は、このオプションボタンを選択して、アラートを送信するまでの秒数を入力します。</li> <li>• アラートをすぐにトリガー (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選択します。</li> </ul>
[頻度 (Frequency)] ペイン	
<p>[各ポーリングでアラートをトリガー (Trigger alert on every poll)]、[トリガーの間隔 (trigger up to...)]</p>	<p>適用するオプション ボタンを選択します。</p> <ul style="list-style-type: none"> <li>• 各ポーリングでアラートをトリガー (Trigger alert on every poll) : 各ポーリングでしきい値条件が一致したとき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 ボタンを選択します。</li> <li>• トリガーの間隔 (trigger up to...) : アラート通知を一定間隔でアクティブにする場合は、このオプション ボタンを選択して、送信するアラートの数とアラートを送信する時間 (分) を入力します。</li> </ul>
[スケジュール (Schedule)] ペイン	
<p>[24 時間毎日 (24-hours daily)]、[開始/停止 (Start/Stop)]</p>	<p>適用するオプション ボタンを選択します。</p> <ul style="list-style-type: none"> <li>• 24 時間毎日 (24-hours daily) : アラートを 1 日 24 時間トリガーする場合は、このオプション ボタンを選択します。</li> <li>• 開始/停止 (Start/Stop) : アラート通知を特定のタイム フレームでアクティブにする場合は、このオプション ボタンを選択し、開始時刻と停止時刻を入力します。オンになっている場合は、日次タスクの開始時間と停止時間を入力します。たとえば、カウンタを毎日午前 9 時から午後 5 時まで、または午後 9 時から午前 9 時までチェックするように設定することができます。</li> </ul>

## アラートの一時停止

一部またはすべてのアラートを一時的に停止する場合があります。特定のノードまたはクラスタ全体でアラートを一時停止することができます。たとえば、新しいリリースにシステムをアップグレードする場合、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いように、アップグレードが完了するまでアラートを一時停止します。

Alert Central でアラートを一時停止するには、次の手順に従ってください。

### 手順

- 
- ステップ 1** [システム (System)] > [ツール (Tools)] > [アラート (Alert)] > [クラスタ/ノードのアラートの一時停止 (Suspend cluster/Node Alerts)] の順に選択します。
- (注) ノードごとの一時停止状態は、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** 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アラートを一時停止するには、[クラスタ全体 (Cluster Wide)] オプションボタンをクリックして、[すべてのアラートを一時停止 (Suspend all alerts)] チェックボックスをオンにします。
  - サーバごとにアラートを一時停止するには、[サーバごと (Per Server)] オプションボタンをクリックし、アラートを一時停止するサーバごとに [一時停止 (Suspend)] チェックボックスをオンにします。
- ステップ 3** [OK] をクリックします。
- (注) アラートを再開するには、[アラート (Alert)] > [クラスタ/ノードのアラートの一時停止 (Suspend cluster/Node Alerts)] の順に選択して一時停止のチェックボックスをオフにします。
- 

## コアダンプのアラートのセットアップと関連ログの収集

コアダンプは再現が難しい場合があるため、コアダンプが発生してから上書きされる前に、関連するログファイルを収集することが特に重要です。

コアダンプの発生時にはすぐに通知を受け取ってトラブルシューティングを支援できるように、コアダンプに関する電子メールアラートをセットアップします。

## 電子メール アラートの有効化

### 手順

- ステップ 1 [システム (System) ]>[ツール (Tools) ]>[Alert Central] の順に選択します。
- ステップ 2 [CoreDumpFileFound]アラートを右クリックし、[アラート/プロパティの設定 (Set Alert/Properties) ]を選択します。
- ステップ 3 [電子メールの有効化 (Enable Email) ]チェックボックスをオンにするなど、ウィザードに従って必要な基準を設定します。
- ステップ 4 [システム (System) ]>[ツール (Tools) ]>[アラート (Alert) ]>[電子メールサーバの設定 (Config Email Server) ] の順に選択します。
- ステップ 5 電子メール サーバの設定を入力します。

## ログの収集

電子メール アラートの受信後にログを収集するには、次の手順に従います。

### 手順

- ステップ 1 アラートを発信したサービスを確認します。電子メールメッセージ内では“Core”で示されます。
- ステップ 2 [ツール (Tools) ]>[Trace & Log Central]>[ファイルの収集 (Collect Files) ] の順に選択し、影響を受けるすべてのサービスの関連ログを選択します。  
たとえば、サービスが Cisco Presence Engine の場合は、Cisco Presence Engine、Cisco XCP Router および Cisco XCP Connection Manager のログを収集します。または、サービスが Cisco XCP Router の場合は、Cisco XCP Router と、Cisco XCP Connection Manager および Cisco Presence Engine のログを収集します。
- ステップ 3 CLI から次のコマンドを実行して、スタック トレースを生成します。  
**utils core active list**  
**utils core active analyze core filename**
- ステップ 4 [ツール (Tools) ]>[Trace & Log Central]>[ファイルの収集 (Collect Files) ] の順に選択し、[RIS Data Collector PerfMon ログ (RIS Data Collector PerfMon Log) ] を選択します。
- ステップ 5 [ツール (Tools) ]>[Syslog ビューア (SysLog Viewer) ] の順に選択してシステム ログを収集します。
  - a) ノードを選択します。
  - b) [システム ログ (System Logs) ]>[メッセージ (messages) ] の順にクリックして、メッセージを表示し、保存します。

- c) [アプリケーションログ (Application Logs) ]>[CiscoSyslog] をクリックして、ログファイルを表示し、保存します。

**ステップ 6** 収集したファイルをシスコのテクニカル サポート ケースに添付します。

---





## 第 8 章

# トレースとログ

---

- [Trace and Log Central](#), 159 ページ
- [ログビューア](#), 213 ページ
- [プラグイン](#), 217 ページ

## Trace and Log Central



---

(注) Trace and Log Central を動作させるには、クライアントマシンのクラスタ内にあるすべてのノードで DNS ルックアップを解決する必要があります。

---

## 準備 (Preparation)

### 証明書のインポート

ノードの証明書をインポートするには、次の手順に従ってください。

ノード、またはクラスタ内の各ノード用に認証局が発行するサーバ認証証明書をインポートできます。

Trace and Log Central オプションを使用する前に、証明書をインポートしておくことを推奨します。証明書をインポートしていないと、Unified RTMT にサインインして Trace and Log Central オプションにアクセスするたびに、ノードのセキュリティ証明書が表示されます。その証明書に表示される情報を変更することはできません。

## 手順

- 
- ステップ 1** 証明書をインポートするには、[ツール (Tools)] > [トレース (Trace)] > [証明書のインポート (Import Certificate)] の順に選択します。  
システムがノード証明書をインポートしたことを示すメッセージが表示されます。
- ステップ 2** [OK] をクリックします。
- 

## トレースのサポートの種類

ここでは、トレースのサポートの種類について説明します。

### Trace & Log Central におけるディスク I/O と CPU 制御

Unified RTMT は、[Trace & Log Central] の重要な操作とジョブの制御をサポートしています。その操作とジョブがオンデマンドで実行されているのか、スケジュールされているのか、または自動なのかは問いません。

ノードが高い IO 条件で実行している場合にオンデマンド操作の要求を行うと、操作のキャンセルを示す警告が表示されます。警告の表示タイミングを制御する IO レートのしきい値は、次のサービスパラメータ (Cisco RIS Data Collector サービス) で設定できることに注意してください。

- TLC Throttling CPU Goal
- TLC Throttling IOWait Goal

これらのパラメータの値は、実際のシステム CPU および IOWait 値と比較されます。目標 (サービスパラメータの値) が実際の値より小さい場合は、警告が表示されます。

### トレース圧縮サポート

この機能により、ROS (Recoverable Outstream) ライブラリでトレース ファイルの圧縮出力がサポートされます。システムは、ファイルが生成されるときにそのファイルを圧縮します。トレース ファイルの圧縮の適用には次の利点があります。

- トレース ファイルの保存に必要な容量の削減。
- ディスク ヘッドの移動が減少することによるコール負荷の大幅な改善。これにより、トレース ファイルの要求が原因で CPU がブロックされることがなくなります。

エンタープライズパラメータ Trace Compression を使用して、トレース圧縮の有効化または無効化を行います。このパラメータのデフォルト値では、[無効化 (Disabled)] が指定されます。

圧縮ファイルには .gz 拡張子が付きます (ファイルがまだ書き込み中の場合は .gzo)。圧縮ファイルを開くには、そのファイル名をダブルクリックします。拡張子にビューアが関連付けられてい

る場合、そのビューアでファイルが開きます。拡張子にビューアが関連付けられていない場合、[プログラムから開く (Open With)] ダイアログボックスが表示されます。使用するビューアを選択し、[この種類のファイルを開くときは、選択したプログラムをいつも使う (Always use this program)] をオンにして、次回からはこのビューア選択プロセスが省略されるようになります。

## [Trace & Log Central] オプションの表示

Unified RTMT の [Trace & Log Central] オプションを表示するには、次の手順に従ってください。



(注) ツリー階層に表示されている任意のオプションから、トレースするサービスやアプリケーションの指定、使用するログとサーバの指定、収集日時のスケジューリング、ファイルをダウンロードする機能の設定、zip ファイルの設定、収集されたトレース ファイルの削除を実行できます。



(注) 暗号化をサポートするデバイスでは、SRTP キー情報はトレース ファイルに出力されません。

### はじめる前に

開始する前に、セキュリティ証明書をインポートします。

### 手順

- ステップ 1** 次のいずれかの操作を実行して、Trace and Log Central にアクセスします。
- クイック起動チャンネル内の [システム (System)] を選択します。
  - [システム (System)] > [ツール (Tools)] > [トレース (Trace)] > [Trace & Log Central] の順に選択します。
  - ツリー階層で [Trace & Log Central] アイコンを選択します。
- ステップ 2** Real-Time Monitoring Tool の Trace and Log Central オプションが表示されたら、次のいずれかの作業を実行します。
- クラスタ内の 1 台以上のサーバに対し、サービス、アプリケーション、およびシステム ログのトレースを収集します。
  - 指定した検索条件が含まれているトレースファイルを収集し、ダウンロードします。それと同時に、後で使用するためにトレース収集条件を保存します。
  - ネットワーク上の 1 台以上のサーバに対してクラッシュ ダンプ ファイルを収集します。
  - 収集したトレース ファイルを表示します。
  - サーバ上のすべてのトレース ファイルを表示します。

- アプリケーションごとにサーバ上で書き込みが行われている現在のトレースファイルを表示します。検索文字列がトレースファイル内で見つかったときに、指定した操作を実行できます。

## ファイルの収集

### トレース ファイルの収集

クラスタ内の 1 台以上のノードに対してサービス、アプリケーション、システム ログのトレースを収集するには、Trace & Log Central の [ファイルの収集 (Collect Files)] オプションを使用します。トレースを収集する日時の範囲、トレース ファイルをダウンロードするディレクトリ、収集されたファイルをサーバから削除するかどうかを指定します。

Trace and Log Central 機能を使用してトレースを収集するには、次の手順に従ってください。



- (注) サービスは、アクティブにされていなくても表示されます。したがって、それらのサービスに対してトレースを収集できます。

指定した検索条件を含んでいるトレースファイルを収集するか、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、クエリー ウィザードを使用します。

#### はじめる前に

次の 1 つまたは複数の操作を実行します。

- さまざまなサービス用のトレースファイルに含める情報を、Cisco Unified Serviceability の [トレース設定 (Trace Configuration)] ウィンドウから設定します。詳細については、『*Cisco Unified Serviceability Administration Guide*』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には、アラームの送信先として SDI または SDL トレース ファイルを Cisco Unified Serviceability の [アラーム設定 (Alarm Configuration)] ウィンドウで選択します。詳細については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。
- TLC Throttling CPU Goal サービス パラメータと TLC Throttling IOWait Goal サービス パラメータ (Cisco RIS Data Collector サービス) の値を設定することで、重要な Trace and Log Central の操作とジョブの調整を設定できます。サービス パラメータの設定の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

## 手順

- ステップ 1** [Trace and Log Central] オプションを開きます。
- ステップ 2** [Trace & Log Central] のツリー階層で、[ファイルを収集する (Collect Files)] をダブルクリックします。  
[トレース収集 (Trace Collection)] ウィザードが表示されます。サービスは、アクティブにされていなくても表示されます。したがって、それらのサービスに対してトレースを収集できます。
- (注) Unified Communications Manager および Cisco Unity Connection クラスタ：クラスタ内のすべてのノードが使用できない場合、どのノードが利用できないかを示すメッセージとともにダイアログ ボックスが表示されます。使用不可能なノードは、[Trace and Log Central] ウィンドウに表示されません。
- (注) Unified Communications Manager および Cisco Unity Connection クラスタ：クラスタ内の特定のノードでだけリストされたサービス/アプリケーションの一部をインストールできます。それら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には、そのサービスまたはアプリケーションがアクティブにされているサーバからトレースを選択します。
- ステップ 3** *Cisco Unity Connection* ユーザはステップ 4 に進みます。Unified Communications Manager または Cisco Business Edition の場合、[CCM サービス/アプリケーションの選択 (Select CCM Services/Application)] タブで次のいずれかの操作を実行します。
- a) クラスタ内のすべてのノードに対してすべてのサービスとアプリケーションのトレースを収集するには、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers)] チェックボックスをオンにして [次へ (Next)] をクリックします。
- (注) スタンドアロン ノードがあり、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers)] チェックボックスがオンの場合、システムは、スタンドアロン ノードのすべてのサービスとアプリケーションのトレースを収集します。
- b) 特定のノード上のすべてのサービスとアプリケーション (または *Cisco Unity Connection* の場合 ノード上の特定のシステムログ) のトレースを収集するには、ノードの横にあるチェックボックスをオンにして [次へ (Next)] をクリックします。
- c) 特定のノード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には、適用するチェックボックスをオンにして、[次へ (Next)] をクリックします。
- d) サービスまたはアプリケーションのトレースを収集しないで次のタブに進むには、[次へ (Next)] をクリックします。  
Cisco Business Edition の場合はステップ 4 に進み、Unified Communications Manager の場合はステップ 5 に進みます。
- ステップ 4** [CUC サービス/アプリケーションの選択 (Select CUC Services/Application)] タブで、次のいずれかのタスクを実行します。
- a) ノードのすべてのシステム ログを収集するには、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers)] チェックボックスをオンにするか、ノードの横にあるチェックボックスをオンにして、[次へ (Next)] をクリックします。

- b) ノード上の特定のシステムログのトレースを収集するには、適用するチェックボックスをオンにして、[次へ (Next) ]をクリックします。
- c) システムログのトレースを収集しないで次のタブに進むには、[次へ (Next) ]をクリックします。

**ステップ 5** [システム サービス/アプリケーションの選択 (Select System Services/Application) ] タブで、次のいずれかのタスクを実行します。

- a) クラスタ内のすべてのノードに対してすべてのシステム ログを収集するには、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers) ] チェックボックスをオンにして [次へ (Next) ] をクリックします。  
(注) スタンドアロン ノードがあり、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers) ] チェックボックスがオンの場合、システムは、スタンドアロン ノードのトレースを収集します。
- b) 特定ノード上のすべてのシステムログのトレースを収集するには、ノードの横にあるチェックボックスをオンにして、[次へ (Next) ] をクリックします。
- c) 特定のノード上の特定のシステムログのトレースを収集するには、適用するチェックボックスをオンにして、[次へ (Next) ] をクリックします。
- d) システムログのトレースを収集しないでトレース収集ウィザードを続行するには、[次へ (Next) ] をクリックします。

**ステップ 6** [収集時間 (Collection Time) ] ペインで、トレースを収集する期間を指定します。次のいずれかのオプションを選択します。

- a) 絶対範囲 (Absolute Range) : トレースの収集範囲をノードタイムゾーンと時間範囲 (開始と終了の日時) で指定します。  
クライアントコンピュータのタイムゾーンにより、[リファレンスサーバ時間帯の選択 (Select Reference Server Time Zone) ] フィールドのデフォルトが設定されます。すべての標準タイムゾーンが [タイムゾーンを選択 (Select Time Zone) ] ドロップダウンリストボックスに表示され、[サマータイム (Daylight Saving) ] が設定されたタイムゾーン用に独立した一連のエントリも表示されます。

Trace and Log Central は、[選択したリファレンスサーバタイムゾーン (Selected Reference Server Time Zone) ] に基づいて、時間範囲内のファイルをダウンロードします。クラスタ内のノードが異なるタイムゾーン内に属している場合、TLC は時刻変更を調整し、同じ期間のファイルを取得します。たとえば、午前 9:00 ~ 午前 10:00 のファイルを指定し、2 番目のノード (node x) が時刻が 1 時間進んでいるタイムゾーンに属している場合、TLC は node x から午前 10:00 ~ 午前 11:00 のファイルをダウンロードします。

トレースを収集する日付範囲を設定するには、[開始日/時間 (From Date/Time) ] フィールドと [終了日/時間 (To Date/Time) ] フィールドのドロップダウンリストボックスを選択します。

- b) 相対範囲 (Relative Range) : トレースの収集範囲を現在時刻までの時間 (分数、時間数、日数、週数、または月数) で指定します。

(注) Unified RTMT はウィザードによる設定とは異なるタイムスタンプのログを返しません。これは特に、指定されたタイムスタンプが既存のログファイルのタイムスタンプより小さい場合に発生します。

ノード上に特定のサービスのログファイルが 11/24/09 から存在し、11/23/09 5:50 から 11/23/09 7:50 までの時間範囲を指定すると、それでも Unified RTMT は既存のログファイルを返します。

**ステップ 7** [ファイルのダウンロード (Download File)] オプショングループボックスで、トレースのダウンロードに使用するオプションを指定します。[パーティションの選択 (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ログが含まれているパーティションを選択します。

Cisco Unified Serviceability は、ユーザがログイン中のアプリケーションのバージョンについてはログをアクティブパーティションに保存し、その他のバージョン (インストールされている場合) についてはログを非アクティブディレクトリに保存します。

つまり、アプライアンスノード上で実行している、Cisco Unified Communications Manager、Cisco Business Edition 5000、または Cisco Unity Connection のバージョンを別のバージョンにアップグレードし、ノードを新しいバージョンで再起動すると、Cisco Unified Serviceability は以前のバージョンのログを非アクティブ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パーティションに保存します。古いバージョンに再度ログインした場合、Cisco Unified Serviceability は新しいバージョンのログを非アクティブ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ディレクトリに保存します。

(注) Cisco Unified Serviceability は、Windows プラットフォームで実行する Cisco Unified Communications Manager または Cisco Unity Connection バージョンのログを保持しません。

**ステップ 8** トレースファイルのダウンロード先のディレクトリを指定するには、[ファイルディレクトリのダウンロード (Download File Directory)] フィールドの横にある [参照 (Browse)] ボタンをクリックし、ディレクトリに移動し、[開く (Open)] をクリックします。デフォルトは <rtmt\_users\_directory>\<server name または server IP address>\<download time> です。

**ステップ 9** 収集したトレースファイルの zip ファイルを作成するには、[ファイルを zip 圧縮する (Zip File)] オプションボタンを選択します。ファイルの zip 圧縮なしでトレースファイルをダウンロードするには、[ファイルを zip 圧縮しない (Do Not Zip Files)] オプションボタンを選択します。

**ステップ 10** 収集したログファイルをノードから削除するには、[収集されたログファイルをサーバから削除する (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 11** [終了 (Finish)] をクリックするか、または設定を中止するには、[キャンセル (Cancel)] をクリックします。

[終了 (Finish)] をクリックした場合、ウィンドウにトレース収集の進捗状況が表示されます。

トレース収集プロセスが完了すると、“ノード<サーバ名または IP アドレス>に対するダウンロードが完了しました (Completed downloading for node <Server name or IP address>)” というメッセージがウィンドウの下部に表示されます。

**ステップ 12** 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ローカルブラウザオプションを使用します。

- (注) サービス パラメータの値を超えた場合、またはシステムが **Code Yellow** 状態の場合、メッセージが表示されます。
- 

## クエリー ウィザード

Trace Collection クエリー ウィザードを使用すると、指定した検索条件が含まれているトレース ファイルを収集し、ダウンロードできます。同時に、後で使用するためにトレース収集条件を保存できます。Trace Collection クエリー ウィザードを使用するには、プロシージャを実行してクエリーを開始し、クエリーを実行します。

### はじめる前に

- さまざまなサービス用のトレース ファイルに含める情報を、[トレース設定 (Trace Configuration) ] ウィンドウから設定します。
- アラームをトレース ファイルに送信するには、アラームの送信先として SDI トレース ファイルを [アラーム設定 (Alarm Configuration) ] ウィンドウで選択します。

## クエリーの開始

### 手順

---

- ステップ 1** Trace & Log Central を開きます。
- ステップ 2** ツリー階層で [クエリー ウィザード (Query Wizard) ] をダブルクリックします。
- ステップ 3** 次のいずれかの操作を実行します。



目的	操作	結果
保存されているクエリーを実行する	<ul style="list-style-type: none"> <li>• [保存クエリー (Saved Query) ] を選択します。</li> <li>• [参照 (Browse) ] を選択して、使用するクエリーがある場所に移動します。</li> <li>• クエリーを選択し、[開く (Open) ] を選択します。</li> </ul>	<ul style="list-style-type: none"> <li>• 単一ノード汎用クエリーを選択すると、[参照 (Browse) ] の隣に RTMT の接続先ノードがチェックマークを付けて表示されます。このクエリーを他のノードに対しても実行する場合は、それらのサーバの隣にチェックマークを付けます。</li> <li>• All Node Generic Query を選択した場合、すべてのノードで [参照 (Browse) ] の横にチェックマークが表示されます。クエリーを実行しないサーバをオフにすることができます。</li> <li>• 通常クエリーを選択すると、そのクエリーの保存時に選択したすべてのノードが、チェックマークを付けて表示されます。リスト内の任意のサーバをオンまたはオフにすることができます。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。</li> </ul>
クエリーを作成する	[クエリーの作成 (Create Query) ] を選択します。	
修正せずにクエリーを実行する	<ul style="list-style-type: none"> <li>• [クエリーの実行 (Run Query) ] を選択します。</li> <li>• “スケジュールの実行”のステップを実行します。</li> </ul>	
クエリーを修正する	ステップ 4 に進みます。	

**ステップ 4** [次へ (Next) ] を選択します。

**ステップ 5** 次のいずれかの操作を実行します。

- [保存クエリー (Saved Query) ] を選択してクエリーを選択した場合は、クエリーに指定してい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サービスとアプリケーションのリストを修正します。
- [クエリーの作成 (Create Query) ] を選択した場合は、トレースを収集するすべてのサービスとアプリケーションを選択する必要があります。

**ステップ 6** [次へ (Next) ] を選択します。

**ステップ 7** 次のいずれかの操作を実行します。

目的	Action
クラスタ内のすべてのサーバに対して特定またはすべてのシステム ログのトレースを収集する	<ul style="list-style-type: none"> <li>• 適用するトレースをオンにします。</li> <li>• [すべてのサーバ上のすべてのサービスを選択する (Select All Services on All Servers) ] をオンにします。</li> <li>• [次へ (Next) ] を選択します。</li> </ul>
クラスタ内のすべてのサーバに対してすべてのサービスとアプリケーションのトレースを収集する	<ul style="list-style-type: none"> <li>• [すべてのサーバ上のすべてのサービスを選択する (Select All Services on All Servers) ] をオンにします。</li> <li>• [次へ (Next) ] を選択します。</li> </ul>
特定のサーバ上のすべてのサービスとアプリケーションのトレースを収集する	<ul style="list-style-type: none"> <li>• サーバ名を確認します。</li> <li>• [次へ (Next) ] を選択します。</li> </ul>

**ステップ 8** トレースを収集する時間範囲を指定するには、次のいずれかの手順を実行します。

目的	Action
選択したサービスに対して、サーバ上のすべてのトレースを収集する	[使用可能なすべてのトレース (All Available Traces) ] を選択します。
絶対的な日付と時刻の範囲内のすべてのトレースを収集する	<ul style="list-style-type: none"> <li>• [絶対範囲 (Absolute Range) ] を選択します。</li> <li>• トレースの収集範囲をサーバタイムゾーンと時間範囲 (開始と終了の日時) で指定します。</li> </ul>

目的	Action
相対的な日付と時刻の範囲内のすべてのトレースを収集する	<ul style="list-style-type: none"> <li>• [相対範囲 (Relative Range)] を選択します。</li> <li>• トレースの収集範囲を現在時刻までの時間 (分数、時間数、日数、週数、または月数) で指定します。</li> </ul>

**ステップ 9** 単語または句を [検索文字列 (Search String)] フィールドに入力して、トレース ファイル内に存在する句または単語を検索します。このツールでは、入力した単語または句に対して完全に一致するものが検索されます。

### 次の作業

クエリーを実行します。

### クエリーの実行

- クラスタ内のすべてのノードが使用できない場合、どのノードが利用できないかを示すメッセージとともにダイアログ ボックスが表示されます。使用不可能なノードは、[Trace & Log Central] ウィンドウに表示されません。
- 一部の閲覧されているサービスまたはアプリケーションをクラスタ内の特定のノード上にだけインストールすることができます。それら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には、そのサービスまたはアプリケーションがアクティブにされているノードからトレースを収集するようにします。
- サービスは、アクティブにされていなくても表示されます。したがって、それらのサービスに対してトレースを収集できます。
- トレース ファイルのダウンロードが完了したら、Trace and Log Central 機能のローカルブラウザ オプションを使用してそれらを表示できます。
- サービス パラメータの値を超過するか、システムが Code Yellow 状態になると、エラーメッセージが表示されます。

### 手順

- ステップ 1** [クエリーの実行 (Run Query)] を選択してクエリーを実行します。
- ステップ 2** [クエリーの保存 (Save Query)] を選択してクエリーを保存し、次のステップに進みます。
- ステップ 3** クエリー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たら、[OK] を選択します。
- ステップ 4** 次の操作を実行します。

目的	操作	結果
他のノード上で実行可能なクエリーを作成する	<ol style="list-style-type: none"> <li>1 [汎用クエリー (Generic Query) ] を選択します。</li> <li>2 [単一ノードクエリー (Single Node Query) ] または [全ノードクエリー (All Node Query) ] を選択します。</li> <li>3 [完了 (Finish) ] を選択します。</li> </ol>	<ul style="list-style-type: none"> <li>• 選択するサービスが単一ノード上にある場合のみ汎用クエリーを作成できます。複数のノード上のサービスを選択した場合は、メッセージが表示されます。通常クエリーとしてクエリを保存するか、単一ノード上のサービスを選択することができます。</li> <li>• [単一ノードクエリー (Single Node Query) ] を選択した場合、そのクエリーを実行すると、そのクエリーを作成したノードがトレース収集ツールによってデフォルトで選択されます。</li> <li>• [全ノードクエリー (All Node Query) ] オプションを選択した場合、そのクエリーを実行するとき、クラスタ内のすべてのサーバがトレース収集ツールによってデフォルトで選択されます。</li> </ul>
クエリーを作成したノードまたはクラスタでクエリを実行する	<ol style="list-style-type: none"> <li>1 [通常クエリー (Regular Query) ] を選択します。</li> <li>2 [完了 (Finish) ] を選択します。</li> </ol>	

**ステップ 5** クエリーを保存する場所を参照し、クエリーの名前を [ファイル名 (File Name) ] フィールドに入力します。

**ステップ 6** [保存 (Save) ] を選択します。

**ステップ 7** 次のいずれかの操作を実行します。

目的	Action
先ほど保存したクエリーを実行する	<ul style="list-style-type: none"> <li>• [クエリーの実行 (Run Query) ] を選択します。</li> </ul>
作成したクエリーを実行しないでクエリー ウィザードを終了する	[キャンセル (Cancel) ] を選択します。

**ステップ 8** クエリーの実行が完了したら、次のいずれかの操作を実行します。

目的	Action
収集したファイルを表示する	<p>ファイルに移動するには、以下のステップに従います。</p> <ol style="list-style-type: none"> <li>1 [クエリー結果 (Query Results)] をダブルクリックします。</li> <li>2 &lt;node&gt; フォルダをダブルクリックします。ここで、&lt;node&gt; は、ウィザードで指定したノードの IP アドレスまたはホスト名です。</li> <li>3 表示するファイルが格納されているフォルダをダブルクリックします。</li> <li>4 ファイルが見つかったら、そのファイルをダブルクリックします。</li> </ol>
トレースファイル、およびクエリーで収集されたトレースファイルのリストを含む結果ファイルをダウンロードする	<ol style="list-style-type: none"> <li>1 ダウンロードするファイルを選択します。</li> <li>2 [ダウンロード (Download)] を選択します。</li> <li>3 ダウンロードの条件を指定します。</li> <li>4 [完了 (Finish)] を選択します。</li> </ol>
トレースファイルと結果ファイルをダウンロードするディレクトリを指定する	<ol style="list-style-type: none"> <li>1 [すべてのファイルのダウンロード (Download all files)] フィールドの隣にある [参照 (Browse)] を選択します。</li> <li>2 対象のディレクトリに移動します。</li> <li>3 [開く (Open)] を選択します。</li> </ol>
収集したトレースファイルの zip ファイルを作成する	[ファイルを zip 圧縮する (Zip File)] を選択します。
収集したログファイルをサーバから削除する	[収集されたログファイルをサーバから削除する (Delete Collected Log Files from Server)] をオンにします。
クエリーを保存する	• [クエリーの保存 (Save Query)] を選択します。

## Cisco Unified Communications Manager のトレース収集のスケジュール

Trace and Log Central 機能の収集のスケジュールオプションを使用して、最大 6 つの同時トレース収集をスケジュールできます。また、トレースファイルをネットワーク上の SFTP または FTP

サーバにダウンロードしたり、別の保存クエリーを実行したり、syslog ファイルを生成したりできます。スケジュールされた収集を入力後に変更するには、そのスケジュールされた収集を削除し、新しい収集イベントとして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) トレース収集ジョブは 10 個までスケジュールできますが、同時に存在できるトレース収集は 6 つだけです。つまり、6 つのジョブだけが同時に実行状態になることができます。

### はじめる前に

次の 1 つまたは複数の操作を実行します。

- さまざまなサービス用のトレースファイルに含める情報を、Cisco Unified Serviceability の [トレース設定 (Trace Configuration)] ウィンドウから設定します。詳細については、『Cisco Unified Serviceability Administration Guide』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には、アラームの送信先として SDI または SDL トレース ファイルを [アラーム設定 (Alarm Configuration)] ウィンドウで選択します。詳細については、『Cisco Unified Serviceability Administration Guide』を参照してください。

### 手順

**ステップ 1** [Trace and Log Central] オプションを開きます。

**ステップ 2** [Trace & Log Central] のツリー階層で、[収集のスケジュール (Schedule Collection)] をダブルクリックします。  
収集のスケジュール ウィザードが表示されます。

- (注) サービスは、アクティブにされていなくても表示されます。したがって、それらのサービスに対してトレースを収集できます。
- (注) クラスタ内のノードが使用できない場合、どのノードが利用できないかを示すメッセージと共にダイアログボックスが表示されます。使用不可能なノードは、[Trace and Log Central] ウィンドウに表示されません。
- (注) 一部の一覧されているサービスおよびアプリケーションをクラスタ内の特定のノード上にインストールすることができます。それら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、そのサービスまたはアプリケーションがアクティブにされているノードからトレースを収集するようにします。

**ステップ 3** [CCM サービス/アプリケーションの選択 (Select CCM Services/Application)] タブで、次のいずれかの操作を実行します。

- (注) スタンドアロンノードがあり、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers)] チェックボックスがオンの場合、システムは、スタンドアロンノードのすべてのサービスとアプリケーションのトレースを収集します。
- すべてのノードに対してすべてのサービスとアプリケーションのトレースを収集するには、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on All Servers)] チェックボックスをオンにして [次へ (Next)] をクリックします。

- 特定ノード上のすべてのサービスとアプリケーションのトレースを収集するには、ノードの横にあるチェックボックスをオンにして、[次へ (Next)] をクリックします。
- 特定のノード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には、適用するチェックボックスをオンにして、[次へ (Next)] をクリックします。
- サービスまたはアプリケーションのトレースを収集しないで収集のスケジュールウィザードを続行するには、[次へ (Next)] をクリックします。

- ステップ 4** [システム サービス/アプリケーションの選択 (Select System Services/Application)] タブで、次のいずれかの操作を実行します。
- (注) スタンドアロンノードがあり、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers)] チェックボックスがオンの場合、システムは、スタンドアロンノードのトレースを収集します。
- すべてのノードに対してすべてのシステム ログを収集するには、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers)] チェックボックスをオンにして [次へ (Next)] をクリックします。
  - 特定ノード上のすべてのシステム ログのトレースを収集するには、ノードの横にあるチェックボックスをオンにして、[次へ (Next)] をクリックします。
  - 特定のノード上の特定のシステム ログのトレースを収集するには、適用するチェックボックスをオンにして、[次へ (Next)] をクリックします。
  - システム ログのトレースを収集しないで収集のスケジュール ウィザードを続行するには、[次へ (Next)] をクリックします。

- ステップ 5** トレースを収集するノードのタイムゾーンと時間範囲を指定します。クライアントコンピュータのタイムゾーンにより、[リファレンスサーバ時間帯の選択 (Select Reference Server Time Zone)] フィールドのデフォルトが設定されます。すべての標準タイムゾーンが [タイムゾーンを選択 (Select Time Zone)] ドロップダウンリストボックスに表示され、[サマータイム (Daylight Saving)] が設定されたタイムゾーン用に独立した一連のエントリも表示されます。

- ステップ 6** トレース収集を開始する日時を指定するには、[開始日時のスケジュール (Schedule Start Date/Time)] フィールドの隣にある下矢印ボタンをクリックします。[日付 (Date)] タブで、該当する日付を選択します。[時間 (Time)] タブで、適切な時間を選択します。

- ステップ 7** トレース収集を終了する日時を指定するには、[終了日時のスケジュール (Schedule End Date/Time)] フィールドの隣にある下矢印ボタンをクリックします。[日付 (Date)] タブで、該当する日付を選択します。[時間 (Time)] タブで、適切な時間を選択します。
- (注) トレース収集は、設定された終了時刻を過ぎても最後まで実行します。ただし、その場合の収集は、Trace and Log Central 機能によってスケジュールから削除されません。

- ステップ 8** [スケジューラ頻度 (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 9** [過去に生成されたファイルを収集 (Collect Files that are generated in the last)] 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現在の時刻までの時間 (分、時間、日、週、または月単位) を指定します。
- ステップ 10** トレースファイルに存在する語句または単語で検索するには、[検索文字列 (Search String)] フィールドに単語または語句を入力します。このツールでは、入力した単語または句に対して一致するものが検索され、その検索条件に一致するファイルが収集されます。入力した単語または句に対して完全に一致するものを検索する場合は、[大文字小文字を区別 (Case Sensitive)] チェックボックスをオンにします。
- ステップ 11** 収集したトレースファイルの zip ファイルを作成するには、[ファイルを zip 圧縮する (Zip File)] チェックボックスをオンにします。
- ステップ 12** 収集したログ ファイルをノードから削除するには、[収集されたログ ファイルをサーバから削除する (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 13** 次の 1 つまたは複数の操作を実行します。
- ファイルをダウンロードし、ステップ 14 に進みます。
  - 別のクエリーを実行し、ステップ 15 に進みます。
  - Syslog を生成します。[Syslog の生成 (Generate Syslog)] を選択した場合は、ステップ 16 に進みます。
- ステップ 14** [SFTP/FTP サーバパラメータ (SFTP/FTP Server Parameters)] グループ ボックスに、Trace and Log Central 機能により結果をダウンロードされるノードのノード クレデンシャルを入力し、[接続のテスト (Test Connection)] をクリックします。Trace and Log Central 機能によって SFTP または FTP サーバへの接続が確認されたら、[OK] をクリックします。
- [ダウンロードディレクトリパス (Download Directory Path)] フィールドは、Trace and Log Central 機能によって収集されたファイルが保存されるディレクトリを指定します。トレース収集のデフォルトでは、SFTP または FTP パラメータのフィールドに指定されたユーザ ID のユーザのホームディレクトリ (/home/<user>/Trace) 内にファイルが保存されます。
- トレースをダウンロードする場合、[Localhost] ダウンロード オプションを選択できます。このオプションは、Cisco Intercompany Media Engine サーバに対してのみ使用可能です。
- Cisco Intercompany Media Engine サーバのローカル ホスト ディレクトリにトレース ファイルをダウンロードする場合、**file get** CLI コマンドを使って、リモート SFTP サーバにファイルをオフロードできます。
- (注) Cisco Intercompany Media Engine では、FTP はサポート対象外です。
- ステップ 15** 別のクエリーの実行オプションを選択した場合は、[参照 (Browser)] 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 機能では、最初のクエリーで結果が生成される場合、指定されたクエリーのみが実行されます。
- ステップ 16** [終了 (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がメッセージに示されます。

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

**ステップ 17** [OK] をクリックします。

**ステップ 18** スケジュールされた収集のリストを表示するには、クイック起動チャネルのトレース部分で、[ジョブのステータス (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、収集のイベントを選択して [削除 (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。

## Cisco Unity Connection のトレース収集のスケジュール

Trace and Log Central 機能の収集のスケジュール オプションを使用して、最大 6 つの同時トレース収集をスケジュールできます。また、トレース ファイルをネットワーク上の SFTP または FTP サーバにダウンロードしたり、別の保存クエリーを実行したり、syslog ファイルを生成したりできます。スケジュールされた収集を入力後に変更するには、そのスケジュールされた収集を削除し、新しい収集イベントとして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) トレース収集ジョブは 10 個までスケジュールできますが、同時に存在できるトレース収集は 6 つだけです。つまり、6 つのジョブだけが同時に実行状態になることができます。

### はじめる前に

次の 1 つまたは複数の操作を実行します。

- さまざまなサービス用のトレース ファイルに含める情報を、Cisco Unified Serviceability の [トレース設定 (Trace Configuration)] ウィンドウから設定します。詳細については、『Cisco Unified Serviceability Administration Guide』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には、アラームの送信先として SDI または SDL トレース ファイルを [アラーム設定 (Alarm Configuration)] ウィンドウで選択します。詳細については、『Cisco Unified Serviceability Administration Guide』を参照してください。

### 手順

**ステップ 1** [Trace and Log Central] オプションを開きます。

**ステップ 2** [Trace & Log Central] のツリー階層で、[収集のスケジュール (Schedule Collection)] をダブルクリックします。

収集のスケジュール ウィザードが表示されます。

- (注) サービスは、アクティブにされていなくても表示されます。したがって、それらのサービスに対してトレースを収集できます。
- (注) Cisco Unity Connection : クラスタ内のすべてのノードが使用できない場合、どのノードが利用できないかを示すメッセージとともにダイアログボックスが表示されます。使用不可能なノードは、[Trace and Log Central] ウィンドウに表示されません。
- (注) Cisco Unity Connection : リストされているサービスおよびアプリケーションの一部をクラスタ内の特定のノードにインストールすることができます。それら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、そのサービスまたはアプリケーションがアクティブにされているノードからトレースを収集するようにします。

**ステップ 3** [CUC サービス/アプリケーションの選択 (Select CUC Services/Application) ] タブで、次のいずれかの操作を実行します。

- ノードのすべてのシステム ログを収集するには、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers) ] チェックボックスをオンにするか、ノードの横にあるチェックボックスをオンにして、[次へ (Next) ] をクリックします。
- ノード上の特定のシステムログのトレースを収集するには、適用するチェックボックスをオンにして、[次へ (Next) ] をクリックします。
- システム ログのトレースを収集しないで収集のスケジュール ウィザードを続行するには、[次へ (Next) ] をクリックします。

**ステップ 4** [システム サービス/アプリケーションの選択 (Select System Services/Application) ] タブで、次のいずれかの操作を実行します。

- (注) スタンドアロンノードがあり、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers) ] チェックボックスがオンの場合、システムは、スタンドアロンノードのトレースを収集します。
- すべてのノードに対してすべてのシステム ログを収集するには、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers) ] チェックボックスをオンにして [次へ (Next) ] をクリックします。
- 特定ノード上のすべてのシステムログのトレースを収集するには、ノードの横にあるチェックボックスをオンにして、[次へ (Next) ] をクリックします。
- 特定のノード上の特定のシステムログのトレースを収集するには、適用するチェックボックスをオンにして、[次へ (Next) ] をクリックします。
- システム ログのトレースを収集しないで収集のスケジュール ウィザードを続行するには、[次へ (Next) ] をクリックします。

**ステップ 5** トレースを収集するノードのタイムゾーンと時間範囲を指定します。クライアントコンピュータのタイムゾーンにより、[リファレンスサーバ時間帯の選択 (Select Reference Server Time Zone) ] フィールドのデフォルトが設定されます。すべての標準タイムゾーンが [タイムゾーンを選択 (Select Time Zone) ] ドロップダウンリストボックスに表示され、[サマータイム (Daylight Saving) ] が設定されたタイムゾーン用に独立した一連のエントリも表示されます。

- ステップ 6** トレース収集を開始する日時を指定するには、[開始日時のスケジュール (Schedule Start Date/Time) ] フィールドの隣にある下矢印ボタンをクリックします。[日付 (Date) ] タブで、該当する日付を選択します。[時間 (Time) ] タブで、適切な時間を選択します。
- ステップ 7** トレース収集を終了する日時を指定するには、[終了日時のスケジュール (Schedule End Date/Time) ] フィールドの隣にある下矢印ボタンをクリックします。[日付 (Date) ] タブで、該当する日付を選択します。[時間 (Time) ] タブで、適切な時間を選択します。  
(注) トレース収集は、設定された終了時刻を過ぎても最後まで実行します。ただし、その場合の収集は、Trace and Log Central 機能によってスケジュールから削除されません。
- ステップ 8** [スケジュールラ頻度 (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 9** [過去に生成されたファイルを収集 (Collect Files that are generated in the last) ] 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現在の時刻までの時間 (分、時間、日、週、または月単位) を指定します。
- ステップ 10** トレースファイルに存在する語句または単語で検索するには、[検索文字列 (Search String) ] フィールドに単語または語句を入力します。このツールでは、入力した単語または句に対して一致するものが検索され、その検索条件に一致するファイルが収集されます。入力した単語または句に対して完全に一致するものを検索する場合は、[大文字小文字を区別 (Case Sensitive) ] チェックボックスをオンにします。
- ステップ 11** 収集したトレースファイルの zip ファイルを作成するには、[ファイルを zip 圧縮する (Zip File) ] チェックボックスをオンにします。
- ステップ 12** 収集したログ ファイルをノードから削除するには、[収集されたログ ファイルをサーバから削除する (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 13** 次の 1 つまたは複数の操作を実行します。
- ファイルをダウンロードします。ファイルのダウンロードまたは別のクエリーの実行を選択した場合は、ステップ 15 に進みます。
  - 別のクエリーを実行します。
  - Syslog を生成します。[Syslog の生成 (Generate Syslog) ] を選択した場合は、ステップ 17 に進みます。
- ステップ 14** [SFTP/FTP サーバパラメータ (SFTP/FTP Server Parameters) ] グループ ボックスに、Trace and Log Central 機能により結果をダウンロードされるノードのノード クレデンシャルを入力し、[接続のテスト (Test Connection) ] をクリックします。Trace and Log Central 機能によって SFTP または FTP サーバへの接続が確認されたら、[OK] をクリックします。  
[ダウンロードディレクトリパス (Download Directory Path) ] フィールドは、Trace and Log Central 機能によって収集されたファイルが保存されるディレクトリを指定します。トレース収集のデフォルトでは、SFTP または FTP パラメータのフィールドに指定されたユーザ ID のユーザのホームディレクトリ (/home/<user>/Trace) 内にファイルが保存されます。
- トレースをダウンロードする場合、[Localhost] ダウンロード オプションを選択できます。このオプションは、Cisco Intercompany Media Engine サーバに対してのみ使用可能です。

Cisco Intercompany Media Engine サーバのローカル ホスト ディレクトリにトレース ファイルをダウンロードする場合、**file get CLI** コマンドを使って、リモート SFTP サーバにファイルをオフロードできます。

(注) Cisco Intercompany Media Engine では、FTP はサポート対象外です。

**ステップ 15** 別のクエリーの実行オプションを選択した場合は、[参照 (Browser)] 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 機能では、最初のクエリーで結果が生成される場合、指定されたクエリーのみが実行されます。

**ステップ 16** [終了 (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がメッセージに示されます。

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

**ステップ 17** [OK] をクリックします。

**ステップ 18** スケジュールされた収集のリストを表示するには、クイック起動チャネルのトレース部分で、[ジョブのステータス (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、収集のイベントを選択して [削除 (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。

## スケジュールの開始

### はじめる前に

- さまざまなサービス用のトレース ファイルに含める情報を、[トレース設定 (Trace Configuration)] ウィンドウから設定します。
- アラームをトレース ファイルに送信するには、アラームの送信先として SDI トレース ファイルを [アラーム設定 (Alarm Configuration)] ウィンドウで選択します。

### 手順

**ステップ 1** Trace & Log Central を開きます。

**ステップ 2** ツリー階層で [収集のスケジュール (Schedule Collection)] をダブルクリックします。

**ステップ 3** 次のいずれかの操作を実行して、ノードのログに関するトレースを収集します。

目的	Action
クラスタ内のすべてのノードに対してすべてのサービスとアプリケーションのトレースを収集する	<ul style="list-style-type: none"> <li>• [すべてのサーバ上のすべてのサービスを選択する (Select All Services on All Servers) ] をオンにします。</li> <li>• [次へ (Next) ] を選択します。</li> </ul>
特定のノード上のすべてのサービスとアプリケーションのトレースを収集する	<ul style="list-style-type: none"> <li>• ノードの名前を確認します。</li> <li>• [次へ (Next) ] を選択します。</li> </ul>
特定のノード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	<ul style="list-style-type: none"> <li>• 適用するトレースをオンにします。</li> <li>• [次へ (Next) ] を選択します。</li> </ul>
サービスまたはアプリケーションのトレースを収集しないでトレース収集ウィザードを続行する	[次へ (Next) ] を選択します。

**ステップ 4** 次のいずれかの操作を実行して、システム ログに関するトレースを収集します。

目的	Action
クラスタ内のすべてのノードのすべてのシステム ログを収集する	<ul style="list-style-type: none"> <li>• [すべてのサーバ上のすべてのサービスを選択する (Select All Services on All Servers) ] をオンにします。</li> <li>• [次へ (Next) ] を選択します。</li> </ul>
特定のノード上のすべてのシステム ログのトレースを収集する	<ul style="list-style-type: none"> <li>• ノードの名前を確認します。</li> <li>• [次へ (Next) ] を選択します。</li> </ul>
特定のノード上の特定のシステム ログのトレースを収集する	<p>適用するトレースをオンにします。</p> <p>たとえば、CSA ログを収集するには、[Cisco Security Agent] をオンにします。ログイン中およびログアウト中のユーザに関する情報が得られるユーザ ログにアクセスするには、[セキュリティ ログ (Security Logs) ] をオンにします。</p>

目的	Action
システム ログのトレースを収集しないでトレース収集ウィザードを続行する	[次へ (Next) ] を選択します。

**ステップ 5**    トレースを収集するノードのタイム ゾーンと時間範囲を指定します。

**ステップ 6**    次の操作を実行して、トレース収集を開始する日時を指定します。

- a) [開始日時のスケジュール (Schedule Start Date/Time) ] フィールドの隣にある下矢印ボタンを選択します。
- b) [日付 (Date) ] タブから、適切な日付を選択します。
- c) [時刻 (Time) ] タブから、適切な時刻を選択します。

**ステップ 7**    トレース収集を終了する日時を指定するには、次の操作を実行します。

- a) [終了日時のスケジュール (Schedule End Date/Time) ] フィールドの隣にある下矢印ボタンを選択します。
- b) [日付 (Date) ] タブから、適切な日付を選択します。
- c) [時刻 (Time) ] タブから、適切な時刻を選択します。

トラブルシューティングのヒント

- クライアント コンピュータの時間帯により、[リファレンス サーバ時間帯の選択 (Select Reference Server Time Zone) ] フィールドのデフォルトが設定されます。すべての標準タイムゾーンが[タイムゾーンを選択 (Select Time Zone) ] ドロップダウンリストボックスに表示され、[サマータイム (Daylight Saving) ] が設定されたすべてのタイムゾーン用に独立した一連のエントリも表示されます。
- トレース収集は、設定された終了時刻を過ぎても最後まで実行します。ただし、その場合の収集は、Trace and Log Central 機能によってスケジュールから削除されません。

**次の作業**

[スケジュールの実行, \(181 ページ\)](#)

## スケジュールの実行

### 手順

- ステップ 1** 設定されたトレース収集を実行する頻度を [スケジューラ頻度 (Scheduler Frequency)] リストボックスから選択します。
- ステップ 2** トレースの収集範囲を現在時刻までの時間 (分数、時間数、日数、週数、または月数) で指定します。
- ステップ 3** 単語または句を [検索文字列 (Search String)] フィールドに入力して、トレース ファイル内に存在する句または単語を検索します。このツールでは、入力した単語または句に対して完全に一致するものが検索され、その検索条件に一致するファイルのみが収集されます。
- ステップ 4** [すべてのファイルを zip 圧縮する (Zip All Files)] をオンにして、収集したトレース ファイルから zip ファイルを作成します。
- ステップ 5** [収集されたログ ファイルをサーバから削除する (Delete Collected Log Files from the Server)] をオンにして、収集されたログ ファイルをサーバから削除します。
- ステップ 6** 次の 1 つまたは複数の操作を実行します。
- ファイルをダウンロードするには、次の手順を実行します。
    - 1 [ファイルのダウンロード (Download Files)] を選択します。
    - 2 [SFTP サーバパラメータ (SFTP Server Parameters)] グループ ボックスに、Trace and Log Central 機能が結果をダウンロードするノードのノード クレデンシャルを入力します。
    - 3 [接続のテスト (Test Connection)] を選択します。
    - 4 Trace and Log Central 機能が SFTP サーバへの接続を検証した後、[OK] を選択します。
  - 別のクエリーを実行するには、次の手順を実行します。
    - 1 [別のクエリーの実行 (Run Another Query)] を選択します。
    - 2 [参照 (Browse)] を選択して、実行するクエリーの場所を指定します。
    - 3 [OK] を選択します。
  - Syslog を生成するには、[Syslog の生成 (Generate Syslog)] を選択します。
- ステップ 7** [完了 (Finish)] を選択します。
- トラブルシューティングのヒント
- クラスタ内のノードが使用できない場合、どのノードが利用できないかを示すメッセージと共にダイアログボックスが表示されます。使用不可能なノードは、[Trace & Log Central] ウィンドウに表示されません。
  - Unified RTMT 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。入力した IP アドレス、ユーザ名、およびパスワードが正しいことを確認してください。

- 一部の一覧されているサービスまたはアプリケーションをクラスタ内の特定のノード上にだけインストールすることができます。それら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には、そのサービスまたはアプリケーションがアクティブにされているサーバからトレースを選択します。
- サービスは、アクティブにされていなくても表示されます。したがって、それらのサービスに対してトレースを収集できます。
- トレース収集は、設定された終了時刻を過ぎても最後まで実行します。ただし、その場合の収集は、Trace and Log Central 機能によってスケジュールから削除されません。
- [ダウンロードディレクトリパス (Download Directory Path) ] フィールドは、Trace and Log Central 機能によって収集されたファイルが保存されるディレクトリを指定します。トレース収集のデフォルトでは、SFTP パラメータのフィールドに指定されたユーザ ID のユーザのホームディレクトリ (/home/<user>/Trace) 内にファイルが保存されます。
- Trace and Log Central 機能では、最初のクエリーで結果が生成される場合、指定されたクエリーのみが実行されます。

## トレース収集ステータスの表示

トレース収集イベントのステータスを表示し、スケジュールされているトレース収集を削除するには、次の手順を使用します。

### 手順

- ステップ 1** Trace & Log Central のツリー階層を開きます。
  - ステップ 2** [ジョブのステータス (Job Status) ] をダブルクリックします。  
[ジョブのステータス (Job Status) ] ウィンドウが表示されます。
  - ステップ 3** [ノードの選択 (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。  
ジョブタイプには以下が含まれることがあります。
    - Scheduled Job
    - OnDemand
    - RealTimeFileMon
    - RealTimeFileSearch
- ステータスには以下が含まれることがあります。
- 保留中 (Pending)



- 実行中 (Running)
- キャンセル (Cancel)
- 終了

**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、[削除 (Delete)] をクリックします。

(注) ステータスが“保留中 (Pending)”または“実行中 (Running)”のジョブと、ジョブタイプが“Schedule Task”または“RealTimeFileSearch”のジョブを削除できます。

## リアルタイム トレース

Trace and Log Central 機能のリアルタイム トレース オプションでは、アプリケーションごとにサーバ上で書き込みが行われている現在のトレース 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すでに開始していた場合、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ファイルの読み取りを開始します。それ以前の内容を読み取ることはできません。

リアルタイム トレースは、リアルタイム データの表示とユーザ イベントのモニタリングのオプションを提供します。

### リアルタイム データの表示

Trace and Log Central 機能のリアルタイム データの表示オプションでは、トレース ファイルをシステムによるデータの書き込みを反映して表示できます。リアルタイム トレースデータは、最大 10 個のサービスについて Generic Log Viewer で表示できます。ただし、1 台のノードの同時セッションは 3 つまでという制限があります。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書き込まれると、Generic Log Viewer は、その内容をビューア内に追加します。



(注) リアルタイムデータの表示オプションでは、サービスがトレースを書き込む頻度によっては、Generic Log Viewer でのデータの表示に遅延が発生します。

### 手順

**ステップ 1** Trace & Log Central のツリー階層を開きます。

**ステップ 2** [リアルタイム トレース (Real Time Trace)] をダブルクリックします。

(注) Unified Communications Manager クラスタおよび Cisco Unity Connection クラスタのみ：クラスタ内のすべてのノードが使用できない場合、どのノードが利用できないかを示すメッセージとともにダイアログボックスが表示されます。使用不可能なノードは、[Trace and Log Central] ウィンドウに表示されません。

**ステップ 3** [リアルタイム データを表示 (View Real Time Data)] をダブルクリックします。

[リアルタイム データ (Real Time Data)] ウィザードが表示されます。

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

**ステップ 5** リアルタイム データを表示する製品、サービス、およびトレースファイルタイプを選択します。

(注) サービスは、アクティブにされていなくても表示されます。したがって、それらのサービスに対してトレースを収集できます。

(注) このウィンドウの下部に、「トレース圧縮が有効な場合、データのバッファリングにより、このウィンドウに表示されるデータが膨大になることがあります (If trace compression is enabled, the data seen in this window can be bursty due to buffering of data.)」というメッセージが表示されます。

**ステップ 6** [終了 (Finish)] をクリックします。選択したサービスのリアルタイム データが Generic Log Viewer に表示されます。

**ステップ 7** 次のいずれかの操作を実行します。

- 新しいトレースが常に表示されるように、カーソルをウィンドウの最後に維持するには、[新しいデータの表示 (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てもカーソルをウィンドウの最下部に移動させない場合は、[新しいデータの表示 (Show New Data)] チェックボックスをオフにします。

**ステップ 8** 他のサービスのデータを表示するには、この手順を繰り返します。全体または単一ノード上での制限数を超えるサービスについてデータを表示しようとすると、メッセージが表示されます。

**ステップ 9** リアルタイム データの表示を終了する場合は、Generic Log Viewer の [閉じる (Close)] をクリックします。

**ヒント** Log Viewer で句または単語で検索するには、[検索文字列 (Search String)] フィールドに単語または句を入力します。大文字と小文字を区別して単語または句を検索する場合は、[大文字と小文字を区別する (Match Case)] チェックボックスをオンにします。

## ユーザ イベントのモニタリング

Trace and Log Central 機能のユーザ イベントのモニタ オプションは、リアルタイム トレース ファイルをモニタし、検索文字列がトレース ファイル内で見つかったら、指定された操作を実行します。システムは、5 秒ごとにトレース ファイルをポーリングします。1 つのポーリング間隔で検索文字列が複数回見つかったら、システムは操作を 1 回だけ実行します。

### はじめる前に

監視されているトレース ファイル内に指定された検索文字列が存在するときにアラームを生成する場合は、LogFileSearchStringFound アラートを有効にします。

## 手順

- ステップ 1** Trace & Log Central のツリー階層を開きます。
- ステップ 2** [リアルタイムトレース (Real Time Trace)] をダブルクリックします。  
(注) Unified Communications Manager クラスタおよび Cisco Unity Connection クラスタのみ：クラスタ内のすべてのノードが使用できない場合、どのノードが利用できないかを示すメッセージとともにダイアログボックスが表示されます。使用不可能なノードは、[Trace and Log Central] ウィンドウに表示されません。
- ステップ 3** [ユーザ イベントのモニタ (Monitor User Event)] をダブルクリックします。  
[ユーザ イベントのモニタ (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。

目的	Action
セットアップ済みのモニタリング イベントを表示する	<ul style="list-style-type: none"> <li>• [設定済みイベントの表示 (View Configured Events)] をクリックします。</li> <li>• ドロップダウン リスト ボックスからノードを選択します。</li> <li>• [終了 (Finish)] をクリックします。</li> </ul> <p>(注) イベントを削除するには、イベントを選択し、[削除 (Delete)] をクリックします。</p>
新しいモニタリング イベントを設定する	<ul style="list-style-type: none"> <li>• [イベントの作成 (Create Events)] を選択します。</li> <li>• [次へ (Next)] を選択します。</li> <li>• ステップ 5 に進みます。</li> </ul>

- ステップ 5** システムでモニタするノードを [ノード (Nodes)] ドロップダウン リスト ボックスから選択し、[次へ (Next)] をクリックします。
- ステップ 6** システムでモニタする製品、サービス、およびトレースファイルタイプを選択し、[次へ (Next)] をクリックします。  
(注) サービスは、アクティブにされていなくても表示されます。したがって、それらのサービスに対してトレースを収集できます。
- ステップ 7** [検索文字列 (Search String)] フィールドで、トレースファイル内で検索する句または単語を指定します。このツールでは、入力した単語または句に対して完全に一致するものが検索されます。
- ステップ 8** システムでトレースファイルをモニタするノードタイムゾーンと時間範囲 (開始と終了の日時) を指定します。  
クライアント コンピュータのタイムゾーンにより、[リファレンス サーバ時間帯の選択 (Select Reference Server Time Zone)] フィールドのデフォルトが設定されます。すべての標準タイムゾーン

ンが [タイムゾーンを選択 (Select Time Zone)] ドロップダウン リスト ボックスに表示され、[サマータイム (Daylight Saving)] が設定されたすべてのタイムゾーン用に独立した一連のエントリも表示されます。

Trace and Log Central は、[選択したリファレンス サーバタイム ゾーン (Selected Reference Server Time Zone)] に基づいて、時間範囲内のファイルをダウンロードします。クラスタ内のノードが異なるタイムゾーン内に属している場合、TLC は時刻変更を調整し、同じ期間のファイルを取得します。たとえば、午前 9:00 ~ 午前 10:00 のファイルを指定し、2 番目のノード (node x) が時刻が 1 時間進んでいるタイムゾーンに属している場合、TLC は node x から午前 10:00 ~ 午前 11:00 のファイルをダウンロードします。

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

**ステップ 9** [検索文字列 (Search String)] フィールドで指定した検索文字列が検出された場合、システムが実行するアクションを、次の中から 1 つまたは複数選択します。

目的	Action
指定した検索文字列が見つかったらアラームを生成する	[アラート (Alert)] をオンにします。 (注) システムでアラームを生成する場合は、TraceCollectionToolEvent アラートを有効にする必要があります。
SysLog Viewer のアプリケーション ログ領域にエラーを記録する	[ローカル Syslog (Local Syslog)] をオンにします。 (注) システムからアラームの説明と推奨処置が提供されます。SysLog Viewer には Unified RTMT からアクセスできます。
syslog メッセージを syslog ノードに保存する	[リモート Syslog (Remote Syslog)] をオンにします。 syslog ノード名を [サーバ名 (Server Name)] フィールドに入力します。 (注) デフォルトでは、重大度が警告、通知、または情報以下にならない限り、監査イベントはリモート syslog ノードに送信されません。

目的	Action
指定した検索文字列が含まれているトレースファイルをダウンロードする	<p>[ファイルのダウンロード (Download File) ] をオンにします。</p> <p>トレース ファイルをダウンロードするノードのノード クレデンシャルを [SFTP サーバパラメータ (SFTP Server Parameters) ] グループボックスに入力します。</p> <p>[接続のテスト (Test Connection) ] を選択します。</p> <p>Trace and Log Central 機能が SFTP サーバへの接続を検証した後、[OK] を選択します。</p> <p>[ダウンロードディレクトリパス (Download Directory Path) ] フィールドは、Trace and Log Central 機能によって収集されたファイルが保存されるディレクトリを指定します。トレース収集のデフォルトでは、SFTP/FTP パラメータのフィールドに指定されたユーザ ID のユーザのホーム ディレクトリ (/home/&lt;user&gt;/Trace) 内にファイルが保存されます。</p> <p>トレースをダウンロードする場合、[Localhost] ダウンロードオプションを選択できます。このオプションは、Cisco Intercompany Media Engine サーバに対してのみ使用可能です。</p> <p>Cisco Intercompany Media Engine サーバのローカル ホスト ディレクトリにトレースファイルをダウンロードする場合、<b>file get</b> CLI コマンドを使って、リモート SFTP サーバにファイルをオフロードできます。</p> <p>(注) Cisco Intercompany Media Engine では、FTP はサポート対象外です。</p>

システムは、5 秒ごとにトレース ファイルをポーリングし、検索文字列が見つかったら、指定された操作を実行します。1 つのポーリング間隔で検索文字列が複数回見つかったとしても、システムは 1 回しか操作を実行しません。

「If trace compression is enabled, there might be a delay in catching the event after it occurs, due to buffering of data」 というメッセージが表示されます。

**ステップ 10** [終了 (Finish) ] をクリックします。

## Cisco Unified Communications Manager のクラッシュ 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、次の手順に従ってください。

## 手順

- ステップ 1** Trace & Log Central のツリー階層を開きます。
- ステップ 2** [クラッシュ ダンプの収集 (Collect Crash Dump)] をダブルクリックします。  
[クラッシュ ダンプの収集 (Collect Crash Dump)] ウィザードが表示されます。
- (注) サービスは、アクティブにされていなくても表示されます。したがって、それらのサービスに対してトレースを収集できます。
  - (注) クラスタ内のノードが使用できない場合、どのノードが利用できないかを示すメッセージと共にダイアログボックスが表示されます。使用不可能なノードは、[Trace and Log Central] ウィンドウに表示されません。
  - (注) リストされているサービスまたはアプリケーションの一部をクラスタ内の特定のノードにインストールすることができます。それら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には、そのサービスまたはアプリケーションがアクティブにされているノードからトレースを収集するようにします。
- ステップ 3** [CCM サービス/アプリケーションの選択 (Select CCM Services/Application)] タブで、次のいずれかの操作を実行します。
- (注) スタンドアロンノードがあり、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers)] チェックボックスがオンの場合、システムは、スタンドアロンノードのすべてのサービスとアプリケーションのトレースを収集します。
  - すべてのノードに対してすべてのサービスとアプリケーションのトレースを収集するには、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on All Servers)] チェックボックスをオンにして [次へ (Next)] をクリックします。
  - 特定ノード上のすべてのサービスとアプリケーションのトレースを収集するには、ノードの横にあるチェックボックスをオンにして、[次へ (Next)] をクリックします。
  - 特定のノード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には、適用するチェックボックスをオンにして、[次へ (Next)] をクリックします。
  - サービスまたはアプリケーションのトレースを収集しないでクラッシュ ダンプの収集ウィザードを続行するには、[次へ (Next)] をクリックします。
- ステップ 4** [システム サービス/アプリケーションの選択 (Select System Services/Application)] タブで、次のいずれかの操作を実行します。
- (注) スタンドアロンノードがあり、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers)] チェックボックスがオンの場合、システムは、スタンドアロンノードのトレースを収集します。
  - すべてのノードに対してすべてのシステム ログを収集するには、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers)] チェックボックスをオンにして [次へ (Next)] をクリックします。
  - 特定ノード上のすべてのシステム ログのトレースを収集するには、ノードの横にあるチェックボックスをオンにして、[次へ (Next)] をクリックします。

- 特定のノード上の特定のシステムログのトレースを収集するには、適用するチェックボックスをオンにして、[次へ (Next)] をクリックします。
- システム ログのトレースを収集しないでクラッシュ ダンプの収集ウィザードを続行するには、[次へ (Next)] をクリックします。

**ステップ 5** [収集時間 (Collection Time)] グループボックスで、トレースを収集する期間を指定します。次のいずれかのオプションを選択します。

- **絶対範囲 (Absolute Range)** : トレースの収集範囲をノードタイムゾーンと時間範囲 (開始と終了の日時) で指定します。

クライアントコンピュータのタイムゾーンにより、[リファレンスサーバ時間帯の選択 (Select Reference Server Time Zone)] フィールドのデフォルトが設定されます。すべての標準タイムゾーンが [タイムゾーンを選択 (Select Time Zone)] ドロップダウンリストボックスに表示され、[サマータイム (Daylight Saving)] が設定されたタイムゾーン用に独立した一連のエントリも表示されます。

Trace Log Central は、[選択したリファレンスサーバタイムゾーン (Selected Reference Server Time Zone)] に基づいて、時間範囲内のファイルをダウンロードします。クラスタ内のノードが異なるタイムゾーン内に属している場合、TLCは時刻変更を調整し、同じ期間のファイルを取得します。たとえば、午前 9:00 ~ 午前 10:00 のファイルを指定し、2 番目のノード (node x) が時刻が 1 時間進んでいるタイムゾーンに属している場合、TLC は node x から午前 10:00 ~ 午前 11:00 のファイルをダウンロードします。

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、[開始日/時間 (From Date/Time)] フィールドと [終了日/時間 (To Date/Time)] フィールドのドロップダウンリストボックスを選択します。

- **相対範囲 (Relative Range)** : クラッシュファイルの収集範囲を現在時刻までの時間 (分数、時間数、日数、週数、または月数) で指定します。

**ステップ 6** [パーティションの選択 (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ログが含まれているパーティションを選択します。

Cisco Unified Serviceability は、ユーザがログイン中のアプリケーションのバージョンについてはログをアクティブパーティションに保存し、その他のバージョン (インストールされている場合) についてはログを非アクティブディレクトリに保存します。

Linux プラットフォーム上で実行している製品のバージョンを別のバージョンにアップグレードし、ノードを新しいバージョンで再起動すると、Cisco Unified Serviceability は以前のバージョンのログを非アクティブ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パーティションに保存します。古いバージョンにログインした場合、Cisco Unified Serviceability は新しいバージョンのログを非アクティブ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ディレクトリに保存します。

- (注) Cisco Unified Serviceability は、Windows プラットフォームで実行する Cisco Unified Communications Manager、IM and Presence Service、および Cisco Unity Connection バージョンのログを保持しません。

- ステップ 7** トレース ファイルのダウンロード先のディレクトリを指定するには、[ファイルディレクトリのダウンロード (Download File Directory)] フィールドの横にある [参照 (Browse)] ボタンをクリックし、ディレクトリに移動し、[開く (Open)] をクリックします。デフォルトは `<rtmt_users_directory>\<server name または server IP address>\<download time>` です。
- ステップ 8** 収集したクラッシュ ダンプ ファイルの zip ファイルを作成するには、[ファイルを zip 圧縮する (Zip File)] オプション ボタンを選択します。ファイルの zip 圧縮なしでクラッシュ ダンプ ファイルをダウンロードするには、[ファイルを zip 圧縮しない (Do Not Zip Files)] オプション ボタンを選択します。
- (注) 2 ギガバイトを超える zip 圧縮済みクラッシュ ダンプ 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 ファイルをノードから削除するには、[収集されたログファイルをサーバから削除する (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** [終了 (Finish)] をクリックします。
- コア ダンプを収集することを示すメッセージが表示されます。続行するには [はい (Yes)] をクリックします。
- (注) [ファイルを zip 圧縮する (Zip File)] オプション ボタンを選択した場合、クラッシュ ダンプ ファイルが 2 ギガバイトを超えると、そのサイズのクラッシュ ダンプ ファイルは [ファイルを zip 圧縮する (Zip File)] オプション ボタンを選択して収集できないことを示すメッセージがシステムによって表示されます。[ファイルを zip 圧縮しない (Do Not Zip Files)] オプション ボタンを選択してから、収集を再試行します。

## Cisco Unity Connection のクラッシュ 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、次の手順に従ってください。

### 手順

- ステップ 1** Trace & Log Central のツリー階層を開きます。
- ステップ 2** [クラッシュ ダンプの収集 (Collect Crash Dump)] をダブルクリックします。  
[クラッシュ ダンプの収集 (Collect Crash Dump)] ウィザードが表示されます。
- (注) サービスは、アクティブにされていなくても表示されます。したがって、それらのサービスに対してトレースを収集できます。
- (注) Cisco Unity Connection : クラスタ内のすべてのノードが使用できない場合、どのノードが利用できないかを示すメッセージとともにダイアログ ボックスが表示されます。使用不可能なノードは、[Trace and Log Central] ウィンドウに表示されません。
- (注) Cisco Unity Connection : リストされているサービスまたはアプリケーションの一部をクラスタ内の特定のノードにインストールすることができます。それら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には、そのサービスまたはアプリケーションがアクティブにされているノードからトレースを収集するようにします。



**ステップ 3** [CUC サービス/アプリケーションの選択 (Select CUC Services/Application) ] タブで、次のいずれかの操作を実行します。

- ノードのすべてのシステム ログを収集するには、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers) ] チェックボックスをオンにするか、ノードの横にあるチェックボックスをオンにして、[次へ (Next) ] をクリックします。
- サーバ上の特定のシステムログのトレースを収集するには、適用するチェックボックスをオンにして、[次へ (Next) ] をクリックします。
- システム ログのトレースを収集しないでクラッシュ ダンプの収集ウィザードを続行するには、[次へ (Next) ] をクリックします。

**ステップ 4** [システム サービス/アプリケーションの選択 (Select System Services/Application) ] タブで、次のいずれかの操作を実行します。

(注) スタンドアロンノードがあり、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers) ] チェックボックスがオンの場合、システムは、スタンドアロンノードのトレースを収集します。

- すべてのノードに対してすべてのシステム ログを収集するには、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers) ] チェックボックスをオンにして [次へ (Next) ] をクリックします。
- 特定ノード上のすべてのシステムログのトレースを収集するには、ノードの横にあるチェックボックスをオンにして、[次へ (Next) ] をクリックします。
- 特定のノード上の特定のシステムログのトレースを収集するには、適用するチェックボックスをオンにして、[次へ (Next) ] をクリックします。
- システム ログのトレースを収集しないでクラッシュ ダンプの収集ウィザードを続行するには、[次へ (Next) ] をクリックします。

**ステップ 5** [収集時間 (Collection Time) ] グループボックスで、トレースを収集する期間を指定します。次のいずれかのオプションを選択します。

- 絶対範囲 (Absolute Range) : トレースの収集範囲をノード タイムゾーンと時間範囲 (開始と終了の日時) で指定します。

クライアント コンピュータのタイムゾーンにより、[リファレンスサーバ時間帯の選択 (Select Reference Server Time Zone) ] フィールドのデフォルトが設定されます。すべての標準タイムゾーンが [タイムゾーンを選択 (Select Time Zone) ] ドロップダウンリストボックスに表示され、[サマー タイム (Daylight Saving) ] が設定されたタイムゾーン用に独立した一連のエントリも表示されます。

Trace Log Central は、[選択したリファレンスサーバタイムゾーン (Selected Reference Server Time Zone) ] に基づいて、時間範囲内のファイルをダウンロードします。クラスタ内のノードが異なるタイムゾーン内に属している場合、TLCは時刻変更を調整し、同じ期間のファイルを取得します。たとえば、午前 9:00 ~ 午前 10:00 のファイルを指定し、2 番目のノード (node x) が時刻が 1 時間進んでいるタイムゾーンに属している場合、TLC は node x から午前 10:00 ~ 午前 11:00 のファイルをダウンロードします。

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、[開始日/時間 (From Date/Time) ] フィールドと [終了日/時間 (To Date/Time) ] フィールドのドロップダウンリストボックスを選択します。

- 相対範囲 (Relative Range) : クラッシュファイルの収集範囲を現在時刻までの時間 (分数、時間数、日数、週数、または月数) で指定します。

**ステップ 6** [パーティションの選択 (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ログが含まれているパーティションを選択します。

Cisco Unified Serviceability は、ユーザがログイン中のアプリケーションのバージョンについてはログをアクティブパーティションに保存し、その他のバージョン (インストールされている場合) についてはログを非アクティブディレクトリに保存します。

Linux プラットフォーム上で実行している製品のバージョンを別のバージョンにアップグレードし、ノードを新しいバージョンで再起動すると、Cisco Unified Serviceability は以前のバージョンのログを非アクティブ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パーティションに保存します。古いバージョンにログインした場合、Cisco Unified Serviceability は新しいバージョンのログを非アクティブ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ディレクトリに保存します。

- (注) Cisco Unified Serviceability は、Windows プラットフォームで実行する Cisco Unified Communications Manager、IM and Presence Service、および Cisco Unity Connection バージョンのログを保持しません。

**ステップ 7** トレースファイルのダウンロード先のディレクトリを指定するには、[ファイルディレクトリのダウンロード (Download File Directory) ]フィールドの横にある[参照 (Browse) ]ボタンをクリックし、ディレクトリに移動し、[開く (Open) ]をクリックします。デフォルトは

<rtmt\_user\_directory>\<server name または server IP address>\<download time>です。ここで、<rtmt\_user\_directory>はRTMTのインストール先のディレクトリです。

**ステップ 8** 収集したクラッシュ ダンプファイルの zip ファイルを作成するには、[ファイルを zip 圧縮する (Zip File) ]オプションボタンを選択します。ファイルの zip 圧縮なしでクラッシュ ダンプファイルをダウンロードするには、[ファイルを zip 圧縮しない (Do Not Zip Files) ]オプションボタンを選択します。

- (注) 2ギガバイトを超える zip 圧縮済みクラッシュ ダンプ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 ダンプファイルをノードから削除するには、[収集されたログファイルをサーバから削除する (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** [終了 (Finish) ]をクリックします。コア ダンプを収集することを示すメッセージが表示されます。続行するには[はい (Yes) ]をクリックします。

- (注) [ファイルを zip 圧縮する (Zip File) ]オプションボタンを選択した場合、クラッシュ ダンプファイルが2ギガバイトを超えると、そのサイズのクラッシュ ダンプファイルは[ファイルを zip 圧縮する (Zip File) ]オプションボタンを選択して収集できないことを示すメッセージがシステムによって表示されます。[ファイルを zip 圧縮しない (Do Not Zip Files) ]オプションボタンを選択してから、収集を再実行します。

## インストール ログの収集

インストールおよびアップグレード ログを収集するには、次の手順に従います。

### 手順

- ステップ 1** [ツール (Tools) ]>[トレース (Trace) ]>[Trace & Log Central] の順に選択します。  
[Trace & Log Central] ウィンドウが表示されます。
- ステップ 2** [Trace & Log Central] のツリー階層で、[インストール ログの収集 (Collect Install Logs) ] をダブルクリックします。  
[インストール ログの収集 (Collect Install Logs) ] ウィザードが表示されます。
- ステップ 3** [サーバオプションの選択 (Select Servers Options) ] ボックスで、どのサーバからインストール ログを収集するかを指定します。
  - 特定のサーバのインストール ログを収集するには、サーバの横にあるチェックボックスをオンにします。
  - すべてのサーバのインストール ログを収集するには、[すべてのサーバを選択 (Select All Servers) ] チェックボックスをオンにします。
- ステップ 4** [ダウンロードファイル オプション (Download File Options) ] では、ログ ファイルをダウンロードするディレクトリを指定します。ログ ファイルのダウンロード先のディレクトリを指定するには、[ファイルディレクトリのダウンロード (Download File Directory) ] フィールドの横にある [参照 (Browse) ] をクリックし、ディレクトリに移動し、[開く (Open) ] をクリックします。デフォルトでは、<rtmt\_users\_directory> が指定されます。
- ステップ 5** [終了 (Finish) ] をクリックします。

## 監査ログの収集

### 監査ログの参照

### 手順

- ステップ 1** Trace & Log Central のツリー階層を開きます。
- ステップ 2** [監査ログの収集 (Collect Audit Logs) ] をダブルクリックします。

監査ログの収集アクション オプション ウィザードが表示されます。

**ステップ 3** [監査ログの参照 (Browse Audit Logs)] チェックボックスをオンにします。

**ステップ 4** [次へ (Next)] をクリックします。  
[ノードの選択オプション (Nodes Selection Options)] ウィザードが表示されます。

**ステップ 5** [Action Options (アクション オプション)] ウィンドウで次のいずれかのアクションを実行します。

(注) スタンドアロン サーバがあり、[すべてのサーバを選択 (Select All Servers)] チェックボックスがオンの場合、システムは、スタンドアロン サーバのすべての監査ログを参照します。

- a) すべてのサーバの監査ログを参照するには、[すべてのサーバを選択 (Select All Servers)] チェックボックスをオンにします。
- b) 特定のサーバの監査ログを参照するには、サーバの横にあるチェックボックスをオンにします。

**ステップ 6** [終了 (Finish)] をクリックします。

**ステップ 7** [リモートブラウズの準備完了 (Remote Browse is Ready)] ウィンドウが表示されます。[閉じる (Close)] をクリックします。  
[ノード (Nodes)] ペインが表示されます。

**ステップ 8** [ノード (Nodes)] ペインの左側で[ノード (Nodes)] フォルダをダブルクリックします。[監査アプリ (Audit App)] フォルダが表示されるまでツリー階層を移動します。

**ステップ 9** ウィンドウの右側のペインに監査ログファイル名が表示されたら、マウスを右クリックして使用するプログラムの種類を選択して各ファイルを表示するか、または選択したファイルをダブルクリックしてデフォルトのビューアでファイルを表示することができます。

**ステップ 10** 監査ログファイルを選択し、次のいずれかのアクションを実行します。

- 収集した監査ログファイルの zip ファイルを作成するには、[ファイルを zip 圧縮する (Zip File)] オプション ボタンをクリックします。  
(注) 2 ギガバイトを超える zip 圧縮済み監査ログファイルはダウンロードできません。
- 収集した監査ログファイルをサーバから削除するには、[サーバ上のファイルを削除 (Delete Files on Server)] チェックボックスをオンにします。
- 選択した監査ログファイルを削除するには、[削除 (Delete)] をクリックします。
- 選択した監査ログファイルを更新するには、[更新 (Refresh)] をクリックします。
- すべての監査ログファイルを更新するには、[すべて更新 (Refresh All)] ボタンをクリックします。

(注) Cisco Unified Serviceability は Windows プラットフォームで実行される Cisco Unified Communications Manager または Cisco Unified Communications Manager IM and Presence Service バージョンからの監査ログを保持しません。

監査ログの参照の手順は完了です。

## 監査ログのダウンロード

### 手順

- 
- ステップ 1** Trace & Log Central のツリー階層を開きます。
- ステップ 2** [監査ログの収集 (Collect Audit Logs) ] をダブルクリックします。  
監査ログの収集アクション オプション ウィザードが表示されます。
- ステップ 3** [監査ログのダウンロード (Download Audit Logs) ] チェックボックスをオンにします。
- ステップ 4** [次へ (Next) ] をクリックします。  
[ノードの選択オプション (Nodes Selection Options) ] ウィザードが表示されます。
- ステップ 5** [Action Options (アクション オプション) ] ウィンドウで次のいずれかのアクションを実行します。
- (注) スタンドアロン サーバがあり、[すべてのサーバを選択 (Select All Servers) ] チェックボックスがオンの場合、システムは、スタンドアロン サーバのすべての監査ログをダウンロードします。
  - a) すべてのサーバの監査ログをダウンロードするには、[すべてのサーバを選択 (Select All Servers) ] チェックボックスをオンにします。
  - b) 特定のサーバの監査ログをダウンロードするには、サーバの横にあるチェックボックスをオンにします。
- ステップ 6** [終了 (Finish) ] をクリックします。
- ステップ 7** 監査ログをダウンロードするには、[次へ (Next) ] をクリックします。  
[監査ログのダウンロード (Download Audit Logs) ] ウィンドウが表示されます。
- ステップ 8** [ノードの選択オプション (Nodes Selection Options) ] ペインで、次のいずれかのアクションを実行します。
- [すべてのサーバを選択 (Select All Servers) ] チェックボックスをオンにします。
  - 特定のノードのチェックボックスをオンにします。
- ステップ 9** [収集時間 (Collection Time) ] 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。
- **絶対範囲 (Absolute Range) :** ログの監査範囲をサーバ タイムゾーンと時間範囲 (開始と終了の日時) で指定します。  
クライアント コンピュータのタイムゾーンにより、[リファレンスサーバ時間帯の選択 (Select Reference Server Time Zone) ] フィールドのデフォルトが設定されます。すべての標準タイムゾーンが [タイムゾーンを選択 (Select Time Zone) ] ドロップ ダウン リスト ボックスに表示され、[サマー タイム (Daylight Saving) ] が設定されたタイムゾーン用に独立した一連のエントリも表示されます。

Trace Log Central は、[選択したリファレンスサーバタイムゾーン (Selected Reference Server Time Zone)] に基づいて、時間範囲内のファイルをダウンロードします。クラスタ内のサーバが異なるタイムゾーン内に属している場合、TLCは時刻変更を調整し、同じ期間のファイルを取得します。たとえば、午前 9:00 ~ 午前 10:00 のファイルを指定し、2 番目のサーバ (server x) が時刻が 1 時間進んでいるタイムゾーンに属している場合、TLC は server x から午前 10:00 ~ 午前 11:00 のファイルをダウンロードします。

- 相対範囲 (Relative Range) : 次の表の値に基づいて、監査ログの収集範囲を現在時刻までの時間の長さ (分数、時間数、日数、週数、または月数) で指定します。

期間	範囲
Minutes	5 ~ 60
Hours	2 ~ 24
日 (Days)	1 ~ 31
週 (Weeks)	1 ~ 4
月 (Months)	1 ~ 12

**ステップ 10** [ダウンロードファイルオプション (Download File Options)] ペインで、次のいずれかのオプションを選択します。

- 監査ログファイルのダウンロード先のディレクトリを指定するには、[ファイルディレクトリのダウンロード (Download File Directory)] フィールドの横にある [参照 (Browse)] ボタンをクリックし、ディレクトリに移動し、[開く (Open)] をクリックします。デフォルトは <Program Files\Cisco\Unified RTMT\JRtmt> です。
- 収集した監査ログファイルの zip ファイルを作成するには、[ファイルを zip 圧縮する (Zip File)] オプション ボタンを選択します。  
(注) 2 ギガバイトを超える zip 圧縮済み監査ログファイルはダウンロードできません。
- 収集した監査ログファイルをサーバから削除するには、[収集されたログファイルをサーバから削除する (Delete Collected Log Files from Server)] チェックボックスをオンにします。

**ステップ 11** [終了 (Finish)] をクリックします。  
監査ログのダウンロードの手順は完了しました。

## 監査ログのダウンロードのスケジュール

### 手順

- ステップ 1 Trace & Log Central のツリー階層を開きます。
- ステップ 2 [監査ログの収集 (Collect Audit Logs) ] をダブルクリックします。  
監査ログの収集アクション オプション ウィザードが表示されます。
- ステップ 3 [監査ログのダウンロードのスケジュール (Schedule Download of Audit Logs) ] チェックボックスをオンにします。
- ステップ 4 [次へ (Next) ] をクリックします。  
[ノードの選択オプション (Nodes Selection Options) ] ウィザードが表示されます。
- ステップ 5 [Action Options (アクション オプション) ] ウィンドウで次のいずれかのアクションを実行します。
  - (注) スタンドアロン ノードがあり、[すべてのサーバを選択 (Select All Servers) ] チェックボックスをオンにすると、システムはスタンドアロン ノードのすべての監査ログを参照またはダウンロードするか、それらのダウンロードをスケジュールします。
  - a) すべてのノードの監査ログのダウンロードをスケジュールするには、[すべてのサーバを選択 (Select All Servers) ] チェックボックスをオンにします。
  - b) 特定のノード上の監査ログのダウンロードをスケジュールするには、ノードの横にあるチェックボックスをオンにします。
- ステップ 6 [終了 (Finish) ] をクリックします。  
[監査ログのダウンロードのスケジュール (Schedule Download of Audit Logs) ] ウィンドウが表示されます。
- ステップ 7 [ノードの選択オプション (Nodes Selection Options) ] ペインで、次のいずれかのアクションを実行します。
  - [すべてのサーバを選択 (Select All Servers) ] チェックボックスをオンにします。
  - 特定のノードのチェックボックスをオンにします。
- ステップ 8 [スケジュールの時間 (Schedule Time) ] ペインで、次の操作を実行します。
  - a) [リファレンス サーバ時間帯の選択 (Select Reference Server Time Zone) ] を強調表示します。
  - b) カレンダーを使用して、[開始日時 (Start Date/Time) ] を強調表示します。
  - c) カレンダーを使用して、[終了日時 (End Date/Time) ] を強調表示します。
  - d) [スケジューラ頻度 (Scheduler Frequency) ] を選択します。毎時、毎日、毎週、または毎月を選択できます。
  - e) 監査ログ ファイルを zip 圧縮する場合は、[すべてのファイルを zip 圧縮する (Zip All Files) ] チェックボックスをオンにします。

- f) 収集した監査ログ ファイルをノードから削除するには、[収集されたログ ファイルをサーバから削除する (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 9** [アクションオプション (Action Options) ] ペインで、[ファイルのダウンロード (Download Files) ] チェックボックスをオンにします。  
[トレースのダウンロード設定 (Trace Download Configuration) ] ダイアログ ウィンドウが表示されます。

**ステップ 10** 次の情報を入力します。

- プロトコル (Protocol) : FTP (デフォルト) または SFTP を選択します。
- ホストの IP アドレス (Host IP Address) : ホスト ノードの IP アドレスを入力します。
- ユーザ名 (User Name) : ユーザ名を入力します。
- パスワード (Password) : パスワードを入力します。
- ポート (Port) : FTP または SFTP のポート情報を入力します。
- ダウンロードディレクトリパス (Download Directory Path) : ファイルがダウンロードされるディレクトリの完全なパスを入力します。
- [テスト接続 (Test Connection) ] をクリックします。接続をテストしたら、ファイルがダウンロードされます。

(注) トレースをダウンロードする場合、[Localhost] ダウンロード オプションを選択できます。このオプションは、Cisco Intercompany Media Engine サーバに対してのみ使用可能です。

Cisco Intercompany Media Engine サーバのローカル ホストディレクトリにトレース ファイルをダウンロードする場合、**file get** CLI コマンドを使って、リモート SFTP サーバにファイルをオフロードできます。

(注) Cisco Intercompany Media Engine では、FTP はサポート対象外です。

監査ログのダウンロードをスケジュールするための手順は完了しました。

## ローカル ブラウズを使用したダウンロード済みトレース ファイルの表示

トレース ファイルを収集し、それらを自分の PC にダウンロードしたら、UNIX タイプの行終了文字を扱うことのできる WordPad などのテキスト エディタを使用してそれらを PC 上で表示できます。あるいは、Unified RTMT 内のビューアを使用してそれらを表示することもできます。



**ヒント** 収集されたトレース 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 機能を使用して収集したログ ファイルを表示するには、次の手順を実行します。PC へのダウンロード時にトレース ファイルを zip 圧縮した場合、Unified RTMT 内のビューアを使用してそれらを表示するには、ファイルを解凍しておく必要があります。



- (注) Trace & Log Central 内では、表示用として最大 5 つの同時ファイルを開くことができます。これにはクエリー ウィザード、ローカルブラウザ、リモートブラウザ機能の使用が含まれません。

### はじめる前に

必要なトレース ファイルを収集します。手順については、トレース ファイルの収集、クエリー ウィザードを使用したトレース ファイルのダウンロード、トレース収集のスケジューリングに関するトピックを参照してください。

### 手順

- ステップ 1** Trace and Log Central を開きます。
- ステップ 2** [ローカルブラウザ (Local Browse) ] をダブルクリックします。
- ステップ 3** ログ ファイルを保存したディレクトリを参照し、表示するファイルを選択します。
- ステップ 4** 結果を表示するには、ファイルをダブルクリックします。  
ファイルタイプに関連付けられたビューアがすでに存在する場合、ファイルはそのビューアで開かれます。そうでない場合は、[プログラムから開く (Open With) ] ダイアログボックスが表示されます。
- ステップ 5** ファイルの表示に使用するプログラムをクリックします。優先プログラムがリスト上にない場合は、[その他 (Other) ] をクリックして別のプログラムを選択します。  
このプログラムをデフォルトのビューアとして使用する場合は、[この種類のファイルを開くときは、選択したプログラムをいつも使う (Always use this program to open these files) ] チェックボックスをオンにします。

Unified RTMT は、ファイルをファイルタイプに応じて適切なビューアで表示します。他に適切なビューアがなければ、Unified RTMT は Generic Log Viewer でファイルを開きます。

## Cisco Unified Communications Manager でのトレース ファイルの表示とダウンロード

システムがトレース ファイルを生成すると、Unified RTMT 内でビューアを使用してノードで表示できます。また、リモートブラウザ機能を使用して PC にトレースをダウンロードすることもできます。

Trace and Log Central 機能を使用してノードでログ ファイルを表示およびダウンロードするには、次の手順を実行します。



- (注) Trace and Log Central 内では、表示用として最大 5 つの同時ファイルを開くことができます。これにはクエリー ウィザード、ローカルブラウザ、リモート ブラウズ機能の使用が含まれません。

### はじめる前に

必要なトレース ファイルを収集します。トレース ファイルの収集、クエリー ウィザードを使用したトレース ファイルのダウンロード、トレース収集のスケジューリングに関するトピックを参照してください。

### 手順

- ステップ 1** [Trace and Log Central] オプションを開きます。
- ステップ 2** [リモートブラウザ (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、[次へ (Next) ] をクリックします。
- [トレース ファイル (Trace Files) ] を選択した場合は、ステップ 4 に進みます。
  - [クラッシュ ダンプ (Crash Dump) ] を選択した場合は、ステップ 7 に進みます。
- (注) サービスは、アクティブにされていなくても表示されます。したがって、それらのサービスに対してトレースを選択できます。
- (注) [クラッシュ ダンプ (Crash Dump) ] を選択すると、ウィザードはクラッシュ ダンプが生じる可能性があるサービスだけを表示します。関心のあるサービスが表示されない場合は、[戻る (Back) ] をクリックし、[トレースファイル (Trace Files) ] を選択します。
- (注) 一部の一覧されているサービスまたはアプリケーションをクラスタ内の特定のノード上にだけインストールすることができます。それら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には、そのサービスまたはアプリケーションがアクティブにされているノードからトレースを選択するようにします。
- ステップ 4** [CCM サービス/アプリケーションの選択 (Select CCM Services/Application) ] タブで、次のいずれかの操作を実行します。
- (注) スタンドアロンノードがあり、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers) ] チェックボックスがオンの場合、システムは、スタンドアロンノードのすべてのサービスとアプリケーションのトレースを収集します。
- すべてのノードに対してすべてのサービスとアプリケーションのトレースを収集するには、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on All Servers) ] チェックボックスをオンにして [次へ (Next) ] をクリックします。
  - 特定ノード上のすべてのサービスとアプリケーションのトレースを収集するには、ノードの横にあるチェックボックスをオンにして、[次へ (Next) ] をクリックします。

- 特定のノード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には、適用するチェックボックスをオンにして、[次へ (Next) ] をクリックします。
- サービスまたはアプリケーションのトレースを収集しないでリモート ブラウズ ウィザードを続行するには、[次へ (Next) ] をクリックします。

**ステップ 5** [システム サービス/アプリケーションの選択 (Select System Services/Application) ] タブで、次のいずれかの操作を実行します。

- (注) スタンドアロンノードがあり、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers) ] チェックボックスがオンの場合、システムは、スタンドアロンノードのシステム ログを収集します。
- a) すべてのノードに対してすべてのシステム ログを収集するには、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers) ] チェックボックスをオンにして [次へ (Next) ] をクリックします。
  - b) 特定ノード上のすべてのシステム ログのトレースを収集するには、ノードの横にあるチェックボックスをオンにして、[次へ (Next) ] をクリックします。
  - c) 特定のノード上の特定のシステム ログのトレースを収集するには、適用するチェックボックスをオンにして、[次へ (Next) ] をクリックします。
  - d) システム ログのトレースを収集しないでリモート ブラウズ ウィザードを続行するには、[次へ (Next) ] をクリックします。
  - e) ステップ 10 に進みます。

**ステップ 6** [CCM サービス/アプリケーションの選択 (Select CCM Services/Application) ] タブで、次のいずれかの操作を実行します。

- (注) スタンドアロンノードがあり、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers) ] チェックボックスがオンの場合、システムは、スタンドアロンノードのクラッシュ ダンプ ファイルを収集します。
- a) すべてのノードに対してすべてのサービスと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には、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers) ] チェックボックスをオンにして [次へ (Next) ] をクリックします。
  - b) 特定ノード上のすべてのサービスと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には、ノードの横にあるチェックボックスをオンにして、[次へ (Next) ] をクリックします。
  - c) 特定のサービスのクラッシュ ダンプ ファイルまたは特定のノードのアプリケーションを選択するには、適用するチェックボックスをオンにして、[次へ (Next) ] をクリックします。
  - d) クラッシュ ダンプ ファイルを収集しないでリモート ブラウズ ウィザードを続行するには、[次へ (Next) ] をクリックします。

Cisco Business Edition の場合はステップ 8 に進み、Unified Communications Manager の場合はステップ 9 に進みます。

**ステップ 7** [システム サービス/アプリケーションの選択 (Select System Services/Application) ] タブで、次のいずれかのタスクを実行します。

- (注) スタンドアロンノードがあり、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers) ] チェックボックスがオンの場合、システムは、スタンドアロンノードのクラッシュ ダンプ ファイルを収集します。

- a) すべてのノードでクラッシュ ダンプ ファイルを選択するには、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers)] チェックボックスをオンにします。
- b) 特定ノード上のすべてのシステム ログのクラッシュ ダンプ ファイルを選択するには、ノードの横にあるチェックボックスをオンにします。
- c) 特定ノード上の特定のシステム ログのクラッシュ ダンプ ファイルを選択するには、適用するチェックボックスをオンにします。
- d) クラッシュ ダンプ ファイルを収集しないでリモート ブラウズ ウィザードを続行するには、次のステップに進みます。

**ステップ 8** [終了 (Finish)] をクリックします。

**ステップ 9** トレースが使用できるようになると、メッセージが表示されます。[閉じる (Close)] をクリックします。

**ステップ 10** 次のいずれかの操作を実行します。

- 結果を表示するには、ツリー階層を使用してファイルを選択します。ログのファイル名がウィンドウの右側のペインに表示されたら、マウスを右クリックして使用するプログラムの種類を選択してファイルを表示するか、ファイルをダブルクリックしてデフォルトのビューアで表示します。

**ヒント** ペイン内に表示されるファイルをソートするには、カラムの見出しをクリックします。たとえば、ファイルを名前でソートするには、[名前 (Name)] カラム見出しをクリックします。

Real-Time Monitoring Tool は、ファイル タイプに応じて適切なビューアでファイルを表示します。他に適切なビューアがなければ、Real-Time Monitoring Tool は Generic Log Viewer でファイルを開きます。

- 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、[ダウンロード (Download)] をクリックし、ダウンロードの条件を指定して、[終了 (Finish)] をクリックします。
  - トレース ファイルのダウンロード先のディレクトリを指定するには、[すべてのファイルのダウンロード (Download all files)] フィールドの横にある [参照 (Browse)] をクリックし、ディレクトリに移動し、[開く (Open)] をクリックします。デフォルトは <rtmt\_users\_directory>\<server name または server IP address>\<download time> です。
  - 収集したトレース ファイルの zip ファイルを作成するには、[ファイルを zip 圧縮する (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ノードから削除するには、[サーバ上のファイルを削除 (Delete Files on server)] チェックボックスをオンにします。
- ノードからトレースファイルを削除するには、ウィンドウの右側のペインに表示されるファイルをクリックし、[削除 (Delete)] をクリックします。
- クラスタ内の特定のサービスまたは特定のノードを更新するには、サービスまたはノード名をクリックし、[更新 (Refresh)] をクリックします。リモートブラウズの準備が完了したことを通知するメッセージが表示されたら、[閉じる (Close)] をクリックします。

- ツリー階層で表示されるクラスタ内のすべてのサービスまたはすべてのノードを更新するには、[すべて更新 (Refresh All)] をクリックします。リモートブラウズの準備が完了したことを通知するメッセージが表示されたら、[閉じる (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、ローカルブラウザで表示できます。

## Cisco Unity Connection でのトレース ファイルの表示とダウンロード

システムがトレース ファイルを生成すると、Unified RTMT 内でビューアを使用してノードで表示できます。また、リモートブラウズ機能を使用して PC にトレースをダウンロードすることもできます。

Trace and Log Central 機能を使用してノードでログ ファイルを表示およびダウンロードするには、次の手順を実行します。



- (注) Trace and Log Central 内では、表示用として最大 5 つの同時ファイルを開くことができます。これにはクエリー ウィザード、ローカルブラウズ、リモートブラウズ機能の使用が含まれません。

### はじめる前に

必要なトレース ファイルを収集します。トレース ファイルの収集、クエリー ウィザードを使用したトレース ファイルのダウンロード、トレース収集のスケジューリングに関するトピックを参照してください。

### 手順

- ステップ 1** [Trace and Log Central] オプションを開きます。
- ステップ 2** [リモートブラウズ (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、[次へ (Next)] をクリックします。
  - (注) サービスは、アクティブにされていなくても表示されます。したがって、それらのサービスに対してトレースを選択できます。
  - (注) [クラッシュ ダンプ (Crash Dump)] を選択すると、ウィザードはクラッシュ ダンプが生じる可能性があるサービスだけを表示します。関心のあるサービスが表示されない場合は、[戻る (Back)] をクリックし、[トレースファイル (Trace Files)] を選択します。
  - (注) Cisco Unity Connection クラスタ：アプリケーションにリストされているサービスの一部をクラスタ内の特定のノードにインストールすることができます。それら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には、そのサービスまたはアプリケーションがアクティブにされているノードからトレースを選択するようにします。

- ステップ 4** [CUC サービス/アプリケーションの選択 (Select CUC Services/Application) ] タブで、次のいずれかの操作を実行します。
- ノードのすべてのシステム ログを収集するには、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers) ] チェックボックスをオンにするか、ノードの横にあるチェックボックスをオンにして、[次へ (Next) ] をクリックします。
  - ノード上の特定のシステム ログのトレースを収集するには、適用するチェックボックスをオンにして、[次へ (Next) ] をクリックします。
  - システム ログのトレースを収集しないでリモート ブラウズ ウィザードを続行するには、[次へ (Next) ] をクリックします。
- ステップ 5** [システム サービス/アプリケーションの選択 (Select System Services/Application) ] タブで、次のいずれかの操作を実行します。
- (注) スタンドアロンノードがあり、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers) ] チェックボックスがオンの場合、システムは、スタンドアロンノードのシステム ログを収集します。
- すべてのノードに対してすべてのシステム ログを収集するには、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers) ] チェックボックスをオンにして [次へ (Next) ] をクリックします。
  - 特定ノード上のすべてのシステム ログのトレースを収集するには、ノードの横にあるチェックボックスをオンにして、[次へ (Next) ] をクリックします。
  - 特定のノード上の特定のシステム ログのトレースを収集するには、適用するチェックボックスをオンにして、[次へ (Next) ] をクリックします。
  - システム ログのトレースを収集しないでリモート ブラウズ ウィザードを続行するには、[次へ (Next) ] をクリックします。
- ステップ 6** [CUC サービス/アプリケーションの選択 (Select CUC Services/Application) ] タブで、次のいずれかのタスクを実行します。
- ノードのクラッシュ ダンプ ファイルを選択するには、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers) ] チェックボックスをオンにするか、ノードの横にあるチェックボックスをオンにして、[次へ (Next) ] をクリックします。
  - ノード上の特定のシステム ログのクラッシュ ダンプ ファイルを選択するには、適用するチェックボックスをオンにして、[次へ (Next) ] をクリックします。
  - クラッシュ ダンプ ファイルを収集しないでリモート ブラウズ ウィザードを続行するには、[次へ (Next) ] をクリックします。
- ステップ 7** [システム サービス/アプリケーションの選択 (Select System Services/Application) ] タブで、次のいずれかのタスクを実行します。
- (注) スタンドアロンノードがあり、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers) ] チェックボックスがオンの場合、システムは、スタンドアロンノードのクラッシュ ダンプ ファイルを収集します。

- すべてのノードでクラッシュ ダンプ ファイルを選択するには、[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers)] チェックボックスをオンにします。
- 特定ノード上のすべてのシステム ログのクラッシュ ダンプ ファイルを選択するには、ノードの横にあるチェックボックスをオンにします。
- 特定ノード上の特定のシステム ログのクラッシュ ダンプ ファイルを選択するには、適用するチェックボックスをオンにします。
- クラッシュ ダンプ ファイルを収集しないでリモート ブラウズ ウィザードを続行するには、次のステップに進みます。

**ステップ 8** [終了 (Finish)] をクリックします。

**ステップ 9** トレースが使用できるようになると、メッセージが表示されます。[閉じる (Close)] をクリックします。

**ステップ 10** 次のいずれかの操作を実行します。

- 結果を表示するには、ツリー階層を使用してファイルを選択します。ログのファイル名がウィンドウの右側のペインに表示されたら、マウスを右クリックして使用するプログラムの種類を選択してファイルを表示するか、ファイルをダブルクリックしてデフォルトのビューアで表示します。

**ヒント** ペイン内に表示されるファイルをソートするには、カラムの見出しをクリックします。たとえば、ファイルを名前でソートするには、[名前 (Name)] カラム見出しをクリックします。

Real-Time Monitoring Tool は、ファイル タイプに応じて適切なビューアでファイルを表示します。他に適切なビューアがなければ、Real-Time Monitoring Tool は Generic Log Viewer でファイルを開きます。

- 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、[ダウンロード (Download)] をクリックし、ダウンロードの条件を指定して、[終了 (Finish)] をクリックします。
  - トレース ファイルのダウンロード先のディレクトリを指定するには、[すべてのファイルのダウンロード (Download all files)] フィールドの横にある [参照 (Browse)] をクリックし、ディレクトリに移動し、[開く (Open)] をクリックします。デフォルトは <rtmt\_user\_directory>\<server name または server IP address>\<download time> です。ここで、<rtmt\_user\_directory> は Unified RTMT のインストール先のディレクトリです。
  - 収集したトレース ファイルの zip ファイルを作成するには、[ファイルを zip 圧縮する (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ノードから削除するには、[サーバ上のファイルを削除 (Delete Files on server)] チェックボックスをオンにします。
- ノードからトレースファイルを削除するには、ウィンドウの右側のペインに表示されるファイルをクリックし、[削除 (Delete)] をクリックします。

- クラスタ内の特定のサービスまたは特定のノードを更新するには、サービスまたはノード名をクリックし、[更新 (Refresh)] をクリックします。リモートブラウザの準備が完了したことを通知するメッセージが表示されたら、[閉じる (Close)] をクリックします。
  - ツリー階層で表示されるクラスタ内のすべてのサービスまたはすべてのノードを更新するには、[すべて更新 (Refresh All)] をクリックします。リモートブラウザの準備が完了したことを通知するメッセージが表示されたら、[閉じる (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、ローカルブラウザで表示できます。

## トレース収集属性の設定

### はじめる前に

トレース ファイルを収集します。

### 手順

- ステップ 1** Trace & Log Central を開きます。
- ステップ 2** [リモートブラウザ (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 ([トレース ファイル (Trace Files)] または [クラッシュ ダンプ (Crash Dump)]) を選択します。
- ステップ 4** [次へ (Next)] を選択します。
- ステップ 5** 次のいずれかの操作を実行します。
- [トレース ファイル (Trace Files)] を選択した場合は、ステップ 6 に進みます。
  - [クラッシュ ダンプ (Crash Dump)] を選択した場合は、ステップ 8 に進みます。
- ステップ 6** [音声/ビデオ (Voice/Video)] または [IM and Presence アプリケーション/サービス (IM and Presence Applications/Services)] タブで、次のいずれかの操作を実行します。

目的	Action
クラスタ内のすべてのサーバに対してすべてのサービスとアプリケーションのトレースを収集する	<ul style="list-style-type: none"> <li>• [すべてのサーバ上のすべてのサービスを選択する (Select All Services on All Servers)] を選択します。</li> <li>• [次へ (Next)] を選択します。</li> </ul>
特定のサーバ上のすべてのサービスとアプリケーションのトレースを収集する	<ul style="list-style-type: none"> <li>• サーバ名を確認します。</li> <li>• [次へ (Next)] を選択します。</li> </ul>



目的	Action
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	<ul style="list-style-type: none"> <li>適用するトレースをオンにします。</li> <li>[次へ (Next) ] を選択します。</li> </ul>
サービスまたはアプリケーションのトレースを収集しないでトレース収集ウィザードを続行する	[次へ (Next) ] を選択します。

**ステップ 7** [システム サービス/アプリケーションの選択 (Select System Services/Application) ] タブで、次のいずれかの操作を実行します。

目的	Action
クラスタ内のすべてのサーバのすべてのシステム ログを収集する	<ul style="list-style-type: none"> <li>[すべてのサーバ上のすべてのサービスを選択する (Select All Services on all Servers) ] をオンにします。</li> <li>[次へ (Next) ] を選択します。</li> </ul>
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	<ul style="list-style-type: none"> <li>サーバ名を確認します。</li> <li>[次へ (Next) ] を選択します。</li> </ul>
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	<ul style="list-style-type: none"> <li>適用するトレースをオンにします。 (注) たとえば、CSA ログを収集するには、[Cisco Security Agent] をオンにします。ログイン中およびログアウト中のユーザに関する情報が得られるユーザ ログにアクセスするには、[セキュリティ ログ (Security Logs) ] をオンにします。</li> <li>[次へ (Next) ] を選択します。</li> </ul>
システム ログのトレースを収集しないでリモートブラウザウィザードを続行する	終了の選択に進みます。

**ステップ 8** [音声/ビデオ (Voice/Video) ] または [IM and Presence アプリケーション/サービス (IM and Presence Applications/Services) ] タブで、次のいずれかの操作を実行します。

目的	Action
クラスタ内のすべてのサーバに対してすべてのサービスとアプリケーションのクラッシュ ダンプ ファイルを収集する	<ul style="list-style-type: none"> <li>• [すべてのサーバ上のすべてのサービスを選択する (Select All Services on All Servers) ] をオンにします。</li> <li>• [次へ (Next) ] を選択します。</li> </ul>
特定のサーバ上のすべてのサービスとアプリケーションのクラッシュ ダンプ ファイルを収集する	<ul style="list-style-type: none"> <li>• サーバ名を確認します。</li> <li>• [次へ (Next) ] を選択します。</li> </ul>
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 ファイルを収集する	<ul style="list-style-type: none"> <li>• 適用するトレースをオンにします。</li> <li>• [次へ (Next) ] を選択します。</li> </ul>

**ステップ 9** [システム サービス/アプリケーションの選択 (Select System Services/Application) ] タブで、次のいずれかの操作を実行します。

目的	Action
クラスタ内のすべてのサーバに対してすべてのサービスとアプリケーションのクラッシュ ダンプ ファイルを収集する	<ul style="list-style-type: none"> <li>• [すべてのサーバ上のすべてのサービスを選択する (Select All Services on All Servers) ] をオンにします。</li> <li>• [次へ (Next) ] を選択します。</li> </ul>
特定のサーバ上のすべてのサービスとアプリケーションのクラッシュ ダンプ ファイルを収集する	<ul style="list-style-type: none"> <li>• サーバ名を確認します。</li> <li>• [次へ (Next) ] を選択します。</li> </ul>
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 ファイルを収集する	<ul style="list-style-type: none"> <li>• 適用するトレースをオンにします。</li> <li>• [次へ (Next) ] を選択します。</li> </ul>
クラッシュ ダンプ ファイルを収集しないでクラッシュ ダンプの収集ウィザードを続行する	ステップ 10 に進みます。

**ステップ 10** [完了 (Finish) ] を選択します。

## 次の作業

トレース結果を表示します。

## トレース結果の表示

- 一部の一覧されているサービスまたはアプリケーションをクラスタ内の特定のノード上にだけインストールすることができます。それら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には、そのサービスまたはアプリケーションがアクティブにされているサーバからトレースを選択します。
- サービスは、アクティブにされていなくても表示されます。したがって、それらのサービスに対してトレースを選択できます。
- トレース ファイルのダウンロードが完了したら、Trace and Log Central 機能のローカル ブラウズ オプションを使用してそれらを表示できます。
- ペイン内に表示されているファイルをソートするには、カラムヘッダーを選択します。たとえば、ファイルを名前でソートするには、[名前 (Name) ] カラム ヘッダーを選択します。
- Real-Time Monitoring Tool は、ファイル タイプに応じて適切なビューアでファイルを表示します。他に適切なビューアがなければ、Real-Time Monitoring Tool は Generic Log Viewer でファイルを開きます。
- IM and Presence Service は、Q931 トランスレータをサポートしません。IM and Presence は、QRT レポート情報をサポートしません。

## はじめる前に

トレース収集属性を設定します。

## 手順

**ステップ 1** トレース結果が使用可能になったことを示すメッセージが表示されたら、[閉じる (Close) ] を選択します。

**ステップ 2** 次のいずれかの操作を実行します。

目的	Action
結果を表示する	次のいずれかの操作を実行して、ファイルを表示します。 マウスを右クリックしてファイルの表示に使用するプログラムの種類を選択します。ファイルをダブルクリックしてデフォルトのビューアでファイルを表示します。

目的	Action
トレース ファイル、およびクエリーで収集されたトレース ファイルのリストを含む結果ファイルをダウンロードする	<ul style="list-style-type: none"> <li>• ダウンロードするファイルを選択します。</li> <li>• [ダウンロード (Download) ] を選択します。</li> <li>• ダウンロードの条件を指定します。</li> <li>• [完了 (Finish) ] を選択します。</li> </ul>
トレース ファイルと結果ファイルをダウンロードするディレクトリを指定する	<ul style="list-style-type: none"> <li>• [すべてのファイルのダウンロード (Download all files) ] フィールドの隣にある [参照 (Browse) ] を選択します。</li> <li>• 対象のディレクトリに移動します。</li> <li>• [開く (Open) ] を選択します。デフォルトでは、 C:\Program Files\Cisco\Presence Serviceability\jrtmt\<server address&gt;\&lt;download="" ip="" li="" time&gt;="" が指定されます。<=""> </server></li></ul>
収集したトレースファイルの zip ファイルを作成する	[ファイルを zip 圧縮する (Zip File) ] 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	[収集されたログ ファイルをサーバから削除する (Delete Collected Log Files from Server) ] 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	<ul style="list-style-type: none"> <li>• ウィンドウの右側のペイン内に表示されているファイルを選択します。</li> <li>• [削除 (Delete) ] を選択します。</li> </ul>
特定のサービスまたはノードを更新する	<ul style="list-style-type: none"> <li>• サーバ名またはサービスを選択します。</li> <li>• [リフレッシュ (Refresh) ] を選択します。</li> <li>• リモート ブラウズの準備が整ったことを示すメッセージが表示されたら、[閉じる (Close) ] を選択します。</li> </ul>
ツリー階層に表示されているすべてのサービスとノードを更新する	<ul style="list-style-type: none"> <li>• [すべて更新 (Refresh All) ] を選択します。</li> <li>• リモート ブラウズの準備が整ったことを示すメッセージが表示されたら、[閉じる (Close) ] を選択します。</li> </ul>

## レポート情報の表示

サーバ上のファイルを表示するか、コンピュータにファイルをダウンロードすることで、QRT のログ ファイルを表示できます。



(注) このセクションは、Cisco Unified Communications Manager にのみ適用されます。

Quality Report Tool (QRT) が生成した IP 電話の問題に関するレポートを表示するには、QRT ビューアを使用します。QRT は、Cisco Unified IP Phone の音声品質と一般的な問題を報告するツールとして役立ちます。QRT のログ ファイルを収集した後、QRT ビューアを使用して Cisco Unified Communications Manager の IP 電話の問題レポートを一覧表示するには、次の手順を使用します。QRT ビューアを使用すると、生成された電話問題レポートをフィルタ、フォーマット、および表示できます。QRT を設定して使用方法の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

### はじめる前に

Quality Report Tool (QRT) のログ ファイルを収集または表示します。トレース ファイルの収集、トレース収集のスケジューリング、およびクエリーウィザードまたはリモートブラウザを使用したトレース ファイルのダウンロードに関するトピックを参照してください。

### 手順

**ステップ 1** Trace and Log Central の、クエリーウィザード、リモートブラウザまたはローカルブラウザオプションを使用して、ログ ファイルのエントリを表示します。

[QRT ビューア (QRT Viewer) ] ウィンドウが表示されます。

- (注) Cisco Extended Functions サービスのログ ファイルのみ QRT 情報が含まれます。QRT データを含むログ ファイル名の形式は、`qrtXXX.xml` です。
- (注) QRT ビューアでは、デフォルトではない特定の構造 (電話機の詳細を含む) の .xml ファイルだけが許可されます。一般的なログ ファイルを開いた場合、次のエラーメッセージが表示されることがあります。

Cisco QRT ビューアを開けません。使用可能なレコードはありません! (Fail to Open Cisco QRT Viewer, No Records Available!)

- ステップ 2** [拡張子 (Extension) ] ドロップダウン リスト ボックス から、レポートに含めるエクステンションを選択します。
- ステップ 3** [デバイス (Device) ] ドロップダウン リスト ボックス から、レポートに含めるデバイスを選択します。
- ステップ 4** [カテゴリ (Category) ] ドロップダウン リスト ボックス から、レポートに含める問題カテゴリを選択します。
- ステップ 5** [フィールドの選択 (Select Fields) ] ドロップダウン リスト ボックス から、レポートに含めるフィールドを選択します。  
(注) フィールドを選択する順序によって、[QRT レポート結果 (QRT Report Result) ] ペインに表示される順序が決まります。
- ステップ 6** [QRT レポート結果 (QRT Report Result) ] ペインでレポートを表示するには、[レコードの表示 (Display Records) ] をクリックします。
- 

## ログの圧縮

Unified Communications Manager 8.0 以降、ログ圧縮機能は次のログ ファイルだけを圧縮します。

- cm/trace/cti/sdl
- cm/trace/cti/sdi
- cm/trace/ccm/sdl
- cm/trace/ccm/sdi

他のログ ファイルは圧縮されず、ハードディスクに直接書き込まれます。

圧縮されたファイルには、.gz の拡張子が付きます。ディスクに現在書き込み中のファイルには、.gzo の拡張子が付きます。

ファイルを表示し追跡するために使用されるすべての CLI コマンドが圧縮ファイルに対して動作して、ファイルを自動的に解凍して、表示または追跡できるようにします。.gz 拡張子、.gzo 拡張子が付くファイル名を指定する点のみが異なります。

file tail コマンドで使用可能なオプションは次のとおりです。

```
file tail activelog cm/trace/cti/sdl recent
```

recent オプションは、圧縮されたディレクトリと併用することで、最新のログ ファイルを継続的に追跡します。無限に継続する追跡なので、現在書き込み中のログ ファイルが閉じている場合、新しいログファイルに切り替える必要はありません。このオプションは、圧縮されたログファイルでのみ可能です。

ログ ファイルは gzip 形式に圧縮されます。このログ ファイルを解凍するには、オープン ソース プログラム 7-Zip を <http://www.7-zip.org> から手に入れることができます。これは、すべての Windows プラットフォームで動作します。7-Zip は、会社のコンピュータも含め、お使いのコンピュータで使用できます。7-Zip には登録も料金の支払いも必要ありません。Linux プラットフォームでは、gzip または gunzip コマンドを使用できます。

## トレース設定の編集

Unified RTMT のトレース設定を編集するには、次の手順に従ってください。



(注) [エラー (Error) ] オプション ボタンがデフォルト設定です。

### 手順

**ステップ 1** [編集 (Edit) ] > [トレースの設定 (Trace Setting) ] の順に選択します。

**ステップ 2** 適用するオプション ボタンをクリックします。

rtmt.log ファイルはユーザの Documents and Settings ディレクトリに保存されます。たとえば、Windows マシンでは、ログは C:\Documents and Settings\\.jrtmt\log に保存されます。

## ログ ビューア

### AuditLog ビューア内のメッセージ

AuditLog ビューアには次のメッセージを表示できます。

- AuditLog ログ : Unified Communications Manager アプリケーションの監査ログに関連するログ。
- vos ログ : プラットフォーム (端末、ポートまたはシステムのネットワーク アドレス) のアクティビティに関連するログ。

次の表に、AuditLog ビューアのボタンについて説明します。

表 19: AuditLog ビューアのボタン

ボタン	機能
更新 (Refresh)	Auditlog ビューア上の現在のログの内容を更新します。 ヒント [自動更新 (Auto Refresh) ] チェックボックスをオンにすることにより、Auditlog ビューアで自動的に現在のログ ファイルが 5 秒ごとに更新されるように設定できます。
クリア (Clear)	現在のログの表示をクリアします。

ボタン	機能
フィルタ	auditapp ログの場合は、選択したユーザ ID に基づき、表示されるログが制限されます。  vos ログの場合は、選択したオプションセット（アドレス、端末、およびタイプ）に基づき、表示されるログが制限されます。  ヒント [逆にフィルタする (Filter Inverse) ] チェックボックスをオンにすると、選択したオプションセット以外のログを表示できます。
フィルタのクリア (Clear Filter)	表示されるログのタイプを制限するフィルタを削除します。
検索 (Find)	現在のログ内で特定の文字列を検索できます。
保存します。	現在選択されているログを PC に保存します。

監査ログメッセージを表示する際にカラムを拡大または縮小するには、2つのカラムの見出しの間にマウスポインタを置いたときに表示される矢印をドラッグします。

カラムの見出しをクリックすることにより、監査ログメッセージを整理できます。カラムの見出しを最初にクリックしたときは、ログは昇順で表示されます。上向きの小さい三角形が、昇順を示します。カラムの見出しを再びクリックすると、ログは降順で表示されます。下向きの小さい三角形が、降順を示します。カラムの見出しをもう一度選択すると、ログのソートは解除されます。

## AuditApp ログの表示

### 手順

- ステップ 1 [システム (System) ] > [ツール (Tools) ] > [AuditLog ビューア (AuditLog Viewer) ] の順に選択します。
- ステップ 2 [ノードの選択 (Select a Node) ] ドロップダウンリストで、表示するログが格納されているサーバを選択します。
- ステップ 3 [AuditApp のログ (AuditApp Logs) ] フォルダをダブルクリックします。
- ステップ 4 現在のログを表示するには、[アーカイブ (Archive) ] フォルダの外にある .log ファイルをクリックします。選択したノード用の AuditApp ログは表形式で表示されます。  
(注) 古いログを表示する場合は、[アーカイブ (Archive) ] フォルダをダブルクリックし、対応するファイルをクリックします。
- ステップ 5 表示するエントリをダブルクリックします。その特定のエントリの監査ログメッセージが新しいウィンドウに表示されます。



ヒント [フィルタ条件 (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して、監査ログメッセージの表示結果をフィルタできます。フィルタを削除するには、[フィルタのクリア (Clear Filter)] をクリックします。フィルタをクリアした後は、すべてのログが表示されます。

## Cisco Unified OS ログの表示

### 手順

- ステップ 1** [システム (System)] > [ツール (Tools)] > [AuditLog ビューア (AuditLog Viewer)] の順に選択します。
- ステップ 2** [ノードの選択 (Select a Node)] ドロップダウンリストで、表示するログが格納されているノードを選択します。
- ステップ 3** [Cisco Unified OS ログ (Cisco Unified OS Logs)] フォルダをダブルクリックします。
- ステップ 4** 現在のログを表示するには、[アーカイブ (Archive)] フォルダの外にある vos-audit.log ファイルをクリックします。選択したノードに対する Cisco Unified OS ログは表形式で表示されます。  
(注) 古いログを表示する場合は、[アーカイブ (Archive)] フォルダをダブルクリックし、対応するファイルをクリックします。
- ステップ 5** 表示するエントリをダブルクリックします。その特定のエントリの Cisco Unified OS ログメッセージが新しいウィンドウに表示されます。
- ヒント [フィルタ (Filter)] をクリックすると表示されるポップアップ ウィンドウのオプションのセットを選択することにより、Cisco Unified OS ログメッセージの表示結果をフィルタできます。フィルタを削除するには、[フィルタのクリア (Clear Filter)] をクリックします。フィルタをクリアした後は、すべてのログが表示されます。

## SysLog ビューアでのメッセージの表示

SysLog ビューアでメッセージを表示できます。



ヒント syslog メッセージをダブルクリックすると、CiscoSyslog メッセージは隣接するペインに推奨処置を含む syslog 定義も表示します。この情報のために Cisco Unified Serviceability のアラーム定義にアクセスする必要はありません。

以下の表で、SysLog ビューアのボタンについて説明します。

表 20: SysLog ビューアのボタン

ボタン	機能
更新 (Refresh)	SysLog ビューア上の現在のログの内容を更新します。 ヒント [自動更新 (Auto Refresh)] チェックボックスをオンにすることにより、SysLog ビューアで自動的に5秒ごとに syslog メッセージが更新されるように設定できます。
クリア (Clear)	現在のログの表示をクリアします。
フィルタ	選択したオプションに基づいて、表示されるメッセージを制限します。
フィルタのクリア (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解除します。
検索 (Find)	現在のログ内で特定の文字列を検索できます。
保存します。	現在選択されているログを PC に保存します。

syslog メッセージを表示しているときに、2つのカラムの見出しの間にマウスを置くと表示される矢印をドラッグして、カラムを大きくしたり小さくしたりします。

カラムの見出しをクリックすると、表示された syslog メッセージを整理できます。カラムの見出しを最初にクリックしたときは、レコードが昇順で表示されます。上向き小さい三角形が、昇順を示します。カラムの見出しを再びクリックすると、レコードは降順で表示されます。下向き小さい三角形が、降順を示します。カラムの見出しをもう一度クリックすると、レコードのソートは解除されます。

## 手順

- 
- ステップ 1** [システム (System) ]>[ツール (Tools) ]>[Syslog ビューア (SysLog Viewer) ]>[Syslog ビューアを開く (Open SysLog Viewer) ]の順に選択します。
- ステップ 2** [ノードの選択 (Select a Node) ] ドロップダウン リスト ボックスで、表示するログが格納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選択します。
- ステップ 4** ログが表示されると、ログアイコンをダブルクリックして、同じウィンドウ内にファイル名を表示します。  
ヒント syslog メッセージの中にウィンドウに表示されていないものがある場合、欠落している syslog メッセージの上にマウス ポインタをスクロールすると、表示が更新されます。
- 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選択します。

完全な syslog メッセージを表示するには、syslog メッセージをダブルクリックします。「SysLog ビューアのボタン」の表で説明したボタンを使用して syslog メッセージを表示することもできます。

**ヒント** [フィルタ条件 (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して、syslog メッセージの表示結果をフィルタできます。フィルタを削除するには、[フィルタのクリア (Clear Filter)] をクリックします。フィルタをクリアした後は、すべてのログが表示されます。

## プラグイン

### アプリケーション プラグインのダウンロードとインストール

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ことにより、Unified RTMT の機能を拡張できます。Cisco.com から Unified RTMT の最新のプラグインをダウンロードできます。プラグインをインストールすると、Unified RTMT 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して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** [アプリケーション (Application)] > [CCO 音声ツールのダウンロード (CCO Voice Tools Download)] の順に選択します。  
ログインプロンプトが表示されます。
- ステップ 2** 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** PC にファイルを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。

### アプリケーション プラグインの起動

プラグインをダウンロードしてインストールすると、RTMT ビューアでアプリケーションにアクセスできます。

## 手順

[システム (System) ]>[ツール (Tools) ]>[プラグイン (Plugin) ]で、起動するプラグインを選択します。

アプリケーションはプラグイン ウィンドウに表示されます。使用方法の詳細については、アプリケーションのマニュアルを参照してください。



付録

# A

## パフォーマンス カウンタとアラート

---

- システム カウンタ, 219 ページ
- 音声およびビデオ カウンタ, 241 ページ
- IM and Presence Service カウンタ, 344 ページ
- Cisco Unity Connection カウンタ, 368 ページ
- システム アラート, 395 ページ
- 音声およびビデオ アラート, 413 ページ
- IM and Presence Service アラート, 455 ページ
- Intercompany Media Engine アラート, 485 ページ
- Cisco Unity Connection アラート, 494 ページ

## システム カウンタ

### Cisco Tomcat Connector

Tomcat Hypertext Transport Protocol (HTTP) および HTTP Secure (HTTPS) Connector オブジェクトは、Tomcat コネクタについての情報を提供します。

Tomcat HTTP コネクタは、要求を受信して応答を送信するエンドポイントを表します。このコネクタは、アプリケーションの Web ページにアクセスしたときに発生する HTTP/HTTPS 要求の処理と HTTP/HTTPS 応答の送信を行います。Web アプリケーション URL の Secure Socket Layer (SSL) ステータスは、各 Tomcat HTTP Connector のインスタンス名の基準を提供します。たとえば、SSL の場合は `https://<IP Address>:8443`、非 SSL の場合は `http://<IP Address>:8080` になります。

次の表に、Tomcat HTTP Connector カウンタに関する情報を示します。

表 21 : Cisco Tomcat Connector

カウンタ	カウンタの説明
Errors	コネクタで発生した HTTP エラー（たとえば、「401 未認証 (401 Unauthorized)」）の合計数。
MBytesReceived	コネクタが受信したデータの量。
MBytesSent	コネクタが送信したデータの量。
Requests	コネクタが処理した要求の総数。
ThreadsTotal	要求処理スレッドの現在の合計数、コネクタの使用可能/使用中のスレッドを含みます。
ThreadsMax	コネクタの要求処理スレッドの最大数。  Webアプリケーションのウィンドウで着信する各要求は、その要求の期間中、1つのスレッドを必要とします。現在使用可能な要求処理スレッドで処理できる数を上回る同時要求を受信した場合は、このカウンタに表示される設定最大数を上限として、追加のスレッドが作成されます。さらに別の同時要求を受信すると、それらの要求は、内部で指定された最大数になるまで、コネクタで作成されたサーバソケット内に累積されます。それ以外の同時要求は、それらの要求を処理するリソースが使用可能になるまで、接続拒否メッセージを受け取ります。
ThreadsBusy	このカウンタは、コネクタのビジー状態/使用中の要求処理スレッドの現在の数を表します。

## Cisco Tomcat JVM

Cisco Tomcat Java Virtual Machine (JVM) オブジェクトは、Cisco Unified Communications Manager の管理、Cisco Unified Serviceability、および Cisco Unity Connection の管理など、Web アプリケーションで使用する共通リソース メモリのプールに関する情報を提供します。動的メモリ ブロックには、Tomcat とその Web アプリケーションで作成されるすべてのオブジェクトが保存されます。

次の表に、Tomcat JVM カウンタに関する情報を示します。

表 22 : Tomcat JVM

カウンタ	カウンタの説明
KBytesMemoryFree	Tomcat Java Virtual Machine の動的メモリ ブロック（ヒープメモリ）の量。  動的メモリの空き容量が少なくなると、追加のメモリが自動的に割り当てられ、KbytesMemoryTotal カウンタに表示される合計メモリ サイズが増加します。ただし、KbytesMemoryMax カウンタに表示される最大容量を上限とします。  使用中のメモリ容量は、KbytesMemoryTotal から KBytesMemoryFree の値を減算することで判断できます。
KBytesMemoryMax	Tomcat Java Virtual Machine の動的メモリ ブロック（ヒープメモリ）の量。
KBytesMemoryTotal	空きメモリと使用中メモリを含む、Tomcat Java Virtual Machine の現在の動的メモリ ブロックの合計サイズ。

## Cisco Tomcat Web Application

Cisco Tomcat Web Application オブジェクトは、の Web アプリケーションを実行する方法についての情報を提供します。

次の例で示すように、Web アプリケーションの URL は、各 Tomcat Web Application のインスタンス名の基準になります。

- Cisco Unified Communications Manager の管理ページ (<https://<IP Address>:8443/ccmadmin>) は、ccmadmin により識別されます。
- Cisco Unified Serviceability (<https://<IP Address>:8443/ccmservice>) は、ccmservice によって識別されます。
- Cisco Unified Communications Manager のユーザ オプション (<https://<IP Address>:8443/ccmuser>) は、ccmuser によって識別されます。
- Cisco Unity Connection の管理ページ (<https://<IP Address>:8443/cuadmin>) は、cuadmin によって識別されます。
- 拡張子を持たない URL (<https://<IP Address>:8443> や <http://<IP Address>:8080>) は \_root によって識別されます。

次の表に、Tomcat Web Application カウンタについての情報を示します。

表 23 : Tomcat Web Application

カウンタ	カウンタの説明
Errors	Cisco Unified Communications Manager 関連、または Cisco Unity Connection 関連の Web アプリケーションで発生した HTTP エラー（たとえば、401 未認証など）の合計数を表します。
Requests	Web アプリケーションが処理する要求の数の合計数。Requests カウンタは、Web アプリケーションにアクセスするたびに増加します。
SessionsActive	Web アプリケーションでアクティブまたは使用中のセッションの数。

## Database Change Notification Client

Database Change Notification Client オブジェクトは、変更通知クライアントについての情報を提供します。次の表に、Database Change Notification Client カウンタに関する情報を示します。

表 24 : Database Change Notification Client

カウンタ	カウンタの説明
MessagesProcessed	処理されたデータベース変更通知の数。このカウンタは、15 秒ごとに更新されます。
MessagesProcessing	現在処理中、またはこのクライアントの変更通知キューで処理待ち状態にある変更通知メッセージの数。このカウンタは、15 秒ごとに更新されます。
QueueHeadPointer	変更通知キューへのヘッドポインタ。ヘッドポインタは、変更通知キュー内の開始ポイントとして機能します。キュー内の通知数は、テールポインタ値からヘッドポインタ値を減算することで判断できます。デフォルトでは、このカウンタは 15 秒ごとに更新されます。
QueueMax	このクライアントで処理される変更通知メッセージの最大数。このカウンタは、Cisco Database Layer Monitor サービスの最後の再起動時から累積されます。



カウンタ	カウンタの説明
QueueTailPointer	変更通知キューのテール ポインタ。テール ポインタは、変更通知キュー内の終了ポイントを表します。キュー内の通知数は、テール ポインタ値からヘッド ポインタ値を減算することで判断できます。デフォルトでは、このカウンタは 15 秒ごとに更新されます。
TablesSubscribed	このクライアントが登録しているテーブルの数。

## Database Change Notification Server

Database Change Notification Server オブジェクトは、さまざまな変更通知関連の統計情報を提供します。次の表に、Database Change Notification Server カウンタに関する情報を示します。

表 25 : Database Change Notification Server

カウンタ	カウンタの説明
Clients	変更を通知するために登録されている変更通知クライアント（サービス/サブレット）の数。
CNProcessed	レポートしてからサーバによって処理される変更通知メッセージの合計数。
Queue Delay	<p>変更通知プロセスで処理するメッセージがあるにもかかわらず、メッセージが処理されていない時間（秒）。この条件は、次の場合に当てはまります。</p> <ul style="list-style-type: none"> <li>Change Notification Requests Queued in Database (QueuedRequestsInDB) と Change Notification Requests Queued in Memory (QueuedRequestsInMemory) がゼロ以外に設定されている場合、または</li> <li>Latest Change Notification Messages Processed カウントが変更されていない場合。</li> </ul> <p>この条件は 15 秒ごとに確認されます。</p>
QueuedRequestsInDB	（共有メモリのキューに入らずに）TCP/IP 直接接続により DBCNQueue (Database Change Notification Queue) テーブルに入れられた変更通知レコードの数。このカウンタは、15 秒ごとに更新されます。
QueuedRequestsInMemory	共有メモリのキューに入る変更通知要求の数。

## Database Change Notification Subscription

Database Change Notification Subscription オブジェクトは、クライアントが変更通知を受信するテーブルの名前を表示します。

SubscribedTable オブジェクトは、変更通知を受信するサービスまたはサブレットを含んだテーブルを表示します。カウンタは増加しないため、この表示は参考目的のみに使用されます。

## Database Local DSN

Database Local Data Source Name (DSN) オブジェクトと LocalDSN カウンタは、ローカルマシンの DSN 情報を提供します。次の表に、Database Local DSN に関する情報を示します。

表 26 : Database Local Data Source Name

カウンタ	カウンタの説明
CcmDbSpace_Used	使用されている Ccm DbSpace の量。
CcmtempDbSpace_Used	使用されている Ccmtemp DbSpace の量。
CNDbSpace_Used	使用されている CN DbSpace の割合 (パーセント)。
LocalDSN	ローカルマシンから参照されている DSN。
SharedMemory_Free	空いている共有メモリの合計。
SharedMemory_Used	使用されている共有メモリの合計。
RootDbSpace_Used	使用されている RootDbSpace の量。

## DB User Host Information カウンタ

DB User Host Information オブジェクトは、DB User Host についての情報を提供します。

DB:User:Host Instance オブジェクトは、DB:User:Host の各インスタンスの接続数を表示します。

## Enterprise Replication DBSpace Monitors

Enterprise Replication DBSpace Monitors オブジェクトは、さまざまな ER DbSpace の使用状況を表示します。次の表に、Enterprise Replication DB Monitors に関する情報を示します。

表 27 : Enterprise Replication DBSpace Monitors

カウンタ	カウンタの説明
ERDbSpace_Used	使用されている Enterprise Replication DbSpace の容量。
ERSBDbSpace_Used	使用されている ERDbSpace の容量。

## Enterprise Replication Perfmon Counters

Enterprise Replication Perfmon Counter オブジェクトは、さまざまな複製カウンタについての情報を提供します。

ServerName:ReplicationQueueDepth カウンタは、サーバ名に続いて、複製キューの項目数を表示します。

## IP

IP オブジェクトは、システムの IPv4 関連の統計についての情報を提供します。次の表に、IP カウンタについての情報を示します。

(注) また、このカウンタは、Cisco Unified Communications Manager をサポートし、システムの IPv6 関連の統計についての情報を提供する IPv6 オブジェクトの一部でもあります。

表 28 : IP カウンタ

カウンタ	カウンタの説明
Frag Creates	このエンティティで生成された IP データグラム フラグメントの数。
Frag Fails	Do not Fragment フラグが設定されたデータグラムの場合など、データグラムをフラグメント化できなかったためにこのエンティティで破棄された IP データグラムの数。
Frag OKs	このエンティティで正常にフラグメント化された IP データグラムの数。
In Delivers	IP ユーザ プロトコルに配信された入力データグラムの数。これにはインターネット制御メッセージプロトコル (ICMP) が含まれます。

カウンタ	カウンタの説明
In Discards	問題が発生しないものの廃棄された入力IPデータグラムの数。考えられる原因の1つに、バッファ領域の不足があります。このカウンタには、再構成の待機中に廃棄されたデータグラムの数は含まれません。
In HdrErrors	ヘッダーエラーで廃棄された入力データグラムの数。これには、不正なチェックサム、バージョン番号の不一致、他の形式エラー、存続可能時間の超過、およびIPオプションの処理中に発見されたその他のエラーが含まれます。
In Receives	すべてのネットワーク インターフェイスから受信された入力データグラムの数。このカウンタには、エラーと共に受信されたデータグラムも含まれます。
In UnknownProtos	正常に受信されたものの、プロトコルが不明またはサポートされないために廃棄されたローカルアドレス宛てのデータグラムの数。
InOut Requests	受信された着信IPデータグラムの数および送信された発信IPデータグラムの数。
Out Discards	送信されずに廃棄された出力IPデータグラムの数。考えられる原因の1つに、バッファ領域の不足があります。
Out Requests	このカウンタは、ICMPを含むローカルIPユーザプロトコルが、要求送信でIPに与えるIPデータグラムの総数を表します。このカウンタには、ForwDatagramsでカウントされたデータグラムの数は含まれません。
Reasm Fails	タイムアウトやエラーなど、IP再構成アルゴリズムによって検出されたIP再構成の失敗の回数。  このカウンタは、破棄されたIPフラグメントの数を表しません。RFC 815のアルゴリズムなど一部のアルゴリズムでは、受信するときにフラグメントを結合するので、フラグメントの数を追跡できなくなる可能性があるためです。
Reasm OKs	正常に再構成されたIPデータグラムの数。
Reasm Reqds	このエンティティで再構成が必要だった受信IPフラグメントの数。

## メモリ (Memory)

Memory オブジェクトは、サーバの物理メモリとスワップメモリの使用状況についての情報を提供します。次の表に、Memory カウンタに関する情報を示します。

表 29: メモリ (Memory)

カウンタ	カウンタの説明
% Mem Used	<p>システムの物理メモリの使用率をパーセントで表示します。このカウンタの値は次のように計算されます。</p> $\text{Total KBytes} - \text{Free KBytes} - \text{Buffers KBytes} - \text{Cached KBytes} + \text{Shared KBytes} / \text{Total KBytes}$ <p>この値は、Used KBytes/Total KBytes に相当します。</p>
% Page Usage	アクティブなページの割合 (パーセント)。
% VM Used	<p>システムの仮想メモリの使用率をパーセントで表示します。このカウンタの値は次のように計算されます。</p> $\text{Total KBytes} - \text{Free KBytes} - \text{Buffers KBytes} - \text{Cached KBytes} + \text{Shared KBytes} + \text{Used Swap KBytes} / (\text{Total KBytes} + \text{Total Swap KBytes})$ <p>この値は、Used VM KBytes/Total VM KBytes に相当します。</p>
Buffers KBytes	システムのバッファ容量 (キロバイト単位)。
Cached KBytes	キャッシュされたメモリの容量 (キロバイト単位)。
Free KBytes	システムで使用可能な合計メモリの総量 (キロバイト単位)。
Free Swap KBytes	システムで使用可能な空きスワップ領域の容量 (キロバイト単位)。
HighFree	<p>上部領域での空きメモリ容量。</p> <p>Linux カーネルは、仮想メモリアドレス空間を複数のメモリ領域に分割します。上位メモリは特定の物理アドレスより上位のメモリで、その容量は、合計メモリとシステムのカーネルタイプによって異なります。</p> <p>4 GB メモリを搭載した Cisco Unified Communications Manager システムの場合、上位メモリはおおよそ 896M ~ 4096M のアドレスを指します。</p>

カウンタ	カウンタの説明
HighTotal	<p>上位領域のメモリの総量。</p> <p>Linux カーネルは、仮想メモリアドレス空間を複数のメモリ領域に分割します。上位メモリは特定の物理アドレスより上位のメモリで、その容量は、合計メモリとシステムのカーネルタイプによって異なります。</p> <p>4 GB メモリを搭載した Cisco Unified Communications Manager システムの場合、上位メモリはおおよそ 896M ~ 4096M のアドレスを指します。</p>
Page Faults Per Sec	<p>システムによるページフォールト（メジャーとマイナーの両方）の 1 秒あたりの件数を表します（2.5 以降のカーネルのみ）。一部のページフォールトは I/O がなくても解決できるため、この値は入力および出力（I/O）を生成したページフォールトのカウントと一致しない場合があります。</p>
Low Total	カーネルの低（非ページ）メモリの合計。
Low Free	カーネルの低（非ページ）メモリの空き容量の合計。
Page Major Faults Per Sec	<p>システムによる 1 秒あたりのメジャーフォールトの件数（2.5 以降のカーネルのみ）。メジャーページフォールトとは、ディスクからメモリページをロードする必要があるページフォールトを指します。</p>
Pages	ディスクからページインしたページの数と、ディスクにページアウトしたページの数合計。
Pages Input	ディスクからページインされたページの数。
Pages Input Per Sec	ディスクからページインされた 1 秒あたりのページのサイズの合計（キロバイト単位）。
Pages Output	ディスクにページアウトされたページの数。
Pages Output Per Sec	ディスクにページアウトされた 1 秒あたりのページのサイズの合計（キロバイト単位）。
Shared KBytes	システムの共有メモリの容量（キロバイト単位）。
SlabCache	<p>プロシージャの slabinfo のすべての個別エントリの合計を表す詳細なカウンタとして、さまざまなカーネルコンポーネントによって作成されている SlabCache で使用されるメモリ。</p>

カウンタ	カウンタの説明
SwapCached	キャッシュメモリとして使用されたスワップ容量。これは、一旦スワップアウトされてからスワップバックされたが、まだスワップファイルに残っているメモリです。
Total KBytes	システムのメモリの総量 (キロバイト単位)。
Total Swap KBytes	このカウンタは、システムのスワップ領域の総量 (キロバイト単位)。
Total VM KBytes	使用中のシステム物理メモリとスワップ領域 (Total Kbytes + Total Swap Kbytes) の総量 (キロバイト単位)。
Used KBytes	<p>使用中のシステム物理メモリの容量。Used KBytes カウンタの値は次のように計算されます。</p> <p>Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes。</p> <p>Used KBytes の値は、top または free コマンド出力に表示される Linux の値とは異なります。top または free コマンド出力に表示される Used の値は、Total KBytes - Free KBytes で計算される値に等しく、Buffers KBytes と Cached KBytes の合計値も含まれます。</p>
Used Swap KBytes	このカウンタは、システムで使用中のスワップ領域の容量をキロバイト単位で表します。
Used VM KBytes	<p>このカウンタは、システム物理メモリと、使用中のスワップ領域の容量をキロバイト単位で表します。値は次のように計算されます。</p> <p>Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes + Used Swap KBytes</p> <p>この値は、Used Mem KBytes + Used Swap KBytes に相当します。</p>

## ネットワーク インターフェイス (Network Interface)

Network Interface オブジェクトは、システムのネットワーク インターフェイスについての情報を提供します。次の表に、Network Interface カウンタに関する情報を示します。

表 30: ネットワーク インターフェイス (Network Interface)

カウンタ	カウンタの説明
Rx Bytes	インターフェイスで受信したフレーミング文字を含めたバイト数。
Rx Dropped	エラーは検出されなかったものの、破棄するように選択されたインバウンドパケットの数。これによって、上位層のプロトコルにパケットが配信されなくなります。また、パケットの破棄によりバッファ領域が解放されます。
Rx Errors	エラーのために上位層のプロトコルに配信できなかったインバウンドパケット (パケット指向インターフェイス) の数と、インバウンド送信ユニット (文字指向または固定長インターフェイス) の数。
Rx Multicast	このインターフェイスで受信したマルチキャストパケットの数。
Rx Packets	このサブレイヤが上位サブレイヤに配信したパケットの数。この数には、このサブレイヤでマルチキャストまたはブロードキャストアドレスにアドレス指定されたパケットは含まれていません。
Total Bytes	受信 (Rx) バイトと送信 (Tx) バイトの総数。
Total Packets	Rx パケットと Tx パケットの総数。
Tx Bytes	インターフェイスから送信されたフレーミング文字を含むオクテットの総数。
Tx Dropped	エラーは検出されなかったものの、破棄するように選択されたアウトバウンドパケットの数。これによって、上位層のプロトコルにパケットが配信されなくなります。また、パケットの破棄によりバッファ領域が解放されます。
Tx Errors	エラーのために送信できなかったアウトバウンドパケット (パケット指向インターフェイス) の数と、アウトバウンド送信ユニット (文字指向または固定長インターフェイス) の数。
Tx Packets	破棄されたものや送信されなかったものも含め、上位レベルのプロトコルが送信を要求したパケットの総数。この値には、このサブレイヤでマルチキャストまたはブロードキャストアドレスにアドレス指定されたパケットは含まれていません。



カウンタ	カウンタの説明
Tx QueueLen	The length of the output packet queue (in packets).

## Number of Replicates Created and State of Replication

Number of Replicates Created and State of Replication オブジェクトは、システムのリアルタイム複製についての情報を提供します。次の表に、Replication カウンタに関する情報を示します。

表 31 : *Number of Replicates Created and State of Replication*

カウンタ	カウンタの説明
Number of Replicates Created	DB 表用に Informix によって作成されたレプリケーションの数。このカウンタは、複製のセットアップ中の情報を表示します。
Replicate_State	レプリケーションの状態。次の値が使用されます。  <b>[0]</b> 初期化中。サーバが定義されていない場合、または、サーバは定義されていてもテンプレートが完了していない場合、カウンタの値は 0 になります。  <b>1</b> レプリケーションセットアップスクリプトがこのノードから起動した。CLI で <b>utils dbreplication status</b> を実行し、エラーの発生場所と発生原因を特定することを推奨します。  <b>2</b> 良好なレプリケーション。  <b>3</b> 不正なレプリケーション。カウンタの値が 3 の場合、クラスタ内の複製が正しく機能していないことを示します。これは、クラスタ内の特定のサーバ上で複製が失敗したことを示すものではありません。CLI で <b>utils dbreplication status</b> を実行し、エラーの発生場所と発生原因を特定することを推奨します。  <b>4</b> レプリケーションセットアップが失敗した。

## パーティション

Partition オブジェクトは、システムのファイル システムとその使用状況についての情報を提供します。次の表に、Partition カウンタに関する情報を示します。これらのカウンタは予備パーティション（存在する場合）でも使用できます。

表 32: パーティション

カウンタ	カウンタの説明
% CPU Time	ディスクに対して発行された I/O 要求の処理にかかった CPU 時間のパーセンテージ。
% Used	このファイルシステムで使用中のディスク領域のパーセンテージ。
% Wait in Read	このカウンタは使用されません。このカウンタの代わりに Await Read Time カウンタが使用されます。このカウンタは、カウンタの値が -1 になると無効になります。
% Wait in Write	このカウンタは使用されません。このカウンタの代わりに Await Read Time カウンタが使用されます。このカウンタは、カウンタの値が -1 になると無効になります。
Await Read Time	サービス対象のデバイスに対して発行された読み取り要求の平均所要時間（ミリ秒単位）。
Await Time	サービス対象のデバイスに対して発行された入出力（I/O）要求の平均所要時間（ミリ秒単位）。この値には、要求がキュー内に存在する時間と、要求を処理する時間が含まれます。
Await Write Time	サービス対象のデバイスに対して発行された書き込み要求の平均所要時間（ミリ秒単位）。
キューの長さ（Queue Length）	ディスクに対して発行された要求の平均キュー長。
Read Bytes Per Sec	ディスクから読み取られた 1 秒あたりのデータ量（バイト単位）。
Total Mbytes	このファイル システムのディスク領域全体の容量（メガバイト単位）。
Used Mbytes	このファイル システムで使用中のディスク領域の容量（メガバイト単位）。

カウンタ	カウンタの説明
Write Bytes Per Sec	ディスクに書き込まれた1秒あたりのデータ量 (バイト単位)。

## プロセス (Process)

Process オブジェクトは、システムで実行されているプロセスについての情報を提供します。次の表に、Process カウンタに関する情報を示します。

表 33: プロセス (Process)

カウンタ	カウンタの説明
% CPU Time	このカウンタは、最後に更新してから経過した CPU 時間におけるタスク占有率を、合計 CPU 時間に対する比率で表します。
% MemoryUsage	このカウンタは、タスクが現在使用している物理メモリを比率で表します。
Data Stack Size	このカウンタは、タスク メモリ ステータスのスタック サイズを表します。
Nice	このカウンタは、タスクの Nice 値を表します。 <ul style="list-style-type: none"> <li>負の Nice 値はプロセスの優先順位が高いことを示します。</li> <li>正の Nice 値はプロセスの優先順位が低いことを表します。</li> </ul> (注) Nice 値が 0 の場合、タスクの割り当てを判断するときに優先順位を調整しないでください。
Page Fault Count	このカウンタは、タスクで発生し、データをメモリにロードすることが必要になったメジャー ページフォールトの数を表します。
PID	このカウンタは、タスク固有のプロセス ID を表します。この ID は定期的にラッピングされますが、値が 0 になることはありません。

カウンタ	カウンタの説明
Process Status	<p>このカウンタは、次のプロセス ステータスを表示します。</p> <p><b>[0]</b> 実行中 (Running)</p> <p><b>1</b> スリープ中</p> <p><b>2</b> 割り込み不能ディスク スリープ</p> <p><b>3</b> ゾンビ</p> <p><b>4</b> 停止 (Stopped)</p> <p><b>5</b> ページング</p> <p><b>[6]</b> 不明</p>
Shared Memory Size	<p>このカウンタは、タスクが使用している共有メモリの容量 (キロバイト) を表示します。他のプロセスが同じメモリを共有することも可能です。</p>
STime	<p>このカウンタは、このプロセスがカーネルモードでスケジューリングしたシステム時間 (STime) を jiffy 単位で表示します。jiffy は CPU 時間の 1 単位に相当し、測定単位として使用されます。1 秒は 100 jiffy です。</p>
Thread Count	<p>このカウンタは、タスクで現在グループ化されているスレッドの数を表示します。負の値 (-1) は、このカウンタが現在使用不可能になっていることを示します。これは、システムのプロセスとスレッドの数の合計がデフォルトのしきい値を超過したために、スレッド統計情報 (Thread オブジェクトのすべてのパフォーマンス カウンタ、および Process オブジェクトの Thread Count カウンタを含む) がオフになった場合に発生します。</p>

カウンタ	カウンタの説明
Total CPU Time Used	このカウンタは、タスクの開始以降、タスクがユーザモードとカーネルモードで使用した合計 CPU 時間を jiffy 単位で表示します。
UTime	このカウンタは、タスクがユーザモードでスケジューリングした時間を jiffy 単位で表示します。
VmData	このカウンタは、タスクでのヒープの仮想メモリ使用状況をキロバイト (KB) 単位で表示します。
VmRSS	このカウンタは、現在の物理メモリにおける仮想メモリ (Vm) 常駐セット サイズ (RSS) をキロバイト (KB) 単位で表示します。これには、コード、データ、およびスタックが含まれます。
VmSize	このカウンタは、タスクでの仮想メモリの合計使用量をキロバイト (KB) 単位で表示します。この値はスワップアウトされたすべてのコード、データ、共有ライブラリ、およびページが含まれます。  仮想イメージ = スワップされたサイズ + 常駐サイズ
Wchan	このカウンタは、プロセスが待機しているチャンネル (システムコール) を表示します。

## プロセッサ

Processor オブジェクトは、さまざまなプロセッサ時間の使用状況を比率で提供します。次の表に、Processor カウンタについての情報を示します。

表 34: プロセッサ

カウンタ	カウンタの説明
% CPU Time	このカウンタは、最後に更新してから経過した中央処理装置 (CPU) 時間における、アイドル時間を除いたプロセッサの占有率を表示します。この占有率は、合計 CPU 時間に対する比率で表されます。
Idle Percentage	このカウンタは、プロセッサがアイドル状態になっており、未処理のディスク入出力 (I/O) 要求がない時間を比率で表示します。

カウンタ	カウンタの説明
IOWait Percentage	このカウンタは、システムに未処理のディスク I/O 要求が存在し、同時にプロセッサがアイドル状態になっていた時間を比率で表します。
Irq Percentage	このカウンタは、デバイスに割り当てられる割り込み要求を実行するためにプロセッサが費やす時間（プロセッサがコンピュータに信号を送信するために費やす時間を含む）を比率で表します。
Nice Percentage	このカウンタは、プロセッサが、Nice 優先順位に従ってユーザレベルで実行するために費やす時間を比率で表示します。
Softirq Percentage	このカウンタは、プロセッサが、CPU のパフォーマンスを向上させるために、ソフト IRQ の実行とタスク切り替えの延期に費やす時間を比率で表します。
System Percentage	このカウンタは、プロセッサがシステム（カーネル）レベルでプロセスを実行している時間を比率で表示します。
User Percentage	このカウンタは、プロセッサがユーザ（アプリケーション）レベルで通常のプロセスを実行している時間を比率で表示します。

## システム (System)

System オブジェクトは、システムのファイル記述子についての情報を提供します。

次の表に、System カウンタについての情報を示します。

表 35: システム (System)

カウンタ	カウンタの説明
Allocated FDs	割り当てられたファイル記述子の数。
Being Used FDs	システムで現在使用されているファイル記述子の数。
Freed FDs	システム上で割り当てられているファイル記述子のうち、開放されているファイル記述子の数。

カウンタ	カウンタの説明
IOPerSecond	このサーバのすべてのディスク パーティションでの 1 秒あたりの入出力 (I/O) 操作の数。システム パフォーマンスの問題が発生した場合、このサーバの集約 I/O 操作の影響を測定するためにこのカウンタの情報を使用します。
IOReadReqMergedPerSecond	このサーバ上でマージされ、すべてのデバイスにキューイングされた読み取り要求の 1 秒あたりの数。
IOWriteReqMergedPerSecond	このサーバ上でマージされ、すべてのデバイスにキューイングされた書き込み要求の 1 秒あたりの数。
IOReadReqPerSecond	このサーバ上ですべてのデバイスに対して発行された読み取り要求の 1 秒あたりの数。
IOWriteReqPerSecond	このサーバ上ですべてのデバイスに対して発行された書き込み要求の 1 秒あたりの数。
IOSectorsReadPerSecond	このサーバ上のすべてのデバイスから読み取られた 1 秒あたりのセクター数。
IOSectorsWrittenPerSecond	このサーバ上のすべてのデバイスに書き込まれた 1 秒あたりのセクター数。
IOKBytesReadPerSecond	このサーバ上のすべてのデバイスから読み取られた 1 秒あたりのキロバイト数。
IOKBytesWrittenPerSecond	このサーバ上のすべてのデバイスに書き込まれた 1 秒あたりのキロバイト数。
IOSectorsReqSizeAvg	このサーバ上のすべてのデバイスに対して発行された要求のセクターの平均サイズ。
IOReqQueueSizeAvg	このサーバ上のすべてのデバイスに対して発行された要求の平均のキューの長さ。
IOAwait	サービス対象のすべてのデバイスに対して発行される I/O 要求の平均時間 (ミリ秒)。これには、要求がキュー内に存在する時間と、要求を処理する時間が含まれます。
IOServiceTime	このサーバ上のすべてのデバイスに対して発行される I/O 要求の平均サービス時間 (ミリ秒)。
IOCpuUtil	I/O 要求がこのサーバ上のデバイスに対して発行される間 (デバイスの帯域幅利用) の CPU 時間の割合。

カウンタ	カウンタの説明
Max FDs	システムで許可されているファイル記述子の最大数。
Total CPU Time	システムが稼働している合計時間 (jiffy 単位)。
Total Processes	システムのプロセス数。
Total Threads	システムのスレッドの数。

## [TCP]

TCP オブジェクトは、システムの TCP 統計についての情報を提供します。

次の表に、TCP カウンタについての情報を示します。

表 36 : [TCP]

カウンタ	カウンタの説明
Active Opens	このカウンタは、TCP 接続が CLOSED 状態から SYS-SENT 状態へ直接遷移した回数を表示します。
Attempt Fails	このカウンタは、TCP 接続が、SYN-RCVD または SYN-RCVD のいずれかの状態から CLOSED 状態に直接遷移した回数を表示します。また、TCP 接続が SYS-RCVD 状態から LISTEN 状態へ直接遷移した回数も表示します。
Curr Estab	このカウンタは、現在 ESTABLISHED 状態または CLOSE-WAIT 状態になっている TCP 接続の数を表示します。
Estab Resets	このカウンタは、TCP 接続が、ESTABLISHED または CLOSE-WAIT のいずれかの状態から CLOSED 状態に直接遷移した回数を表示します。
In Segs	このカウンタは、受信したセグメント (エラー受信したセグメントを含む) の総数を表示します。この数には、現在確立されている接続で受信したセグメントのみが含まれます。
InOut Segs	このカウンタは、送信したセグメントの総数と受信したセグメントの総数を表示します。



カウンタ	カウンタの説明
Out Segs	このカウンタは、送信したセグメントの総数を表示します。このカウンタには、現在確立されている接続で送信されるセグメントのみが含まれますが、再送信されたオクテットは除外されます。
Passive Opens	このカウンタは、TCP 接続が LISTEN 状態から SYN-RCVD 状態に直接遷移した回数を表示します。
RetransSegs	このカウンタは、以前に送信されたオクテットが1つ以上含まれているために再送信されたセグメントの総数を表示します。

## Thread

Thread オブジェクトは、システムで実行されているスレッドの一覧を表示します。

次の表に、Thread カウンタについての情報を示します。

表 37: Thread

カウンタ	カウンタの説明
% CPU Time	このカウンタは、前回の更新以降に経過した CPU 時間におけるスレッドの占有率を表示します。このカウンタは、占有率を合計 CPU 時間に対する比率で表現します。
PID	このカウンタは、スレッド リーダー プロセス ID を表示します。

## AXL Web Service

AXL Web Service オブジェクトは、システムで実行されている AXL Web Service に関する情報を提供します。次の表に、AXL Web Service カウンタについての情報を示します。

表 38: AXL Web Service

カウンタ	カウンタの説明
ThrottleCount	このカウンタは、前回の Cisco AXL Web Service の再起動以降に実行された Administrative XML Layer (AXL) スロットリングの回数を表します。AXL サービスが処理できるよりも多くの変更要求を受信すると、スロットリングが発生します。

カウンタ	カウンタの説明
ThrottleState	このカウンタは、Administrative XML Layer (AXL) スロットリングが現在アクティブ (スロットリングが有効) かどうかを示します。このカウンタの値が1の場合、現在のスロットリングが有効であることを示します。つまり、アプリケーションが AXL を介して Cisco Unified Communications Manager に書き込み要求を送信しようとしています。読み込み要求の許可と処理は、AXL スロットリングが有効であっても行われます。ゼロの値は、スロットリングがこの時点で発生しておらず、すべての読み取りおよび書き込み要求が処理されることを示します。

## Ramfs

Ramfs オブジェクトは、ram ファイル システムに関する情報を提供します。次の表に、Ramfs カウンタについての情報を示します。

表 39 : Ramfs

カウンタ	カウンタの説明
FilesTotal	このカウンタは、RAM ベースのファイル システム (ramfs) ファイルの総数を表します。
SpaceFree	このカウンタは、ram ベースのファイル システム (ramfs) における空きデータ ブロックの容量を表します。ブロックとは、ファイル システム用に統一されたデータ ストレージサイズの単位です。ブロック サイズによって、ファイル システムがデータの読み取りおよび書き込みに使用するサイズが指定されます。Cisco Unified Communications Manager システムでは、ブロック サイズは 4096 バイトです。
SpaceUsed	このカウンタは、ram ベースのファイル システム (ramfs) 内のデータ ブロックの容量を表します。ブロックとは、ファイル システム用に統一されたデータ ストレージサイズの単位です。ブロック サイズによって、ファイル システムがデータの読み取りおよび書き込みに使用するサイズが指定されます。Cisco Unified Communications Manager システムでは、ブロック サイズは 4096 バイトです。

# 音声およびビデオ カウンタ

## Cisco Analog Access

Cisco Analog Access オブジェクトは、登録済みの Cisco アナログ アクセス ゲートウェイについての情報を提供します。次の表に、Cisco Analog Access カウンタに関する情報を示します。

表 40 : Cisco Analog Access

カウンタ	カウンタの説明
OutboundBusyAttempts	このカウンタは、すべてのポートがビジー状態だったときに、Cisco Unified Communications Manager がアナログ アクセス ゲートウェイ経由でコールを試行した回数の合計を示します。
PortsActive	このカウンタは、現在使用中の（アクティブな）ポートの数を示します。ポートは、そのポートでコールが進行中のときにアクティブ表示されます。
PortsOutOfService	このカウンタは、現在アウト オブ サービスのポートの数を示します。カウンタは、ループスタート トランクおよびグラウンドスタート トランクだけに適用されます。

## Cisco Annunciator Device

Cisco Annunciator Device オブジェクトは、登録済みの Cisco アナンシエータ デバイスについての情報を提供します。次の表には、Cisco Annunciator カウンタについての情報が含まれます。

表 41 : Cisco Annunciator Device

カウンタ	カウンタの説明
OutOfResources	このカウンタは、Cisco Unified Communications Manager がアナンシエータ デバイスからアナンシエータ リソースの割り当てを試行して、すべてのリソースがすでに使用中であるなどの理由で失敗した回数の合計を表します。
ResourceActive	このカウンタは、アナンシエータ デバイスに対して現在アクティブな（使用中の）アナンシエータ リソースの総数を表します。

カウンタ	カウンタの説明
ResourceAvailable	このカウンタは、非アクティブで、現時点ではアナンシエータデバイスでまだ使用可能なリソースの総数を表します。
ResourceTotal	このカウンタは、アナンシエータ デバイスに対して設定されているアナンシエータ リソースの総数を表します。

## Cisco Call Restriction

Cisco Call Restriction オブジェクトは、論理パーティション ポリシー制限による失敗の数を表します。次の表に、Cisco Call Restriction カウンタに関する情報を示します。

表 42 : Cisco Call Restriction

カウンタ	カウンタの説明
AdHocConferenceFailures	このカウンタは、会議にすでに存在するデバイスのジオロケーションと会議に招待されているデバイスの間のコールパスが論理パーティション ポリシーによって制限されたために、アドホック会議に参加者を追加できなかった試行回数を表します。
BasicCallFailures	このカウンタは、着信側と発信側のジオロケーション間の論理パーティション ポリシー制限のために、失敗した基本コールの回数を表します。基本コールとは、転送などの補足サービスを利用しないコールです。
ForwardingFailures	このカウンタは、関与する 2 者のジオロケーション間の論理パーティション ポリシー制限のために、着信コールの転送に失敗した試行回数を表します。
LogicalPartitionFailuresTotal	このカウンタは、発信側と着信側のジオロケーション間のコールの制限のために失敗したコールの試行の合計回数を表します。これには、転送、アドホック会議、ミーティング、ピックアップ、コールパーク、共有回線、基本コールの失敗の回数が含まれます。
MeetMeConferenceFailures	このカウンタは、会議にすでに存在するデバイスのジオロケーションと会議への参加を試行しているデバイスの間のコールパスが、論理パーティション ポリシーのために制限されたために参加者をミーティング会議に追加できなかった試行回数を表します。

カウンタ	カウンタの説明
MidCallFailures	このカウンタは、着信側または接続先のジオロケーション間の制限のために、初期ポリシー チェック後に失敗したコールの回数を表示します。
ParkRetrievalFailures	このカウンタは、コールの取得を試行していたデバイスに、パークされた通話者のジオロケーションを含む論理パーティション ポリシー制限があるために、コールパーク操作の実行に失敗した試行回数を表示します。
PickUpFailures	このカウンタは、ピックアップが試行されているデバイスに、発信側デバイスのジオロケーションを含む論理パーティション ポリシー制限があるために、ピックアップ操作の実行に失敗した試行回数を表示します。
SharedLineFailures	このカウンタは、発信者または着信側に、共有回線を持つデバイスのジオロケーションを含む論理パーティション ポリシー制限があるために、共有回線の使用に失敗した試行回数を表示します。
TransferFailures	このカウンタは、転送された通話者のジオロケーションと転送先の間のコールの制限のために失敗したコール転送の試行の回数を表示します。

## Cisco CallManager

Cisco CallManager オブジェクトは、Cisco Unified Communications Manager に登録されたコール、アプリケーション、およびデバイスに関する情報を提供します。次の表には、Cisco CallManager カウンタについての情報が含まれます。

表 43 : Cisco CallManager

カウンタ	カウンタの説明
AnnunciatorOutOfResources	このカウンタは、使用可能なアナンシエータ リソースがなかった場合に、Cisco Unified Communications Manager が Cisco Unified Communications Manager に登録されているリソースからアナンシエータ リソースの割り当てを試行した回数の合計を表示します。
AnnunciatorResourceActive	このカウンタは、Cisco Unified Communications Manager に登録されているすべてのアナンシエータ デバイスで現在使用されているアナンシエータ リソースの総数を表示します。

カウンタ	カウンタの説明
AnnunciatorResourceAvailable	このカウンタは、非アクティブで、現在使用可能なアナンシエータ リソースの総数を表します。
AnnunciatorResourceTotal	このカウンタは、Cisco Unified Communications Manager に現在登録されているすべてのアナンシエータ デバイスから提供されているアナンシエータ リソースの総数を表します。
AuthenticatedCallsActive	このカウンタは、Cisco Unified Communications Manager で現在アクティブな（使用中の）認証済みコールの数を示します。認証済みコールとは、コールに関係するすべてのエンドポイントが認証されているコールを意味します。認証済み電話機は、トランスポート層セキュリティ（TLS）認証された Skinny プロトコル シグナリングを Cisco Unified Communications Manager で使用します。
AuthenticatedCallsCompleted	このカウンタは、Cisco Unified Communications Manager を介して接続された後で接続解除された認証済みコールの数を表します。認証済みコールとは、コールに関係するすべてのエンドポイントが認証されているコールを意味します。認証済み電話機は、TLS 認証された Skinny プロトコル シグナリングを Cisco Unified Communications Manager で使用します。
AuthenticatedPartiallyRegisteredPhone	このカウンタは、部分的に登録された認証済み SIP 電話機の数を表します。
AuthenticatedRegisteredPhones	このカウンタは、Cisco Unified Communications Manager に登録された認証済み電話機の総数を表します。認証済み電話機は、TLS 認証された Skinny プロトコル シグナリングを Cisco Unified Communications Manager で使用します。
BRIChannelsActive	このカウンタは、この Cisco Unified Communications Manager 上で現在アクティブなコールの BRI 音声チャンネルの数を表します。
BRIspansInService	このカウンタは、現在使用可能な BRI スパンの数を表します。
CallManagerHeartBeat	このカウンタは、Cisco Unified Communications Manager のハートビートを表します。この増分カウントは、Cisco Unified Communications Manager が起動して動作していることを示します。このカウントが増加していない場合は、Cisco Unified Communications Manager がダウンしていることを示します。

カウンタ	カウンタの説明
CallsActive	このカウンタは、現在使用中の（アクティブな）音声ストリーミング接続またはビデオ ストリーミング接続の数、つまり、Cisco Unified Communications Manager に接続されている音声パスが実際に存在するコールの数を表します。
CallsAttempted	このカウンタは、試行されたコールの総数を表します。試行されたコールは、どの番号がダイヤルされたか、または宛先に接続されたかに関係なく、電話機がオフフックになるとき、およびオンフックに戻るときに常に発生します。機能操作（たとえば、転送や会議）中のコールの試行も、試行されたコールと見なされる場合があります。
CallsCompleted	このカウンタは、Cisco Unified Communications Manager を介して実際に接続された（音声パスまたはビデオ ストリームが確立された）コールの数を表します。この数は、コールが終了したときに増加します。
CallsInProgress	<p>このカウンタは、Cisco Unified Communications Manager 上で現在進行中の音声コールまたはビデオ コールの数を表します。すべてのアクティブ コールが含まれます。</p> <p><b>CallsInProgress</b> カウンタは、Skinny Client Control Protocol (SCCP) 電話機として登録されている電話機がオフフックになったときに増加します。その値は電話機がオンフックに戻るまで保持されます。</p> <p>SIP 電話機として登録される Cisco Unified IP Phone 7902、7905、7912、7940、および 7960 の場合は、ダイヤルソフトキーが押されたときに <b>CallsInProgress</b> カウンタが増加します。</p> <p>その他のすべての SIP を実行している電話機の場合は、最初の数字が押されたときに <b>CallsInProgress</b> カウンタが増加します。</p> <p>進行中のすべての音声コールまたはビデオ コールが接続されたときに、<b>CallsInProgress</b> の数は <b>CallsActive</b> の数を表します。電話機がオンフックに戻ったときに、カウンタは 1 つ減少します。</p>

カウンタ	カウンタの説明
CM_MediaTermPointsRequestsThrottled	このカウンタは、制御のために拒否されたメディアターミネーションポイント (MTP) リソース要求の総数を表します (MTP が Cisco CallManager サービス パラメータである MTP and Transcoder Resource Throttling Percentage で指定された設定済みの制御比率を超えて使用されていたため、この MTP からのリソースを割り当てることができませんでした)。このカウンタは、この Cisco Unified Communications Manager ノード上の MTP が要求され、その要求が MTP 制御によって拒否されるたびに増分します。カウンタの値は、Cisco CallManager サービスが開始されてから現在までの実行の合計を反映しています。
CM_TranscoderRequestsThrottled	このカウンタは、制御のために拒否されたトランスコーダ リソース要求の総数を表します (トランスコーダが Cisco CallManager サービス パラメータである MTP and Transcoder Resource Throttling Percentage で指定された設定済みの制御比率を超えて使用されていたため、このトランスコーダからのリソースを割り当てることができませんでした)。このカウンタは、この Cisco Unified Communications Manager ノード上のトランスコーダが要求され、その要求がトランスコーダ制御によって拒否されるたびに増分します。カウンタの値は Cisco CallManager サービスが開始されてから現在までの実行の合計を反映しています。
EncryptedCallsActive	このカウンタは、この Cisco Unified Communications Manager で現在アクティブな (使用中の) 暗号化済みコールの数を表します。暗号済みコールとは、コールに関係するすべてのエンドポイントが暗号化されているコールを意味します。
EncryptedCallsCompleted	このカウンタは、この Cisco Unified Communications Manager を介して接続された後で接続解除された暗号化済みコールの数を表します。暗号済みコールとは、コールに関係するすべてのエンドポイントが暗号化されているコールを意味します。
EncryptedPartiallyRegisteredPhones	このカウンタは、部分的に登録された暗号化済み SIP 電話機の数を表します。
EncryptedRegisteredPhones	このカウンタは、この Cisco Unified Communications Manager に登録されている暗号化済み電話機の総数を表します。
FXOPortsActive	このカウンタは、Cisco Unified Communications Manager で現在使用中の (アクティブな) FXO ポートの数を表します。
FXOPortsInService	このカウンタは、システムで現在使用可能な FXO ポートの数を表します。



カウンタ	カウンタの説明
FXSPortsActive	このカウンタは、Cisco Unified Communications Manager で現在使用中の（アクティブな）FXS ポートの数を表します。
FXSPortsInService	このカウンタは、システムで現在使用可能な FXS ポートの数を表します。
HuntListsInService	このカウンタは、Cisco Unified Communications Manager で現在稼働中のハントリストの数を表します。
HWConferenceActive	このカウンタは、Cisco Unified Communications Manager に現在登録されているすべてのハードウェア会議ブリッジデバイスから提供されているハードウェア会議リソースの総数を表します。
HWConferenceCompleted	このカウンタは、Cisco Unified Communications Manager から割り当てられたハードウェア会議ブリッジ（Cisco Catalyst 6000、Cisco Catalyst 4000、Cisco VG200、Cisco シリーズ 26xx、36xx などのハードウェアベースの会議デバイス）を使用して完了した会議の総数を表します。つまり、会議ブリッジは割り当てられて、開放されています。会議は、最初のコールがブリッジに接続されたときにアクティブになります。会議は、最後のコールがブリッジから接続解除されたときに完了します。
HWConferenceOutOfResources	このカウンタは、使用可能なハードウェア会議リソースがなかった場合に、Cisco Unified Communications Manager が Cisco Unified Communications Manager に登録されているリソースからハードウェア会議リソースの割り当てを試行した回数の合計を表します。
HWConferenceResourceActive	このカウンタは、Cisco Unified Communications Manager に登録されているすべてのハードウェア会議デバイス（Cisco Catalyst 6000、Catalyst 4000、Cisco VG200、Cisco シリーズ 26xx、36xx など）上で使用中の会議リソースの総数を表します。1つ以上のコールがブリッジに接続されている場合、会議はアクティブであると見なされます。

カウンタ	カウンタの説明
HWConferenceResourceAvailable	このカウンタは、Cisco Unified Communications Manager から割り当てられたすべてのハードウェア会議デバイス（Cisco Catalyst 6000、Catalyst 4000、Cisco VG200、Cisco シリーズ 26xx、36xx など）に割り当て可能で完了した使用されていないハードウェア会議リソースの数を表します。つまり、会議ブリッジは割り当てられて、開放されています。会議は、最初のコールがブリッジに接続されたときにアクティブになります。会議は、最後のコールがブリッジから接続解除されたときに完了します。
HWConferenceResourceTotal	このカウンタは、Cisco Unified Communications Manager に登録されているすべてのハードウェア会議デバイスのアクティブな会議の数を表します。
InitializationState	このカウンタは、Cisco Unified Communications Manager の現在の初期化状態を表します。Cisco Unified Communications Manager には、次の初期化状態の値があります。 1 : Database、2 : Regions、3 : Locations、4 : QoS Policy、5 : Time Of Day、6 : AAR Neighborhoods、7 : Digit Analysis、8 : Route Plan、9 : Call Control、10 : RSVP Session Manager、11 : Supplementary Services、12 : Directory、13 : SDL Link、14 : Device、100 : Initialization Complete  このカウンタを使用しても、すべての状態が表示されるわけではありません。このカウンタはエラーの発生を示すものではなく、単純に、パフォーマンス モニタのリフレッシュ期間内に状態が初期化され完了したことを示すものです。
IVRResourceActive	このカウンタは、Cisco Unified Communications Manager に登録されているすべての IVR デバイスで現在使用されている IVR リソースの総数を表します。
IVROutOfResources	このカウンタは、使用可能な IVR リソースがなかった場合に、Cisco Unified Communications Manager が Cisco Unified Communications Manager に登録されているリソースから IVR リソースの割り当てを試行した回数の合計を表します。
IVRResourceAvailable	このカウンタは、Cisco Unified Communications Manager に現在登録されているすべての IVR デバイスから提供されている IVR リソースの総数を表します。
IVRResourceTotal	このカウンタは、Cisco Unified Communications Manager に現在登録されているすべての IVR デバイスから提供されている IVR リソースの総数を表します。

カウンタ	カウンタの説明
LocationOutOfResources	このカウンタは、その場所を経由したコールが帯域幅不足のために失敗した回数の合計を表します。
MCUConferencesActive	このカウンタは、Cisco Unified Communications Manager に登録されているすべての Cisco TelePresence MCU 会議ブリッジデバイス上のアクティブな会議の総数を表します。
MCUConferencesCompleted	このカウンタは、Cisco Unified Communications Manager から割り当てられた Cisco TelePresence MCU 会議ブリッジを使用し、完了した（つまり、会議ブリッジが割り当てられ、解放された）会議の総数を表します。会議は、最初のコールがブリッジに接続されたときにアクティブになります。会議は、最後のコールがブリッジから接続解除されたときに終了します。
MCUHttpConnectionErrors	このカウンタは、Cisco Unified Communications Manager が、Cisco TelePresence MCU 会議ブリッジデバイスへの HTTP 接続を作成しようとした際に、Cisco Telepresence MCU 会議ブリッジ側の接続エラーが原因で失敗した回数の合計を示します。
MCUHttpNon200OKResponse	このカウンタは、送信された HTTP クエリーに対して、Cisco Unified Communications Manager が Cisco TelePresence MCU 会議ブリッジから [200 OK HTTP] 以外の応答を受信した回数の合計を表します。
MCUOutOfResources	このカウンタは、Cisco Unified Communications Manager が Cisco TelePresence MCU 会議ブリッジデバイスから会議リソースを割り当てようとして失敗した回数を表します。たとえば、他のすべてのリソースが使われている場合、会議リソースの割り当ては失敗します。
MOHMulticastResourceActive	このカウンタは、Cisco Unified Communications Manager に登録されているすべての MOH サーバで現在使用中の（アクティブな）マルチキャスト MOH リソースの総数を表します。
MOHMulticastResourceAvailable	このカウンタは、Cisco Unified Communications Manager に登録されているすべての MOH サーバで使用されていないアクティブなマルチキャスト MOH 接続の総数を表します。
MOHOutOfResources	このカウンタは、Cisco Unified Communications Manager に登録されているすべての MOH サーバ上で使用可能なすべてのリソースがすでにアクティブであった場合に、Media Resource Manager が MOH リソースの割り当てを試行した回数の合計を表します。

カウンタ	カウンタの説明
MOHTotalMulticastResources	このカウンタは、Cisco Unified Communications Manager に現在登録されているすべての MOH サーバから提供されているマルチキャスト MOH リソースまたはマルチキャスト MOH 接続の総数を表します。
MOHTotalUnicastResources	このカウンタは、Cisco Unified Communications Manager に現在登録されているすべての MOH サーバから提供されているユニキャスト MOH リソースまたはユニキャスト MOH ストリームの総数を表します。各 MOH ユニキャストリソースは、1つのストリームを使用します。
MOHUnicastResourceActive	このカウンタは、Cisco Unified Communications Manager に登録されているすべての MOH サーバで現在使用中の（アクティブな）ユニキャスト MOH リソースの総数を表します。各 MOH ユニキャストリソースは、1つのストリームを使用します。
MOHUnicastResourceAvailable	このカウンタは、Cisco Unified Communications Manager に登録されているすべての MOH サーバで現在使用可能なユニキャスト MOH リソースの総数を表します。各 MOH ユニキャストリソースは、1つのストリームを使用します。
MTPOutOfResources	このカウンタは、Cisco Unified Communications Manager に登録されているメディアターミネーションポイント（MTP）デバイスから MTP リソースの割り当てを Cisco Unified Communications Manager が試みて失敗した回数の合計を表します。これは、MTP として動作する使用可能なトランスコーダがなかったことを意味しています。
MTPResourceActive	このカウンタは、Cisco Unified Communications Manager に登録されているすべての MTP デバイス上で現在使用中の（アクティブな）MTP リソースの総数を表します。各 MTP リソースは、2つのストリームを使用します。使用中の MTP は、コールで使用するために割り当てられている 1つの MTP リソースを表します。
MTPResourceAvailable	このカウンタは、Cisco Unified Communications Manager に登録されているすべての MTP デバイス上に割り当て可能な、現在使用されていない MTP リソースの総数を表します。各 MTP リソースは、2つのストリームを使用します。使用中の MTP は、コールで使用するために割り当てられている 1つの MTP リソースを表します。

カウンタ	カウンタの説明
MTPResourceTotal	このカウンタは、Cisco Unified Communications Manager に現在登録されているすべての MTP デバイスから提供されている MTP リソースの総数を表します。
MTP_RequestsThrottled	このカウンタは、制御のために拒否された MTP リソース要求の総数を表します (MTP が Cisco CallManager サービス パラメータである MTP and Transcoder Resource Throttling Percentage で指定された設定済みの制御比率を超えて使用されていたため、この MTP からのリソースを割り当てることができませんでした)。このカウンタは、この MTP からリソースが要求され、その要求が制御によって拒否されるたびに増分します。このカウンタの値は、MTP デバイスが Cisco CallManager サービスに登録されてから現在までの実行の合計を反映しています。
PartiallyRegisteredPhone	このカウンタは、部分的に登録された SIP を実行している電話機の数を表します。
PRChannelsActive	このカウンタは、Cisco Unified Communications Manager で現在アクティブなコールの PRI 音声チャンネルの数を表します。
PRISpansInService	このカウンタは、現在使用可能な PRI スパンの数を表します。
RegisteredAnalogAccess	このカウンタは、システムに登録されている、登録済み Cisco アナログ アクセス ゲートウェイの数を表します。カウントには、Cisco アナログ アクセス ポートの数は含まれません。
RegisteredHardwarePhones	このカウンタは、現在システムに登録されている Cisco ハードウェア IP Phone (Cisco Unified IP Phone 7960、7940、7910 など) の数を表します。
RegisteredMGCPGateway	このカウンタは、現在システムに登録されている MGCP ゲートウェイの数を表します。
RegisteredOtherStationDevices	このカウンタは、現在システムに登録されている Cisco ハードウェア IP Phone 以外の端末デバイス (Cisco IP SoftPhone、CTI ポート、CTI ルート ポイント、Cisco ボイスメール ポートなど) の数を表します。

カウンタ	カウンタの説明
SIPLineServerAuthorizationChallenges	このカウンタは、Cisco Unified Communications Manager サーバが SIP を実行している電話機に対して発行した着信 SIP 要求の認証確認の回数を表示します。認証確認は、ダイジェスト認証が有効な SIP を実行している電話機から Cisco Unified Communications Manager に SIP 回線要求を送信したときに発生します。
SIPLineServerAuthorizationFailures	このカウンタは、SIP 電話機から Cisco Unified Communications Manager サーバに対する着信 SIP 要求の認証確認の失敗回数を表示します。認証の失敗は、ダイジェスト認証が有効な SIP 電話機から Cisco Unified Communications Manager にクレデンシャルが不正な SIP 回線要求を送信したときに発生します。
SIPTrunkAuthorization	このカウンタは、Cisco Unified Communications Manager が SIP トランクに対して発行した着信 SIP 要求のアプリケーションレベルの認証チェックの回数を表示します。アプリケーションレベルの認証チェックは、Cisco Unified Communications Manager が、着信 SIP 要求を Cisco Unified Communications Manager の管理の [SIP トランク セキュリティ プロファイルの設定 (SIP Trunk Security Profile Configuration) ] ウィンドウのアプリケーションレベルの設定と比較するときに実行されます。
SIPTrunkAuthorizationFailures	このカウンタは、Cisco Unified Communications Manager SIP トランクで発生した着信 SIP 要求のアプリケーションレベルの認証の失敗回数を表示します。アプリケーションレベルの認証の失敗は、Cisco Unified Communications Manager が、着信 SIP 要求と、Cisco Unified Communications Manager の管理の [SIP トランク セキュリティ プロファイルの設定 (SIP Trunk Security Profile Configuration) ] ウィンドウのアプリケーションレベルの認証設定を比較し、そのウィンドウ上の1つ以上の SIP 機能に対する認証が許可されていないことを検出した場合に発生します。
SIPTrunkServerAuthenticationChallenges	このカウンタは、Cisco Unified Communications Manager が SIP トランクに対して発行した着信 SIP 要求の認証確認の回数を表示します。認証確認は、ダイジェスト認証が有効な SIP トランクから Cisco Unified Communications Manager に SIP 要求を送信したときに発生します。

カウンタ	カウンタの説明
SIPTrunkServerAuthenticationFailures	このカウンタは、SIP トランクから Cisco Unified Communications Manager に対する着信 SIP 要求で発生した認証確認の失敗回数を表します。認証の失敗は、ダイジェスト認証が有効な SIP トランクから Cisco Unified Communications Manager にクレデンシャルが不正な SIP 要求を送信したときに発生します。
SWConferenceActive	このカウンタは、Cisco Unified Communications Manager に登録されているすべてのソフトウェア会議デバイスのアクティブな会議の数を表します。
SWConferenceCompleted	このカウンタは、Cisco Unified Communications Manager から割り当てられたソフトウェア会議ブリッジを使用して完了した会議の総数を表します。つまり、会議ブリッジは割り当てられて、開放されています。会議は、最初のコールがブリッジに接続されたときにアクティブになります。会議は、最後のコールがブリッジから接続解除されたときに完了します。
SWConferenceOutOfResources	このカウンタは、使用可能なソフトウェア会議リソースがなかった場合に、Cisco Unified Communications Manager が Cisco Unified Communications Manager に登録されているリソースからソフトウェア会議リソースの割り当てを試行した回数の合計を表します。カウンタには、新規の参加者を既存の会議に追加することに失敗した試行回数が含まれます。
SWConferenceResourceActive	このカウンタは、Cisco Unified Communications Manager に登録されているすべてのソフトウェア会議デバイス上で使用中の会議リソースの総数を表します。1つ以上のコールがブリッジに接続されている場合、会議はアクティブであると見なされます。1つのリソースは1つのストリームと同等です。
SWConferenceResourceAvailable	このカウンタは、Cisco Unified Communications Manager に対して同時に開始できる新規のソフトウェアベースの会議の数を表します。新規の各会議に対して最低でも3つのストリームが使用可能である必要があります。1つのリソースは1つのストリームと同等です。
SWConferenceResourceTotal	このカウンタは、Cisco Unified Communications Manager に現在登録されているすべてのソフトウェア会議ブリッジデバイスから提供されているソフトウェア会議リソースの総数を表します。
SystemCallsAttempted	このカウンタは、サーバから発信されたコールと Unity メッセージ待機インジケータ (MWI) に試行されたコールの総数を表します。

カウンタ	カウンタの説明
T1ChannelsActive	このカウンタは、Cisco Unified Communications Manager で現在アクティブなコールの T1 CAS 音声チャンネルの数を表します。
T1SpansInService	このカウンタは、現在使用可能な T1 CAS スパンの数を表します。
TLSConnectedSIPTrunks	このカウンタは、トランスポート層セキュリティ (TLS) で設定および接続された SIP トランクの数を表します。
TLSConnectedWSM	このカウンタは、トランスポート層セキュリティ (TLS) で設定され、Motorola WSM に接続された WSM コネクタの数を表します。
TranscoderOutOfResources	このカウンタは、使用可能なトランスコーダリソースがなかった場合に、Cisco Unified Communications Manager が Cisco Unified Communications Manager に登録されているトランスコーダデバイスからトランスコーダリソースの割り当てを試行した回数合計を表します。
TranscoderResourceActive	このカウンタは、Cisco Unified Communications Manager に登録されているすべてのトランスコーダデバイス上で使用中のトランスコーダの総数を表します。使用中のトランスコーダは、コールで使用するために割り当てられている 1 つのトランスコーダリソースを表します。各トランスコーダリソースは、2 つのストリームを使用します。
TranscoderResourceAvailable	このカウンタは、Cisco Unified Communications Manager に登録されているすべてのトランスコーダデバイスに割り当て可能な、現在使用されていないトランスコーダの総数を表します。各トランスコーダリソースは、2 つのストリームを使用します。
TranscoderResourceTotal	このカウンタは、Cisco Unified Communications Manager に現在登録されているすべてのトランスコーダデバイスから提供されているトランスコーダリソースの総数を表します。
VCBConferenceActive	このカウンタは、Cisco Unified Communications Manager に登録されているすべてのビデオ会議ブリッジデバイス上のアクティブなビデオ会議の総数を表します。
VCBConferenceAvailable	このカウンタは、Cisco Unified Communications Manager に登録されているすべてのビデオ会議ブリッジデバイス上の新規ビデオ会議の総数を表します。



カウンタ	カウンタの説明
VCBConferenceCompleted	このカウンタは、Cisco Unified Communications Manager から割り当てられたビデオ会議ブリッジを使用して完了したビデオ会議の総数を表します。つまり、会議ブリッジは割り当てられて、開放されています。会議は、最初のコールがブリッジに接続されたときにアクティブになります。会議は、最後のコールがブリッジから接続解除されたときに完了します。
VCBConferenceTotal	このカウンタは、Cisco Unified Communications Manager に登録されているすべてのビデオ会議ブリッジデバイス上でサポートされているビデオ会議の総数を表します。
VCBOutOfConferences	このカウンタは、使用可能なビデオ会議リソースがなかった場合に、Cisco Unified Communications Manager が Cisco Unified Communications Manager に登録されているリソースからビデオ会議リソースの割り当てを試行した回数の合計を表します。
VCBOutOfResources	このカウンタは、失敗した新規ビデオ会議要求の総数を表します。設定されている数の会議がすでに使用中であるなどの理由で、会議の要求が失敗する場合があります。
VCBResourceActive	このカウンタは、Cisco Unified Communications Manager に登録されているすべてのビデオ会議デバイスで現在使用されているビデオ会議リソースの総数を表します。
VCBResourceAvailable	このカウンタは、非アクティブで、現在使用可能なビデオ会議リソースの総数を表します。
VCBResourceTotal	このカウンタは、Cisco Unified Communications Manager に現在登録されているすべてのビデオ会議ブリッジデバイスから提供されているビデオ会議リソースの総数を表します。
VideoCallsActive	このカウンタは、Cisco Unified Communications Manager に登録されているすべてのビデオ会議ブリッジデバイス上のアクティブなビデオ ストリーミング接続を持つアクティブなビデオ コールの総数を表します。
VideoCallsCompleted	このカウンタは、ビデオ ストリームに実際に接続され、その後開放されたビデオ コールの数を表します。
VideoOutOfResources	このカウンタは、使用可能なビデオストリーミング リソースがなかった場合に、Cisco Unified Communications Manager が Cisco Unified Communications Manager に登録されているビデオ会議ブリッジ デバイスの 1 つからビデオストリーミング リソースの割り当てを試行した回数の合計を表します。

カウンタ	カウンタの説明
XCODE_RequestsThrottled	このカウンタは、制御のために拒否されたトランスコーダ リソース要求の総数を表します（トランスコーダが Cisco CallManager サービス パラメータである MTP and Transcoder Resource Throttling Percentage で指定された設定済みの制御比率を超えて使用されていたため、このトランスコーダからのリソースを割り当てることができませんでした）。このカウンタは、このトランスコーダからリソースが要求され、その要求が制御によって拒否されるたびに増分します。このカウンタの値は、トランスコーダ デバイスが Cisco CallManager サービスに登録されてから現在までの実行の合計を反映しています。

## Cisco CallManager System Performance

Cisco CallManager System Performance オブジェクトは、Cisco Unified Communications Manager に関するシステム パフォーマンスの情報を提供します。次の表には、Cisco CallManager システム パフォーマンス カウンタについての情報が含まれます。

表 44 : Cisco CallManager System Performance

カウンタ	カウンタの説明
AverageExpectedDelay	このカウンタは、着信メッセージを処理する前の現在の平均予測遅延を表します。
CallsRejectedDueToICTThrottling	このカウンタは、Cisco CallManager サービスの開始以降に、クラスタ間トランク（ICT）コール制御のため拒否されたコールの総数を表します。5 秒あたり 140 コールのしきい値制限に達すると、ICT は新しいコールの制御（拒否）を開始します。ICT コール制御が発生する原因の 1 つは、ICT を経由するコールが ルートループ状態になることです。
CallThrottlingGenericCounter3	このカウンタは、コール制御で使用される汎用カウンタを表します。
CodeRedEntryExit	このカウンタは、Cisco Unified Communications Manager が Code Red 状態（コールスロットリングモード）を開始したか、または終了したかを示します。有効な値は、0（Exit）および 1（Entry）です。

カウンタ	カウンタの説明
CodeYellowEntryExit	このカウンタは、Cisco Unified Communications Manager が Code Yellow 状態（コールスロットリング モード）を開始したか、または終了したかを示します。有効な値は、0（Exit）および1（Entry）です。
EngineeringCounter1	Cisco Engineering Special ビルドによる指示がない限り、このカウンタは使用しないでください。シスコは、診断の目的でこのカウンタの情報を使用します。
EngineeringCounter2	Cisco Engineering Special ビルドによる指示がない限り、このカウンタは使用しないでください。シスコは、診断の目的でこのカウンタの情報を使用します。
EngineeringCounter3	Cisco Engineering Special ビルドによる指示がない限り、このカウンタは使用しないでください。シスコは、診断の目的でこのカウンタの情報を使用します。
EngineeringCounter4	Cisco Engineering Special ビルドによる指示がない限り、このカウンタは使用しないでください。シスコは、診断の目的でこのカウンタの情報を使用します。
EngineeringCounter5	Cisco Engineering Special ビルドによる指示がない限り、このカウンタは使用しないでください。シスコは、診断の目的でこのカウンタの情報を使用します。
EngineeringCounter6	Cisco Engineering Special ビルドによる指示がない限り、このカウンタは使用しないでください。シスコは、診断の目的でこのカウンタの情報を使用します。
EngineeringCounter7	Cisco Engineering Special ビルドによる指示がない限り、このカウンタは使用しないでください。シスコは、診断の目的でこのカウンタの情報を使用します。
EngineeringCounter8	Cisco Engineering Special ビルドによる指示がない限り、このカウンタは使用しないでください。シスコは、診断の目的でこのカウンタの情報を使用します。

カウンタ	カウンタの説明
QueueSignalsPresent 1-High	このカウンタは、Cisco Unified Communications Manager のキューの高優先順位信号の数を表します。高優先順位信号には、主に、タイムアウトイベント、内部 Cisco Unified Communications Manager キープアライブ、特定のゲートキーパーイベント、内部プロセスの作成などのイベントが含まれています。多数の高優先順位イベントは、Cisco Unified Communications Manager のパフォーマンスを低下させ、コール接続の遅延やダイヤルトーン消失の原因となります。このカウンタを QueueSignalsProcessed 1-High カウンタと併用して、Cisco Unified Communications Manager 上の処理の遅延を判別します。
QueueSignalsPresent 2-Normal	このカウンタは、Cisco Unified Communications Manager のキューの通常優先順位信号の数を表します。通常優先順位信号には、主に、コール処理機能、キー操作、オンフックとオフフックの通知などのイベントが含まれています。多数の通常優先順位のイベントは、Cisco Unified Communications Manager のパフォーマンスを低下させ、ダイヤルトーンの遅延、コール接続の遅延、またはダイヤルトーンの消失の原因となる場合があります。このカウンタを QueueSignalsProcessed 2-Normal カウンタと併用して、Cisco Unified Communications Manager 上のコール処理の遅延を判別します。通常優先順位信号が処理を開始する前に、高優先順位信号を完了する必要があることに注意してください。したがって、高優先順位カウンタを確認し、遅延の可能性について正確な状況を把握する必要があります。
QueueSignalsPresent 3-Low	このカウンタは、Cisco Unified Communications Manager のキューの低優先順位信号の数を表します。低優先順位信号には、主に、端末デバイスの登録（初期端末登録要求メッセージは除く）などのイベントが含まれています。このキュー内の多数の信号は、特に、デバイス登録遅延のイベントの原因となります。
QueueSignalsPresent 4-Lowest	このカウンタは、Cisco Unified Communications Manager のキューの最低優先順位信号の数を表します。最低優先順位信号には、主に、デバイス登録中の初期端末登録要求メッセージなどのイベントが含まれています。このキュー内の多数の信号は、特に、デバイス登録遅延のイベントの原因となります。
QueueSignalsProcessed 1-High	このカウンタは、Cisco Unified Communications Manager によって1秒間隔で処理される高優先順位信号の数を表します。このカウンタを QueueSignalsPresent 1-High カウンタと併用して、このキューの処理の遅延を判別します。

カウンタ	カウンタの説明
QueueSignalsProcessed 2-Normal	このカウンタは、Cisco Unified Communications Manager によって1秒間隔で処理される通常優先順位信号の数を表します。このカウンタを QueueSignalsPresent 2-Normal カウンタと併用して、このキューの処理の遅延を判別します。高優先順位信号は通常優先順位信号の前に処理されることに注意してください。
QueueSignalsProcessed 3-Low	このカウンタは、Cisco Unified Communications Manager によって1秒間隔で処理される低優先順位信号の数を表します。このカウンタを QueueSignalsPresent 3-Low カウンタと併用して、このキューの処理の遅延を判別します。処理される信号の数は、この時間間隔でデバイス登録アクティビティが処理される量の指標となります。
QueueSignalsProcessed 4-Lowest	このカウンタは、Cisco Unified Communications Manager によって1秒間隔で処理される最低優先順位信号の数を表します。このカウンタを QueueSignalsPresent 4-Lowest カウンタと併用して、このキューの処理の遅延を判別します。処理される信号の数は、この時間間隔で Cisco Unified Communications Manager 登録プロセスを開始したデバイスの数の指標となります。
QueueSignalsProcessed Total	このカウンタは、高、通常、低、最低のすべてのキュー レベルについて、それぞれ1秒間に Cisco Unified Communications Manager によって処理されるすべてのキュー信号の合計を表します。
SkinnyDevicesThrottled	このカウンタは、制御される Skinny デバイスの総数を表します。Skinny デバイスが生成したイベントの総数が、設定されている最大しきい値（デフォルト値は2000 イベント）を5秒間隔内で上回ったとき、Skinny デバイスは制御されます（シャットダウンと再登録を求められます）。
ThrottlingSampleActivity	このカウンタは、設定されたサンプルサイズのうち、averageExpectedDelay の値がゼロではないサンプルがいくつあるかを示します。このカウンタは、averageExpectedDelay の値が0のサンプルがあった場合にリセットされます。このプロセスは、サンプルのバッチごとに繰り返されます。バッチは、設定されたサンプルサイズを表します。
TotalCodeYellowEntry	このカウンタは、Cisco Unified Communications Manager コール処理が Code Yellow 状態に入る回数を表します。このカウンタは、Cisco Unified Communications Manager プロセスの開始時から累積されます。

## Cisco CTIManager

Cisco CTI Manager オブジェクトは、Cisco CTI Manager についての情報を提供します。次の表には、Cisco CTIManager カウンタについての情報が含まれます。

表 45 : Cisco CTI Manager

カウンタ	カウンタの説明
CcmLinkActive	このカウンタは、アクティブな Cisco Unified Communications Manager リンクの総数を表します。該当する場合、CTI Manager は、1つのクラスタ内のすべてのアクティブなサーバへのリンクを維持します。
CTIConnectionActive	このカウンタは、現在 CTIManager に接続されている CTI クライアントの総数を表します。このカウンタは、新しい接続が確立されると1つ増加し、接続が開放されると1つ減少します。CTIManager の MaxCTIConnections サービス パラメータは、アクティブな接続の最大数を設定します。
DevicesOpen	このカウンタは、CTIアプリケーションによって制御またはモニタされる Cisco Unified Communications Manager に設定されているデバイスの総数を表します。デバイスには、ハードウェア IP Phone、CTI ポート、CTI ルート ポイントなどがあります。
LinesOpen	このカウンタは、CTIアプリケーションを制御またはモニタする Cisco Unified Communications Manager に設定されている回線の総数を表します。
QbeVersion	このカウンタは、CTIManager が使用する Quick Buffer Encoding (QBE) インターフェイスのバージョン番号を表します。

## Cisco Dual-Mode Mobility

Cisco Dual-Mode Mobility オブジェクトは、Cisco Unified Communications Manager のデュアルモード モビリティ アプリケーションについての情報を提供します。次の表には、Cisco Dual-Mode Mobility カウンタについての情報が含まれます。

表 46 : Cisco Dual-Mode Mobility

カウンタ	カウンタの説明
CallsAnchored	このカウンタは、Cisco Unified Communications Manager 内で固定されたデュアルモード電話機で送信または受信するコールの数を表します。このカウンタは、デュアルモード電話機でコールが送信または受信されたときに増加します。デュアルモード電話機から別のデュアルモード電話機を呼び出した場合、カウンタは2つ増加します。
DMMSRegistered	このカウンタは、無線 LAN (WLAN) に登録された Dual-mode Mobile Station (DMMS) 加入者の数を表します。
FollowMeAborted	このカウンタは、失敗した follow-me 操作の数を表します。
FollowMeAttempted	このカウンタは、Cisco Unified Communications Manager が試行した follow-me 操作の数を表します。このカウンタは、Wireless Service Manager (WSM) からの SIP 302 (一時的に移動) メッセージが受信され、Cisco Unified Communications Manager が WLAN の DMMS にコールをリダイレクトしたときに増加します。
FollowMeCompleted	このカウンタは、正常に完了した follow-me 操作の数を表します。このカウンタは、WLAN 内の DMMS がコールに回答し、発信側デバイスとのメディア (音声パス) が正常に確立されたときに増加します。
FollowMeInProgress	このカウンタは、現在進行中の follow-me 操作の数を表します。このカウンタは、follow-me 操作が試行されたときに増加し、follow-me 操作が中断または完了したときに減少します。
H1HandOutAttempted	このカウンタは、デュアルモード電話機が試行した H1 hand-out 操作の数を表します。このカウンタは、Cisco Unified Communications Manager が DMMS から H1 の番号へのコールを処理したときに増加します。
H1HandOutCompleted	このカウンタは、正常に完了した H1 hand-out 操作の数を表します。このカウンタは、WLAN 内の DMMS がメディア (音声パス) を正常に再確立したときに増加します。
H2HandOutCompleted	このカウンタは、正常に完了した H2 hand-out 操作の数を表します。このカウンタは、WLAN の DMMS がメディア (音声パス) を正常に再確立したときに増加します。

カウンタ	カウンタの説明
H2HandOutsAttempted	このカウンタは、デュアルモード電話機が試行した H2 hand-out 操作の数を表します。このカウンタは、Cisco Unified Communications Manager が DMMS から H2 の番号へのコールを受信したときに増加します。
HandInAborted	このカウンタは、失敗した hand-in 操作の数を表します。
HandInAttempted	このカウンタは、デュアルモード電話機が試行した hand-in 操作の数を表します。
HandInCompleted	このカウンタは、正常に完了した hand-in 操作の数を表します。このカウンタは、WLAN の DMMS がメディア（音声パス）を正常に再確立したときに増加します。
HandInInProgress	このカウンタは、現在進行中の hand-in 操作の数を表します。このカウンタは、hand-in 操作が試行されたときに増加し、hand-in 操作が中断または完了したときに減少します。
HandOutAborted	このカウンタは、失敗した hand-out 操作の数を表します。
HandOutInProgress	このカウンタは、現在進行中の H1 および H2 hand-out 操作の数を表します。このカウンタは、H1 または H2 hand-out 操作が試行されたときに増加し、H1 または H2 hand-out 操作が中断または完了したときに減少します。

## Cisco エクステンション モビリティ

Cisco Extension Mobility オブジェクトは、エクステンション モビリティ アプリケーションについての情報を提供します。次の表に、Cisco Extension Mobility カウンタに関する情報を示します。

表 47: Cisco Extension Mobility アプリケーション

カウンタ	カウンタの説明
RequestsHandled	このカウンタは、Cisco CallManager サービスの最後の再起動以降にエクステンション モビリティ アプリケーションが処理した HTTP 要求の総数を表します。標準的なログインは、2つの HTTP 要求で構成されています。1つは、デバイスの初期ログイン状態の照会、もう1つは、デバイス上のユーザへのログインです。同様に、標準的なログアウトも2つの HTTP 要求になります。



カウンタ	カウンタの説明
RequestsInProgress	このカウンタは、エクステンションモビリティアプリケーションが現在処理している HTTP 要求の数を表します。標準的なログインは、2つの HTTP 要求で構成されています。1つは、デバイスの初期ログイン状態の照会、もう1つは、デバイス上のユーザへのログインです。同様に、標準的なログアウトも2つの HTTP 要求になります。
RequestsThrottled	このカウンタは、制御のために失敗したログイン要求またはログアウト要求の総数を表します。
LoginsSuccessful	このカウンタは、エクステンション モビリティ サービスを使用して正常に完了したログイン要求の総数を表します。
LogoutsSuccessful	このカウンタは、エクステンション モビリティ サービスを使用して正常に完了したログアウト要求の総数を表します。
Total Login/LogoutRequestsAttempted	このカウンタは、このエクステンション モビリティ サービスを使用して試行されたログイン要求およびログアウト要求の総数を表します。この数には、成功した試行と失敗した試行の両方が含まれます。

## Cisco Gatekeeper

Cisco Gatekeeper オブジェクトは、登録済みの Cisco ゲートキーパー デバイスについての情報を提供します。次の表には、Cisco ゲートキーパー デバイス カウンタについての情報が含まれます。

表 48 : Cisco Gatekeeper

カウンタ	カウンタの説明
ACFsReceived	このカウンタは、設定済みゲートキーパーとその代替ゲートキーパーから受信された RAS アドミッション確認メッセージの総数を表します。
ARQsAttempted	このカウンタは、設定済みゲートキーパーとその代替ゲートキーパーを使用して試行された RAS アドミッション要求メッセージの総数を表します。
RasRetries	このカウンタは、設定済みゲートキーパーとその代替ゲートキーパー上のすべての RAS 確認応答メッセージの消失や遅延による再試行回数を表します。

カウンタ	カウンタの説明
VideoOutOfResources	このカウンタは、帯域幅の不足などが原因で失敗した、設定済みゲートキーパーまたはその代替ゲートキーパーへのビデオストリーム要求の総数を表します。

## Cisco H.323

Cisco H.323 オブジェクトは、登録済みの Cisco H.323 デバイスについての情報を提供します。次の表に、Cisco H.323 デバイス カウンタに関する情報を示します。

表 49 : Cisco H.323

カウンタ	カウンタの説明
CallsActive	このカウンタは、設定済みの H.323 デバイス上で現在アクティブな（使用中の）ストリーミング接続の数、つまり、接続されている音声パスが実際に存在するコールの数を表します。
CallsAttempted	このカウンタは、デバイス上で試行されたコールの総数を表します。成功したコールの試行と失敗したコールの試行の両方が含まれます。
CallsCompleted	このカウンタは、デバイスから発信され成功したコールの総数を表します。
CallsInProgress	このカウンタは、デバイス上で現在進行中のコールの数を表します。
CallsRejectedDueToICTCallThrottling	このカウンタは、Cisco CallManager サービスの開始以降に、クラスト間トランク（ICT）コール制御のため拒否されたコールの総数を表します。5 秒あたり 140 コールのしきい値制限に達すると、ICT は新しいコールの制御（拒否）を開始します。ICT コール制御が発生する原因の 1 つは、ICT を経由するコールがルートループ状態になることです。
VideoCallsActive	このカウンタは、Cisco Unified Communications Manager に登録されているすべての H.323 トランク上で現在アクティブな（使用中の）ビデオストリーミング接続を持つビデオコールの数、つまり、Cisco Unified Communications Manager 上にビデオストリーミング接続が実際に存在するコールの数を表します。

カウンタ	カウンタの説明
VideoCallsCompleted	このカウンタは、Cisco Unified Communications Manager に登録されているすべての H.323 トランクに対するビデオストリームに実際に接続されたビデオ コールを表します。この数は、コールが終了したときに増加します。

## Cisco Hunt Lists

Cisco Hunt Lists オブジェクトは、Cisco Unified Communications Manager の管理で定義されたハントラストについての情報を提供します。次の表には、Cisco Hunt List のカウンタについての情報が含まれます。

表 50 : Cisco Hunt Lists

カウンタ	カウンタの説明
CallsAbandoned	このカウンタは、ハントラストを介して発生し、放棄されたコールの数を表します。放棄されたコールとは、コールに 응답する前に発信者が切断したコールです。
CallsActive	このカウンタは、ハントラストを介して発生し、現在アクティブな（使用中の）コールの数を表します。アクティブなコールとは、配布され、応答された、音声パスが接続されているコールを意味します。
CallsBusyAttempts	このカウンタは、回線グループまたはルートグループのいずれか（あるいはその両方）のすべてのメンバーがビジー状態だったときに、ハントラストを介して試行されたコールの回数を表します。
CallsInProgress	このカウンタは、ハントラストを介して現在進行中のコールの数を表します。進行中のコールとは、着信呼分配機能によって回線グループまたはルートグループのメンバーへの拡張が試行され、まだ応答されていないコールを意味します。ハントラストメンバーの例としては、回線、端末デバイス、トランクデバイス、トランクデバイスのポートやチャネルがあります。
CallsRingNoAnswer	このカウンタは、ハントラストを介したコールのうち、着信側が呼び出しに 응답しなかったコールの総数を表します。

カウンタ	カウンタの説明
HuntListInService	このカウンタは、特定のハントリストが現在インサービスであるかどうかを指定します。値 0 は、ハントリストがアウトオブサービスであることを示します。値 1 は、ハントリストがインサービスであることを示します。ハントリストがアウトオブサービスになる理由として、ハントリストがその Cisco Unified Communications Manager のグループに基づいて、プライマリ Cisco Unified Communications Manager で実行されていないか、または、ハントリストが Cisco Unified Communications Manager の管理で無効化されていることが挙げられます。
MembersAvailable	このカウンタは、インサービスハントリストに属している回線グループとルートグループの、使用可能なメンバーまたはアイドルメンバーの総数を表します。使用可能なメンバーは、現在コールを処理しており、新規のコールを受け入れます。アイドルメンバーは、コールを処理せずに新規のコールを受け入れます。ハントリストメンバーは、ルートグループ、回線グループ、またはそれらの組み合わせで構成することができます。回線グループのメンバーとは、IP Phone またはボイスメールポートの回線のディレクトリ番号を意味します。ルートグループのメンバーとは、ステーションゲートウェイ、トランクゲートウェイ、またはトランクゲートウェイのポートやチャネルを意味します。

## Cisco HW Conference Bridge Device

Cisco HW Conference Bridge Device オブジェクトは、登録済みの Cisco ハードウェア会議ブリッジデバイスについての情報を提供します。次の表には、Cisco ハードウェア会議ブリッジデバイスカウンタについての情報が含まれます。

表 51 : Cisco HW Conference Bridge Device

カウンタ	カウンタの説明
HWConferenceActive	このカウンタは、ハードウェア会議ブリッジデバイス上で現在アクティブな（使用中の）会議の数を表します。1つのリソースは1つのストリームを表します。
HWConferenceCompleted	このカウンタは、ハードウェア会議デバイス上に割り当てられ、開放された会議の総数を表します。会議は、最初のコールがブリッジに接続されたときに開始します。会議は、最後のコールがブリッジから接続解除されたときに完了します。

カウンタ	カウンタの説明
OutOfResources	このカウンタは、ハードウェア会議デバイスから会議リソースの割り当てを試行して、すべてのリソースがすでに使用中であるなどの理由で失敗した回数の合計を表します。
ResourceActive	このカウンタは、このハードウェア会議デバイスに対して現在使用中の（アクティブな）リソースの数を表します。1つのリソースは1つのストリームを表します。
ResourceAvailable	このカウンタは、非アクティブで、ハードウェア会議デバイスで現在まだ使用可能なリソースの総数を表します。1つのリソースは1つのストリームを表します。
ResourceTotal	このカウンタは、ハードウェア会議ブリッジデバイス用リソースの総数を表します。このカウンタは、ResourceAvailable カウンタと ResourceActive カウンタを合計した数になります。1つのリソースは1つのストリームを表します。

## Cisco IP Manager Assistant

Cisco IP Manager Assistant (IPMA) Service オブジェクトは、Cisco Unified Communications Manager Assistant アプリケーションに関する情報を提供します。次の表には、Cisco IPMA カウンタについての情報が含まれます。

表 52 : Cisco IP Manager Assistant Service

カウンタ	カウンタの説明
AssistantsActive	このカウンタは、現在アクティブなアシスタント コンソールの数を表します。アクティブなアシスタント コンソールは、アシスタントが Assistant Console デスクトップアプリケーションからログインする場合に存在します。
LinesOpen	このカウンタは、Cisco Unified Communications Manager Assistant アプリケーションによってオープンされた電話回線の数を表します。オープン電話回線は、アプリケーションが CTI からの回線制御を前提としている場合に存在します。
ManagersActive	このカウンタは、Cisco IPMA がサービスを提供しているマネージャの現在の数を表します。

カウンタ	カウンタの説明
SessionsCurrent	このカウンタは、現在 Cisco Unified Communications Manager Assistant アプリケーションを使用しているマネージャとアシスタントの総数を表します。各マネージャと各アシスタントは、アクティブセッションを構成します。したがって、1組のマネージャとアシスタントに対して、このカウンタは2つのセッションを反映します。

## Cisco LBM service

Cisco LBM service オブジェクトは、Cisco Unified Communications Manager で定義されている LBM サービスについての情報を提供します。次の表には、Cisco LBM service カウンタについての情報が含まれます。

表 53 : Cisco LBM service

カウンタ	カウンタの説明
Is Hub[1] or Spoke[0]	このカウンタは、ロケーション帯域幅マネージャの状態を表します。スポーク状態では0、ハブ状態は1の値で表されます。
LocalHubNodesConnected	このカウンタは、接続されたローカルハブノードの数を表します。
LocalSpokesNodesConnected	このカウンタは、接続されたローカルスポークノードの数を表します。
RemoteHubNodesConnectedInsecure	このカウンタは、接続されたセキュアでないリモートハブノードの数を表します。
RemoteHubNodesConnectedSecure	このカウンタは、接続されたセキュアなリモートハブノードの数を表します。

## Cisco Lines

Cisco Lines オブジェクトは、ダイヤルしてデバイスに接続できる Cisco 回線（ディレクトリ番号）の数を表します。回線は、エンドポイントで終了するすべてのディレクトリ番号を表します。割り当てられたディレクトリ番号は、回線を識別します。Cisco Lines オブジェクトには、デジタルアクセスゲートウェイまたはアナログアクセスゲートウェイのパターンなどのワイルドカードを含むディレクトリ番号は含まれていません。

Active カウンタは、回線の状態についてアクティブまたは非アクティブのいずれかを表します。0 は、回線が使用されていないことを示します。数値が 0 より大きい場合、回線がアクティブであることを示します。数値はその回線で現在進行中のコールの数を表します。複数のコールがアクティブである場合、明確な保留状態（ユーザ保留）、またはネットワーク保留操作（たとえば、転送が進行中のため転送保留にされている状態）のいずれかの理由で、コールが保留状態であることを示します。これは、任意のデバイスに割り当てられるすべてのディレクトリ番号に適用されます。

## Cisco Locations LBM

Cisco Location LBM オブジェクトは、Cisco Unified Communications Manager のクラスタで定義されているロケーションについての情報を提供します。次の表には、Cisco ロケーションカウンタについての情報が含まれます。

表 54 : Cisco Locations LBM

カウンタ	カウンタの説明
BandwidthAvailable	このカウンタは、1つのロケーション、または2つのロケーション間のリンクでの現在の音声帯域幅を示します。値 0 は、使用可能な音声帯域幅がないことを示します。
BandwidthMaximum	このカウンタは、1つのロケーション、または2つのロケーション間のリンクで、現在使用可能な最大音声帯域幅を示します。値 0 は、使用可能な音声帯域幅がないことを示します。
BandwidthOversubscription	このカウンタは、1つのロケーション、または2つのロケーション間のリンクで、現在オーバーサブスクリプションが発生している音声帯域幅を示します。値が 0 の場合、帯域幅のオーバーサブスクリプションが発生していないことを示します。
CallsInProgress	このカウンタは、特定の Cisco Location Bandwidth Manager で現在進行中のコールの数を表します。
ImmersiveOutOfResources	これは、イマーシブなビデオ帯域幅不足のため障害が発生した、1つのロケーション、または2つのロケーション間のリンクに関連付けられている、イマーシブビデオコールの帯域幅予約の総数を表します。

カウンタ	カウンタの説明
ImmersiveVideoBandwidthAvailable	このカウンタは、1つのロケーション、または2つのロケーション間のリンクで、ビデオに現在使用可能な最大帯域幅を示します。値0は、ビデオに割り当てられている帯域幅がないことを示します。
ImmersiveVideoBandwidthMaximum	このカウンタは、1つのロケーション、または2つのロケーション間のリンクで、ビデオに現在使用可能な帯域幅を示します。値0は、使用可能な帯域幅がないことを示します。
ImmersiveVideoBandwidthOversubscription	このカウンタは、1つのロケーション、または2つのロケーション間のリンクで、現在オーバーサブスクリプションが発生しているイマーシブビデオ帯域幅を示します。値が0の場合、帯域幅のオーバーサブスクリプションが発生していないことを示します。
OutOfResources	このカウンタは、音声帯域幅不足のため障害が発生した、1つの指定ロケーション、または2つのロケーション間のリンクに関連付けられている、音声コール帯域幅予約の総数を表します。
VideoBandwidthAvailable	このカウンタは、1つのロケーション、または2つのロケーション間のリンクで、ビデオに現在使用可能な帯域幅を示します。値0は、使用可能な帯域幅がないことを示します。
VideoBandwidthMaximum	このカウンタは、1つのロケーション、または2つのロケーション間のリンクで、ビデオに使用可能な最大帯域幅を示します。値0は、ビデオに割り当てられている帯域幅がないことを示します。
VideoOversubscription	このカウンタは、1つのロケーション、または2つのロケーション間のリンクで、現在オーバーサブスクリプションが発生しているビデオ帯域幅容量を示します。値が0の場合、帯域幅のオーバーサブスクリプションが発生していないことを示します。
VideoOutOfResources	このカウンタは、ビデオ帯域幅不足のため障害が発生した、1つの指定ロケーション、または2つのロケーション間のリンクに関連付けられている、ビデオコール帯域幅予約の総数を表します。



## Cisco Locations RSVP

Cisco Location RSVP オブジェクトは、Cisco Unified Communications Manager で定義されている RSVP についての情報を提供します。次の表に、Cisco location RSVP カウンタに関する情報を示します。

表 55 : *Cisco Locations RSVP*

カウンタ	カウンタの説明
RSVP AudioReservationErrorCounts	このカウンタは、オーディオストリーム内の RSVP 予約エラーの数を表します。
RSVP MandatoryConnectionsInProgress	このカウンタは、必須の RSVP を使用した進行中の接続の数を表します。
RSVP OptionalConnectionsInProgress	このカウンタは、オプションの RSVP を使用した進行中の接続の数を表します。
RSVP TotalCallsFailed	このカウンタは、RSVP 予約の失敗によって失敗した全コールの数を表します。
RSVP VideoCallsFailed	このカウンタは、RSVP 予約の失敗によって失敗したビデオコールの数を表します。
RSVP VideoReservationErrorCounts	このカウンタは、ビデオストリーム内の RSVP 予約エラーの数を表します。

## Cisco Media Streaming Application

Cisco IP Voice Media Streaming Application オブジェクトは、登録済みの MTP、MOH サーバ、会議ブリッジサーバ、およびアナウンシエータについての情報を提供します。次の表に、Cisco IP Voice Media Streaming Application カウンタに関する情報を示します。



(注) デバイスプールに関連付けられている Cisco Unified Communications Manager グループ内の Cisco Unified Communications Manager ごとに 1 つのオブジェクトが存在します。アナウンシエータ デバイスはそのデバイスプールを使用するように設定されています。

表 56 : Cisco Media Streaming Application

カウンタ	カウンタの説明
ANNConnectionsLost	このカウンタは、Cisco IP Voice Media Streaming Application の最後の再起動以降に Cisco Unified Communications Manager 接続が失われた回数の合計を表します。
ANNConnectionState	このカウンタは、アナウンサーに関連付けられている各 Cisco Unified Communications Manager について、Cisco Unified Communications Manager への現在の登録状態を表します。0 は Cisco Unified Communications Manager への登録がないことを示します。1 は、プライマリ Cisco Unified Communications Manager への登録を示します。2 は、セカンダリ Cisco Unified Communications Manager への接続を示します (Cisco Unified Communications Manager には接続されていますが、プライマリ Cisco Unified Communications Manager 接続が失敗するまでは登録されません)。
ANNConnectionsTotal	このカウンタは、Cisco IP Voice Media Streaming Application サービスの開始以降に開始されたアナウンサー インスタンスの総数を表します。
ANNInstancesActive	このカウンタは、アクティブに再生している (現在使用中の) アナウンスの数を表します。
ANNStreamsActive	このカウンタは、すべての接続に対して現在アクティブなシンプレックス (単方向) ストリームの総数を表します。各ストリームの方向は、1つのストリームとしてカウントされます。1つの内部ストリームがオーディオ入力を提供し、別の出力ストリームがエンドポイント デバイスへの入力を提供します。
ANNStreamsAvailable	このカウンタは、アナウンサー デバイスに対して割り当てられている使用可能なストリームの残りの数を表します。このカウンタは、設定されている接続の数 (Cisco IP Voice Media Streaming App サービス パラメータで、Annunciator、Call Count に対して定義されている) の2倍の数で開始され、アクティブなストリームが開始されるたびに1つずつ減少します。
ANNStreamsTotal	このカウンタは、Cisco IP Voice Media Streaming Application サービスの開始以降にアナウンサー デバイスに接続されたシンプレックス (単方向) ストリームの総数を表します。
CFBConferencesActive	このカウンタは、アクティブな (現在使用中の) 会議の数を表します。

カウンタ	カウンタの説明
CFBConferencesTotal	このカウンタは、Cisco IP Voice Media Streaming Application サービスの開始以降に開始された会議の総数を表します。
CFBConnectionsLost	このカウンタは、Cisco IP Voice Media Streaming Application の最後の再起動以降に Cisco Unified Communications Manager 接続が失われた回数の合計を表します。
CFBConnectionState	このカウンタは、SW Conference Bridge に関連付けられている各 Cisco Unified Communications Manager について、Cisco Unified Communications Manager への現在の登録状態を表します。0 は Cisco Unified Communications Manager への登録がないことを示します。1 は、プライマリ Cisco Unified Communications Manager への登録を示します。2 は、セカンダリ Cisco Unified Communications Manager への接続を示します（Cisco Unified Communications Manager には接続されていますが、プライマリ Cisco Unified Communications Manager 接続が失敗するまでは登録されません）。
CFBStreamsActive	このカウンタは、すべての会議に対して現在アクティブなシンプレックス（単方向）ストリームの総数を表します。各ストリームの方向は、1つのストリームとしてカウントされます。三者間会議では、アクティブなストリームの数は6になります。
CFBStreamsAvailable	このカウンタは、会議ブリッジに対して割り当てられている使用可能なストリームの残りの数を表します。このカウンタは、設定されている接続の数（Cisco IP Voice Media Streaming App サービス パラメータで、Conference Bridge、Call Count に対して定義されている）の2倍の数で開始され、アクティブなストリームが開始されるたびに1つつ減少します。
CFBStreamsTotal	このカウンタは、Cisco IP Voice Media Streaming Application サービスの開始以降に会議ブリッジに接続されたシンプレックス（単方向）ストリームの総数を表します。

カウンタ	カウンタの説明
MOHAudioSourcesActive	<p>このカウンタは、この MOH サーバ用のアクティブな（現在使用中の）オーディオ ソースの数を表します。受信しているデバイスが存在しない場合、これらのオーディオ ソースの一部はアクティブなストリーミング オーディオ データではない可能性があります。マルチキャスト オーディオ ソースは常にストリーミング オーディオとなるため、例外となります。</p> <p>オーディオ ソースが使用中の場合、受信側が切断された後でも、このカウンタには設定済みの MOH コーデックごとに常に 1 つの入カストリームが存在します。ユニキャストストリームでは、デバイスが接続してストリームを受信するまでは、受信するオーディオ データがなく、ストリームが一時停止状態になる場合があります。各 MOH マルチキャスト リソースは、オーディオ ソースとコーデックの組み合わせごとに 1 つのストリームを使用します。たとえば、マルチキャスト、G.711 mu-law、ワイドバンドコーデックに対してデフォルトオーディオ ソースを設定した場合、2 つのストリーム（デフォルトオーディオ ソースと G.711 mu-law、およびデフォルト オーディオ ソースとワイドバンド）が使用されます。</p>
MOHConnectionsLost	<p>このカウンタは、Cisco IP Voice Media Streaming Application の最後の再起動以降に Cisco Unified Communications Manager 接続が失われた回数の合計を表します。</p>
MOHConnectionState	<p>このカウンタは、MOH に関連付けられている各 Cisco Unified Communications Manager について、Cisco Unified Communications Manager への現在の登録状態を表します。0 は Cisco Unified Communications Manager への登録がないことを示します。1 は、プライマリ Cisco Unified Communications Manager への登録を示します。2 は、セカンダリ Cisco Unified Communications Manager への接続を示します（Cisco Unified Communications Manager には接続されていますが、プライマリ Cisco Unified Communications Manager 接続が失敗するまでは登録されません）。</p>

カウンタ	カウンタの説明
MOHStreamsActive	<p>このカウンタは、すべての接続に対してアクティブな（現在使用中の）シンプレックス（単方向）ストリームの総数を表します。ユニキャスト オーディオ ソースを受信しているデバイスごとに1つの出力ストリームが存在し、アクティブ オーディオ ソースごとに1つの入力ストリームが存在します。値はMOHコーデックの数で乗算されます。</p> <p>以前に使用されたことがあるオーディオ ソースには、設定済みの MOH コーデックごとに必ず1つの入力ストリームが存在します。ユニキャストストリームでは、デバイスが接続してストリームを受信するまでは、受信するオーディオ データがなく、ストリームが一時停止状態になる場合があります。各 MOH マルチキャスト リソースは、オーディオ ソースとコーデックの組み合わせごとに1つのストリームを使用します。たとえば、マルチキャスト、G.711 mu-law、ワイドバンドコーデックに対してデフォルトオーディオソースを設定した場合、2つのストリーム（デフォルトオーディオソースと G.711 mu-law、およびデフォルトオーディオソースとワイドバンド）が使用されます。</p>
MOHStreamsAvailable	<p>このカウンタは、MOH デバイスに対して割り当てられている使用可能なストリームの残りの数を表します。このカウンタは、設定済み半二重ユニキャスト接続の数に408を加えた数で開始され、アクティブストリームが開始されるたびに1つずつ減少します。カウンタは、各マルチキャストオーディオソースに対して2つずつ減少します。値は設定済みの MOH コーデックの数で乗算されます。カウンタは、各ユニキャストオーディオソースに対して1つずつ減少します。値は設定済み MOH コーデックの数で乗算されます。</p>
MOHStreamsTotal	<p>このカウンタは、Cisco IP Voice Media Streaming Application サービスの開始以降に MOH サーバに接続されたシンプレックス（単方向）ストリームの総数を表します。</p>
MTPConnectionsLost	<p>このカウンタは、Cisco IP Voice Streaming Application の最後の再起動以降に Cisco Unified Communications Manager 接続が失われた回数の合計を表します。</p>

カウンタ	カウンタの説明
MTPConnectionState	このカウンタは、MTPに関連付けられている各 Cisco Unified Communications Manager について、Cisco Unified Communications Manager への現在の登録状態を表します。0 は Cisco Unified Communications Manager への登録がないことを示します。1 は、プライマリ Cisco Unified Communications Manager への登録を示します。2 は、セカンダリ Cisco Unified Communications Manager への接続を示します（Cisco Unified Communications Manager には接続されていますが、プライマリ Cisco Unified Communications Manager 接続が失敗するまでは登録されません）。
MTPConnectionsTotal	このカウンタは、Cisco IP Voice Media Streaming Application サービスの開始以降に開始された MTP インスタンスの総数を表します。
MTPInstancesActive	このカウンタは、アクティブな（現在使用中の）MTP インスタンスの数を表します。
MTPStreamsActive	このカウンタは、すべての接続に対して現在アクティブなシンプレックス（単方向）ストリームの総数を表します。各ストリームの方向は、1つのストリームとしてカウントされます。
MTPStreamsAvailable	このカウンタは、MTP デバイスに対して割り当てられている使用可能なストリームの残りの数を表します。このカウンタは、設定されている接続の数（Cisco IP Voice Media Streaming App サービス パラメータで、MTP、Call Count に対して定義されている）の2倍の数で開始され、アクティブなストリームが開始されるたびに1つずつ減少します。
MTPStreamsTotal	このカウンタは、Cisco IP Voice Media Streaming Application サービスの開始以降に MTP デバイスに接続されたシンプレックス（単方向）ストリームの総数を表します。
IVRInstancesActive	このカウンタは、現在アクティブな音声自動応答の数を表します。
IVRStreamsActive	このカウンタは、すべての接続に対して現在アクティブなシンプレックス（単方向）ストリームの総数を表します。各ストリームの方向は、1つのストリームとしてカウントされます。1つの内部ストリームがオーディオ入力を提供し、別の出力ストリームがエンドポイント デバイスへの入力を提供します。

カウンタ	カウンタの説明
IVRStreamsAvailable	このカウンタは、IVR デバイスに対して割り当てられている使用可能なストリームの残りの数を表します。このカウンタは、設定されている接続の数（Cisco IP Voice Media Streaming App サービス パラメータで、IVR、Call Count に対して定義されている）の3倍の数で開始され、アクティブなストリームが開始されるたびに1つずつ減少します。
IVRConnectionsTotal	このカウンタは、Cisco IP Voice Media Streaming Application サービスの開始以降に開始された IVR インスタンスの総数を表します。
IVRStreamsTotal	このカウンタは、Cisco IP Voice Media Streaming Application サービスの開始以降に IVR デバイスに接続されたシンプレックス（単方向）ストリームの総数を表します。
IVRConnectionsLost	このカウンタは、Cisco IP Voice Media Streaming Application の最後の再起動以降に Cisco Unified Communications Manager 接続が失われた回数の合計を表します。
IVRErrors	このカウンタは、Cisco IP Voice Media Streaming Application の最後の再起動以降に IVR が再生に失敗した回数の合計を表します。

## Cisco Messaging Interface

Cisco Messaging Interface オブジェクトは、Cisco Messaging Interface (CMI) サービスについての情報を提供します。次の表には、Cisco Messaging Interface (CMI) カウンタについての情報が含まれます。

表 57 : *Cisco Messaging Interface*

カウンタ	カウンタの説明
HeartBeat	このカウンタは、CMI サービスのハートビートを表します。このカウンタが増加している場合は、CMI サービスが稼働中であることを示します。カウンタが増加していない場合は、CMI サービスがダウンしていることを示します。
SMDIMessageCountInbound	このカウンタは、CMI サービスの最後の再起動以降に発生したインバウンド SMDI メッセージの数を表します。

カウンタ	カウンタの説明
SMDIMessageCountInbound24Hour	このカウンタは、最後の 24 時間以内に発生したインバウンド SMDI メッセージの数を表します。
SMDIMessageCountOutbound	このカウンタは、CMI サービスの最後の再起動以降に発生したアウトバウンド SMDI メッセージの数を表します。
SMDIMessageCountOutbound24Hour	このカウンタは、最後の 24 時間以内に発生したアウトバウンド SMDI メッセージの数を表します。
StartTime	このカウンタは、CMI サービスが開始された時間をミリ秒単位で表します。コンピュータ内のリアルタイム クロックは、現在時刻とサービス開始以降の経過時間をミリ秒単位で示す単なる参照ポイントであり、この時間の基準を提供します。参照ポイントは、1970 年 1 月 1 日の午前 0 時に指定されています。

## Cisco MGCP BRI Device

Cisco メディア ゲートウェイ コントロール プロトコル (MGCP) Foreign Exchange Office (FXO) Device オブジェクトは、登録済みの Cisco MGCP BRI デバイスについての情報を提供します。次の表には、Cisco MGCP BRI デバイス カウンタについての情報が含まれます。

表 58 : Cisco MGCP BRI Device

カウンタ	カウンタの説明
CallsCompleted	このカウンタは、この MGCP 基本速度 インターフェイス (BRI) デバイスから発信され成功したコールの総数を表します。
Channel 1 Status	このカウンタは、MGCP BRI デバイスに関連付けられている、指定された B チャネルの状態を表します。次の値が使用されます。0 (Unknown) は、チャネルの状態を判別できなかったことを示します。1 (Out of service) は、このチャネルが使用不可であることを示します。2 (Idle) は、このチャネルにはアクティブなコールがなく、使用可能な状態であることを示します。3 (Busy) は、このチャネルにアクティブコールが存在することを示します。4 (Reserved) は、このチャネルが D チャネルとして、または BRI 用の Synch チャネルとして使用されるように予約されていることを示します。



カウンタ	カウンタの説明
Channel 2 Status	このカウンタは、MGCP BRI デバイスに関連付けられている、指定された B チャンネルの状態を表します。次の値が使用されます。0 (Unknown) は、チャンネルの状態を判別できなかったことを示します。1 (Out of service) は、このチャンネルが使用不可であることを示します。2 (Idle) は、このチャンネルにはアクティブなコールがなく、使用可能な状態であることを示します。3 (Busy) は、このチャンネルにアクティブコールが存在することを示します。4 (Reserved) は、このチャンネルが D チャンネルとして、または BRI 用の Synch チャンネルとして使用されるように予約されていることを示します。
DatalinkInService	このカウンタは、対応するデジタルアクセス ゲートウェイ上のデータリンク (D チャンネル) の状態を表します。この値は、データリンクがアップ (イン サービス) の場合は 1 に設定され、データリンクがダウン (アウト オブ サービス) の場合は 0 に設定されます。
OutboundBusyAttempts	このカウンタは、使用可能な音声チャンネルがない場合に、MGCP BRI デバイスを介してコールが試行された回数の合計を表します。

## Cisco MGCP FXO Device

Cisco メディア ゲートウェイ コントロール プロトコル (MGCP) Foreign Exchange Office (FXO) Device オブジェクトは、登録済みの Cisco MGCP FXO デバイスについての情報を提供します。次の表には、Cisco MGCP FXO デバイス カウンタについての情報が含まれます。

表 59 : Cisco MGCP FXO Device

カウンタ	カウンタの説明
CallsCompleted	このカウンタは、MGCP FXO デバイス上のポートから発信され成功したコールの総数を表します。
OutboundBusyAttempts	このカウンタは、使用可能な音声チャンネルがない場合に、この MGCP FXO デバイス上のポートを介してコールが試行された回数の合計を表します。
PortStatus	このカウンタは、この MGCP FXO デバイスに関連付けられている FXO ポートの状態を表します。

## Cisco MGCP FXS Device

Cisco MGCP Foreign Exchange Station (FXS) Device オブジェクトは、登録済みの Cisco MGCP FXS デバイスについての情報を提供します。このオブジェクトのインスタンスは、Cisco Catalyst 6000 24 port FXS Analog Interface Module ゲートウェイ上の各ポートに対して1つずつ作成されます。たとえば、完全に設定された Catalyst 6000 Analog Interface Module の場合、このオブジェクトの個々の 24 のインスタンスが表現されます。次の表には、Cisco MGCP FXS デバイス カウンタについての情報が含まれます。

表 60 : Cisco MGCP FXS Device

カウンタ	カウンタの説明
CallsCompleted	このカウンタは、MGCPFXS デバイス上のこのポートから発信され成功したコールの総数を表します。
OutboundBusyAttempts	このカウンタは、使用可能な音声チャンネルがない場合に、この MGCPFXS デバイス上のポートを介してコールが試行された回数合計を表します。
PortStatus	このカウンタは、MGCP FXS デバイスに関連付けられている FXS ポートの状態を表します。

## Cisco MGCP Gateways

Cisco MGCP Gateways オブジェクトは、登録済みの MGCP ゲートウェイについての情報を提供します。次の表に、Cisco MGCP Gateway カウンタに関する情報を示します。

表 61 : Cisco MGCP Gateways

カウンタ	カウンタの説明
BRChannelsActive	このカウンタは、ゲートウェイのコールで現在アクティブな BRI 音声チャンネルの数を表します。
BRISpansInService	このカウンタは、ゲートウェイで現在使用可能な BRI スパンの数を表します。
FXOPortsActive	このカウンタは、ゲートウェイのコールで現在アクティブな FXO ポートの数を表します。
FXOPortsInService	このカウンタは、ゲートウェイで現在使用可能な FXO ポートの数を表します。

カウンタ	カウンタの説明
FXSPortsActive	このカウンタは、ゲートウェイのコールで現在アクティブな FXS ポートの数を表します。
FXSPortsInService	このカウンタは、ゲートウェイで現在使用可能な FXS ポートの数を表します。
PRChannelsActive	このカウンタは、ゲートウェイのコールで現在アクティブな PRI 音声チャンネルの数を表します。
PRISpansInService	このカウンタは、ゲートウェイで現在使用可能な PRI スパンの数を表します。
T1ChannelsActive	このカウンタは、ゲートウェイのコールで現在アクティブな T1 CAS 音声チャンネルの数を表します。
T1SpansInService	このカウンタは、ゲートウェイで現在使用可能な T1 CAS スパンの数を表します。

## Cisco MGCP PRI Device

Cisco MGCP Primary Rate Interface (PRI) Device オブジェクトは、登録済みの Cisco MGCP PRI デバイスについての情報を提供します。次の表には、Cisco MGCP PRI デバイスカウンタについての情報が含まれます。

表 62 : Cisco MGCP PRI Device

カウンタ	カウンタの説明
CallsActive	このカウンタは、この MGCP PRI デバイス上で現在アクティブな（使用中の）コールの数を表します。
CallsCompleted	このカウンタは、この MGCP PRI デバイスから発信され成功したコールの総数を表します。

カウンタ	カウンタの説明
Channel 1 Status ~ Channel 15 Status (連続した番号)	このカウンタは、MGCP PRI デバイスに関連付けられている、指定された B チャンネルの状態を表します。次の値が使用されます。0 (Unknown) は、チャンネルの状態を判別できなかったことを示します。1 (Out of service) は、このチャンネルが使用不可であることを示します。2 (Idle) は、このチャンネルにはアクティブなコールがなく、使用可能な状態であることを示します。3 (Busy) は、このチャンネルにアクティブコールが存在することを示します。4 (Reserved) は、このチャンネルが D チャンネルとして、または E-1 用の Synch チャンネルとして使用されるように予約されていることを示します。
Channel 16 Status	このカウンタは、MGCP PRI デバイスに関連付けられている、指定された B チャンネルの状態を表します。次の値が使用されます。0 : Unknown、1 : Out of service、2 : Idle、3 : Busy、4 : Reserved (E1 PRI インターフェイスの場合、このチャンネルは、D チャンネルとして使用するよう予約されています)。
Channel 17 Status ~ Channel 31 Status (連続した番号)	このカウンタは、MGCP PRI デバイスに関連付けられている、指定された B チャンネルの状態を表します。0 : Unknown、1 : Out of service、2 : Idle、3 : Busy、4 : Reserved
DatalinkInService	このカウンタは、対応するデジタルアクセス ゲートウェイ上のデータリンク (D チャンネル) の状態を表します。この値は、データリンクがアップ (イン サービス) の場合は 1 に設定され、データリンクがダウン (アウト オブ サービス) の場合は 0 に設定されます。
OutboundBusyAttempts	このカウンタは、使用可能な音声チャンネルがない場合に、MGCP PRI デバイスを介してコールが試行された回数の合計を表します。

## Cisco MGCP T1 CAS Device

Cisco MGCP T1 個別線信号方式 (CAS) Device オブジェクトは、登録済みの Cisco MGCP T1 CAS デバイスについての情報を提供します。次の表には、Cisco MGCP T1 CAS デバイス カウンタについての情報が含まれます。

表 63 : Cisco MGCP T1 CAS Device

カウンタ	カウンタの説明
CallsActive	このカウンタは、この MGCP T1 CAS デバイス上で現在アクティブな（使用中の）コールの数を表します。
CallsCompleted	このカウンタは、この MGCP T1 CAS デバイスから発信され成功したコールの総数を表します。
Channel 1 Status ~ Channel 24 Status (連続した番号)	このカウンタは、MGCP T1 CAS デバイスに関連付けられている、指定された B チャンネルの状態を表します。次の値が使用されます。0 (Unknown) は、チャンネルの状態を判別できなかったことを示します。1 (Outofservice) は、このチャンネルが使用不可であることを示します。2 (Idle) は、このチャンネルにはアクティブなコールがなく、使用可能な状態であることを示します。3 (Busy) は、このチャンネルにアクティブコールが存在することを示します。4 (Reserved) は、このチャンネルが D チャンネルとして、または E-1 用の Synch チャンネルとして使用されるように予約されていることを示します。
OutboundBusyAttempts	このカウンタは、使用可能な音声チャンネルがない場合に、MGCP T1 CAS デバイスを介してコールが試行された回数の合計を表します。

## Cisco Mobility Manager

Cisco Mobility Manager オブジェクトは、登録された Cisco Unified Mobility Manager デバイスに関する情報を提供します。次の表には、Cisco Unified Mobility Manager デバイス カウンタについての情報が含まれます。

表 64 : Cisco Mobility Manager

カウンタ	カウンタの説明
MobileCallsAnchored	このカウンタは、現在 Cisco Unified Communications Manager 上で固定されているシングルモード/デュアルモード電話機のコールに関連付けられているパスの総数を表します。コールの固定は、コールが企業ゲートウェイに入り、モビリティ アプリケーションに接続するときに実行されます。モビリティ アプリケーションは、この後、リダイレクションを使用してコールを企業ゲートウェイに返送します。たとえば、デュアルモード電話機間のコールの場合、このカウンタは 2 つ増加します。つまり、起点のコールで 1 つ増加し、終端のコールで 1 つ増加します。このカウンタは、コールが終了したときに減少します。
MobilityHandinsAborted	このカウンタは、中断された hand-in 操作の総数を表します。
MobileHandinsCompleted	このカウンタは、デュアルモード電話機で完了した hand-in 操作の総数を表します。hand-in 操作は、コールが企業ネットワーク内で正常に接続され、電話機が WAN から WLAN に移動したときに完了します。
MobilityHandinsFailed	このカウンタは、失敗した hand-in 操作（セルラー ネットワークから無線ネットワークに移動したモバイル デバイス上のコール）の総数を表します。
MobilityHandoutsAborted	このカウンタは、中断された hand-out 操作の総数を表します。
MobileHandoutsCompleted	このカウンタは、完了した hand-out 操作（企業 WLAN ネットワークからセルラー ネットワークに移動したモバイル デバイス上のコール）の総数を表します。hand-out 操作は、コールが正常に接続されたときに完了します。

カウンタ	カウンタの説明
MobileHandoutsFailed	このカウンタは、失敗した hand-out 操作（セルラーネットワークから無線ネットワークに移動したモバイルデバイス上のコール）の総数を表します。
MobilityFollowMeCallsAttempted	このカウンタは、試行された follow-me コールの総数を表します。
MobilityFollowMeCallsIgnoredDueToAnswerTooSoon	このカウンタは、AnswerTooSoon タイマーがオフになる前に無視された follow-me コールの総数を表します。
MobilityIVRCallsAttempted	このカウンタは、試行された IVR コールの総数を表します。
MobilityIVRCallsFailed	このカウンタは、失敗した IVR コールの総数を表します。
MobilityIVRCallsSucceeded	このカウンタは、成功した IVR コールの総数を表します。
MobilitySCCPDualModeRegistered	このカウンタは、登録されているデュアルモード SCCP デバイスの総数を表します。
MobilitySIPDualModeRegistered	このカウンタは、登録されているデュアルモード SIP デバイスの総数を表します。

## Cisco Music On Hold (MoH) Device

Cisco Music On Hold (MoH) Device オブジェクトは、登録済みの Cisco MOH デバイスについての情報を提供します。次の表には、Cisco MOH デバイス カウンタについての情報が含まれます。

表 65 : Cisco MOH Device

カウンタ	カウンタの説明
MOHHighestActiveResources	このカウンタは、MOH サーバに対して同時にアクティブになる MOH 接続の最大数を表します。この数には、マルチキャスト接続とユニキャスト接続の両方が含まれています。

カウンタ	カウンタの説明
MOHMulticastResourceActive	<p>このカウンタは、MOH サーバから提供されるマルチキャストアドレスへの、現在アクティブなマルチキャスト接続の数を表します。</p> <p>各MOH マルチキャストリソースは、オーディオソースとコーデックの組み合わせごとに1つのストリームを使用します。たとえば、マルチキャスト、G.711 mu-law、ワイドバンドコーデックに対してデフォルトオーディオソースを設定した場合、2つのストリーム（デフォルトオーディオソースと G.711 mu-law、およびデフォルトオーディオソースとワイドバンド）が使用されます。</p>
MOHMulticastResourceAvailable	<p>このカウンタは、MOH サーバから提供される、非アクティブで現在も MOHサーバで使用可能なマルチキャストアドレスへの、マルチキャスト MOH 接続の数を表します。</p> <p>各MOH マルチキャストリソースは、オーディオソースとコーデックの組み合わせごとに1つのストリームを使用します。たとえば、マルチキャスト、G.711 mu-law、ワイドバンドコーデックに対してデフォルトオーディオソースを設定した場合、2つのストリーム（デフォルトオーディオソースと G.711 mu-law、およびデフォルトオーディオソースとワイドバンド）が使用されます。</p>
MOHOutOfResources	<p>このカウンタは、Cisco Unified Communications Manager に登録されているすべての MOH サーバ上で使用可能なすべてのリソースがすでにアクティブであった場合に、Media Resource Manager が MOH リソースの割り当てを試行した回数の合計を表します。</p>
MOHTotalMulticastResources	<p>このカウンタは、MOH サーバから提供されるマルチキャストアドレスに対して許可されている、マルチキャスト MOH 接続の総数を表します。</p> <p>各MOH マルチキャストリソースは、オーディオソースとコーデックの組み合わせごとに1つのストリームを使用します。たとえば、マルチキャスト、G.711 mu-law、ワイドバンドコーデックに対してデフォルトオーディオソースを設定した場合、2つのストリーム（デフォルトオーディオソースと G.711 mu-law、およびデフォルトオーディオソースとワイドバンド）が使用されます。</p>



カウンタ	カウンタの説明
MOHTotalUnicastResources	このカウンタは、MOHサーバによって許可されているユニキャスト MOH 接続の総数を表します。 各 MOH ユニキャスト リソースは、1つのストリームを使用します。
MOHUnicastResourceActive	このカウンタは、MOHサーバへのアクティブなユニキャスト MOH 接続の数を表します。 各 MOH ユニキャスト リソースは、1つのストリームを使用します。
MOHUnicastResourceAvailable	このカウンタは、非アクティブで、MOHサーバで現在も使用可能なユニキャスト MOH 接続の数を表します。 各 MOH ユニキャスト リソースは、1つのストリームを使用します。

## Cisco MTP Device

Cisco Media Termination Point (MTP) Device オブジェクトは、登録済みの Cisco MTP デバイスについての情報を提供します。次の表には、Cisco MTP デバイス カウンタについての情報が含まれます。

表 66: Cisco MTP Device

カウンタ	カウンタの説明
OutOfResources	このカウンタは、MTP デバイスから MTP リソースの割り当てを試行して、すべてのリソースがすでに使用中であるなどの理由で失敗した回数の合計を表します。
ResourceActive	このカウンタは、MTP デバイスに対して現在使用中の（アクティブな）MTP リソースの数を表します。 各 MTP リソースは、2つのストリームを使用します。使用中の MTP は、コールで使用するために割り当てられている1つの MTP リソースを表します。
ResourceAvailable	このカウンタは、非アクティブで、MTP デバイスに対して現在も使用可能な MTP リソースの総数を表します。 各 MTP リソースは、2つのストリームを使用します。使用中の MTP は、コールで使用するために割り当てられている1つの MTP リソースを表します。

カウンタ	カウンタの説明
ResourceTotal	このカウンタは、MTP デバイスが提供する MTP リソースの総数を表します。このカウンタは、ResourceAvailable カウンタと ResourceActive カウンタを合計した数になります。

## Cisco Phones

Cisco Phones オブジェクトは、ハードウェアベースのデバイスとその他の端末デバイスの両方を含む、登録されている Cisco Unified IP Phone の数についての情報を提供します。

CallsAttempted カウンタは、この電話機から試行されたコールの数を表します。この数は、電話機がオフフックおよびオンフックになるたびに増加します。

## Cisco Presence の機能

Cisco Presence オブジェクトは、短縮ダイヤルやコールリストのビジーランプフィールド (BLF) の登録に関連する統計など、プレゼンス登録についての情報を提供します。次の表には、Cisco Presence 機能についての情報が含まれます。

表 67 : Cisco Presence

カウンタ	カウンタの説明
ActiveCallListAndTrunkSubscriptions	このカウンタは、コール リスト機能のアクティブなプレゼンス登録と SIP トランクを介したプレゼンス登録を表します。
ActiveSubscriptions	このカウンタは、すべてのアクティブな着信と発信のプレゼンス登録を表します。
CallListAndTrunkSubscriptionsThrottled	このカウンタは、コール リスト機能の制御のために拒否されたコール リストのプレゼンス登録とトランク側のプレゼンス登録の累計数を表します。
IncomingLineSideSubscriptions	このカウンタは、回線側で受信されたプレゼンス登録の累計数を表します。
IncomingTrunkSideSubscriptions	このカウンタは、トランク側で受信されたプレゼンス登録の累計数を表します。
OutgoingTrunkSideSubscriptions	このカウンタは、トランク側で送信されたプレゼンス登録の累計数を表します。

## Cisco QSIG Feature

Cisco QSIG Feature オブジェクトは、コール転送やパス置換など、さまざまな QSIG 機能の操作についての情報を提供します。次の表に、Cisco QSIG Feature カウンタに関する情報を示します。

表 68 : Cisco QSIG Feature

カウンタ	カウンタの説明
CallForwardByRerouteCompleted	このカウンタは、再ルーティングにより自動転送され成功したコールの数を表します。再ルーティングによる自動転送は、自動転送されるコールのパスを、発信元の観点から最適化します（使用中の B チャンネルの数を最少化します）。このカウンタは、Cisco CallManager の Call Forward by Reroute Enabled サービスパラメータが有効または無効にされたとき、または Cisco CallManager サービスが再起動されたときにリセットされます。
PathReplacementCompleted	このカウンタは、正常に実行されたパス置換の数を表します。QSIG ネットワークにおけるパス置換は、コールに含まれる 2 つのエッジ PINX (PBX) 間のパスを最適化します。このカウンタは、Cisco CallManager の Path Replacement Enabled サービスパラメータが有効または無効にされたとき、または Cisco CallManager サービスが再起動されたときにリセットされます。

## Cisco Signaling Performance

Cisco Signaling Performance オブジェクトは、Cisco Unified Communications Manager の転送通信に関するコールシグナリング データを提供します。次の表に、Cisco Signaling Performance カウンタに関する情報を示します。

表 69 : Cisco Signaling Performance

カウンタ	カウンタの説明
UDPPacketsThrottled	このカウンタは、1 つの IP アドレスから許可されている毎秒あたりの着信パケット数のしきい値を超過したことによって制御（ドロップ）された着信 UDP パケットの総数を表します。しきい値は、Cisco Unified Communications Manager Administration の SIP Station UDP Port Throttle Threshold と SIP Trunk UDP Port Throttle Threshold の各サービスパラメータで設定します。このカウンタは、Cisco CallManager Service の最後の再起動以降、制御された UDP パケットを受信するたびに増加します。

## Cisco SIP

Cisco Session Initiation Protocol (SIP) オブジェクトは、設定済みの SIP デバイスについての情報を提供します。次の表には、Cisco SIP のカウンタについての情報が含まれます。

表 70 : Cisco SIP

カウンタ	カウンタの説明
CallsActive	このカウンタは、この SIP デバイス上で現在アクティブな（使用中の）コールの数を表します。
CallsAttempted	このカウンタは、この SIP デバイス上で試行されたコールの数を表します。成功したコールの試行と失敗したコールの試行の両方が含まれます。
CallsCompleted	このカウンタは、SIP デバイスから実際に接続された（音声パスが確立された）コールの数を表します。この数は、コールが終了したときに増加します。
CallsInProgress	このカウンタは、SIP デバイス上で現在進行中の、すべてのアクティブ コールを含むコールの数を表します。進行中のすべてのコールが接続されたときに、CallsInProgress の数は CallsActive の数と等しくなります。
VideoCallsActive	このカウンタは、この SIP デバイス上で現在アクティブな（使用中の）ストリーミング ビデオ接続を持つビデオ コールを表します。
VideoCallsCompleted	このカウンタは、この SIP デバイスのビデオ ストリームに実際に接続されたビデオコールの数を表します。この数は、コールが終了したときに増加します。

## Cisco SIP Line Normalization

Cisco SIP line normalization パフォーマンス オブジェクトには、初期化エラー、実行時エラー、スクリプト ステータスなどの SIP 回線正規化スクリプトの側面をモニタできるようにするカウンタが含まれています。SIP 回線では、パフォーマンス カウンタは各スクリプトに 1 セットのみ含まれます。これは、2つのエンドポイントが同じスクリプトを共有する場合も同様です。次の表に、Cisco SIP line normalization カウンタに関する情報を示します。

表示名	説明
DeviceResetAutomatically	<p>このカウンタは、Cisco Unified Communications Manager がデバイス（SIP 電話）を自動的にリセットした回数を表します。[スクリプト実行エラーの復旧処理（Script Execution Error Recovery Action）] フィールドまたは [システムリソースエラーの復旧処理（System Resource Error Recovery Action）] フィールドで指定された値が [デバイスのリセット（Reset Device）] に設定されている場合にのみ自動リセットが行われます。このカウンタは、エラーが原因で Unified Communications Manager がデバイス（SIP 電話）を自動的にリセットするたびに増加します。スクリプト設定を変更した後にスクリプトがリセットされると、このカウンタは再開されます。</p>
ErrorExecution	<p>このカウンタは、スクリプトの実行中に発生した実行エラーの数を表します。実行エラーは、メッセージハンドラの実行中に発生することがあります。実行エラーの原因として考えられるのは、リソースエラーや関数呼び出し内での引数の不一致などの問題です。</p> <p>実行エラーが発生すると、Unified Communications Manager は次の処理を実行します。</p> <ul style="list-style-type: none"> <li>• 自動的にメッセージを元の内容に復元してから、追加のエラー処理アクションを適用します。</li> <li>• カウンタの値を増分します。</li> <li>• Cisco Unified Communications Manager の管理ページにある [スクリプト実行エラーの復旧処理（Script Execution Error Recovery Action）] フィールドと [システムリソースエラーの復旧処理（System Resource Error Recovery Action）] フィールドの値に基づいて、適切な処理を実行します。</li> </ul> <p>スクリプト内の失敗した行の番号などの詳細については、SIPNormalizationScriptError アラームを確認してください。スクリプトの問題を修正し、必要に応じて修正したスクリプトをアップロードし、スクリプトの設定ページの上にある [リセット（Reset）] ボタンをクリックしてスクリプトをリセットします。カウンタは、スクリプト設定の変更後、スクリプトが最後にリセットされて以降の実行エラーごとに増加します。カウンタを再起動するには、スクリプトの設定変更とスクリプトのリセットの両方を実行する必要があります。</p> <p>スクリプトの問題を修正した後もカウンタが増加し続ける場合は、スクリプトを調べ直してください。</p>

表示名	説明
ErrorInit	<p>このカウンタは、スクリプトがメモリに正常にロードされたものの、<b>Unified Communications Manager</b> での初期化に失敗した後に発生したスクリプト エラーの数を表します。スクリプトが初期化に失敗する原因として考えられるのは、リソースエラー、関数呼び出し内での引数の不一致などです。</p> <p>スクリプト内の失敗した行の番号などの詳細については、<b>SIPNormalizationScriptError</b> アラームを確認してください。スクリプトの問題を修正し、必要に応じて修正したスクリプトをアップロードし、スクリプトの設定ページの上部にある [リセット (Reset) ] ボタンをクリックしてスクリプトをリセットします。スクリプトのインスタンスのカウンタは、初期化エラーが発生するたびに増加します。このカウンタは、スクリプトの設定変更とともに行われた最新のスクリプト リセットからのカウントを提供します。カウンタを再起動するには、スクリプトの設定変更とスクリプトのリセットの両方を実行する必要があります。スクリプトの問題を修正した後もカウンタが増加し続ける場合は、スクリプトを調べ直してください。初期化中にエラーが発生した場合、<b>Unified Communications Manager</b> は自動的にスクリプトを無効にします。</p>
ErrorInternal	<p>このカウンタは、スクリプトの実行中に発生した内部エラーの数を表します。内部エラーが発生することはほとんどありません。このカウンタの値がゼロより大きい場合は、スクリプトの内容または実行に関係のない不具合がシステム内に存在します。<b>SDI</b> トレースを収集し、テクニカルアシスタンスセンター (TAC) に問い合わせてください。</p>
ErrorLoad	<p>このカウンタは、スクリプトが <b>Unified Communications Manager</b> のメモリにロードされたときに発生したスクリプト エラーの数を表します。</p> <p>スクリプトはメモリの問題または構文エラーが原因でロードに失敗する可能性があります。構文エラーがある場合は、スクリプトライン番号などの詳細について <b>SIPNormalizationScriptError</b> アラームを確認し、構文エラーについてスクリプトを確認し、必要に応じて修正したスクリプトをアップロードして、スクリプトの設定ページの上部にある [リセット (Reset) ] ボタンをクリックしてスクリプトをリセットします。</p> <p>スクリプトのインスタンスのカウンタは、スクリプト設定の変更後、スクリプトが最後にリセットされて以降のロードエラーごとに増加します。カウンタを再起動するには、スクリプトの設定変更とスクリプトのリセットの両方を実行する必要があります。スクリプトの問題を修正した後もカウンタが増加し続ける場合は、スクリプトを調べ直してください。</p>

表示名	説明
ErrorResource	<p>このカウンタは、スクリプトでリソース エラーが発生したかどうかを示します。</p> <p>リソース エラーは2種類あります。1つは[メモリしきい値 (Memory Threshold) ]フィールドの値を超えることで、もう1つは[Lua 命令しきい値 (Lua Instruction Threshold) ]フィールドの値を超えることです。どちらのフィールドも、Cisco Unified Communications Manager の管理ページにある[SIP 正規化スクリプト設定 (SIP Normalization Script Configuration) ]ウィンドウに表示されます。いずれかの状況が発生した場合、Unified Communications Manager はすぐにスクリプトを閉じて SIPNormalizationScriptError アラームを発行します。</p> <p>スクリプトのロード中または初期化中にリソース エラーが発生した場合は、スクリプトが無効になります。実行中にリソース エラーが発生した場合は、Cisco Unified Communications Manager の管理ページにある[SIP 正規化スクリプト設定 (SIP Normalization Script Configuration) ]ウィンドウの[システム リソース エラーの復旧処理 (System Resource Error Recovery Action) ]フィールドで設定した設定済みシステム リソース エラー復旧処理が実行されます。</p>
MemoryUsage	<p>このカウンタは、このスクリプトを使用するすべての SIP 電話への蓄積に基づいてこのスクリプトが消費するメモリ量をバイト単位で示します。このカウンタは、スクリプトが使用するメモリの量に合わせて増減します。このカウンタは、スクリプトを閉じるとクリアされ (閉じたスクリプトはメモリを使用しないため)、スクリプトを開くと (有効になると) 再開されます。このカウンタの数値が高い場合は、リソースの問題が発生していることを示します。</p> <p>MemoryUsagePercentage カウンタと SIPNormalizationResourceWarning アラームを確認してください。このアラームは、リソースの使用量が内部的に設定されたしきい値を超えた場合に発生します。</p>
MemoryUsagePercentage	<p>このカウンタは、このスクリプトを使用するすべての SIP 電話への蓄積に基づいてこのスクリプトが消費するメモリの総量のパーセントを示します。</p> <p>このカウンタの値は、MemoryUsage カウンタの値を[メモリしきい値 (Memory Threshold) ]フィールド ([SIP 正規化スクリプト設定 (SIP Normalization Script Configuration) ]ウィンドウ内) の値で割り、その結果に 100 を掛けてパーセント値にすることで求められます。</p> <p>このカウンタは、MemoryUsage カウンタに合わせて増減します。このカウンタは、スクリプトを閉じるとクリアされ (閉じたスクリプトはメモリを使用しないため)、スクリプトを開くと (有効になると) 再開されます。このカウンタが内部的に制御されたリソースのしきい値に達すると、SIPNormalizationResourceWarning アラームが発行されます。</p>

表示名	説明
MessageRollback	<p>このカウンタは、スクリプト実行中のエラーのためにメッセージがスクリプトによって変更されなかった回数を表します。これは、[スクリプト実行エラーの復旧処理 (Script Execution Error Recovery Action)] フィールドの値が[メッセージのロールバックのみ (Message Rollback Only)] に設定されている場合にのみ発生します。</p> <p>実行エラーが発生すると、Unified Communications Manager は自動的にメッセージを元のコンテンツに復元してから、追加のエラー処理アクションを適用します。エラー処理にロールバックしか指定されていない場合、正規化の試行の前に実行されるアクションは元のメッセージへのロールバックだけです。その他の設定可能な[スクリプト実行エラーの復旧処理 (Script Execution Error Recovery Action)] 設定に対しては、メッセージが元のコンテンツにリストアされてから指定されたアクションが発生します。</p>
msgAddContentBody	<p>このカウンタは、スクリプトがメッセージにコンテンツ本文を追加した回数を表します。スクリプト内で <code>msg:addContentBody</code> API を使用している場合 (「msg」は使用しているメッセージの変数名とする)、このAPIが正常に実行されるたびにこのカウンタが増加します。カウンタが予想どおりに動作しない場合は、スクリプトロジックにエラーがないか調べてください。</p>
msgAddHeader	<p>このカウンタは、スクリプトがメッセージに SIP ヘッダーを追加した回数を表します。スクリプト内で <code>msg:addHeader</code> API を使用している場合 (「msg」は使用しているメッセージの変数名とする)、このAPIが正常に実行されるたびにこのカウンタが増加します。カウンタが予想どおりに動作しない場合は、スクリプトロジックにエラーがないか調べてください。</p>
msgAddHeaderUriParameter	<p>このカウンタは、スクリプトがメッセージの SIP ヘッダーに SIP ヘッダー URI パラメータを追加した回数を表します。スクリプト内で <code>msg:addHeaderUriParameter</code> API を使用している場合 (「msg」は使用しているメッセージの変数名とする)、このAPIが正常に実行されるたびにこのカウンタが増加します。カウンタが予想どおりに動作しない場合は、スクリプトロジックにエラーがないか調べてください。</p>
msgAddHeaderValueParameter	<p>このカウンタは、スクリプトがメッセージの SIP ヘッダーに SIP ヘッダー値パラメータを追加した回数を表します。スクリプト内で <code>msg:addHeaderValueParameter</code> API を使用している場合 (「msg」は使用しているメッセージの変数名とする)、このAPIが正常に実行されるたびにこのカウンタが増加します。カウンタが予想どおりに動作しない場合は、スクリプトロジックにエラーがないか調べてください。</p>



表示名	説明
msgApplyNumberMask	このカウンタは、スクリプトがメッセージの SIP ヘッダーに番号マスクを適用した回数を表します。スクリプト内で <code>msg:applyNumberMask</code> API を使用している場合（「msg」は使用しているメッセージの変数名とする）、この API が正常に実行されるたびにこのカウンタが増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
msgBlock	このカウンタは、スクリプトがメッセージをブロックした回数を表します。スクリプト内で <code>msg:block</code> API を使用している場合（「msg」は使用しているメッセージの変数名とする）、この API が正常に実行されるたびにこのカウンタが増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
msgConvertDiversioontoHI	このカウンタは、スクリプトがメッセージの Diversion ヘッダーを History-Info ヘッダーに変換した回数を表します。スクリプト内で <code>msg:convertDiversionToHI</code> API を使用している場合（「msg」は使用しているメッセージの変数名とする）、この API が正常に実行されるたびにこのカウンタが増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
msgConvertHItoDiverion	このカウンタは、スクリプトがメッセージの History-Info ヘッダーを Diversion ヘッダーに変換した回数を表します。スクリプト内で <code>msg:convertHItoDiversion</code> API を使用している場合（「msg」は使用しているメッセージの変数名とする）、この API が正常に実行されるたびにこのカウンタが増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
msgModifyHeader	このカウンタは、スクリプトがメッセージの SIP ヘッダーを変更した回数を表します。スクリプト内で <code>msg:modifyHeader</code> API を使用している場合（「msg」は使用しているメッセージの変数名とする）、この API が正常に実行されるたびにこのカウンタが増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
msgRemoveContentBody	このカウンタは、スクリプトがメッセージからコンテンツ本文を削除した回数を表します。スクリプト内で <code>msg:removeContentBody</code> API を使用している場合（「msg」は使用しているメッセージの変数名とする）、この API が正常に実行されるたびにこのカウンタが増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。

表示名	説明
msgRemoveHeader	このカウンタは、スクリプトがメッセージから SIP ヘッダーを削除した回数を表します。スクリプト内で <code>msg:removeHeader</code> API を使用している場合（「msg」は使用しているメッセージの変数名とする）、この API が正常に実行されるたびにこのカウンタが増加します。カウンタが予想どおりに動作しない場合は、スクリプトロジックにエラーがないか調べてください。
msgRemoveHeaderValue	このカウンタは、スクリプトがメッセージから SIP ヘッダー値を削除した回数を表します。スクリプト内で <code>msg:removeHeaderValue</code> API を使用している場合（「msg」は使用しているメッセージの変数名とする）、この API が正常に実行されるたびにこのカウンタが増加します。カウンタが予想どおりに動作しない場合は、スクリプトロジックにエラーがないか調べてください。
msgRemoveUnreliableSdp	このカウンタは、スクリプトが信頼できない 18x SIP メッセージから SDP 本文を削除した回数を表します。スクリプト内で <code>msg:removeUnreliableSDP</code> API を使用している場合（「msg」は使用しているメッセージの変数名とする）、この API が正常に実行されるたびにこのカウンタが増加します。カウンタが予想どおりに動作しない場合は、スクリプトロジックにエラーがないか調べてください。
msgSetRequestUri	このカウンタは、スクリプトがメッセージの要求 URI を変更した回数を表します。スクリプト内で <code>msg:setRequestUri</code> API を使用している場合（「msg」は使用しているメッセージの変数名とする）、この API が正常に実行されるたびにこのカウンタが増加します。カウンタが予想どおりに動作しない場合は、スクリプトロジックにエラーがないか調べてください。
msgSetResponseCode	このカウンタは、スクリプトがメッセージの応答コードまたは応答フレーズを変更した回数を表します。スクリプト内で <code>msg:setResponseCode</code> API を使用している場合（「msg」は使用しているメッセージの変数名とする）、この API が正常に実行されるたびにこのカウンタが増加します。カウンタが予想どおりに動作しない場合は、スクリプトロジックにエラーがないか調べてください。
msgSetSdp	このカウンタは、スクリプトがメッセージの SDP をセットした回数を表します。スクリプト内で <code>msg:setSdp</code> API を使用している場合（「msg」は使用しているメッセージの変数名とする）、この API が正常に実行されるたびにこのカウンタが増加します。カウンタが予想どおりに動作しない場合は、スクリプトロジックにエラーがないか調べてください。

表示名	説明
ptAddContentBody	このカウンタは、スクリプトが PassThrough オブジェクトにコンテンツ本文を追加した回数を表します。スクリプト内で pt:addContentBody API を使用している場合（「pt」は使用している PassThrough オブジェクトの名前とする）、この API が正常に実行されるたびにこのカウンタが増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
ptAddHeader	このカウンタは、スクリプトが PassThrough オブジェクトに SIP ヘッダーを追加した回数を表します。スクリプト内で pt:addHeader API を使用している場合（「pt」は使用している PassThrough オブジェクトの名前とする）、この API が正常に実行されるたびにこのカウンタが増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
ptAddHeaderUriParameter	このカウンタは、スクリプトが PassThrough オブジェクトに SIP ヘッダー URI パラメータを追加した回数を表します。スクリプト内で pt:addHeaderUriParameter API を使用している場合（「pt」は使用している PassThrough オブジェクトの名前とする）、この API が正常に実行されるたびにこのカウンタが増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
ptAddHeaderValueParameter	このカウンタは、スクリプトが PassThrough オブジェクトに SIP ヘッダー値パラメータを追加した回数を表します。スクリプト内で pt:addHeaderValueParameter API を使用している場合（「pt」は使用している PassThrough オブジェクトの名前とする）、この API が正常に実行されるたびにこのカウンタが増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
ptAddRequestUriParameter	このカウンタは、スクリプトが PassThrough オブジェクトに要求 URI パラメータを追加した回数を表します。スクリプト内で pt:addRequestUriParameter API を使用している場合（「pt」は使用している PassThrough オブジェクトの名前とする）、この API が正常に実行されるたびにこのカウンタが増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。

表示名	説明
ScriptActive	<p>このカウンタは、スクリプトが現在アクティブになっている（SIP 電話で実行されている）かどうかを示します。値0は、スクリプトが閉じている（無効である）ことを示します。値1は、スクリプトが起動し、動作可能であることを示します。</p> <p>実行する必要があるスクリプトを開くには、スクリプトが開かれていない理由を示している可能性があるアラームを確認し、エラーがある場合は修正し、必要に応じて新しいスクリプトをアップロードし、スクリプトをリセットします。</p>
ScriptClosed	<p>このカウンタは、Unified Communications Manager がスクリプトを閉じた回数を表します。スクリプトは、1台の SIP 電話で閉じられていても、他の SIP 電話では有効な場合があります。最後にこのスクリプトを使用した SIP 電話が手動でリセットされたか、（エラーにより）自動的にリセットしたか、または削除された場合は、Unified Communications Manager はこのスクリプトを閉じます。このカウントは、スクリプト設定が変更された後にそのスクリプトがリセットし、Cisco CallManager が再起動したときに再起動します。</p>

表示名	説明
ScriptDisabledAutomatically	<p>このカウンタは、システムが自動的にスクリプトを無効にした回数を表示します。スクリプトが無効にされたかどうかは、Cisco Unified Communications Manager の管理ページにある [SIP 正規化スクリプト設定 (SIP Normalization Script Configuration) ] ウィンドウの [スクリプト実行エラーの復旧処理 (Script Execution Error Recovery Action) ] フィールドと [システムリソースエラーの復旧処理 (System Resource Error Recovery Action) ] フィールドに指定した値によって決定されます。これらのフィールドのいずれかが [スクリプトの無効化 (Disable Script) ] にセットされている場合、自動スクリプト無効化が発生します。スクリプトは、ロード中および初期化中にスクリプト エラー条件が発生した場合にも無効になります。</p> <p>このカウンタは、スクリプトの設定変更に伴うデバイスの最新の手動リセットからのカウントを提供します (デバイスのリセットだけではカウントはリセットされません。リセットが発生する前に、スクリプトが変更されている必要があります)。このカウンタは、Unified Communications Manager がスクリプトエラーにより自動的にスクリプトを無効にするたびに増加します。</p> <p>このカウンタの数値が予想よりも高い場合は、次の手順を実行してください。</p> <ul style="list-style-type: none"> <li>• SIPNormalizationScriptError アラームと SIPNormalizationAutoResetDisabled アラームを調べます。</li> <li>• RTMT のリソース関連のアラームとカウンタを調べて、リソースの問題が発生しているかどうかを判断します。</li> <li>• SDI トレース ファイルに予期しない SIP 正規化イベントがあるかどうかを調べます。</li> </ul>

表示名	説明
ScriptOpened	<p>このカウンタは、Unified Communications Manager がスクリプトを開こうとした回数を表します。スクリプトを開くには、Unified Communications Manager のメモリにスクリプトをロードし、初期化して、実行可能な状態にする必要があります。このカウンタの値が1より大きくなっている場合は、予期しない理由あるいはロード中または初期化中のエラーにより、Unified Communications Manager がこのスクリプトを2回以上開こうとしたことを意味します。このエラーは、実行エラー、リソースエラー、あるいはスクリプト内の無効な構文により発生する場合があります。ScriptResetAutomatically カウンタが増加する場合は、このカウンタが1より大きいことが予測されます。</p> <p>このカウンタの数値が予想よりも高い場合は、次の手順を実行してください。</p> <ul style="list-style-type: none"> <li>• SIPNormalizationScriptClosed、SIPNormalizationScriptError、SIPNormalizationResourceWarning などのアラームを調べます。</li> <li>• RTMT のリソース関連のアラームとカウンタを調べて、リソースの問題が発生しているかどうかを判断します。</li> <li>• SDI トレース ファイルに予期しない SIP 正規化イベントがあるかどうかを調べます。</li> </ul> <p>このカウントは、スクリプトの設定が変更された後にスクリプトがリセットされたとき、および Unified Communications Manager が再起動したときに再開されます。</p>

表示名	説明
ScriptResetAutomatically	<p>このカウンタは、システムが自動的にスクリプトをリセットした回数を表示します。スクリプトのリセットは、Cisco Unified Communications Manager の管理ページにある [SIP 正規化スクリプト設定 (SIP Normalization Script Configuration) ] ウィンドウの [スクリプト実行エラーの復旧処理 (Script Execution Error Recovery Action) ] フィールドと [システム リソース エラーの復旧処理 (System Resource Error Recovery Action) ] フィールドに指定した値に基づいて行われます。自動リセットは、これらのフィールドのいずれかの値が [スクリプトのリセット (Reset Script) ] の場合に発生する可能性があります。</p> <p>このカウンタは、スクリプト設定の変更後にスクリプトが最後にリセットされた後でそのスクリプトが自動的にリセットされる回数を指定します。このカウンタは、Unified Communications Manager がスクリプトエラーにより自動的にスクリプトをリセットにするたびに増加します。</p> <p>このカウンタの数値が予想よりも高い場合は、次の手順を実行してください。</p> <ul style="list-style-type: none"> <li>• SIPNormalizationScriptError アラームを調べます。</li> <li>• RTMT のリソース関連のアラームとカウンタを調べて、リソースの問題が発生しているかどうかを判断します。</li> <li>• SDI トレース ファイルに予期しない SIP 正規化イベントがあるかどうかを調べます。</li> </ul>
ScriptResetManually	<p>このカウンタは、Cisco Unified Communications Manager の管理ページまたはその他の方法 (AXL、またはスクリプトを使用した最後の SIP 電話でのリセットなど) によりスクリプトが手動でリセットされた回数を表示します。このカウンタは、スクリプトが設定変更によりリセットされると増加します。このカウンタは、スクリプトが削除されたとき、または Cisco CallManager が再起動したときにリセットされます。</p>

## Cisco SIP Normalization

Cisco SIP Normalization パフォーマンス オブジェクトには、初期化エラー、実行時エラー、スクリプト ステータスなどの正規化スクリプトの側面をモニタできるようにするカウンタが含まれています。これらのカウンタのインスタンスは、スクリプトに関連付けられている各デバイスによって新規に作成されます。次の表に、Cisco SIP Normalization カウンタに関する情報を示します。

表 71 : Cisco SIP Normalization

[表示名 (Display Name) ]	説明
DeviceResetAutomatically	<p>このカウンタは、Cisco Unified Communications Manager がデバイス (SIP トランク) を自動的にリセットした回数を表します。デバイスのリセットは、Cisco Unified Communications Manager の管理の [SIP 正規化スクリプト設定 (SIP Normalization Script Configuration) ] ウィンドウの [スクリプト実行エラーの復旧処理 (Script Execution Error Recovery Action) ] フィールドと [システム リソース エラーの復旧処理 (System Resource Error Recovery Action) ] フィールドに指定した値に基づいて行われます。スクリプトエラーが原因でデバイス (SIP トランク) がリセットされると、カウンタの値が増加します。このカウントは、デバイスを手動でリセットするとリセットされます。</p>
DeviceResetManually	<p>このカウンタは、Cisco Unified Communications Manager の管理でデバイス (SIP トランク) が手動でリセットされた回数、または AXL などのその他の方法でリセットされた回数を表します。設定変更が原因でスクリプトに関連付けられたデバイスがリセットされると、カウンタの値が増加します。</p> <p>カウンタは、次の場合に再起動されます。</p> <ul style="list-style-type: none"> <li>• SIP トランクが削除された場合。</li> <li>• トランクのスクリプトが変更または削除された場合。</li> <li>• Cisco Unified Communications Manager が再起動した場合。</li> </ul>



[表示名 (Display Name) ]	説明
ErrorExecution	<p>このカウンタは、スクリプトの実行中に発生した実行エラーの数を表します。実行エラーは、メッセージハンドラの実行中に発生することがあります。実行エラーの原因として考えられるのは、リソースエラーや関数呼び出し内での引数の不一致などです。</p> <p>実行エラーが発生すると、Unified Communications Manager は次の処理を実行します。</p> <ul style="list-style-type: none"> <li>• 自動的にメッセージを元の内容に復元してから、追加のエラー処理アクションを適用します。</li> <li>• カウンタの値を増分します。</li> <li>• Cisco Unified Communications Manager の管理ページにある [スクリプト実行エラーの復旧処理 (Script Execution Error Recovery Action) ] フィールドと [システムリソースエラーの復旧処理 (System Resource Error Recovery Action) ] フィールドの値に基づいて、適切な処理を実行します。</li> </ul> <p>スクリプト内の失敗した行の番号などの詳細については、SIPNormalizationScriptError アラームを確認してください。スクリプトの問題を修正し、必要に応じて修正したスクリプトをアップロードして、トランクをリセットします。このカウンタは、実行エラーが発生するたびに増加します。このカウンタは、スクリプトの設定変更に伴う最新のトランク リセットからのカウントを提供します (デバイスのリセットだけではカウントはリセットされません。リセットが発生する前に、スクリプトの設定も変更されている必要があります) 。</p> <p>スクリプトの問題を修正した後もカウンタが増加し続ける場合は、スクリプトを調べ直してください。</p>

[表示名 (Display Name) ]	説明
ErrorInit	<p>このカウンタは、スクリプトがメモリに正常にロードされたものの、Unified Communications Manager での初期化に失敗した後に発生したスクリプト エラーの数を表します。スクリプトが初期化に失敗する原因として考えられるのは、リソースエラー、関数呼び出し内での引数の不一致、必要なテーブルが返されなかったことなどです。</p> <p>スクリプト内の失敗した行の番号などの詳細については、SIPNormalizationScriptError アラームを確認してください。スクリプトの問題を修正し、必要に応じて修正したスクリプトをアップロードして、トランクをリセットします。このカウンタは、初期化エラーが発生するたびに増加します。このカウンタは、スクリプトの設定変更に伴う最新のトランク リセットからのカウントを提供します (デバイスのリセットだけではカウントはリセットされません。リセットが発生する前に、スクリプトの設定も変更されている必要があります)。スクリプトの問題を修正した後もカウンタが増加し続ける場合は、スクリプトを調べ直してください。初期化中にエラーが発生した場合、Unified Communications Manager は自動的にスクリプトを無効にします。</p>
ErrorInternal	<p>このカウンタは、スクリプトの実行中に発生した内部エラーの数を表します。内部エラーが発生することはほとんどありません。このカウンタの値がゼロより大きい場合は、スクリプトの内容または実行に関係のない不具合がシステム内に存在します。SDI トレースを収集し、テクニカルアシスタンスセンター (TAC) に問い合わせてください。</p>
ErrorLoad	<p>このカウンタは、スクリプトが Cisco Unified Communications Manager のメモリにロードされたときに発生したスクリプト エラーの数を表します。スクリプトがロードに失敗する原因として考えられるのは、メモリの問題または構文エラーです。</p> <p>詳細については、SIPNormalizationScriptError アラームを確認してください。スクリプトに構文エラーがないか確認し、必要に応じて修正したスクリプトをアップロードして、トランクをリセットします。このカウンタは、ロードエラーが発生するたびに増加します。このカウンタは、スクリプトの設定変更に伴う最新のトランク リセットからのカウントを提供します (デバイスのリセットだけではカウントはリセットされません。リセットが発生する前に、スクリプトの設定も変更されている必要があります)。スクリプトの問題を修正した後もカウンタが増加し続ける場合は、スクリプトを調べ直してください。</p>

[表示名 (Display Name) ]	説明
ErrorResource	<p>このカウンタは、スクリプトでリソース エラーが発生したかどうかを示します。</p> <p>リソース エラーは 2 種類あります。1 つは [メモリしきい値 (Memory Threshold) ] フィールドの値を超えることで、もう 1 つは [Lua 命令しきい値 (Lua Instruction Threshold) ] フィールドの値を超えることです (どちらのフィールドも、Cisco Unified Communications Manager の管理ページにある [SIP 正規化スクリプト設定 (SIP Normalization Script Configuration) ] ウィンドウに表示されます)。いずれかの状況が発生した場合、Cisco Unified Communications Manager はすぐにスクリプトを閉じて SIPNormalizationScriptError アラームを発行します。</p> <p>スクリプトのロード中または初期化中にリソース エラーが発生した場合は、スクリプトが無効になります。実行中にリソースエラーが発生した場合は、設定されたシステムリソースエラーの復旧処理が実行されます (この処理は、Cisco Unified Communications Manager の管理の [SIP 正規化スクリプト設定 (SIP Normalization Script Configuration) ] ウィンドウの [システムリソースエラーの復旧処理 (System Resource Error Recovery Action) ] フィールドの設定によって定義されます)。</p>
MemoryUsage	<p>このカウンタは、スクリプトが使用するメモリの量をバイト単位で示します。このカウンタは、スクリプトが使用するメモリの量に合わせて増減します。このカウントは、スクリプトが閉じるとクリアされ (閉じたスクリプトはメモリを使用しないため)、スクリプトが開くと (有効になると) 再開されます。このカウンタの数値が高い場合は、リソースの問題が発生していることを示します。MemoryUsagePercentage カウンタと SIPNormalizationResourceWarning アラームを確認してください。SIPNormalizationResourceWarning アラームは、リソースの使用量が内部的に設定されたしきい値を超えた場合に発生します。</p>

[表示名 (Display Name) ]	説明
MemoryUsagePercentage	<p>このカウンタは、スクリプトが使用するメモリの総量のパーセント値を示します。</p> <p>このカウンタの値は、MemoryUsage カウンタの値を ([SIP 正規化スクリプト設定 (SIP Normalization Script Configuration) ] ウィンドウの) [メモリしきい値 (Memory Threshold) ] フィールドの値で割り、その結果に 100 を掛けてパーセント値にすることで求められます。</p> <p>このカウンタは、MemoryUsage カウンタに合わせて増減します。このカウンタは、スクリプトが閉じるとクリアされ (閉じたスクリプトはメモリを使用しないため)、スクリプトが開くと (有効になると) 再開されます。このカウンタが内部的に制御されたリソースのしきい値に達すると、SIPNormalizationResourceWarning アラームが発行されます。</p>
MessageRollback	<p>このカウンタは、システムが自動的にメッセージをロールバックした回数を表示します。Cisco Cisco Unified Communications Manager の管理ページにある [SIP 正規化スクリプト設定 (SIP Normalization Script Configuration) ] ウィンドウの [スクリプト実行エラーの復旧処理 (Script Execution Error Recovery Action) ] フィールドで指定されているエラー処理の使用により、メッセージがロールバックされます。</p> <p>実行エラーが発生すると、Unified Communications Manager は自動的にメッセージを元の内容に復元してから、追加のエラー処理アクションを適用します。エラー処理にロールバックしか指定されていない場合、正規化の試行の前に実行されるアクションは元のメッセージへのロールバックだけです。その他の [スクリプト実行エラーの復旧処理 (Script Execution Error Recovery Action) ] が指定されている場合は、メッセージのロールバックが必ず最初に実行され、その後、スクリプトの無効化、スクリプトの自動リセット、トランクの自動リセットなどの指定された処理が実行されます。</p>
msgAddContentBody	<p>このカウンタは、スクリプトがメッセージにコンテンツ本文を追加した回数を表示します。スクリプトで msg:addContentBody API を使用している場合、このカウンタは msg:addContentBody API が正常に実行されるたびに増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。</p>

[表示名 (Display Name) ]	説明
msgAddHeader	このカウンタは、スクリプトがメッセージに SIP ヘッダーを追加した回数を表します。スクリプトで msg:addHeader API を使用している場合、このカウンタは msg:addHeader API が正常に実行されるたびに増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
msgAddHeaderUriParameter	このカウンタは、スクリプトがメッセージの SIP ヘッダーに SIP ヘッダー URI パラメータを追加した回数を表します。スクリプトで msg:addHeaderUriParameter API を使用している場合、このカウンタは msg:addHeaderUriParameter API が正常に実行されるたびに増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
msgAddHeaderValueParameter	このカウンタは、スクリプトがメッセージの SIP ヘッダーに SIP ヘッダー値パラメータを追加した回数を表します。スクリプトで msg:addHeaderValueParameter API を使用している場合、このカウンタは msg:addHeaderValueParameter API が正常に実行されるたびに増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
msgApplyNumberMask	このカウンタは、スクリプトがメッセージの SIP ヘッダーに番号マスクを適用した回数を表します。スクリプトで msg:applyNumberMask API を使用している場合、このカウンタは msg:applyNumberMask API が正常に実行されるたびに増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
msgBlock	このカウンタは、スクリプトがメッセージをブロックした回数を表します。スクリプトで msg:block API を使用している場合、このカウンタは msg:block API が正常に実行されるたびに増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
msgConvertDiversionToHI	このカウンタは、スクリプトがメッセージの Diversion ヘッダーを History-Info ヘッダーに変換した回数を表します。スクリプトで msg:convertDiversionToHI API を使用している場合、このカウンタは msg:convertDiversionToHI API が正常に実行されるたびに増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。

[表示名 (Display Name) ]	説明
msgConvertHIToDiversion	このカウンタは、スクリプトがメッセージの Diversion ヘッダーを History-Info ヘッダーに変換した回数を表します。スクリプトで msg:convertDiversionToHI API を使用している場合、このカウンタは msg:convertDiversionToHI API が正常に実行されるたびに増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
msgModifyHeader	このカウンタは、スクリプトがメッセージの SIP ヘッダーを変更した回数を表します。スクリプトで msg:modifyHeader API を使用している場合、このカウンタは msg:modifyHeader API が正常に実行されるたびに増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
msgRemoveContentBody	このカウンタは、スクリプトがメッセージからコンテンツ本文を削除した回数を表します。スクリプトで msg:removeContentBody API を使用している場合、このカウンタは msg:removeContentBody API が正常に実行されるたびに増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
msgRemoveHeader	このカウンタは、スクリプトがメッセージから SIP ヘッダーを削除した回数を表します。スクリプトで msg:removeHeader API を使用している場合、このカウンタは msg:removeHeader API が正常に実行されるたびに増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
msgRemoveHeaderValue	このカウンタは、スクリプトがメッセージから SIP ヘッダー値を削除した回数を表します。スクリプトで msg:removeHeaderValue API を使用している場合、このカウンタは msg:removeHeaderValue API が正常に実行されるたびに増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
msgSetRequestUri	このカウンタは、スクリプトがメッセージの要求 URI を変更した回数を表します。スクリプトで msg:setRequestUri API を使用している場合、このカウンタは msg:setRequestUri API が正常に実行されるたびに増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。

[表示名 (Display Name) ]	説明
msgSetResponseCode	このカウンタは、スクリプトがメッセージの応答コードや応答フレーズを変更した回数を表示します。スクリプトで <code>msg:setResponseCode</code> API を使用している場合、このカウンタは <code>msg:setResponseCode</code> API が正常に実行されるたびに増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
msgSetSdp	このカウンタは、スクリプトがメッセージの SDP を設定した回数を表示します。スクリプトで <code>msg:setSdp</code> API を使用している場合、このカウンタは <code>msg:setSdp</code> API が正常に実行されるたびに増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
ptAddContentBody	このカウンタは、スクリプトが PassThrough (pt) オブジェクトにコンテンツ本文を追加した回数を表示します。スクリプトで <code>pt:addContentBody</code> API を使用している場合、このカウンタは <code>pt:addContentBody</code> API が正常に実行されるたびに増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
ptAddHeader	このカウンタは、スクリプトが PassThrough (pt) オブジェクトに SIP ヘッダーを追加した回数を表示します。スクリプトで <code>pt:addHeader</code> API を使用している場合、このカウンタは <code>pt:addHeader</code> API が正常に実行されるたびに増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
ptAddHeaderUriParameter	このカウンタは、スクリプトが PassThrough (pt) オブジェクトに SIP ヘッダー URI パラメータを追加した回数を表示します。スクリプトで <code>pt:addHeaderUriParameter</code> API を使用している場合、このカウンタは <code>pt:addHeaderUriParameter</code> API が正常に実行されるたびに増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。
ptAddHeaderValueParameter	このカウンタは、スクリプトが PassThrough (pt) オブジェクトに SIP ヘッダー値パラメータを追加した回数を表示します。スクリプトで <code>pt:addHeaderValueParameter</code> API を使用している場合、このカウンタは <code>pt:addHeaderValueParameter</code> API が正常に実行されるたびに増加します。カウンタが予想どおりに動作しない場合は、スクリプト ロジックにエラーがないか調べてください。

[表示名 (Display Name) ]	説明
ptAddRequestUriParameter	<p>このカウンタは、スクリプトが PassThrough (pt) オブジェクトに要求 URI パラメータを追加した回数を表示します。スクリプトで pt:addRequestUriParameter API を使用している場合、このカウンタは pt:addRequestUriParameter API が正常に実行されるたびに増加します。カウンタが予想どおりに動作しない場合は、スクリプトロジックにエラーがないか調べてください。</p>
ScriptActive	<p>このカウンタは、スクリプトが現在アクティブになっている（トランクで実行されている）かどうかを示します。カウンタに表示される値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 0 : スクリプトが閉じている（無効になっている）ことを示します。</li> <li>• 1 : スクリプトが開いていて実行可能な状態になっていることを示します。</li> </ul> <p>このトランクで実行されている必要があるスクリプトを開くには、次の操作を実行します。</p> <ol style="list-style-type: none"> <li>1 スクリプトが開いていない理由を示している可能性があるアラームがないか確認します。</li> <li>2 エラーをすべて修正します。</li> <li>3 必要に応じて新しいスクリプトをアップロードします。</li> <li>4 トランクをリセットします。</li> </ol>
ScriptClosed	<p>このカウンタは、Cisco Unified Communications Manager がスクリプトが閉じた回数を表示します。</p> <p>スクリプトが閉じている場合、このデバイスでスクリプトを使用できません。</p> <p>Unified CM は、次の基準の 1 台にスクリプトを閉じます。</p> <ul style="list-style-type: none"> <li>• デバイスが手動でリセットされた場合。</li> <li>• デバイスが（エラーにより）自動的にリセットされた場合。</li> <li>• デバイスが削除された場合。</li> </ul> <p>このカウンタは、スクリプトの設定が変更された後に SIP トランクがリセットされたとき、および Unified Communications Manager が再起動したときに再開されます。</p>



[表示名 (Display Name) ]	説明
ScriptDisabledAutomatically	<p>このカウンタは、システムが自動的にスクリプトを無効にした回数を表示します。スクリプトを無効にするかどうかは、Cisco Unified Communications Manager の管理ページにある [SIP 正規化スクリプト設定 (SIP Normalization Script Configuration) ] ウィンドウの [スクリプト実行エラーの復旧処理 (Script Execution Error Recovery Action) ] フィールドと [システム リソース エラーの復旧処理 (System Resource Error Recovery Action) ] フィールドに指定した値によって決定されます。スクリプトは、ロード中および初期化中にスクリプト エラー条件が発生した場合にも無効になります。このカウンタは、スクリプトの設定変更に伴うデバイスの最新の手動リセットからのカウントを提供します (デバイスのリセットだけではカウントはリセットされません。リセットが発生する前に、スクリプトが変更されている必要があります)。このカウンタは、Unified Communications Manager がスクリプト エラーにより自動的にスクリプトを無効にするたびに増加します。</p> <p>このカウンタの数値が予想よりも高い場合は、次の操作を実行してください。</p> <ul style="list-style-type: none"> <li>• SIPNormalizationScriptError アラームと SIPNormalizationAutoResetDisabled アラームを調べます。</li> <li>• RTMT のリソース関連のアラームとカウンタを調べて、リソースの問題が発生しているかどうかを判断します。</li> <li>• SDI トレース ファイルに予期しない SIP 正規化イベントがあるかどうかを調べます。</li> </ul>

[表示名 (Display Name) ]	説明
ScriptOpened	<p>このカウンタは、Unified Communications Manager がスクリプトを開こうとした回数を表します。スクリプトを開くには、Unified Communications Manager のメモリにスクリプトをロードし、初期化して、実行可能な状態にする必要があります。このカウンタの値が1より大きくなっている場合は、予期しない理由あるいはロード中または初期化中のエラーにより、Unified Communications Manager がこの SIP トランクのスクリプトを2回以上開こうとしたことを意味します。このエラーは、実行エラー、リソースエラー、あるいはスクリプト内の無効な構文により発生する場合があります。DeviceResetManually、DeviceResetAutomatically、または ScriptResetAutomatically のいずれかのカウンタが増加すると、このカウンタは1より大きくなります。DeviceResetManually カウンタは、予期されたイベント (SIP トランクのメンテナンス期間など) が原因でスクリプトが閉じたときに増加します。</p> <p>このカウンタの数値が予期しない理由で高くなっている場合は、次の操作を実行してください。</p> <ul style="list-style-type: none"> <li>• SIPNormalizationScriptClosed、SIPNormalizationScriptError、SIPNormalizationResourceWarning などのアラームを調べます。</li> <li>• RTMTのリソース関連のアラームとカウンタを調べて、リソースの問題が発生しているかどうかを判断します。</li> <li>• SDI トレース ファイルに予期しない SIP 正規化イベントがあるかどうかを調べます。</li> </ul> <p>このカウンタは、スクリプトの設定が変更された後に SIP トランクがリセットされたとき、および Unified Communications Manager が再起動したときに再開されます。</p>

[表示名 (Display Name) ]	説明
ScriptResetAutomatically	<p>このカウンタは、システムが自動的にスクリプトをリセットした回数を表示します。スクリプトのリセットは、Cisco Cisco Unified Communications Manager の管理ページにある [SIP 正規化スクリプト設定 (SIP Normalization Script Configuration) ] ウィンドウの [スクリプト実行エラーの復旧処理 (Script Execution Error Recovery Action) ] フィールドと [システム リソース エラーの復旧処理 (System Resource Error Recovery Action) ] フィールドに指定した値に基づいて行われます。このカウンタは、デバイスの最後の手動リセットの後に行われたスクリプトの自動リセットの回数を示します。このカウンタは、Unified Communications Manager がスクリプト エラーにより自動的にスクリプトをリセットするたびに増加します。</p> <p>このカウンタの数値が予想よりも高い場合は、次の操作を実行してください。</p> <ul style="list-style-type: none"> <li>• SIPNormalizationScriptError アラームを調べます。</li> <li>• RTMT のリソース関連のアラームとカウンタを調べて、リソースの問題が発生しているかどうかを判断します。</li> <li>• SDI トレース ファイルに予期しない SIP 正規化イベントがあるかどうかを調べます。</li> </ul>

## Cisco SIP Stack

Cisco SIP Stack オブジェクトは、Session Initiation Protocol (SIP) デバイス (SIP プロキシ、SIP リダイレクトサーバ、SIP レジストラ、SIP ユーザエージェントなど) で生成または使用される SIP スタックの統計についての情報を提供します。次の表には、Cisco SIP Stack カウンタについての情報が含まれます。

表 72 : Cisco SIP Stack

カウンタ	カウンタの説明
AckIns	このカウンタは、SIP デバイスが受信した ACK 要求の総数を表示します。
AckOuts	このカウンタは、SIP デバイスが送信した ACK 要求の総数を表示します。
ByeIns	このカウンタは、SIP デバイスが受信した BYE 要求の総数を表示します。この数には再送信が含まれます。

カウンタ	カウンタの説明
ByeOuts	このカウンタは、SIP デバイスが送信した BYE 要求の総数を表します。この数には再送信が含まれます。
CancelIns	このカウンタは、SIP デバイスが受信した CANCEL 要求の総数を表します。この数には再送信が含まれます。
CancelOuts	このカウンタは、SIP デバイスが送信した CANCEL 要求の総数を表します。この数には再送信が含まれます。
CCBsAllocated	このカウンタは、SIP スタックで現在使用中の呼制御ブロック (CCB) の数を表します。アクティブな各 SIP ダイアログは、1 つの CCB を使用します。
GlobalFailedClassIns	このカウンタは、SIP デバイスが受信した 6xx クラス SIP 応答の総数を表します。この数には再送信が含まれます。このクラスの応答は、クライアント機能を提供する SIP デバイスが失敗応答メッセージを受信したことを示します。一般に、こうした応答は、サーバが Request-URI の特定のインスタンスだけではなく、特定の着信側に関する明確な情報を保持していることを示します。
GlobalFailedClassOuts	このカウンタは、SIP デバイスが送信した 6xx クラス SIP 応答の総数を表します。この数には再送信が含まれます。このクラスの応答は、サーバ機能を提供する SIP デバイスが失敗応答メッセージを受信したことを示します。一般に、こうした応答は、サーバが Request-URI の特定のインスタンスだけではなく、特定の着信側に関する明確な情報を保持していることを示します。
InfoClassIns	このカウンタは、SIP デバイスが受信した 1xx クラス SIP 応答の総数を表します。この数には再送信が含まれます。このクラスの応答は、SIP 要求の進行についての情報を提供します。
InfoClassOuts	このカウンタは、SIP デバイスが送信した 1xx クラス SIP 応答の総数を表します。この数には再送信が含まれます。このクラスの応答は、SIP 要求の処理の進行についての情報を提供します。
InfoIns	このカウンタは、SIP デバイスが受信した INFO 要求の総数を表します。この数には再送信が含まれます。
InfoOuts	このカウンタは、SIP デバイスが送信した INFO 要求の総数を表します。この数には再送信が含まれます。

カウンタ	カウンタの説明
InviteIns	このカウンタは、SIP デバイスが受信した INVITE 要求の総数を表します。この数には再送信が含まれます。
InviteOuts	このカウンタは、SIP デバイスが送信した INVITE 要求の総数を表します。この数には再送信が含まれます。
NotifyIns	このカウンタは、SIP デバイスが受信した NOTIFY 要求の総数を表します。この数には再送信が含まれます。
NotifyOuts	このカウンタは、SIP デバイスが送信した NOTIFY 要求の総数を表します。この数には再送信が含まれます。
OptionsIns	このカウンタは、SIP デバイスが受信した OPTIONS 要求の総数を表します。この数には再送信が含まれます。
OptionsOuts	このカウンタは、SIP デバイスが送信した OPTIONS 要求の総数を表します。この数には再送信が含まれます。
PRackIns	このカウンタは、SIP デバイスが受信した PRACK 要求の総数を表します。この数には再送信が含まれます。
PRackOuts	このカウンタは、SIP デバイスが送信した PRACK 要求の総数を表します。この数には再送信が含まれます。
PublishIns	このカウンタは、SIP デバイスが受信した PUBLISH 要求の総数を表します。この数には再送信が含まれます。
PublishOuts	このカウンタは、SIP デバイスが送信した PUBLISH 要求の総数を表します。この数には再送信が含まれます。
RedirClassIns	このカウンタは、SIP デバイスが受信した 3xx クラス SIP 応答の総数を表します。この数には再送信が含まれます。このクラスの応答は、着信側から到達可能なアドレスへのリダイレクションについての情報を提供します。
RedirClassOuts	このカウンタは、SIP デバイスが送信した 3xx クラス SIP 応答の総数を表します。この数には再送信が含まれます。このクラスの応答は、着信側から到達可能なアドレスへのリダイレクションについての情報を提供します。
ReferIns	このカウンタは、SIP デバイスが受信した REFER 要求の総数を表します。この数には再送信が含まれます。

カウンタ	カウンタの説明
ReferOuts	このカウンタは、SIP デバイスが送信した REFER 要求の総数を表します。この数には再送信が含まれます。
RegisterIns	このカウンタは、SIP デバイスが受信した REGISTER 要求の総数を表します。この数には再送信が含まれます。
RegisterOuts	このカウンタは、SIP デバイスが送信した REGISTER 要求の総数を表します。この数には再送信が含まれます。
RequestsFailedClassIns	このカウンタは、SIP デバイスが受信した 4xx クラス SIP 応答の総数を表します。この数には再送信が含まれます。このクラスの応答は、クライアント機能を提供する SIP デバイスによる要求の失敗を示します。
RequestsFailedClassOuts	このカウンタは、SIP デバイスが送信した 4xx クラス SIP 応答の総数を表します。この数には再送信が含まれます。このクラスの応答は、サーバ機能を提供する SIP デバイスによる要求の失敗を示します。
RetryByes	このカウンタは、SIP デバイスが送信した BYE 再試行の総数を表します。最初の BYE の試行回数を判別するには、sipStatsByeOuts カウンタの値からこのカウンタの値を減算します。
RetryCancels	このカウンタは、SIP デバイスが送信した CANCEL 再試行の総数を表します。最初の CANCEL の試行回数を判別するには、sipStatsCancelOuts カウンタの値からこのカウンタの値を減算します。
RetryInfo	このカウンタは、SIP デバイスが送信した INFO 再試行の総数を表します。最初の INFO の試行回数を判別するには、sipStatsInfoOuts カウンタの値からこのカウンタの値を減算します。
RetryInvites	このカウンタは、SIP デバイスが送信した INVITE 再試行の総数を表します。最初の INVITE の試行回数を判別するには、sipStatsInviteOuts カウンタの値からこのカウンタの値を減算します。
RetryNotify	このカウンタは、SIP デバイスが送信した NOTIFY 再試行の総数を表します。最初の NOTIFY の試行回数を判別するには、sipStatsNotifyOuts カウンタの値からこのカウンタの値を減算します。

カウンタ	カウンタの説明
RetryPRACK	このカウンタは、SIP デバイスが送信した PRACK 再試行の総数を表します。最初の PRACK の試行回数を判別するには、sipStatsPRACKOuts カウンタの値からこのカウンタの値を減算します。
RetryPublish	このカウンタは、SIP デバイスが送信した PUBLISH の再試行回数の合計を表します。最初の PUBLISH の試行回数を判別するには、sipStatsPublishOuts カウンタの値からこのカウンタの値を減算します。
RetryRefer	このカウンタは、SIP デバイスが送信した REFER 再試行の総数を表します。最初の REFER の試行回数を判別するには、sipStatsReferOuts カウンタの値からこのカウンタの値を減算します。
RetryRegisters	このカウンタは、SIP デバイスが送信した REGISTER 再試行の総数を表します。最初の REGISTER の試行回数を判別するには、sipStatsRegisterOuts カウンタの値からこのカウンタの値を減算します。
RetryRel1xx	このカウンタは、SIP デバイスが送信した Reliable 1xx の再試行回数の合計を表します。
RetryRequestsOut	このカウンタは、SIP デバイスが送信した Request の再試行回数の合計を表します。
RetryResponsesFinal	このカウンタは、SIP デバイスが送信した Final Response の再試行回数の合計を表します。
RetryResponsesNonFinal	このカウンタは、SIP デバイスが送信した非 Final Response の再試行回数の合計を表します。
RetrySubscribe	このカウンタは、SIP デバイスが送信した SUBSCRIBE 再試行の総数を表します。最初の SUBSCRIBE の試行回数を判別するには、sipStatsSubscribeOuts カウンタの値からこのカウンタの値を減算します。
RetryUpdate	このカウンタは、SIP デバイスが送信した UPDATE 再試行の総数を表します。最初の UPDATE の試行回数を判別するには、sipStatsUpdateOuts カウンタの値からこのカウンタの値を減算します。

カウンタ	カウンタの説明
SCBsAllocated	このカウンタは、SIP スタックで現在使用中の Subscription Control Blocks (SCB) の数を表します。各登録で 1 つの SCB を使用します。
ServerFailedClassIns	このカウンタは、SIP デバイスが受信した 5xx クラス SIP 応答の総数を表します。この数には再送信が含まれます。このクラスの応答は、クライアント機能を提供する SIP デバイスが失敗応答を受信したことを示します。
ServerFailedClassOuts	このカウンタは、SIP デバイスが送信した 5xx クラス SIP 応答の総数を表します。この数には再送信が含まれます。このクラスの応答は、サーバ機能を提供する SIP デバイスが失敗応答を受信したことを示します。
SIPGenericCounter1	Cisco Engineering Special ビルドによる指示がない限り、このカウンタは使用しないでください。シスコは、診断の目的でこのカウンタの情報を使用します。
SIPGenericCounter2	Cisco Engineering Special ビルドによる指示がない限り、このカウンタは使用しないでください。シスコは、診断の目的でこのカウンタの情報を使用します。
SIPGenericCounter3	Cisco Engineering Special ビルドによる指示がない限り、このカウンタは使用しないでください。シスコは、診断の目的でこのカウンタの情報を使用します。
SIPGenericCounter4	Cisco Engineering Special ビルドによる指示がない限り、このカウンタは使用しないでください。シスコは、診断の目的でこのカウンタの情報を使用します。
SIPHandlerSDLQueueSignalsPresent	このカウンタは、SIPHandler コンポーネントの 4 つの SDL プライオリティキューに現在ある SDL 信号の数を表します。SIPHandler コンポーネントには SIP スタックが含まれます。



カウンタ	カウンタの説明
StatusCode1xxIns	<p>このカウンタは、SIP デバイスが受信した 1xx 応答メッセージ（再送信を含む）の総数を表します。このカウントには、次の 1xx 応答が含まれます。</p> <ul style="list-style-type: none"><li>• 100 試行中</li><li>• 180 呼び出し中</li><li>• 181 コール転送中</li><li>• 182 キューイング済み</li><li>• 183 セッション中</li></ul>
StatusCode1xxOuts	<p>このカウンタは、SIP デバイスが送信した 1xx 応答メッセージ（再送信を含む）の総数を表します。このカウントには、次の 1xx 応答が含まれます。</p> <ul style="list-style-type: none"><li>• 100 試行中</li><li>• 180 呼び出し中</li><li>• 181 コール転送中</li><li>• 182 キューイング済み</li><li>• 183 セッション中</li></ul>
StatusCode2xxIns	<p>このカウンタは、SIP デバイスが受信した 2xx 応答メッセージ（再送信を含む）の総数を表します。このカウントには、次の 2xx 応答が含まれます。</p> <ul style="list-style-type: none"><li>• 200 OK</li><li>• 202 受理成功</li></ul>
StatusCode2xxOuts	<p>このカウンタは、SIP デバイスが送信した 2xx 応答メッセージ（再送信を含む）の総数を表します。このカウントには、次の 2xx 応答が含まれます。</p> <ul style="list-style-type: none"><li>• 200 OK</li><li>• 202 受理成功</li></ul>

カウンタ	カウンタの説明
StatusCode3xxins	<p>このカウンタは、SIP デバイスが受信した 3xx 応答メッセージ（再送信を含む）の総数を表します。このカウントには、次の 3xx 応答が含まれます。</p> <ul style="list-style-type: none"><li>• 300 複数の選択肢</li><li>• 301 永続的に移動</li><li>• 302 一時的に移動</li><li>• 303 非互換の帯域幅ユニット</li><li>• 305 プロキシの使用</li><li>• 380 代替サービス</li></ul>
StatusCode302Outs	<p>このカウンタは、SIP デバイスが送信した 302（一時的に移動）応答メッセージ（再送信を含む）の総数を表します。</p>

カウンタ	カウンタの説明
StatusCode4xxIns	

カウンタ	カウンタの説明
	<p>このカウンタは、SIP デバイスが受信した 4xx 応答メッセージ（再送信を含む）の総数を表します。このカウントには、次の 4xx 応答が含まれます。</p> <ul style="list-style-type: none"> <li>• 400 不正な要求</li> <li>• 401 未認証</li> <li>• 402 支払いが必要</li> <li>• 403 禁止</li> <li>• 404 Not Found</li> <li>• 405 メソッドが許可されない</li> <li>• 406 受理されない</li> <li>• 407 プロキシ認証が必要</li> <li>• 408 要求タイムアウト</li> <li>• 409 競合</li> <li>• 410 消失</li> <li>• 413 要求エンティティが大きすぎる</li> <li>• 414 Request-URI が長すぎる</li> <li>• 415 サポートされないメディア タイプ</li> <li>• 416 サポートされない URI スキーマ</li> <li>• 417 不明なリソース優先順位</li> <li>• 420 不正な拡張子</li> <li>• 422 セッション有効期限の値が小さすぎる</li> <li>• 423 間隔が短すぎる</li> <li>• 480 一時的な使用不可</li> <li>• 481 コール/トランザクションが存在しない</li> <li>• 482 ループが検出された</li> <li>• 483 ホップが多すぎる</li> <li>• 484 アドレスが不完全</li> <li>• 485 あいまい</li> <li>• 486 Busy Here</li> <li>• 487 Request Terminated</li> </ul>

カウンタ	カウンタの説明
	<ul style="list-style-type: none"><li>• 488 ここでは受理されない</li><li>• 489 不正な登録イベント</li><li>• 491 要求保留中</li></ul>

カウンタ	カウンタの説明
StatusCode4xxOuts	

カウンタ	カウンタの説明
	<p>このカウンタは、SIP デバイスが送信した 4xx 応答メッセージ（再送信を含む）の総数を表します。このカウントには、次の 4xx 応答が含まれます。</p> <ul style="list-style-type: none"> <li>• 400 不正な要求</li> <li>• 401 未認証</li> <li>• 402 支払いが必要</li> <li>• 403 禁止</li> <li>• 404 Not Found</li> <li>• 405 メソッドが許可されない</li> <li>• 406 受理されない</li> <li>• 407 プロキシ認証が必要</li> <li>• 408 要求タイムアウト</li> <li>• 409 競合</li> <li>• 410 消失</li> <li>• 413 要求エンティティが大きすぎる</li> <li>• 414 Request-URI が長すぎる</li> <li>• 415 サポートされないメディア タイプ</li> <li>• 416 サポートされない URI スキーマ</li> <li>• 417 不明なリソース優先順位</li> <li>• 420 不正な拡張子</li> <li>• 422 セッション有効期限の値が小さすぎる</li> <li>• 423 間隔が短すぎる</li> <li>• 480 一時的な使用不可</li> <li>• 481 コール/トランザクションが存在しない</li> <li>• 482 ループが検出された</li> <li>• 483 ホップが多すぎる</li> <li>• 484 アドレスが不完全</li> <li>• 485 あいまい</li> <li>• 486 Busy Here</li> <li>• 487 Request Terminated</li> </ul>

カウンタ	カウンタの説明
	<ul style="list-style-type: none"> <li>• 488 ここでは受理されない</li> <li>• 489 不正な登録イベント</li> <li>• 491 要求保留中</li> </ul>
StatusCode5xxIns	<p>このカウンタは、SIP デバイスが受信した 5xx 応答メッセージ（再送信を含む）の総数を表します。このカウントには、次の 5xx 応答が含まれます。</p> <ul style="list-style-type: none"> <li>• 500 サーバの内部エラー</li> <li>• 501 実装されない</li> <li>• 502 不正なゲートウェイ</li> <li>• 503 Service Unavailable</li> <li>• 504 サーバ タイムアウト</li> <li>• 505 未サポートのバージョン</li> <li>• 580 前提条件の失敗</li> </ul>
StatusCode5xxOuts	<p>このカウンタは、SIP デバイスが送信した 5xx 応答メッセージ（再送信を含む）の総数を表します。このカウントには、次の 5xx 応答が含まれます。</p> <ul style="list-style-type: none"> <li>• 500 サーバの内部エラー</li> <li>• 501 実装されない</li> <li>• 502 不正なゲートウェイ</li> <li>• 503 Service Unavailable</li> <li>• 504 サーバ タイムアウト</li> <li>• 505 未サポートのバージョン</li> <li>• 580 前提条件の失敗</li> </ul>



カウンタ	カウンタの説明
StatusCode6xxIns	このカウンタは、SIP デバイスが受信した 6xx 応答メッセージ（再送信を含む）の総数を表します。このカウントには、次の 6xx 応答が含まれます。 <ul style="list-style-type: none"> <li>• 600 すべて通話中</li> <li>• 603 拒否</li> <li>• 604 どこにも存在しない</li> <li>• 606 受理されない</li> </ul>
StatusCode6xxOuts	このカウンタは、SIP デバイスが送信した 6xx 応答メッセージ（再送信を含む）の総数を表します。このカウントには、次の 6xx 応答が含まれます。 <ul style="list-style-type: none"> <li>• 600 すべて通話中</li> <li>• 603 拒否</li> <li>• 604 どこにも存在しない</li> <li>• 606 受理されない</li> </ul>
SubscribeIns	このカウンタは、SIP デバイスが受信した SUBSCRIBE 要求の総数を表します。この数には再送信が含まれます。
SubscribeOuts	このカウンタは、SIP デバイスが送信した SUBSCRIBE 要求の総数を表します。この数には再送信が含まれます。
SuccessClassIns	このカウンタは、SIP デバイスが受信した 2xx クラス SIP 応答の総数を表します。この数には再送信が含まれます。このクラスの応答は、SIP 要求の正常な完了についての情報を提供します。
SuccessClassOuts	このカウンタは、SIP デバイスが送信した 2xx クラス SIP 応答の総数を表します。この数には再送信が含まれます。このクラスの応答は、SIP 要求の正常な完了についての情報を提供します。
SummaryRequestsIn	このカウンタは、SIP デバイスが受信した SIP 要求メッセージの総数を表します。この数には再送信が含まれます。

カウンタ	カウンタの説明
SummaryRequestsOut	このカウンタは、デバイスが送信した SIP 要求メッセージの総数を表します。この数には、このデバイスから発信するメッセージと、このデバイスでリレーするメッセージが含まれます。特定のメッセージが複数回送信されると、再送信として、または分岐（転送）の結果として再送されるメッセージなどのそれぞれの送信は、別々にカウントされます。
SummaryResponsesIn	このカウンタは、SIP デバイスが受信した SIP 応答メッセージの総数を表します。この数には再送信が含まれます。
SummaryResponsesOut	このカウンタは、SIP デバイスが送信（発信およびリレー）した SIP 応答メッセージの総数を表します。この数には再送信が含まれます。
UpdateIns	このカウンタは、SIP デバイスが受信した UPDATE 要求の総数を表します。この数には再送信が含まれます。
UpdateOuts	このカウンタは、SIP デバイスが送信した UPDATE 要求の総数を表します。この数には再送信が含まれます。

## Cisco SIP Station

Cisco SIP Station オブジェクトは、SIP 回線側デバイスについての情報を提供します。次の表に、Cisco SIP Station カウンタに関する情報を示します。

表 73 : Cisco SIP Station

カウンタ	カウンタの説明
ConfigMismatchesPersistent	このカウンタは、Cisco Unified Communications Manager の最後の再起動以降に、TFTP サーバと Cisco Unified Communications Manager との設定バージョンの不一致が原因で、SIP を実行している電話機を永続的に登録できなかった回数を表します。このカウンタは、Cisco Unified Communications Manager が不一致を解決できず、手動操作（設定の更新やデバイスのリセットなど）が必要になるたびに増加します。

カウンタ	カウンタの説明
ConfigMismatchesTemporary	このカウンタは、Cisco CallManager サービスの最後の再起動以降に、TFTP サーバと Cisco Unified Communications Manager との設定バージョンの不一致が原因で、SIP を実行している電話機を一時的に登録できなかった回数を表します。このカウンタは、Cisco Unified Communications Manager が自動的に不一致を解決するたびに増加します。
DBTimeouts	このカウンタは、システムがデータベースからデバイス設定の取得を試行している間に、タイムアウトが発生したために失敗した新規登録の数を表します。
NewRegAccepted	このカウンタは、Cisco CallManager サービスの最後の再起動以降に、NewRegistration キューから削除されて処理された新しい REGISTRATION 要求の総数を表します。
NewRegQueueSize	このカウンタは、現在 NewRegistration キューにある REGISTRATION 要求の数を表します。デバイスから受信され、現在このキューに登録されていない REGISTRATION 要求は、処理される前にこのキューに配置されます。
NewRegRejected	このカウンタは、Cisco CallManager サービスの最後の再起動以降に、486（ここは通話中）応答によって拒否され、NewRegistration キューに配置されなかった新しい REGISTRATION 要求の総数を表します。NewRegistration キューがプログラムされたサイズを超えると、REGISTRATION 要求は拒否されます。
TokensAccepted	このカウンタは、Cisco Communications Manager の最後の再起動以降に許可されたトークン要求の総数を表します。Cisco Unified Communications Manager は、未処理のトークンの数が Cisco CallManager の Maximum Phone Fallback Queue Depth サービス パラメータに指定された数を下回る限り、トークンを許可します。
TokensOutstanding	このカウンタは、トークンが許可されていても、まだ登録されていないデバイスの数を表します。登録する前に、より優先順位の高い Cisco Unified Communications Manager サーバに再接続しているデバイスに対してトークンを許可する必要があります。トークンは、Cisco Unified Communications Manager が、フェールオーバー後にオンラインに戻ったときに、登録要求によって過負荷にならないように保護します。

カウンタ	カウンタの説明
TokensRejected	このカウンタは、Cisco Unified Communications Manager の最後の再起動以降に拒否されたトークン要求の総数を表します。Cisco Unified Communications Manager は、未処理のトークンの数が Cisco CallManager の Maximum Phone Fallback Queue Depth サービス パラメータに指定された数を超えた場合に、トークン要求を拒否します。

## Cisco SW Conf Bridge Device

Cisco SW Conference Bridge Device オブジェクトは、登録済みの Cisco ソフトウェア会議ブリッジデバイスについての情報を提供します。次の表には、Cisco ソフトウェア会議ブリッジデバイスのカウンタについての情報が含まれます。

表 74 : Cisco SW Conf Bridge Device

カウンタ	カウンタの説明
OutOfResources	このカウンタは、ソフトウェア会議デバイスから会議リソースの割り当てを試行して、すべてのリソースがすでに使用中であったために失敗した回数の合計を表します。
ResourceActive	このカウンタは、ソフトウェア会議デバイスで現在使用中の（アクティブな）リソースの数を表します。1つのリソースは1つのストリームを表します。
ResourceAvailable	このカウンタは、非アクティブで、ソフトウェア会議デバイスで現在まだ使用可能なリソースの総数を表します。1つのリソースは1つのストリームを表します。
ResourceTotal	このカウンタは、ソフトウェア会議デバイスが提供する会議リソースの総数を表します。1つのリソースは1つのストリームを表します。このカウンタは、ResourceAvailable カウンタと ResourceActive カウンタを合計した数になります。
SWConferenceActive	このカウンタは、ソフトウェア会議デバイス上で現在アクティブな（使用中の）ソフトウェアベースの会議の数を表します。
SWConferenceCompleted	このカウンタは、ソフトウェア会議デバイス上に割り当てられ、開放された会議の総数を表します。会議は、最初のコールがブリッジに接続されたときに開始します。会議は、最後のコールがブリッジから接続解除されたときに完了します。

## Cisco Telepresence MCU Conference Bridge Device

Cisco Telepresence MCU Conference Bridge Device オブジェクトは、登録された MCU 会議ブリッジデバイスについての情報を提供します。次の表に、Cisco Telepresence MCU Conference Bridge Device カウンタに関する情報を示します。

表 75 : Cisco Telepresence MCU Conference Bridge Device

カウンタ	カウンタの説明
ConferencesActive	このカウンタは、Cisco Unified Communications Manager に登録されているすべての Cisco TelePresence MCU 会議ブリッジデバイス上のアクティブな会議の総数を表します。
ConferencesCompleted	このカウンタは、Cisco Unified Communications Manager から割り当てられた Cisco TelePresence MCU 会議ブリッジを使用し、完了した（つまり、会議ブリッジが割り当てられ、解放された）会議の総数を表します。会議は、最初のコールがブリッジに接続されたときにアクティブになります。会議は、最後のコールがブリッジから接続解除されたときに終了します。
HttpConnectionErrors	このカウンタは、Cisco Unified Communications Manager が、Cisco TelePresence MCU 会議ブリッジデバイスへの HTTP 接続を作成しようとした際に、Cisco TelePresence MCU 会議ブリッジ側の接続エラーが原因で失敗した回数の合計を示します。
HttpNon200OKResponse	このカウンタは、送信された HTTP クエリーに対して、Cisco Unified Communications Manager が Cisco TelePresence MCU 会議ブリッジから [200 OK HTTP] 以外の応答を受信した回数の合計を表します。
OutOfResources	このカウンタは、Cisco Unified Communications Manager が Cisco TelePresence MCU 会議ブリッジデバイスから会議リソースを割り当てようとして失敗した回数を表します。たとえば、他のすべてのリソースが使われている場合、会議リソースの割り当ては失敗します。

## Cisco TFTP Server

Cisco トリビアルファイル転送プロトコル (TFTP) Server オブジェクトは、Cisco TFTP サーバについての情報を提供します。次の表に、Cisco TFTP サーバのカウンタに関する情報を示します。

表 76 : Cisco TFTP Server

カウンタ	カウンタの説明
BuildAbortCount	このカウンタは、Build all 要求を受信したときに、構築プロセスが中断された回数を表します。このカウンタは、グループレベル変更通知の結果として、デバイス/ユニット/ソフトキー/ダイヤル規則の構築が中断されたときに増加します。
BuildCount	このカウンタは、TFTP サービスの開始以降に、TFTP サーバが、すべてのデバイスに影響するデータベース変更通知に対応してすべての設定ファイルを構築した回数を表します。このカウンタは、TFTP サーバがすべての設定ファイルを新しく構築するたびに1つずつ増加します。
BuildDeviceCount	このカウンタは、すべての設定ファイルの最後の構築時に処理されたデバイスの数を表します。このカウンタは、デバイス変更通知の処理中にも更新されます。このカウンタは、新しいデバイスが追加されたときに増加し、既存のデバイスが削除されたときに減少します。
BuildDialruleCount	このカウンタは、設定ファイルの最後の構築時に処理されたダイヤル規則の数を表します。このカウンタは、ダイヤル規則変更通知の処理中にも更新されます。このカウンタは、新しいダイヤル規則が追加されたときに増加し、既存のダイヤル規則が削除されたときに減少します。
BuildDuration	このカウンタは、設定ファイルの最後の構築時に要した時間を秒単位で表します。
BuildSignCount	このカウンタは、セキュリティが有効な電話デバイスの数を表します。この電話デバイスの設定ファイルは、全設定ファイルの最後の構築時に、Cisco Unified Communications Manager サーバキーでデジタル署名されています。このカウンタは、セキュリティが有効な電話デバイス変更通知の処理中にも更新されません。
BuildSoftKeyCount	このカウンタは、設定ファイルの最後の構築時に処理されたソフトキーの数を表します。このカウンタは、新しいソフトキーが追加されたときに増加し、既存のソフトキーが削除されたときに減少します。

カウンタ	カウンタの説明
BuildUnitCount	このカウンタは、すべての設定ファイルの最後の構築時に処理されたゲートウェイの数を表します。このカウンタは、ユニット変更通知の処理中にも更新されます。このカウンタは、新しいゲートウェイが追加されたときに増加し、既存のゲートウェイが削除されたときに減少します。
ChangeNotifications	このカウンタは、TFTP サーバが受信したすべての Cisco Unified Communications Manager データベース変更通知の総数を表します。Cisco Unified Communications Manager の管理でデバイス設定が更新されるたびに、TFTP サーバにデータベース変更通知が送信され、更新されたデバイス用の XML ファイルを再構築します。
DeviceChangeNotifications	このカウンタは、TFTP サーバがデータベース変更通知を受信して、デバイスの設定ファイルの作成、更新、削除を行った回数を表します。
DialruleChangeNotifications	このカウンタは、TFTP サーバがデータベース変更通知を受信して、ダイヤル規則の設定ファイルの作成、更新、削除を行った回数を表します。
EncryptCount	このカウンタは、暗号化された設定ファイルの数を表します。このカウンタは、設定ファイルが正常に暗号化されるたびに更新されます。
GKFoundCount	このカウンタは、キャッシュ内で検出された GK ファイルの数を表します。このカウンタは、キャッシュ内で GK ファイルが検出されるたびに更新されます。
GKNotFoundCount	このカウンタは、キャッシュ内で検出されなかった GK ファイルの数を表します。このカウンタは、GK ファイル取得要求に対して、キャッシュ内でファイルが見つからないことを示す結果が出るたびに更新されます。
HeartBeat	このカウンタは、TFTP サーバのハートビートを表します。このカウンタが増加している場合は、TFTP サーバが稼働中であることを示します。カウンタが増加していない場合は、TFTP サーバがダウンしていることを示します。
HttpConnectRequests	このカウンタは、現在 HTTP GET ファイル要求を行っているクライアントの数を表します。

カウンタ	カウンタの説明
HttpRequests	このカウンタは、HTTPサーバが処理したファイル要求（XML設定ファイル、電話機ファームウェアファイル、オーディオファイルなどに対する要求）の総数を表します。このカウンタは、HTTP サービス開始以降の RequestsProcessed、RequestsNotFound、RequestsOverflow、RequestsAborted、RequestsInProgress の各カウンタを合計した数になります。
HttpRequestsAborted	このカウンタは、HTTPサーバが予期せずに取り消した（中断した）HTTP要求の総数を表します。（装置の電源が入っていないなどの理由で）要求側デバイスに到達できない場合、またはネットワーク接続の問題によりファイル転送が中断された場合は、要求が中断される可能性があります。
HttpRequestsNotFound	このカウンタは、要求されたファイルが検出されなかった場合のHTTP要求の総数を表します。HTTPサーバが要求されたファイルを検出しない場合、メッセージが要求側デバイスに送信されます。
HttpRequestsOverflow	このカウンタは、許容されるクライアント接続が最大数に達したときに拒否されたHTTP要求の総数を表します。TFTPサーバが設定ファイルを構築中に要求を受信したか、他のリソース制限による拒否の可能性があります。Cisco TFTP 拡張サービスパラメータの Maximum Serving Count は、許容される接続の最大数を設定します。
HttpRequestsProcessed	このカウンタは、HTTPサーバが正常に処理したHTTP要求の総数を表します。
HttpServedFromDisk	このカウンタは、ディスク上に存在し、メモリにキャッシュされないファイルに関してHTTPサーバが完了した要求の数を表します。
LDFoundCount	このカウンタは、キャッシュ内で検出されたLDファイルの数を表します。このカウンタは、キャッシュメモリ内でLDファイルが検出されるたびに更新されます。
LDNotFoundCount	このカウンタは、キャッシュメモリ内で検出されなかったLDファイルの数を表します。このカウンタは、LDファイル取得要求に対して、キャッシュ内でファイルが見つからないことを示す結果が出るたびに更新されます。
MaxServingCount	このカウンタは、TFTPで同時に処理できるクライアント接続の最大数を表します。Cisco TFTP 拡張サービスパラメータの Maximum Serving Count は、この値を設定します。



カウンタ	カウンタの説明
Requests	このカウンタは、TFTPサーバが処理するファイル要求（XML設定ファイル、電話機ファームウェアファイル、オーディオファイルなどに対する要求）の総数を表します。このカウンタは、TFTP サービス開始以降の RequestsProcessed、RequestsNotFound、RequestsOverflow、RequestsAborted、RequestsInProgress の各カウンタを合計した数になります。
RequestsAborted	このカウンタは、TFTPサーバが予期せずに取り消した（中断した）TFTP 要求の総数を表します。（装置の電源が入っていないなどの理由で）要求側デバイスに到達できない場合、またはネットワーク接続の問題によりファイル転送が中断された場合は、要求が中断される可能性があります。
RequestsInProgress	このカウンタは、TFTPサーバが現在処理しているファイル要求の数を表します。このカウンタは、新しいファイル要求のたびに増加し、ファイル要求が完了するたびに減少します。このカウンタは、TFTPサーバの現在の負荷を示します。
RequestsNotFound	このカウンタは、要求されたファイルが検出されなかった場合のTFTP要求の総数を表します。TFTPサーバが要求されたファイルを検出しない場合、メッセージが要求側デバイスに送信されます。このカウンタがセキュアに設定されたクラスタ内で増加する場合、通常、このイベントはエラー状態を示します。ただし、クラスタが非セキュアに設定されている場合、CTLファイルが存在しない（検出されない）ことが普通であり、その結果、要求側デバイスにメッセージが送信され、このカウンタがそれに対応して増加します。非セキュアに設定されたクラスタの場合、これは通常の状態であり、エラー状態を示すものではありません。
RequestsOverflow	このカウンタは、許容されるクライアント接続の最大数を超過したために拒否されたTFTP要求、TFTPサーバが設定ファイルを構築中に要求を受信したために拒否されたTFTP要求、または他のリソース制限により拒否されたTFTP要求の総数を表します。Cisco TFTP 拡張サービス パラメータの Maximum Serving Count は、許容される接続の最大数を設定します。
RequestsProcessed	このカウンタは、TFTPサーバが正常に処理したTFTP要求の総数を表します。

カウンタ	カウンタの説明
SegmentsAcknowledged	このカウンタは、クライアント デバイスが確認応答したデータセグメントの総数を表します。ファイルは512バイトのデータセグメントで要求側デバイスに送信され、デバイスは、512バイトの各セグメントに対する確認応答メッセージを TFTP サーバに送信します。先行データ セグメントの確認応答の受信時に追加の各データ セグメントが送信されます。これは、ファイル全体が要求側デバイスに正常に転送されるまで続きます。
SegmentsFromDisk	このカウンタは、TFTP サーバがファイル进行处理する間にディスク上のファイルから読み取ったデータ セグメントの数を表します。
SegmentSent	このカウンタは、TFTP サーバが送信したデータセグメントの総数を表します。ファイルは、512バイトのデータセグメントで要求側デバイスに送信されます。
SEPFoundCount	このカウンタは、キャッシュ内で正常に検出された SEP ファイルの数を表します。このカウンタは、キャッシュ内で SEP ファイルが検出されるたびに更新されます。
SEPNotFoundCount	このカウンタは、キャッシュ内で検出されなかった SEP ファイルの数を表します。このカウンタは、SEP ファイル取得要求に対して、キャッシュ メモリ内でファイルが検出されないことを示す結果が出るたびに更新されます。
SIPFoundCount	このカウンタは、キャッシュ内で正常に検出された SIP ファイルの数を表します。このカウンタは、キャッシュ内で SIP ファイルが検出されるたびに更新されます。
SIPNotFoundCount	このカウンタは、キャッシュ内で検出されなかった SIP ファイルの数を表します。このカウンタは、SIP ファイル取得要求に対して、キャッシュ メモリ内でファイルが検出されないことを示す結果が出るたびに更新されます。
SoftkeyChangeNotifications	このカウンタは、TFTP サーバがデータベース変更通知を受信して、ソフトキーの設定ファイルの作成、更新、削除を行った回数を表します。
UnitChangeNotifications	このカウンタは、TFTP サーバがデータベース変更通知を受信して、ゲートウェイ関連の設定ファイルの作成、更新、削除を行った回数を表します。

## Cisco Transcode Device

Cisco Transcode Device オブジェクトは、登録済みの Cisco トランスコーディング デバイスについての情報を提供します。次の表には、Cisco トランスコーダ デバイスのカウンタについての情報が含まれます。

表 77 : *Cisco Transcode Device*

カウンタ	カウンタの説明
OutOfResources	このカウンタは、トランスコーダ デバイスからトランスコーダ リソースの割り当てを試行して、すべてのリソースがすでに使用中であるなどの理由で失敗した回数の合計を表します。
ResourceActive	このカウンタは、トランスコーダ デバイスに対して現在使用中の（アクティブな）トランスコーダ リソースの数を表します。 各トランスコーダ リソースは、2つのストリームを使用します。
ResourceAvailable	このカウンタは、非アクティブで、トランスコーダ デバイスで現在まだ使用可能なリソースの総数を表します。 各トランスコーダ リソースは、2つのストリームを使用します。
ResourceTotal	このカウンタは、トランスコーダ デバイスが提供したトランスコーダ リソースの総数を表します。ResourceActive カウンタと ResourceAvailable カウンタの合計数と等しい数になります。

## Cisco Video Conference Bridge

Cisco Video Conference Bridge オブジェクトは、登録済みの Cisco ビデオ会議ブリッジ デバイスについての情報を提供します。次の表に、Cisco Video Conference Bridge Device カウンタに関する情報を示します。

表 78 : *Cisco Video Conference Bridge*

カウンタ	カウンタの説明
ConferencesActive	このカウンタは、ビデオ会議ブリッジ デバイス上で現在アクティブな（使用中の）ビデオ会議の総数を表します。システムでは、最初のコールがブリッジに接続されたときに会議がアクティブになるよう指定されています。

カウンタ	カウンタの説明
ConferencesAvailable	このカウンタは、非アクティブで、ビデオ会議デバイス上でまだ使用可能なビデオ会議の数を表します。
ConferencesCompleted	このカウンタは、ビデオ会議デバイス上に割り当てられ、開放されたビデオ会議の総数を表します。会議は、最初のコールがブリッジに接続されたときに開始します。会議は、最後のコールがブリッジから接続解除されたときに完了します。
ConferencesTotal	このカウンタは、ビデオ会議デバイスに対して設定されているビデオ会議の総数を表します。
OutOfConferences	このカウンタは、ビデオ会議デバイスからビデオ会議の開始を試行して、許可されているアクティブな会議の最大数（TotalConferences カウンタで指定）をデバイスがすでに使用しているために失敗した回数の合計を表します。
OutOfResources	このカウンタは、ビデオ会議デバイスから会議リソースの割り当てを試行して、すべてのリソースがすでに使用中であるなどの理由で失敗した回数の合計を表します。
ResourceActive	このカウンタは、ビデオ会議ブリッジデバイス上で現在アクティブな（使用中の）リソースの総数を表します。参加者1名につき、1つのリソースが使用されます。
ResourceAvailable	このカウンタは、非アクティブで、ビデオ会議ブリッジデバイスへの追加の参加者を処理するデバイスでまだ使用可能なリソースの総数を表します。
ResourceTotal	このカウンタは、ビデオ会議ブリッジデバイス上に設定されているリソースの総数を表します。参加者1名につき、1つのリソースが使用されます。

## Cisco Web Dialer

Cisco Web Dialer オブジェクトは、Cisco Web Dialer アプリケーションと Redirector Servlet に関する情報を提供します。次の表には、Cisco Web Dialer のカウンタについての情報が含まれます。

表 79 : Cisco Web Dialer

カウンタ	カウンタの説明
CallsCompleted	このカウンタは、Cisco Web Dialer アプリケーションが正常に完了した Make Call 要求と End Call 要求の数を表します。
CallsFailed	このカウンタは、失敗した Make Call 要求と End Call 要求の数を表します。
RedirectorSessionsHandled	このカウンタは、サービスを最後に開始してから Redirector Servlet が処理した HTTP セッションの総数を表します。
RedirectorSessionsInProgress	このカウンタは、現在 Redirector Servlet によって処理されている HTTP セッションの数を表します。
RequestsCompleted	このカウンタは、Web Dialer Servlet が正常に完了した Make Call 要求と End Call 要求の数を表します。
RequestsFailed	このカウンタは、失敗した Make Call 要求と End Call 要求の数を表します。
SessionsHandled	このカウンタは、サービスを最後に開始してから Cisco Web Dialer Servlet が処理した CTI セッションの総数を表します。
SessionsInProgress	このカウンタは、Cisco Web Dialer Servlet が現在処理している CTI セッションの数を表します。

## Cisco WSM Connector

WSM オブジェクトは、Cisco Unified Communications Manager に設定されている WSMConnectors の情報を提供します。各 WSMConnector は、物理的な Motorola WSM デバイスを表します。次の表に、Cisco WSM Connector カウンタに関する情報を示します。

表 80 : Cisco WSM Connector

カウンタ	カウンタの説明
CallsActive	このカウンタは、WSMConnector デバイス上で現在アクティブな（使用中の）コールの数を表します。
CallsAttempted	このカウンタは、WSMConnector デバイス上で試行されたコールの数を表します。成功したコールの試行と失敗したコールの試行の両方が含まれます。

カウンタ	カウンタの説明
CallsCompleted	このカウンタは、WSMConnector デバイスを介して接続された（音声パスが確立された）コールの数を表します。このカウンタは、コールが終了したときに増加します。
CallsInProgress	このカウンタは、WSMConnector デバイス上で現在進行中のコールの数を表します。この数にはすべてのアクティブ コールが含まれます。CallsInProgress の数が CallsActive の数と等しい場合は、すべてのコールが接続されていることを示します。
DMMSRegistered	このカウンタは、WSM に登録された DMMS 加入者の数を表します。

## IME Client

IME Client オブジェクトは、Cisco Unified Communications Manager サーバ上の Cisco IME クライアントに関する情報を提供します。次の表に、Cisco IME Client カウンタに関する情報を示します。

表 81 : Cisco IME Client

カウンタ	カウンタの説明
CallsAccepted	このカウンタは、Cisco Unified Communications Manager が正常に受信し、着信側が応答した結果 IP コールが確立した Cisco IME コールの数を表します。
CallsAttempted	このカウンタは、Cisco Unified Communications Manager が Cisco IME を介して受信したコールの数を表します。この数には、受け入れられたコール、失敗したコール、およびビジー、未応答のコールが含まれます。このカウンタは、Cisco Unified Communications Manager が Cisco IME を通じてコールを受信するたびに増加します。
CallsReceived	このカウンタは、Cisco Unified Communications Manager が Cisco IME を介して受信するコールの数を表します。この数には、受け入れられたコール、失敗したコール、およびビジー、未応答のコールが含まれます。このカウンタは、コールが開始したときに増加します。
CallsSetup	このカウンタは、Cisco Unified Communications Manager が正常に発信し、リモートパーティが応答した結果 IP コールが確立した Cisco IME コールの数を表します。

カウンタ	カウンタの説明
DomainsUnique	このカウンタは、Cisco IME クライアントによって検出されたピア エンタープライズの固有ドメイン名の数を表します。このカウンタは、システム全体の使用状況を示すインジケータの役割を果たします。
FallbackCallsFailed	このカウンタは、失敗したフォールバックの試行の合計数を表します。
FallbackCallsSuccessful	このカウンタは、品質の問題により PSTN ミッドコールにフォールバックした Cisco IME コールの合計数を表します。このカウンタには、Cisco Unified Communications Manager が開始したコールと受信したコールが含まれます。
IMESetupsFailed	このカウンタは、Cisco IME ルートを使用できたにもかかわらず、IP ネットワーク経由でターゲットに接続できなかったために、PSTN を介して設定されたコールの試行の合計数を表します。
RoutesLearned	このカウンタは、Cisco IME によって認識され、Cisco Unified Communications Manager のルーティングテーブルでルートとして提示される個々の電話番号の合計数を表します。この数が大きくなりすぎると、サーバがクラスタ別の制限を超え、クラスタにサーバを追加する必要が生じる場合があります。
RoutesPublished	このカウンタは、すべての Cisco IME クライアントインスタンスの IME 分散キャッシュに正常にパブリッシュされた DID の合計数を表します。このカウンタで動的に測定を行うことで、自分でプロビジョニングした使用法を評価したり、ネットワークで DID の格納が正常に実施された比率を把握したりすることができます。
RoutesRejected	このカウンタは、管理者が番号またはドメインをブラックリストに掲載したために拒否された認識済みルートの数を表します。このカウンタは、検証のブロックのために今後 VoIP コールが発生しない状況の数を示しています。
VCRUploadRequests	このカウンタは、Cisco Unified Communications Manager が IME 分散キャッシュへの格納のために Cisco IME サーバに送信した音声コール レコード (VCR) アップロード要求の数を表します。

## IME Client Instance

IME Client Instance オブジェクトは、Cisco Unified Communications Manager サーバ上の Cisco IME クライアント インスタンスに関する情報を示します。次の表に、Cisco IME Client Instance カウンタに関する情報を示します。

表 82 : *IME Client*

カウンタ	カウンタの説明
IMEServiceStatus	<p>このカウンタは、特定の Cisco IME クライアント インスタンス (Cisco Unified Communications Manager) の Cisco IME サービスに対する接続の全体的な健全性を表します。カウンタに表示される可能性がある値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 0 : 不明な状態であることを示します (Cisco IME サービスが非アクティブであることを意味している場合があります)。この値が 0 の場合、接続が不明な状態になっている間、1 時間に 1 回アラートが生成されます。</li> <li>• 1 : 健全な状態であること、つまり、Cisco IME サービスがアクティブで、Cisco Unified Communications Manager が Cisco IME クライアント インスタンスのプライマリおよびバックアップ サーバ (設定されている場合) への接続を正常に確立していることを示します。</li> <li>• 2 : 不健全な状態であること、つまり、Cisco IME サービスはアクティブですが、Cisco Unified Communications Manager が Cisco IME クライアント インスタンスのプライマリおよびバックアップ サーバ (設定されている場合) への接続を正常に確立していないことを示します。</li> </ul>

## SAML シングル サインオン

次の表に、SAML シングル サインオン カウンタに関する情報が掲載されています。

表 83 : *SAML* シングル サインオン カウンタ

カウンタ	カウンタの説明
SAML_REQUESTS	このカウンタは、設定済みの ID プロバイダーに送信される SAML 要求の総数を表します。



カウンタ	カウンタの説明
SAML_RESPONSES	このカウンタは、設定済みの ID プロバイダーから受信した SAML 応答の総数を表します。

さらに、次の SAML SSO カウンタは、Unified RTMT に表示されますが、Cisco Unified Communications Manager 10.0(1) で機能しません。

- OAUTH\_TOKENS\_ISSUED
- OAUTH\_TOKENS\_ACTIVE
- OAUTH\_TOKENS\_VALIDATED
- OAUTH\_TOKENS\_EXPIRED
- OAUTH\_TOKENS\_REVOKED

## Cisco IVR デバイス

このオブジェクトは、登録済みの Cisco Interactive Voice Response (IVR) デバイスに関する情報を提供します。

カウンタ	カウンタの説明
ResourceTotal	このカウンタは、この IVR デバイスに設定された IVR リソースの合計数を表します。
ResourceActive	このカウンタは、この IVR デバイスで現在アクティブな IVR リソースの合計数を表します。
ResourceAvailable	このカウンタは、非アクティブで、IVR デバイスで現在まだ使用可能なリソースの合計数を表します。
OutOfResources	このカウンタは、IVR デバイスから IVR リソースの割り当てを試行して、すべてのリソースが使用中であったために失敗した回数の合計を表します。

# IM and Presence Service カウンタ

## Cisco Client Profile Agent

このオブジェクトは Cisco Client Profile (SOAP) インターフェイスに関する情報を提供します。次の表に、クライアントプロファイルエージェントのカウンタについての情報が含まれます。

表 84: Cisco Client Profile Agent カウンタ

カウンタ	カウンタの説明
SoapCrossClusterRedirect	このカウンタは、Cisco UP SOAP インターフェイスで受信され、ピア クラスタ内のノードにリダイレクトされたログイン要求の数を表します。
SoapLoginFailures	このカウンタは、Cisco UP SOAP インターフェイスでの受信に失敗したログイン要求の数を表します。
SoapNodeRedirect	このカウンタは、Cisco UP SOAP インターフェイスで受信され、他のノードにリダイレクトされたログイン要求の数を表します。

## Cisco Presence Engine

Cisco Presence Engine オブジェクトは、Presence Engine で送受信される SIP メッセージに関する情報を提供します。

次の表に、Cisco Presence Engine のパフォーマンスのカウンタについての情報が含まれます。

表 85: Cisco Presence Engine カウンタ

カウンタ	カウンタの説明
サブスクライブ	
SubscribesReceived	このカウンタは、Presence Engine で受信された SUBSCRIBE メッセージの数を表します。これには、初回サブスクライブ、更新、取得、およびサブスクライブ解除が含まれます。
SubscribesSent	このカウンタは、Presence Engine から送信された SUBSCRIBE メッセージの総数を表します。

カウンタ	カウンタの説明
SubscribesReceivedPresence	このカウンタは、イベントタイプ presence を使用して Presence Engine で受信された SUBSCRIBE メッセージの数を表します。
SubscribesReceivedProfileConfig	このカウンタは、イベントタイプ profileconfig を使用して Presence Engine で受信された SUBSCRIBE メッセージの数を表します。
SubscribesInitial	このカウンタは、受信された初回 SUBSCRIBE メッセージ（カレンダー以外）の数を表します。
SubscribesRefresh	このカウンタは、受信された更新 SUBSCRIBE メッセージ（カレンダー以外）の数を表します。
SubscribesFetch	このカウンタは、受信された取得 SUBSCRIBE メッセージ（カレンダー以外）の数を表します。
SubscribesRemove	このカウンタは、受信された削除 SUBSCRIBE メッセージ（カレンダー以外）の数を表します。
ActiveSubscriptions	このカウンタは、現在アクティブなサブスクリプション（カレンダー以外）の数を表します。
SubscribesRedirect3xx	このカウンタは、3xx 応答によってリダイレクトされた SUBSCRIBE メッセージの数を表します。
SubscribesRejected4xx	このカウンタは、4xx 応答によって拒否された SUBSCRIBE メッセージの数を表します。
SubscribesRejected5xx	このカウンタは、5xx 応答によって拒否された SUBSCRIBE メッセージの数を表します。
SubscribesRejected6xx	このカウンタは、6xx 応答によって拒否された SUBSCRIBE メッセージの数を表します。
SubscribesRejectedWith503	このカウンタは、503 応答によって拒否された SUBSCRIBE メッセージの数を表します。
SubscriptionActiveSentForeign	このカウンタは、Presence Engine から外部ドメインへ送信されたアクティブなサブスクリプションの数を表します。
SubscriptionActiveReceivedFromForeign	このカウンタは、Presence Engine が外部ドメインから受信したアクティブなサブスクリプションの数を表します。
WatcherInfoPresenceSubscriptions	このカウンタは、ウォッチャ情報プレゼンスサブスクリプションの数を表します。

カウンタ	カウンタの説明
カレンダー (Calendar)	
ActiveCalendarSubscriptions	このカウンタは、現在アクティブなカレンダーサブスクリプションの数を表します。
SubscribesSentCalendarInitial	このカウンタは、Presence Engine からカレンダー サーバに送信された初回 SUBSCRIBE メッセージの数を表します。
SubscribesSentCalendarRefresh	このカウンタは、Presence Engine からカレンダー サーバに送信された更新 SUBSCRIBE メッセージの数を表します。
SubscribesSentCalendarRetry	このカウンタは、Presence Engine からカレンダー サーバに送信された再試行 SUBSCRIBE メッセージの数を表します。
SubscribesReceivedCalendar	このカウンタは、イベント タイプ calendar を使用して Presence Engine で受信された SUBSCRIBE メッセージの数を表します。
NotifiesReceivedCalendar	このカウンタは、イベント タイプ calendar を使用した Presence Engine による NOTIFY メッセージの数を表します。
NotifiesSentCalendar	このカウンタは、イベント タイプ calendar を使用して Presence Engine から送信された NOTIFY メッセージの数を表します。
MeetingsStarted	このカウンタは、カレンダーの統合によって開始された会議の数を表します。
MeetingsEnded	このカウンタは、カレンダーの統合によって終了した会議の数を表します。
パブリッシュ	
PublicationsProcessed	このカウンタは、Presence Engine で正常に処理されたパブリケーションの数を表します。
PublishInitial	このカウンタは、受信された初回 PUBLISH メッセージの数を表します。
PublishRefresh	このカウンタは、受信された更新 PUBLISH メッセージの数を表します。
PublishModify	このカウンタは、受信された変更 PUBLISH メッセージの数を表します。

カウンタ	カウンタの説明
PublishRemove	このカウンタは、受信された削除PUBLISHメッセージの数を表します。
通知	
NotificationsInQueue	このカウンタは、Presence Engine によってキューイングされた発信 NOTIFY メッセージの現在の数を表します。
NotifiesSent	このカウンタは、Presence Engine から正常に送信された NOTIFY メッセージの数を表します。
NotifiesReceived	このカウンタは、Presence Engine がバックエンドサブスクリプションから受信した NOTIFY メッセージの数を表します。
NotifiesSentPresence	このカウンタは、イベントタイプ presence を使用して Presence Engine から送信された NOTIFY メッセージの数を表します。
NotifiesSentProfileConfig	このカウンタは、イベントタイプ profileconfig を使用して Presence Engine から送信された NOTIFY メッセージの数を表します。
NotifiesRetried	このカウンタは、送信が再試行された NOTIFY メッセージの数を表します。
NotifiesTimeouts	このカウンタは、タイムアウトした NOTIFY メッセージの数を表します。
NotifiesRejected3xx	このカウンタは、3xx 応答によって拒否された NOTIFY メッセージの数を表します。
NotifiesRejected4xx	このカウンタは、4xx 応答によって拒否された NOTIFY メッセージの数を表します。
NotifiesRejected5xx	このカウンタは、5xx 応答によって拒否された NOTIFY メッセージの数を表します。
NotifiesRejected503	このカウンタは、503 応答によって拒否された NOTIFY メッセージの数を表します。
NotifiesRejected6xx	このカウンタは、6xx 応答によって拒否された NOTIFY メッセージの数を表します。
WatcherInfoPresenceNotifications	このカウンタは、ウォッチャ情報プレゼンス通知の数を表します。

カウンタ	カウンタの説明
WatcherInfoPresenceSubscriptions	このカウンタは、ウォッチャ情報プレゼンスサブスクリプションの数を表します。
HighWaterMark	
HighWaterMark	このカウンタは、負荷が上限値に達した回数を表します。
アクティブ ビュー	
ActiveViews	このカウンタは、Presence Engine のアクティブ ビューの数を表します。
アクティブ リソース	
ActiveResources	このカウンタは、Presence Engine のアクティブ リソースの数を表します。
JSM	
ActiveJsmSessions	このカウンタは、Presence Engine と JSM 間のクライアントエミュレーションセッションの数を表します。
XMPP	
XMPPPresenceReceived	このカウンタは、受信された XMPP プレゼンスパケットの数を表します。
XMPPPresenceFiltered	このカウンタは、受信されたフィルタリング済み XMPP プレゼンスパケットの数を表します。
XMPPPresenceNotificationsSent	このカウンタは、構成されたプレゼンスの更新が JSM に送信された件数を表します。
XMPPIMReceived	このカウンタは、Presence Engine で受信された XMPP インスタントメッセージパケットの数を表します。
XMPPIMSent	このカウンタは、Presence Engine から送信された XMPP インスタントメッセージパケットの数を表します。
XMPPIMTcInviteErrors	このカウンタは、Presence Engine によって拒否された XMPP TC 招待の数を表します。
XMPPIMResourceNotFoundErrors	このカウンタは、未登録の SIP リソースに関する XMPP インスタントメッセージパケットの受信件数を表します。

カウンタ	カウンタの説明
XMPPIMIgnored	このカウンタは、Presence Engine によってドロップされた XMPP インスタント メッセージ パケットの数を表します。
XMPPIMGoneGenerated	このカウンタは、プレゼンス イベントで RFI に送信された送信済みメッセージの数を表します。
RFIErrors	このカウンタは、XMPP メッセージを RFI レイヤに送信したときのエラー数を表します。
RFIMessageQueueSize	このカウンタは、RFI が一時停止しているためキューに入れられている XMPP メッセージの現在の数を表します。
SIP	
SIPIMReceived	このカウンタは、Presence Engine で受信された SIP インスタント メッセージ パケットの数を表します。
SIPIMSent	このカウンタは、Presence Engine から送信された SIP インスタント メッセージ パケットの数を表します。
SIPIMGoneGenerated	このカウンタは、プレゼンス イベントでプロキシに送信された送信済みメッセージの数を表します。
SIPIMRetry	このカウンタは、プロキシに再送された SIP インスタント メッセージの数を表します。
SIPIMTimeout	このカウンタは、プロキシへの送信時にタイムアウトした SIP インスタント メッセージ パケットの数を表します。
SIPIMReject3xx	このカウンタは、プロキシへの SIP インスタント メッセージ パケットの送信時に発生した 3xx エラーの数を表します。
SIPIMReject4xx	このカウンタは、プロキシへの SIP インスタント メッセージ パケットの送信時に発生した 4xx エラーの数を表します。
SIPIMReject5xx	このカウンタは、プロキシへの SIP インスタント メッセージ パケットの送信時に発生した 5xx エラーの数を表します。
SIPIMReject6xx	このカウンタは、プロキシへの SIP インスタント メッセージ パケットの送信時に発生した 6xx エラーの数を表します。
ActiveIMSessions	このカウンタは、SIP と XMPP 間のアクティブなインスタントメッセージセッションの数を表します。
Roster Sync	

カウンタ	カウンタの説明
RosterSyncAddBuddySuccess	このカウンタは、Roster Sync Agent で正常に処理されたバディ追加要求の数を表します。
RosterSyncAddBuddyFailure	このカウンタは、Roster Sync Agent での処理に失敗したバディ追加要求の数を表します。
RosterSyncUpdateBuddySuccess	このカウンタは、Roster Sync Agent で正常に処理されたバディ更新要求の数を表します。
RosterSyncUpdateBuddyFailure	このカウンタは、Roster Sync Agent での処理に失敗したバディ更新要求の数を表します。
RosterSyncDeleteBuddySuccess	このカウンタは、Roster Sync Agent で正常に処理されたバディ削除要求の数を表します。
RosterSyncDeleteBuddyFailure	このカウンタは、Roster Sync Agent での処理に失敗したバディ削除要求の数を表します。
RosterSyncSubscribeSuccess	このカウンタは、Roster Sync Agent で正常に処理されたサブスクライブ要求の数を表します。
RosterSyncSubscribeFailure	このカウンタは、Roster Sync Agent での処理に失敗したサブスクライブ要求の数を表します。
RosterSyncUnSubscribeSuccess	このカウンタは、Roster Sync Agent で正常に処理されたサブスクライブ解除要求の数を表します。
RosterSyncUnSubscribeFailure	このカウンタは、Roster Sync Agent での処理に失敗したサブスクライブ解除要求の数を表します。
PolicyUpdateSent	このカウンタは、XCP に送信されたプライバシーポリシーの更新の数を表します。
PolicyUpdateReceived	このカウンタは、XCP から受信したプライバシーポリシーの更新の数を表します。
RosterSyncUnSubscribedSuccess	このカウンタは、Roster Sync Agent で正常に処理されたサブスクライブ解除済み要求の数を表します。
RosterSyncUnSubscribedFailure	このカウンタは、Roster Sync Agent での処理に失敗したサブスクライブ解除済み要求の数を表します。



## Cisco Server Recovery Manager

このオブジェクトは、Cisco Server Recovery Manager (SRM) の状態に関する情報を提供します。次の表には、SRM カウンタについての情報が含まれます。

表 86: Cisco Server Recovery Manager カウンタ

カウンタ	カウンタの説明
SRMState	<p>このカウンタは、SRM の状態を表します。</p> <ul style="list-style-type: none"> <li>• 0 = 不明</li> <li>• 1 = 初期化中</li> <li>• 2 = アイドル状態</li> <li>• 3 = 有効な標準</li> <li>• 4 = バックアップの有効化</li> <li>• 5 = テイク オーバー中</li> <li>• 6 = テイク バック中</li> <li>• 7 = フェール オーバー中</li> <li>• 8 = フェール オーバー済み</li> <li>• 9 = フェール オーバーした対象サービス</li> <li>• 10 = フォールバック中</li> <li>• 11 = 失敗</li> <li>• 12 = ダウン状態</li> </ul>

## Cisco SIP Proxy

次の表には、Cisco SIP Proxy カウンタについての情報が含まれます。

表 87: プロキシ カウンタ

カウンタ	カウンタの説明
CTIGWConferenceReq	このカウンタは、CTIGW で受信された会議コール要求の数を表します。
CTIGWInboundCalls	このカウンタは、CTIGW で受信された着信コールの数を表します。

カウンタ	カウンタの説明
CTIGWLineOpenRequest	このカウンタは、CTIGW で受信された LineOpen 要求の数を表します。
CTIGWMakeCallRequest	このカウンタは、CTIGW で受信された MakeCall 要求の数を表します。
CTIGWRefreshCount	このカウンタは、MOC クライアントから送信された IM and Presence サーバで受信された INVITE の更新の数を表します。
CTIGWRetrieveReq	このカウンタは、CTIGW で受信されたコール取得要求の数を表します。
CTIGWSip4XXRes	このカウンタは、CTIGW から送信された SIP 4XX 応答の数を表します。
CTIGWSip5XXRes	このカウンタは、CTIGW から送信された SIP 5XX 応答の数を表します。
CTIGWSSXrefReq	このカウンタは、CTIGW で受信されたコールのシングル ステップ転送要求の数を表します。
CTIGWUsersAuthorized	このカウンタは、CTIGW によって認証されたユーザの数を表します。
CTIGWUsersCurrentlyAuthorized	このカウンタは、リモート コール制御を行うため現在 MOC にログインしているユーザの数を表します。
CTIGWXrefReq	このカウンタは、CTIGW で受信されたコール転送要求の数を表します。
HttpRequests	このカウンタは、処理された HTTP 要求の数を表します。
IMCTRLActiveSessions	このカウンタは、アクティブなフェデレーション IM セッションの現在の数を表します。
IMGWActiveSessions	このカウンタは、プロキシによって管理されているアクティブな SIP XMPP IM セッションの現在の数を表します。
IMGWClientMessageSent	このカウンタは、XMPP IM ゲートウェイから SIP クライアントに送信された SIP メッセージの現在の数を表します。
IMGWPeMessageReceived	このカウンタは、XMPP IM ゲートウェイがローカル PE から受信した SIP メッセージの現在の数を表します。

カウンタ	カウンタの説明
IMGWPeMessageSent	このカウンタは、ローカル PE に送信された、XMPP IM ゲートウェイに関する SIP メッセージの現在の数を表示します。
Ipc_Requests	このカウンタは、SCP プロセスからの IPC 要求の数を表示します。
NumIdleSipdWorkers	このカウンタは、現在のインスタンスでアイドル状態の sipd ワーカー プロセスの数を表示します。
NumSipdWorker	このカウンタは、現在のインスタンスにおける sipd ワーカー プロセスの数を表示します。
Proxy_Due_Timer_Events	このカウンタは、キューに入れられた期限切れのタイマー イベントの数を表示します。
Proxy_Timer_Events	このカウンタは、期限切れのタイマー イベントの数を表示します。
PWSAppUserLoginRequest	このカウンタは、Presence Web Service モジュールで受信されたアプリケーション ユーザ ログイン要求の数を表示します。
PWSAppUserLogoutRequest	このカウンタは、Presence Web Service モジュールで受信されたアプリケーション ユーザ ログアウト要求の数を表示します。
PWSEndpointExpired	このカウンタは、更新前に期限が切れたサブスクリプションの数を表示します。
PWSEndpointRefreshRequest	このカウンタは、Presence Web Service モジュールで受信されたエンドポイント更新要求の数を表示します。
PWSEndUserLoginRequest	このカウンタは、Presence Web Service モジュールで受信されたエンド ユーザ ログイン要求の数を表示します。
PWSEndUserLogoutRequest	このカウンタは、Presence Web Service モジュールで受信されたエンド ユーザ ログアウト要求の数を表示します。
PWSGetPolledPresenceRequest	このカウンタは、Presence Web Service モジュールで受信された GetPolledPresence 要求の数を表示します。
PWSGetSubscribedPresenceRequest	このカウンタは、Presence Web Service モジュールで受信された GetSubscribedPresence 要求の数を表示します。
PWSPresenceNotifies	このカウンタは、Presence Web Service モジュールから送信されたプレゼンス通知の数を表示します。

カウンタ	カウンタの説明
PWSRegisterEndpointRequest	このカウンタは、Presence Web Service モジュールで受信されたエンドポイント登録要求の数を表します。
PWSSetPresenceRequest	このカウンタは、Presence Web Service モジュールで受信されたSetPresence 要求の数を表します。
PWSSipNotifies	このカウンタは、Presence Web Service モジュールで受信されたSIP 通知の数を表します。
PWSSipPublishRequests	このカウンタは、Presence Web Service モジュールから送信されたSIP パブリッシュ要求の数を表します。
PWSSipSubscribeRequests	このカウンタは、Presence Web Service モジュールから送信されたSIP サブスクライブ要求の数を表します。
PWSSipUnpublishRequests	このカウンタは、Presence Web Service モジュールから送信されたSIP パブリッシュ解除要求の数を表します。
PWSSipUnsubscribeRequests	このカウンタは、Presence Web Service モジュールから送信されたSIP サブスクライブ解除要求の数を表します。
PWSSubscribeExpired	このカウンタは、更新前に期限が切れたエンドポイント登録の数を表します。
PWSSubscribeRefreshRequest	このカウンタは、Presence Web Service モジュールで受信されたサブスクライブ更新要求の数を表します。
PWSSubscribeRequest	このカウンタは、Presence Web Service モジュールで受信されたサブスクライブ要求の数を表します。
PWSUnregisterEndpointRequest	このカウンタは、Presence Web Service モジュールで受信されたエンドポイント登録解除要求の数を表します。
PWSUnsubscribeRequest	このカウンタは、Presence Web Service モジュールで受信されたサブスクライブ解除要求の数を表します。
ServerLoadStatus	このカウンタは、サーバのロードステータスをスケール0 (アイドル) ~ 3 (スワンプ) で表します。
SIPClientImMessage	このカウンタは、プロキシで受信されたSIP クライアントインスタントメッセージの数を表します。
SIPClientRegistered	このカウンタは、プロキシで受信されたSIP クライアント登録要求の数を表します。

カウンタ	カウンタの説明
SIPClientRegisterFailed	このカウンタは、プロキシでの受信に失敗した SIP クライアント登録要求の数を表します。
Sip_Tcp_Requests	このカウンタは、TCP 伝送を介して受信された SIP 要求の数を表します。
Sip_Udp_Requests	このカウンタは、UDP 伝送を介して受信された SIP 要求の数を表します。
SIPInviteRequestIn	このカウンタは、プロキシで受信された INVITE 要求の数を表します。
SIPInviteRequestInForeign	このカウンタは、企業の境界を超えてプロキシで受信された INVITE 要求の現在の数を表します。
SIPInviteRequestOut	このカウンタは、プロキシから送信された INVITE 要求の数を表します。
SIPInviteRequestOutForeign	このカウンタは、企業の境界を超えてプロキシから送信された INVITE 要求の現在の数を表します。
SIPMessageRequestIn	このカウンタは、プロキシで受信された MESSAGE 要求の数を表します。
SIPMessageRequestInForeign	このカウンタは、企業の境界を超えてプロキシで受信された MESSAGE 要求の現在の数を表します。
SIPMessageRequestOutForeign	このカウンタは、企業の境界を超えてプロキシから送信された MESSAGE 要求の現在の数を表します。
SIPNotifyRequestIn	このカウンタは、プロキシで受信された NOTIFY 要求の数を表します。
SIPNotifyRequestInForeign	このカウンタは、企業の境界を超えてプロキシで受信された NOTIFY 要求の現在の数を表します。
SIPNotifyRequestOutForeign	このカウンタは、企業の境界を超えてプロキシから送信された NOTIFY 要求の現在の数を表します。
SIPRegisterRequestIn	このカウンタは、プロキシで受信された REGISTER 要求の数を表します。
SIPRequestInForeign	このカウンタは、企業の境界を超えてプロキシで直接受信された要求の現在の数を表します。

カウンタ	カウンタの説明
SIPRequestOutForeign	このカウンタは、企業の境界を超えてプロキシから直接送信された要求の現在の数を表示します。
SIPRetransmits	このカウンタは、プロキシによって実行された再送信の件数を表示します。
SIPSubscribeRequestIn	このカウンタは、プロキシで受信された SUBSCRIBE 要求の数を表示します。
SIPSubscribeRequestInForeign	このカウンタは、企業の境界を超えてプロキシで受信された SUBSCRIBE 要求の現在の数を表示します。
SIPSubscribeRequestOutForeign	このカウンタは、企業の境界を超えてプロキシから送信された SUBSCRIBE 要求の現在の数を表示します。

## Cisco Sync Agent

このオブジェクトは、同期中に発生したエラーの数に関する情報を提供します。次の表に、Cisco Sync Agent カウンタの情報を示します。

表 88 : Cisco Sync Agent カウンタ

カウンタ	カウンタの説明
NumberOfSyncErrors	このカウンタは、同期中に発生したエラーの数を表示します。Cisco Sync Agent が再起動すると、カウントが 0 にリセットされます。 このカウンタはサブスクリバノードで常に 0 になります。

## Cisco XCP 認証コンポーネント

次の表には、Cisco XCP 認証パフォーマンス カウンタについての情報が含まれます。

表 89 : Cisco XCP 認証コンポーネントのカウンタ

カウンタ	カウンタの説明
SASLPlainSuccess	このカウンタは、成功した SASL plain 認証の合計回数を表示します。

カウンタ	カウンタの説明
SASLPlainFailed	このカウンタは、失敗した SASL plain 認証の合計回数を表示します。
VtgTokenSuccess	このカウンタは、成功した vtg-token 認証の回数を表示します。
VtgTokenFailed	このカウンタは、失敗した vtg-token 認証の回数を表示します。
FailedLicense	このカウンタは、ライセンスがないため失敗した認証の合計回数を表示します。
FailedSASLCredentials	このカウンタは、ユーザ名とパスワードが無効なため失敗した SASL plain 認証の合計回数を表示します。
FailedTokenCredentials	このカウンタは、ユーザ名とパスワードが無効なため失敗した vtg-token 認証の合計回数を表示します。

## Cisco XCP CM

次の表に、Cisco XCP Connection Manager (CM) のパフォーマンス カウンタの情報を示します。

表 90: Cisco XCP CM カウンタ

カウンタ	カウンタの説明
CmConnectedSockets	このカウンタは、Web Connection Manager コンポーネント内の接続されているソケットの数を表します。
CmFailedRequests	このカウンタは、失敗した接続要求の総数を表します。

## Cisco XCP コンポーネント スタンザ トラフィック

次の表に、Cisco XCP コンポーネント スタンザ トラフィックのパフォーマンス カウンタに関する情報を示します。

表 91 : Cisco XCP コンポーネント スタンザ トラフィック カウンタ

カウンタ	カウンタの説明
CompStanzaBytesSent	このカウンタは、1 コンポーネントあたりの送信バイト数を表します。
CompStanzaBytesRecv	このカウンタは、1 コンポーネントあたりの受信バイト数を表します。
CompStanzaErrorsRecv	このカウンタは、送信された1 コンポーネントあたりのエラー数を表します。
CompStanzaErrorsSent	このカウンタは、受信された1 コンポーネントあたりのエラー数を表します。
CompStanzaPacketsDropped	このカウンタは、ドロップされた1 コンポーネントあたりのパケット数を表します。
CompStanzaStanzasSent	このカウンタは、送信された1 コンポーネントあたりのスタンザ数を表します。
CompStanzaStanzasRecv	このカウンタは、受信された1 コンポーネントあたりのスタンザ数を表します。
CompStanzaMessagePacketsSent	このカウンタは、送信された1 コンポーネントあたりのメッセージパケット数を表します。
CompStanzaMessagePacketsRecv	このカウンタは、受信された1 コンポーネントあたりのメッセージパケット数を表します。
CompStanzaPresencePacketsSent	このカウンタは、送信された1 コンポーネントあたりのプレゼンスパケット数を表します。
CompStanzaPresencePacketsRecv	このカウンタは、受信された1 コンポーネントあたりのプレゼンスパケット数を表します。
CompStanzaIQPacketsRecv	このカウンタは、受信された1 コンポーネントあたりのIQパケット数を表します。
CompStanzaIQPacketsSent	このカウンタは、送信された1 コンポーネントあたりのIQパケット数を表します。



## Cisco XCP JDS

次の表に、Cisco XCP JDS のパフォーマンス カウンタに関する情報を示します。

表 92: *Cisco XCP JDS* カウンタ

カウンタ	カウンタの説明
JdsLDAPSuccess	このカウンタは、成功した LDAP 検索の合計回数を表します。
JdsLDAPFailed	このカウンタは、失敗した LDAP 検索の合計回数を表します。
JdsInvalidRequests	このカウンタは、Cisco XCP JDS で拒否されたため LDAP に送信されなかった無効な LDAP 検索要求の数を表します。

## Cisco XCP JSM

次の表に、XCP JSM Performance カウンタについての情報が含まれます。

表 93: *Cisco XCP JSM* カウンタ

カウンタ	カウンタの説明
JsmMessagesIn	このカウンタは、JSM コンポーネントによって受信されたメッセージスタンプ数を表します。
JsmMessagesOut	このカウンタは、JSM コンポーネントによって送信されたメッセージスタンプ数を表します。
JsmPresenceIn	このコンポーネントは、JSM コンポーネントによって受信されたプレゼンススタンプ数を表します。
JsmPresenceOut	このコンポーネントは、JSM コンポーネントによって送信されたプレゼンススタンプ数を表します。

カウンタ	カウンタの説明
JsmIMSessions	このカウンタは、IM and Presence service の実行中 JSM セッションの総数を表します。IM and Presence では、プレゼンス エンジンが起動時に、ライセンスを持つユーザに対して JSM クライアントのエミュレーションセッションを作成します。ユーザが各自のクライアントにサインインしている間に、追加の JSM セッションも作成されます。複数のユーザが複数のクライアントに同時にログインすると、1 人のユーザに複数の追加 JSM セッションが作成される場合があります。
JsmOnlineUsers	このカウンタは、1 つ以上の JSM セッションを所有するユーザの数を表します。IM and Presence では、プレゼンスエンジンは、ライセンスを持つユーザに対して JSM クライアントのエミュレーションセッションを作成します。このカウンタの値は、プレゼンス エンジン <b>ActiveJsmSessions</b> カウンタの値に一致する必要があります。
JsmLoginRate	このカウンタは、JSM コンポーネントによって追跡される現在のログインレートを表します。
JsmSuccessfulLogins	このカウンタは、ログイン成功の総数を表します。
JsmFailedLogins	このカウンタは、IM and Presence では常に 0 になります。失敗したログインについては、Cisco XCP 認証コンポーネントのカウンタを参照してください。
JsmTotalMessagePackets	このカウンタは、JSM コンポーネントによって処理される合計メッセージ パケットを表します。
JsmTotalPresencePackets	このカウンタは、JSM コンポーネントによって処理される合計既存パケットを表します。
JsmTotalIQPackets	このカウンタは、JSM で処理される iq パケットの総数を表します。

カウンタ	カウンタの説明
JsmMsgsInLastSlice	このカウンタは、最後のスライスの JSM コンポーネントによって処理されるメッセージの合計を表します。
JsmAverageMessageSize	このカウンタは、JSM コンポーネントで処理された平均メッセージサイズを表します。
JsmTotalStateChangePackets	このカウンタは、IM and Presence では常に 0 に設定され、将来使用するために予約されます。
JsmStateChangePacketsInSlice	このカウンタは、IM and Presence では常に 0 に設定され、将来使用するために予約されます。
JsmAverageStateChangeSize	このカウンタは、IM and Presence では常に 0 に設定され、将来使用するために予約されます。

## Cisco XCP JSM IQ ネームスペース

次の表に、Cisco XCP JSM IQ ネームスペースのパフォーマンス カウンタに関する情報を示します。

表 94: Cisco XCP JSM IQ ネームスペース

カウンタ	カウンタの説明
JSM IQ ネームスペース	このカウンタは、処理された 1 ネームスペースあたりの IQ パケット数を表します。

## Cisco XCP JSM セッション

次の表に、Cisco XCP JSM セッションのパフォーマンス カウンタに関する情報を示します。

表 95: Cisco XCP JSM セッション カウンタ

カウンタ	カウンタの説明
JsmSessionIQIn	このカウンタは、JSM で受信された 1 セッションあたりの IQ パケット数を表します。

カウンタ	カウンタの説明
JsmSessionIQOut	このカウンタは、JSM から送信された 1 セッションあたりの IQ パケット数を表します。
JsmSessionMessagesIn	このカウンタは、JSM で受信された 1 セッションあたりメッセージパケット数を表します。
JsmSessionMessagesOut	このカウンタは、JSM から送信された 1 セッションあたりのメッセージパケット数を表します。
JsmSessionPresenceIn	このカウンタは、JSM で受信された 1 セッションあたりのプレゼンスパケット数を表します。
JsmSessionPresenceOut	このカウンタは、JSM で受信された 1 セッションあたりのプレゼンスパケット数を表します。
JsmSessionRosterSize	このカウンタは 1 セッションあたりの個々の参加者サイズを表します。

## Cisco XCP MA の基本

次の表に、Cisco XCP Message Archiver の基本パフォーマンス カウンタに関する情報を示します。

表 96 : Cisco XCP MA の基本カウンタ

カウンタ	カウンタの説明
ReceivedPackets	このカウンタは、IM and Presence によって受信され、Message Archiver コンポーネントでアーカイブされるパケットの総数を表します。
SentPackets	このカウンタは、IM and Presence から送信され、Message Archiver コンポーネントでアーカイブされるパケットの総数を表します。
SuccessfulDBWriters	このカウンタは、データベースに書き込まれた確認済み IM レコードを表します。
FailedDBWriters	このカウンタは、失敗したデータベースへの書き込みを表します。

カウンタ	カウンタの説明
PacketsDropped	このカウンタは、isTyping パケットのように Message Archiver で受信されたがデータベースに書き込まれていないパケットの数を表します。
DBQueueSize	このカウンタは、Message Archiver がデータベースへの書き込みを保留してキューイングしたパケットの数を表します。

## Cisco XCP マネージド ファイル転送

次の表に、Cisco XCP マネージド ファイル転送のパフォーマンス カウンタに関する情報を示します。

表 97: マネージド ファイル転送カウンタ

カウンタ	カウンタの説明
MFTBytesDownloadedLastTimeslice	このカウンタは、最後のレポート インターバル（通常は 60 秒）の間にダウンロードされたバイト数を表します。
MFTBytesUpoadedLastTimeslice	このカウンタは、最後のレポート インターバル（通常は 60 秒）の間にアップロードされたバイト数を表します。
MFTFilesDownloaded	このカウンタは、ダウンロードされたファイルの総数を表します。
MFTFilesDownloadedLastTimeslice	このカウンタは、最後のレポート インターバル（通常は 60 秒）の間にダウンロードされたファイル数を表します。
MFTFilesUploaded	このカウンタは、アップロードされたファイルの総数を表します。
MFTFilesUploadedLastTimeslice	このカウンタは、最後のレポート インターバル（通常は 60 秒）の間にアップロードされたファイル数を表します。

## Cisco XCP Router

次の表に、Cisco XCP ルータのパフォーマンス カウンタに関する情報を示します。

表 98: Cisco XCP ルータ カウンタ

カウンタ	カウンタの説明
RouterNormalPackets	このカウンタは、Cisco XCP ルータが処理する通常のパケットの総数を表します。
RouterXdbPackets	このカウンタは、Cisco XCP ルータが処理するxdb パケットの総数を表します。
RouterRoutePackets	このカウンタは、Cisco XCP ルータが処理するルート パケットの総数を表します。
RouterLogPackets	このカウンタは、Cisco XCP ルータが処理するログ パケットの総数を表します。

## Cisco XCP SIP S2S

次の表に、Cisco XCP SIP のサーバ間 (S2S) パフォーマンス カウンタの情報を示します。

表 99: Cisco SIP S2S カウンタ

カウンタ	カウンタの説明
SIPS2SIncomingDomains	このカウンタは、着信サブスクリプションのある外部ドメインの総数を表します。
SIPS2SOutgoingDomains	このカウンタは、発信サブスクリプションのある外部ドメインの総数を表します。
SIPS2SSubscriptionsOut	このカウンタは、アクティブな SIP 発信サブスクリプションの総数を表します。
SIPS2SSubscriptionsIn	このカウンタは、アクティブな SIP 着信サブスクリプションの総数を表します。
SIPS2SSubscriptionsPending	このカウンタは、保留中の SIP 発信サブスクリプションの総数を表します。
SIPS2SNotifyIn	このカウンタは、受信された SIP NOTIFY メッセージの総数を表します。
SIPS2SNotifyOut	このカウンタは、送信された SIP NOTIFY メッセージの総数を表します。

カウンタ	カウンタの説明
SIPS2SMessageIn	このカウンタは、受信された SIP MESSAGE メッセージの総数を表します。
SIPS2SMessageOut	このカウンタは、送信された SIP MESSAGE メッセージの総数を表します。
SIPS2SByeIn	このカウンタは、受信された SIP BYE メッセージの総数を表します。
SIPS2SInviteIn	このカウンタは、受信された SIP INVITE メッセージの総数を表します。
SIPS2SInviteOut	このカウンタは、送信された SIP INVITE メッセージの総数を表します。

## Cisco XCP S2S

次の表に、Cisco XCP のサーバ間 (S2S) パフォーマンス カウンタの情報を示します。

表 100 : Cisco XCP S2S カウンタ

カウンタ	カウンタの説明
S2SIncomingDomains	このカウンタは、着信サブスクリプションのある外部ドメインの総数を表します。
S2SOutgoingDomains	このカウンタは、発信サブスクリプションのある外部ドメインの総数を表します。
S2SFailedDialbackIn	このカウンタは、失敗した着信ダイヤルバックの総数を表します。
S2SFailedDialbackOut	このカウンタは、失敗した発信ダイヤルバックの総数を表します。

## Cisco XCP TC

次の表に、Cisco XCP Text Conferencing (TC) のパフォーマンス カウンタに関する情報を示します。

表 101 : Cisco XCP TC カウンタ

カウンタ	カウンタの説明
TcTotalRooms	このカウンタは、全種類のテキストチャットルームの総数を表します。
TcAdhocRooms	このカウンタは、アドホックのテキストチャットルームの総数を表します。
TcPersistentRooms	このカウンタは、永続的なテキストチャットルームの総数を表します。
TcCreatedRooms	このカウンタは、作成されたテキストチャットルームの総数を表します。
TcDeletedRooms	このカウンタは、削除されたテキストチャットルームの総数を表します。
TcMessagesIn	このカウンタは、受信されたグループチャットメッセージの総数を表します。
TcMessagesOut	このカウンタは、送信されたグループチャットメッセージの総数を表します。
TcDirectedMessagesIn	このカウンタは、受信したプライベートおよび招待メッセージの総数を表します。
TcMessagesPersisted	このカウンタは、外部データベースに保存されたメッセージの総数を表します。
TcMessagesIgnored	このカウンタは、外部データベースに保存されていないメッセージの総数を表します。

## Cisco XCP TC ルーム

次の表に、Cisco XCP TC ルームのパフォーマンス カウンタに関する情報を示します。

表 102 : Cisco XCP TC ルーム カウンタ

カウンタ	カウンタの説明
TCRoomNumOccupants	このカウンタは、1 チャットルームあたりの占有者数を表します。



カウンタ	カウンタの説明
TCRoomBytesSent	このカウンタは、1 チャットルームあたりの送信バイト数を表します。
TCRoomBytesRecv	このカウンタは、1 チャットルームあたりの受信バイト数を表します。
TCRoomStanzasSent	このカウンタは、送信された1チャットルームあたりのスタンザ数を表します。
TCRoomStanzasRecv	このカウンタは、1チャットルームあたりの受信スタンザ数を表します。
TCRoomMsgPacketSent	このカウンタは、1チャットルームあたりの送信メッセージ数を表します。
TCRoomMsgPacketsRecv	このカウンタは、1チャットルームあたりの受信メッセージ数を表します。
TCRoomPresencePacketsSent	このカウンタは、1チャットルームあたりの送信プレゼンス パケット数を表します。
TCRoomPresencePacketsRecv	このカウンタは、1チャットルームあたりの受信プレゼンス パケット数を表します。
TCRoomIQPacketsSent	このカウンタは、送信された1チャットルームあたりの IQ パケット数を表します。
TCRoomIQPacketsRecv	このカウンタは、受信された1チャットルームあたりの IQ パケット数を表します。

## Cisco XCP WebCM

次の表に、Cisco XCP Web Connection Manager のパフォーマンス カウンタに関する情報を示します。

表 103 : Cisco XCP WebCM カウンタ

カウンタ	カウンタの説明
WebCMConnectedSockets	このカウンタは、接続されたXMPPクライアントセッションの累計数を表します。

カウンタ	カウンタの説明
WebCMFailedRequests	このカウンタは、失敗した接続要求の総数を表します。

## Cisco Unity Connection カウンタ

### CUC Data Store

CUC Data Store オブジェクトは、登録済みのデータベースの Cisco Unity Connection による使用率に関する情報を提供します。次の表に、CUC Data Store カウンタに関する情報を示します。

表 104 : CUC Data Store

カウンタ	カウンタの説明
Allocated Memory [kb]	データベース サーバの仮想アドレス容量 (KB 単位)。
Database Connections	データベース サーバへの合計接続数。
Disk Free (percentage)	すべてのチャンクにおける使用可能な空き容量のパーセンテージ。
Disk Reads	過去 30 秒間のすべてのデータ チャンク (行) でのディスク読み取り操作の数の合計。
Disk Reads/second	1 秒あたりのディスクからの読み取り操作の数。
Disk Writes	過去 30 秒間のディスクへの書き込み操作の数。
Disk Writes/second	1 秒あたりのディスクへの書き込み操作の数。
Shared Memory [kb]	データベース サーバの共有メモリの使用されている量 (KB 単位)。

### CUC Data Store: Databases

CUC Data: Databases オブジェクトは、Cisco Unity Connection で使用されるデータベースに関する情報を提供します。

表 105 : CUC Data Store: Databases

カウンタ	カウンタの説明
Disk Free/chunk [kb]	選択したデータ チャンクで使用可能な空き領域の容量（キロバイト単位）。
Disk Reads/chunk	選択したデータ チャンクに対する読み取り操作の回数。
Disk Writes/chunk	選択したデータ チャンクに対する書き込み操作の数。

## CUC Digital Notifications

CUC Digital Notifications オブジェクトは、SMS および SMTP 通知の合計数に関する情報を提供します。次の表に、CUC Digital Notification カウンタに関する情報を示します。

表 106 : CUC Digital Notifications

カウンタ	カウンタの説明
SMS Notifications Failed	接続に失敗した SMS 通知の合計数。
SMS Notifications Total	Cisco Unity Connection がサブスクライバに送信した SMS 通知の合計数。
SMTP Notifications Total	Cisco Unity Connection がサブスクライバに送信した SMTP 通知の合計数。
HTML Notifications with Summary of voice messages	サマリー通知の数を維持するカウンタ。
HTML Notifications with Summary of voice messages in Last One Minute	過去 1 分間のサマリー通知の数を維持するカウンタ。
Scheduled Notifications Total	送信されたスケジュール済みサマリー通知の数を維持するカウンタ。
Scheduled Notifications in Last One Minute	過去 1 分間に送信されたスケジュール済みサマリー通知の数を維持するカウンタ。
Scheduled Notifications dropped due to Parent Schedule off	親スケジュールがオフであるためにドロップされた（送信されなかった）スケジュール済みサマリー通知の数を維持するカウンタ。

カウンタ	カウンタの説明
Scheduled Notifications dropped due to Parent Schedule off in Last One Minute	親スケジュールがオフであるために過去1分間にドロップされた（送信されなかった）スケジュール済みサマリー通知の数を維持するカウンタ。
Missed Call Notifications Total	Cisco Unity Connection から送信された不在着信通知の合計数。

## CUC Directory Services

CUC Directory Services オブジェクトは、Cisco Unity Connection で使用するディレクトリ サービスのパフォーマンスに関する情報を提供します。

Directory Search Duration Average [s] カウンタは、Cisco Unity Connection サーバに対するディレクトリ検索要求を完了するための平均時間（秒）を表します。

## CUC Feeder

CUC Feeder オブジェクトは、フィーダによって処理された全要求の数を保持します。次の表に、CUC Feeder カウンタに関する情報を示します。

カウンタ	カウンタの説明
Total objects requests processed	フィーダが処理した HTTP[S]/CCI オブジェクト要求の合計数。
Objects requests processed in last 15 minutes	過去 15 分間にフィーダが処理した HTTP[S]/CCI オブジェクト要求の合計数。
Total object requests processed	フィーダが処理した HTTP[S]/CCI オブジェクト要求の合計数。
Object requests processed in last 15 minutes	過去 15 分間にフィーダが処理した HTTP[S]/CCI オブジェクト要求の合計数。

## CUC メールボックス同期

メールボックス同期サービスは、Unity Connection と Exchange 間のメッセージを同期します。

次の表には、メールボックス同期カウンタについての情報が含まれます。

カウンタ	カウンタの説明
アクティブなスレッド数	Cisco Unity Connection は、Cisco Unity Connection から Exchange Server へ、またはその逆方向へのボイスメールを同期するためにスレッドを維持します。このカウンタは、ボイスメールの同期でアクティブに使用しているスレッドの数を常に指定します。
バックグラウンドキュー サイズ	メールボックス同期には、バックグラウンド、標準、および時間制限の 3 種類のプライオリティ キューがあります。バックグラウンドキューは最も低いプライオリティです。このキューには、1 時間ごとに行われる各メールボックスのバックグラウンドによってスケジュール設定される項目があります。
標準キュー サイズ	標準キューは中程度のプライオリティです。このキューには、ユーザが実行するメッセージ処理（メッセージの作成、既読、未読、削除など）、または Cisco Unity Connection Administration の [ユニファイドメッセージング (Unified Messaging)] ページで管理者が更新する設定によってスケジュール設定される項目があります。
時間制限キュー サイズ	時間制限キューは最も高いプライオリティです。このキューには、サブスクリプションを有効にするために Cisco Unity Connection から Exchange Server に送信したキープアライブメッセージによってスケジュール設定される項目があります。これが適用されるのは、2003 Exchange Server のみです。
接続エラー合計数	これは、CuMbxSync プロセスがデータベースからデータを取得または更新するのに失敗する回数を示します。
メールボックス追加合計数	これは、ユーザメールボックスがサブスクリプション用に設定された回数を示します。Unity Connection と Exchange の間でエラーが発生すると、ユーザメールボックスが削除または再追加されます。

カウンタ	カウンタの説明
メールボックス削除合計数	これは、ユーザメールボックスがサブスクリプション解除用に設定された回数を示します。 Unity Connection と Exchange の間でエラーが発生すると、ユーザメールボックスが削除または再追加されます。
再同期合計数	これは、ユーザメールボックスが Exchange Server と再同期する合計回数を示します。Cisco Unity Connection は、すべてのユーザメールボックスのバックグラウンド再同期を 1 時間ごとに行います。
再試行合計数	Cisco Unity Connection と Exchange Server 間で通信障害が発生するたびに、Unity Connection は特定のユーザメールボックスのメールボックス同期を再試行します。このカウンタは、このような場合の数を指定します。
作業項目合計数	これは、作成、既読、未読、削除などのメッセージ処理がユーザメールボックスで実行された回数を示します。

## CUC Message Store

CUC Message Store オブジェクトは、Cisco Unity Connection メッセージストアのパフォーマンスに関する情報を提供します。次の表に、CUC Message Store カウンタに関する情報を示します。

表 107 : CUC Message Store

カウンタ	カウンタの説明
Bad Mail Total	MTA サーバの最後の再起動以降に Bad Mail フォルダに送信されたメッセージの総数。
Delivery Receipts Total	MTA サーバの最後の再起動以降の送信確認の合計数。
Incoming Recalls	他のネットワーク ロケーションのリモート送信者によって開始されたメッセージのローカル コピーを取り消すための着信要求の数。
Intersite Messages Delivered Per Minute	過去 1 分間に配信されたサイト間メッセージの数。

カウンタ	カウンタの説明
Intersite Messages Delivered Total	MTA サーバの最後の再起動以降に配信されたサイト間メッセージの合計数。
Intersite Messages Received Per Minute	過去 1 分間に受信したサイト間メッセージの数。
Intersite Messages Received Total	MTA サーバの最後の再起動以降に受信したサイト間メッセージの合計数。
Intersite Messages Total	MTA サーバの最後の再起動以降に配信および受信したサイト間メッセージの合計数。
Local Recalls	このサーバ上のローカル送信者が開始したメッセージ取り消しの数。
Message Size Average [kb]	各サンプルでの MTA のキロ バイト単位での平均サイズ。
Messages Delivered Total	MTA サーバの最後の再起動以降に配信されたメッセージの合計数。
Messages Received Per Minute	MTA が 1 分間に受信したメッセージの合計数。
Messages Received Total	MTA サーバの最後の再起動以降に受信したメッセージの合計数。
Non-delivery Receipts Total	MTA サーバの最後の再起動以降の未送信確認の合計数。
Number of Items Recalled	メッセージの取り消しの合計数。この数には複数の受信者に送信されたメッセージの個別のコピーも含まれるため、 <b>Total Recalls, Local and Remote</b> パフォーマンス カウンタをはるかに上回る数になる可能性があります。
Queued Messages Current	現在 MTA にキューイングされているメッセージ数。
Read Receipts Total	MTA サーバの最後の再起動以降の受信確認の合計数。
Retries Total	MTA サーバの最後の再起動以降の再試行の合計数。
Total dispatch message folder items delivered	MTA の開始以降に個々のユーザのメール ボックスに配信されるディスパッチ メッセージの合計数。この数には複数の受信者に送信されたメッセージの個々のコピーの数が含まれます。
Total dispatch messages accepted	MTA サーバの最後の再起動以降に受理されたディスパッチ メッセージの合計数。

カウンタ	カウンタの説明
Total dispatch messages delivered	MTA の開始以降に配信されたディスパッチ メッセージの合計数。この数には、受信者数に関係なく、各メッセージが1回だけ含まれます。
Total dispatch message items rejected	MTA サーバの最後の再起動以降に拒否されたディスパッチ メッセージの個々のコピーの合計数。
Total dispatch messages removed due to acceptance	MTA サーバの最後の再起動以降に、メッセージが他のユーザによって受理されていたためユーザのメール ボックスから除外されていたディスパッチ メッセージの合計数。
Total recalls, local and remote	ローカル送信者およびリモート送信者が開始したメッセージ取り消しの合計数。この数は、 <b>Incoming Recalls</b> パフォーマンス カウンタおよび <b>Local Recalls</b> パフォーマンス カウンタの合計と一致します。
VPIM Message Decode Duration Average [s]	MIME 形式のボイス メッセージを元の形式にデコードするための平均時間 (秒)。
VPIM Message Encode Duration Average [s]	MIME 形式にボイス メッセージをエンコードする平均時間 (秒)。
VPIM Messages Delivered Per Minute	Cisco Unity Connection メッセージストアが 1 分間に配信した VPIM メッセージの数。
VPIM Messages Delivered Total	Cisco Unity Connection メッセージストアが配信した VPIM メッセージの合計数。
VPIM Messages Received Per Minute	Cisco Unity Connection メッセージストアが 1 分間に受信した VPIM メッセージの数。
VPIM Messages Received Total	Cisco Unity Connection メッセージストアが受信した VPIM メッセージの合計数。
VPIM Messages Total	Cisco Unity Connection メッセージストアが処理した VPIM メッセージの合計数。
Messages Undelivered Mailbox Quota Full Notification Total	メールボックス クォータが満杯のときに送信された不在着信通知の合計数。
Video Messages Delivered Total	MTA サーバの最後の再起動以降に配信されたビデオ メッセージの合計数。



カウンタ	カウンタの説明
Video Messages Delivered Per Minute	MTA サーバの最後の再起動以降、1 分間に配信されたビデオメッセージの合計数。
Video Messages Processed by MTA Total	MTA サーバの最後の再起動以降、MTA サーバで処理された（成功と失敗の両方の）ビデオメッセージの合計数。
Video Messages Processed by MTA Per Minute	MTA サーバの最後の再起動以降、1 分間に MTA サーバで処理された（成功と失敗の両方の）ビデオメッセージの合計数。

## CUC Message Store: Databases

CUC Message Store: Databases オブジェクトは、Cisco Unity Connection で使用されるメッセージストア データベースに関する情報を提供します。

Messages Delivered Per Message Store カウンタは、MTA サーバが最後に再起動されて以降、1 メッセージストアあたりに配信されたメッセージの総数を表します。

## CUC Personal Call Transfer Rules

CUC Personal Call Transfer Rules オブジェクトは、パーソナル着信転送ルール（PCTR）の数と使用状況についての情報を提供します。次の表に、CUC Personal Call Transfer Rules カウンタに関する情報を示します。

表 108 : CUC Personal Call Transfer Rules

カウンタ	カウンタの説明
Applicable Rule Found	ルール処理が開始され、適用可能な転送ルールが見つかったパーソナル着信転送ルール（PCTR）のコール。
Destinations Tried	転送ルールが適用されている間に試行された転送先の数。
PCTR Calls	パーソナル着信転送ルール（PCTR）による処理を適用された（ユーザ割り当ての COS が PCTR で有効化されている、ユーザは Cisco Unified Communications Manager ユーザである、ユーザは PCTR を無効にしていない）コール。
Rules Evaluated	パーソナル着信転送ルール（PCTR）のコールでのルール処理中に評価されたルールの数。
Subscriber Reached	転送ルールが適用されている間にサブスクライバに到達した回数。

カウンタ	カウンタの説明
転送が失敗しました (Transfer Failed)	パーソナル着信転送ルールが適用されている間に、Cisco Unity Connection が転送先へのコールの転送に失敗した回数。転送の失敗には、呼び出された転送先が接続済み、通話中、RNA 状態、またはタイムアウトになっている場合を除くすべての状態が含まれます。転送中に発信者が電話を切ることも転送の失敗と見なされます。
Voicemail Reached	転送ルールが適用されている間にボイスメールが到達した回数。

## CUC Phone System

CUC Phone System オブジェクトは、電話システム統合のパフォーマンスに関する情報を提供します。次の表に、CUC Phone System カウンタについての情報を示します。

表 109 : CUC Phone System

カウンタ	カウンタの説明
Call Count Current	Cisco Unity Connection サーバへの着信および発信コールの現在の数。
Call Count Total	Cisco Unity Connection サーバへの着信および発信コールの合計数。
Call Duration Average [s]	Cisco Unity Connection サーバからの着信コールと発信コールの平均持続時間 (秒)。
Call Duration Total [s]	Cisco Unity Connection サーバからの着信コールと発信コールの合計持続時間 (秒)。
Calls Unanswered Total	Cisco Unity Connection サーバでの無応答コールの合計数。
Incoming Calls CFB Current	話中転送として受信した着信コールの現在の数。
Incoming Calls CFB Total	話中転送として受信した着信コールの合計数。
Incoming Calls CFNA Current	無応答時転送として受信した着信コールの現在の数。
Incoming Calls CFNA Total	無応答時転送として受信した着信コールの合計数。
Incoming Calls Current	着信コールの現在の数。

カウンタ	カウンタの説明
Incoming Calls Direct Current	直接コールとして受信した着信コールの現在の数。
Incoming Calls Direct Total	直接コールとして受信した着信コールの合計数。
Incoming Calls Duration Average [s]	Cisco Unity Connection サーバへのすべての着信コールの平均持続時間 (秒)。
Incoming Calls Duration Total [s]	Cisco Unity Connection サーバへのすべての着信コールの合計持続時間 (秒)。
Incoming Calls No Info Total	統合情報を持たない着信コールの合計数。
Incoming Calls Total	着信コールの合計数。
Message Notification Duration Average [s]	Cisco Unity Connection サーバからのすべてのメッセージ通知を完了するまでの平均時間 (秒)。
Message Notification Duration Total [s]	Cisco Unity Connection サーバからのすべてのメッセージ通知を完了するまでの合計時間 (秒)。
Message Notifications Failed	宛先番号への接続に失敗したメッセージ通知の合計数。
Message Notifications Total	Cisco Unity Connection がサブスクライバに送信したメッセージ通知の合計数。
MWI Request Duration Average [ms]	Cisco Unity Connection サーバからのすべての MWI 要求の平均持続時間 (ミリ秒単位)。
MWI Request Duration Total [ms]	Cisco Unity Connection サーバからのすべての MWI 要求の合計持続時間 (ミリ秒単位)。
MWI Requests Failed Total	宛先番号への接続または MWI 操作の完了に失敗した MWI 要求の合計数。
MWI Requests Total	Cisco Unity Connection が送信した MWI 要求の合計数。
Outgoing Calls Duration Average [s]	Cisco Unity Connection サーバからのすべての発信コールの平均持続時間 (秒)。
Outgoing Calls Duration Total [s]	Cisco Unity Connection サーバからのすべての発信コールの合計持続時間 (秒)。
Outgoing Calls Release Transfers Completed	Cisco Unity Connection サーバからの完了リリース転送の数。

カウンタ	カウンタの説明
Outgoing Calls Release Transfers Failed	宛先番号への接続に失敗した Cisco Unity Connection サーバからのリリース転送の数。
Outgoing Calls Release Transfers Total	Cisco Unity Connection サーバから試行されたリリース転送の合計数。
Outgoing Calls Supervised Transfers Completed	Cisco Unity Connection サーバからの完了監視転送の数。
Outgoing Calls Supervised Transfers Dropped	進行中にドロップされた Cisco Unity Connection サーバからの監視転送の数。
Outgoing Calls Supervised Transfers Failed	宛先番号への接続に失敗した Cisco Unity Connection サーバからの監視転送の数。
Outgoing Calls Supervised Transfers Total	Cisco Unity Connection サーバからの監視転送の合計数。
Outgoing Calls Transfers Total	Cisco Unity Connection が試行したリリース転送および監視転送の合計数。
Pager Notifications Duration Average [s]	Cisco Unity Connection サーバからのすべてのポケットベル通知を完了するまでの平均時間 (秒)。
Pager Notifications Duration Total [s]	Cisco Unity Connection サーバからのすべてのポケットベル通知を完了するまでの合計時間 (秒)。
Pager Notifications Failed	宛先番号への接続に失敗したポケットベル通知の合計数。
Pager Notifications Total	Cisco Unity Connection がサブスクライバに送信したポケットベル通知の合計数。
Port Idle Duration [s]	Cisco Unity Connection サーバへの着信コール間でいずれかのポートがアイドル状態のままになっている合計時間 (秒)。
Port Idle Duration Average [s]	Cisco Unity Connection サーバへの着信コール間でいずれかのポートがアイドル状態のままになっている平均時間 (秒)。
Ports Idle Current	Cisco Unity Connection サーバで使用されていない統合ポートの現在の数。
Ports In Use Current	Cisco Unity Connection サーバで使用中の統合ポートの現在の数。

カウンタ	カウンタの説明
Ports Locked	Cisco Unity Connection がもう応答しないかまたは使用不可能なポートの現在の数。
Missed Call Total	Cisco Unity Connection サーバによってトリガーされた不在着信通知の合計数。

## CUC Phone System: Ports

CUC Phone System: Ports オブジェクトは、Cisco Unity Connection のボイス メッセージング ポートに関する情報を提供します。次の表に、CUC Phone System: Ports カウンタに関する情報を示します。

表 110 : CUC Phone System: Ports

カウンタ	カウンタの説明
Port Calls	Cisco Unity Connection サーバの最後の再起動以降に、このポートで受信したコールの合計数。これには、着信、MWI 発信、通知発信、TRAP 発信、および VPIM 発信など、すべてのタイプのコールが含まれます。
Port Idle Percent	Cisco Unity Connection サーバ上のアイドルポートの分配の割合 (パーセント)。
Port Usage Duration Average [s]	ポートでアクティブにコールが処理されていた平均時間 (秒)。
Port Usage Duration Total [s]	ポートでアクティブにコールが処理されていた合計時間 (秒)
Port Usage Percent	Cisco Unity Connection サーバ上ポートへのコールの分配の割合 (パーセント)。

## CUC Replication

CUC Replication オブジェクトは、Cisco Unity Connection の冗長性のためのレプリケーションに関する情報を提供します。次の表に、CUC Replication カウンタに関する情報を示します。

表 111 : CUC Replication

カウンタ	カウンタの説明
File Replication Latency [s]	レプリケーションが開始される前にファイルが存在していた期間。
File Replication Latency Max [s]	サービスが開始されてからのファイル レプリケーションの最大遅延。
File Transfer Rate [kbytes/s]	レプリケーションされた各ファイルの転送速度。
Files Replicated Total	サービスの開始以降にレプリケーションされたファイルの数。
Transfer Rate [bytes/s]	秒単位で転送されるバイト数。

## CUC Replicator: Remote Connection Locations

CUC Replicator: Remote Connection Locations オブジェクトは、リモート接続のロケーションのレプリケーションに関する情報を提供します。次の表に、CUC Replicator: Remote Connection Locations カウンタに関する情報を示します。

表 112 : CUC Replicator: Remote Connection Locations

カウンタ	カウンタの説明
Dependencies Requests Received	Connection ロケーションから受信した要求されたレプリケーション依存関係の数。
Dependencies Requests Sent	Connection ロケーションへ送信したレプリケーション依存関係要求の数。
Message Receive Failures	障害のため受信されなかったこの Connection ロケーションからのレプリケーション メッセージの数。
Message Send Failures	障害のため送信されなかったこの Connection ロケーションへのレプリケーション メッセージの数。
Messages Received	Connection ロケーションから受信したレプリケーション メッセージの数。
Messages Sent	Connection ロケーションへ送信したレプリケーション メッセージの数。

カウンタ	カウンタの説明
NDR Messages Received	Connection ロケーションから受信したレプリケーション NDR メッセージの数。
USN Requests Received	Connection ロケーションから受信した USN 要求の数。これは通常、USN のタイムアウトがリモート ノードで発生したことを示します。

## CUC Sessions: Calendar Access

CUC Sessions: Calendar Access オブジェクトは、Cisco Unity Connection のカレンダーの統合に関する情報を提供します。次の表に、CUC Sessions: Calendar Access カウンタに関する情報を示します。

表 113 : CUC Sessions: Calendar Access

カウンタ	カウンタの説明
Connections To Exchange Failure - Total	Exchange 接続失敗の合計数。
Connections To MP Failure - Total	MeetingPlace 接続失敗の合計数。
Exchange Requests - Total	Exchange カレンダー要求の合計数。
Exchange Response Time [ms] - Current	ミリ秒単位での現在の Exchange 応答時間。
Meeting Join Request - Total	会議への参加要求の合計数。
MP Request - Total	MeetingPlace カレンダー要求の合計数。
MP Response Time [ms] - Current	ミリ秒単位での現在の MeetingPlace 応答時間。

## CUC Sessions: E-mail Access

CUC Sessions: E-mail Access オブジェクトは、電子メールの音声セッションに関する情報を提供します。次の表に、CUC Sessions: E-mail Access カウンタに関する情報を示します。

表 114 : CUC Sessions: E-mail Access

カウンタ	カウンタの説明
Messages Read - Total	Cisco Unity Connection の最後の再起動以降、読み取られた電子メール メッセージの合計数。
Session Duration Average [ms]	コール単位で測定されたすべての電子メールセッションの平均持続時間（ミリ秒単位）。
Session Duration Total [ms]	コール単位で測定されたすべてのメールセッションの合計持続時間（ミリ秒単位）。
Sessions - Current	アクティブな電子メール音声セッションの数。
Sessions - Total	Cisco Unity Connection の最後の再起動以降の電子メール音声セッションの合計数。

## CUC Sessions: IMAP Server

CUC Sessions: IMAP Server オブジェクトは、IMAP サーバに関する情報を提供します。次の表に、CUC Sessions: IMAP Server カウンタに関する情報を示します。

表 115 : CUC Sessions: IMAP Server

カウンタ	カウンタの説明
Commands per minute	1分あたりの IMAP コマンド数
Connection Length Average [s]	過去1分間における IMAP サーバへの接続の平均持続時間（秒）
Current IDLE Sessions	IMAP サーバ上のアイドルセッション数。
Errors Total	IMAP サーバの最後の再起動以降、IMAP サーバが返した IMAP エラーの合計数。
EXAMINE Requests Total	IMAP サーバの最後の再起動以降、IMAP サーバに送信された EXAMINE 要求の合計数。
Failed Login Requests Total	IMAP サーバの最後の再起動以降、IMAP サーバに送信されて失敗した LOGIN 要求の合計数。
FETCH Requests Total	IMAP サーバの最後の再起動以降、IMAP サーバに送信された FETCH 要求の合計数。



カウンタ	カウンタの説明
Login Requests Total	IMAP サーバの最後の再起動以降、IMAP サーバに送信された LOGIN 要求の合計数。
Logout Requests Total	IMAP サーバの最後の再起動以降、IMAP サーバに送信された LOGOUT 要求の合計数。
Messages Read Total	IMAP サーバの最後の再起動以降、メッセージの本文を返した IMAP FETCH コマンドの合計数。
Messages Read/hour	過去 1 時間にメッセージの本文を返した IMAP FETCH コマンドの数。
Messages/fetch Average	IMAP FETCH コマンドが返したメッセージの平均数。
NOOP Requests Total	IMAP サーバの最後の再起動以降、IMAP サーバに送信された NOOP 要求の合計数。
Response Time [ms]	IMAP コマンドの応答時間（ミリ秒）。
SEARCH Requests Total	IMAP サーバの最後の再起動以降、IMAP サーバに送信された SEARCH 要求の合計数。
Socket Connections Current	IMAP サーバへのアクティブなソケット接続の数。
Socket Connections Total	IMAP サーバの最後の再起動以降、IMAP サーバに対して実行されたソケット接続の合計数。
STARTTLS Requests Total	IMAP サーバの最後の再起動以降、IMAP サーバに送信された STARTTLS 要求の合計数。このカウンタは、クライアントが IMAP SSL ポートに直接接続したときに増加します。
STATUS Requests Total	IMAP サーバの最後の再起動以降、IMAP サーバに送信された STATUS 要求の合計数。
TLS Connections Current	IMAP サーバへのアクティブな Transport Layer Security 接続の数。
TLS Errors Total	IMAP サーバの最後の再起動以降の、IMAP サーバへの失敗した TLS 接続の合計数。
Unsolicited Notify Response Time Average [ms]	IMAP サーバに対する Unsolicited NOTIFY 応答時間の平均（ミリ秒）。

カウンタ	カウンタの説明
Unsolicited Notify Responses Total	IMAP サーバの最後の再起動以降、IMAP サーバによって返された Unsolicited Notify 応答の合計数。

## CUC Sessions: RSS

CUC Sessions: RSS オブジェクトは RSS セッションに関する情報を提供します。次の表に、CUC Sessions: RSS カウンタに関する情報を示します。

表 116 : CUC Sessions: RSS

カウンタ	カウンタの説明
RSS Messages Offered Total	ストリーミング用に提供された RSS メッセージの合計数。
RSS Messages Streamed Total	Cisco Unity Connection サーバがストリーム配信した RSS メッセージの合計数。
RSS Sessions Current	RSS セッションの現在の数。
RSS Sessions Total	RSS セッションの合計数。

## CUC Sessions: SMTP サーバ

CUC Sessions: SMTP Server オブジェクトは、SMTP サーバセッションに関する情報を提供します。次の表に、CUC Sessions: SMTP Server カウンタに関する情報を示します。

表 117 : CUC Sessions: SMTP サーバ

カウンタ	カウンタの説明
Total Delivered Messages	システムの起動以降に配信された SMTP メッセージの数。
[合計メッセージ数 (Total Messages) ]	システムの起動以降に配信または受信された SMTP メッセージの数。
Total Received Messages	システムの起動以降に受信された SMTP メッセージの数。

## CUC Sessions: SpeechView Processor

CUC Sessions: SpeechView Processor オブジェクトは、SpeechView プロセッサ サービスについての情報を提供します。次の表に、CUC Sessions: SpeechView Processor カウンタに関する情報を示します。

表 118 : CUC Sessions: SpeechView Processor

カウンタ	カウンタの説明
Average wait time	外部サービスから成功したトランスクリプションを受信するのに必要な平均時間。
Total failures	SpeechView Processor サービスの最後の再起動以降の失敗したトランスクリプションの合計数。
Total timeouts	SpeechView Processor サービスの最後の再起動以降、タイムアウトが発生したトランスクリプションの合計数。
Transcribed messages	SpeechView Processor サービスの最後の再起動以降の成功したトランスクリプションの合計数。

## CUC Sessions: TRaP

CUC Sessions: TRaP オブジェクトは、電話での録音および再生 (TRaP) セッションに関する情報を提供します。次の表に、CUC Sessions: TRaP カウンタに関する情報を示します。

表 119 : CUC Sessions: TRaP

カウンタ	カウンタの説明
Reverse TRaP Session Duration Average [s]	すべてのリバース TRaP セッションの平均持続時間 (秒)。
Reverse TRaP Session Duration Total [s]	すべてのリバース TRaP セッションの合計持続時間 (秒)。
Reverse TRaP Sessions Current	現在のアクティブなリバース TRaP セッションの数。
Reverse TRaP Sessions Total	Cisco Unity Connection の最後の起動以降のリバース TRaP セッションの合計数。
TRaP Session Duration Average [s]	すべての TRaP セッションの平均持続時間 (秒)。

カウンタ	カウンタの説明
TRaP Session Duration Total [s]	すべての TRaP セッションの合計持続時間 (秒)。
TRaP Sessions Current	現在のアクティブな TRaP セッションの数。
TRaP Sessions Total	Cisco Unity Connection の最後の起動以降の TRaP セッションの合計数。

## CUC Sessions: TTS

CUC Sessions: TTS オブジェクトは、音声合成 (TTS) セッションに関する情報を提供します。次の表に、CUC Sessions: TTS カウンタに関する情報を示します。

表 120 : CUC Sessions: TTS

カウンタ	カウンタの説明
Session Duration Average [s]	すべての TTS セッションの平均持続時間 (秒)。
Session Duration Total [s]	すべての TTS セッションの合計持続時間 (秒)。
Sessions Current	アクティブな TTS 音声セッションの現在の数。
Sessions Total	Cisco Unity Connection の最後の起動以降の TTS 音声セッションの合計数。

## CUC Sessions: Unified Client

CUC Sessions: Unified Client オブジェクトは、Cisco Unity Connection に対する Unified Client に関する情報を提供します。

Connections Total カウンタは、Unified Client IMAP 要求の合計数を表します。

## CUC Sessions: Video

CUC Sessions: Video オブジェクトは、ビデオサーバでのビデオセッションに関する情報を提供します。次の表に、CUC Sessions: Video カウンタに関する情報を示します。

表 121 : CUC Sessions: Video

カウンタ	カウンタの説明
Audio calls Negotiated Total	ビデオオファーに関係なくネゴシエートされた音声コールの合計数。
Audio Calls Negotiated In Last One Minute	過去1分間にビデオオファーに関係なくネゴシエートされた音声コールの合計数。
Outgoing Video calls Release Transfer	スイッチへのリリースとして転送された発信ビデオ コールの合計数。
Supervise Transfer Calls Total	Cisco Unity Connection の最後の再起動以降にビデオ コールから開始された監視転送の合計数。
Video calls downgraded to Audio Total	Cisco Unity Connection の最後の再起動以降に音声にダウングレードされたビデオ コールの合計数。
Video calls downgraded to Audio In Last One Minute	過去1分間に音声にダウングレードされたビデオ コールの合計数。
Video calls downgraded with prompt total	プロンプト「このコールの持続期間中のみ、音声を使用したビデオサービスを使用できません (Video services are not available using audio only for duration of this call)」によりダウングレードされたビデオ コールの合計数。
Video calls downgraded with prompt in Last One Minute	過去1分間に、プロンプト「このコールの持続期間中のみ、音声を使用したビデオサービスを使用できません (Video services are not available using audio only for duration of this call)」によりダウングレードされたビデオ コールの合計数。
Video Sessions Total	Unity Connection からビデオ サーバに送信されたビデオ セッション要求の合計数。
Video Sessions Current	Unity Connection からビデオ サーバに送信された現在のビデオ セッション要求の合計数。
Video Session Playbacks Total	Cisco Unity Connection の最後の再起動以降のビデオ セッション再生の合計数。
Video Session Playbacks Current	現在のビデオ セッション再生の合計数。

カウンタ	カウンタの説明
Video Media File Playbacks Total	Unity Connection の最後の再起動以降の、ビデオ サーバからのイメージ再生の合計数。
Video Media File Playbacks Current	ビデオ サーバからのビデオ メディア ファイル再生の現在の数。
Video Recordings Total	Unity Connection の最後の再起動以降、ビデオ サーバに保存されたビデオ録画の合計数。
Video Recordings Current	ビデオサーバに保存されたビデオ録画の現在の数。
Video Playback Completed Events from MS Total	Unity Connection の最後の再起動以降のビデオ再生完了イベントの合計数。
Video Playback Completed Events from MS In Last One Minute	直近1分以降のビデオサーバからのビデオ再生完了イベントの合計数。
Video Keep Alive Total	Unity Connection の最後の再起動以降、Unity Connection によってビデオサーバに送信されたキープアライブの合計数。
Video Keep Alive In Last One Minute	直近1分以降に Unity Connection によってビデオサーバに送信されたキープアライブの合計数。
Video Get Media Capabilities Total	Unity Connection の最後の再起動以降、Unity Connection によってビデオサーバに送信された GetMediaCapabilities の合計数。
Video Get Media Capabilities In Last One Minute	直近1分以降に Unity Connection によってビデオサーバに送信された GetMediaCapabilities の合計数。
Video SignIn Total	Unity Connection の最後の再起動以降、Unity Connection によってビデオサーバに送信されたサインイン要求の合計数。
Video SignIn Total In Last One Minute	直近1分以降に Unity Connection によってビデオサーバに送信されたサインイン要求の合計数。

カウンタ	カウンタの説明
KeyFrame Request sent Total	Cisco Unity Connection の最後の再起動以降、ビデオ録画中にエンドポイントに送信されたキーフレーム要求の合計数。
KeyFrame Request sent In Last One Minute	Cisco Unity Connection の最後の再起動以降、ビデオ録画中にエンドポイントに送信されたキーフレーム要求の合計数。
Video Record Successful Total	Cisco Unity Connection の最後の再起動以降、正常に完了したビデオ録画の合計数。
Video Sessions Failed Total	Cisco Unity Connection の最後の再起動以降、失敗したビデオセッションの合計数。
Video Session Failed In Last One Minute	過去1分間に失敗したビデオセッションの合計数。
Media Sense Timeout Total	Cisco Unity Connection の最後の再起動以降の、MediaSense サーバに接続中の接続タイムアウトエラーの合計数。このカウンタは、次のイベントに適用されます。 <ul style="list-style-type: none"> <li>• ビデオ コール中</li> <li>• サインイン時</li> <li>• MediaSense サーバによるメディア機能の交換中</li> </ul>
Video Play Failed Total	Cisco Unity Connection の最後の再起動以降に、音声メッセージとして再生されたビデオメッセージの合計数。

## CUC Sessions: Voice

CUC Sessions: Voice オブジェクトは、音声セッションに関する情報を提供します。次の表に、CUC Sessions: Voice カウンタに関する情報を示します。

表 122 : CUC Sessions: Voice

カウンタ	カウンタの説明
Delay - Directory Search [ms]	発信者がディレクトリ全体の検索を試みる時に発生する遅延（ミリ秒）。検索条件を入力してから結果が返されるまでの時間を測定します。
Delay - Opening Greeting [ms]	発信者が音声を聞くまでの遅延（ミリ秒）。システムがコールを受信してから、発信者に対して音声ストリームを開始するまでの時間を測定します。
Delay - Subscriber Delete Message [ms]	Cisco Unity Connection のサブスクライバがメッセージの削除を試みる時に発生する遅延（ミリ秒）。最後のメッセージ削除プロンプトから、削除の確認までの時間を測定します。
Delay - Subscriber Logon [ms]	Cisco Unity Connection のサブスクライバが認証を行う時に発生する遅延（ミリ秒）。
Delay - Subscriber Message Count [ms]	Cisco Unity Connection のサブスクライバが、サブスクライバのメッセージボックスでメッセージ数をカウントする時に発生する遅延（ミリ秒）。
Delay - Subscriber Message Header [ms]	発信者が Cisco Unity Connection でメッセージのヘッダー情報を収集する間に発生する遅延（ミリ秒）。
Failsafes Total	フェールセーフ カンバセーションが再生された回数の合計。
G.711a Sessions Current	アクティブ G.711 (a-law) 音声セッションの現在の数。
G.711a Sessions Total	Cisco Unity Connection の最後の再起動以降のアクティブ G.711 (a-law) 音声セッションの合計数。
G.711u Sessions Current	アクティブ G.711 (u-law) 音声セッションの現在の数。
G.711u Sessions Total	Cisco Unity Connection の最後の再起動以降のアクティブ G.711 (u-law) 音声セッションの合計数。
G.722 Sessions Current	アクティブ G.722 音声セッションの現在の数。
G.722 Sessions Total	Cisco Unity Connection の最後の再起動以降のアクティブ G.722 音声セッションの合計数。
G.729 Sessions Current	アクティブ G.729 音声セッションの現在の数。
G.729 Sessions Total	Cisco Unity Connection の最後の再起動以降のアクティブ G.729 音声セッションの合計数。



カウンタ	カウンタの説明
iLBC Sessions Current	アクティブ iLBC 音声セッションの現在の数。
iLBC Sessions Total	Cisco Unity Connection の最後の再起動以降のアクティブ iLBC 音声セッションの合計数。
Meeting search delay delay [ms]	Cisco Unity Connection のサブスクライバが会議を検索するために発生する遅延 (ミリ秒)。
Messages Deleted	Cisco Unity Connection が最後に再起動された時からの、TUI によって削除された音声メッセージの合計数。
Messages Forwarded	Cisco Unity Connection が最後に再起動された時からの、TUI によって転送された音声メッセージの合計数。
Messages Read	Cisco Unity Connection が最後に再起動された時からの、TUI によって読み取られた音声メッセージの合計数。
Messages Replied	Cisco Unity Connection が最後に再起動された時からの、TUI によって応答を受信された音声メッセージの合計数。
Messages Sent	Cisco Unity Connection が最後に再起動された時からの、TUI によって送信された音声メッセージの合計数。
MRCP Define Grammar Delay [ms]	MRCP 定義文法要求に応答するまでの遅延 (ミリ秒単位)。
MRCP Define Grammar Delay Average [ms]	MRCP 定義文法要求に応答するまでの平均遅延 (ミリ秒)。
MRCP Define Grammar Delay Max [ms]	MRCP 定義文法要求に応答するまでの最大遅延 (ミリ秒)。
MRCP Delay [ms]	MRCP 要求に応答するまでの遅延 (ミリ秒)。
MRCP Delay Average [ms]	MRCP 要求に応答するまでの平均遅延 (ミリ秒)。
MRCP Delay Max [ms]	MRCP 要求に応答するまでの最大遅延 (ミリ秒)。
Sessions Current	コーデックのアクティブな音声セッションの現在の数。
Sessions Total	Cisco Unity Connection の最後の再起動以降の、任意のコーデックの音声セッションの総数 (G.711 mu-law と G.729)。
Subscriber Lookup Delay [ms]	Cisco Unity Connection サブスクライバが DTMF ID でサブスクライバを検索し、ロードするために発生する遅延 (ミリ秒)。

## CUC Sessions: VUI

CUC Sessions: VUI オブジェクトは、音声ユーザ インターフェイス (VUI) に関する情報を提供します。次の表には、CUC Sessions: VUI カウンタに関する情報が含まれます。

表 123 : CUC Sessions: VUI

カウンタ	カウンタの説明
Delay - Subscriber Message Access [ms]	ユーザがメッセージにアクセスしようとしたときに発生する遅延 (ミリ秒)。このカウンタは、メッセージを聞くことを指示する音声コマンドが発行されてから、メッセージが実際に再生されるまでの時間を測定します。
Matches Total	VUI カンバセーションでの一致数の合計。
Messages Read	Cisco Unity Connection が最後に再起動された時からの、VUI によって読み取られたメッセージの合計数。
No-matches Total	VUI カンバセーションでの不一致の数の合計。
Session Duration Average/call [s]	コール単位で測定された VUI セッションの平均持続時間 (秒)。
Session Duration Total [s]	すべての VUI セッションの持続時間 (秒)。
Sessions Current	任意のコーデックでのアクティブな VUI セッションの現在の数。
Sessions Total	任意のコーデックでの VUI セッションと音声セッションの数の合計。

## CUC Sessions: Web

CUC Sessions: Web オブジェクトは、Cisco Personal Communications Assistant (Cisco PCA) セッションと Cisco Unity Connection の管理セッションについての情報を提供します。次の表に、CUC Sessions: Web カウンタに関する情報を示します。

表 124 : CUC Sessions: Web

カウンタ	カウンタの説明
CPCA Authentication Delay Max [s]	ユーザーの受信トレイまたはアシスタントへの認証の最大遅延 (秒)。

カウンタ	カウンタの説明
CPCA Failed Authentications Total	失敗した認証の数。
CPCA Pages Served Total	Cisco Unity Connection サーバによって処理された CPCA の総ページ数。
CPCA Requests In Queue Current	CPCA キューで処理を待っている要求の数。
CPCA Server Busy Pages Total	Cisco Unity Connection サーバによって処理が戻されたサーバビジー状態の総ページ数。
CPCA Sessions Current	CPCA セッションの現在の数。
CPCA Sessions Total	CPCA セッションの合計数。
CPCA Authentication Delay Max [s]	[システム管理者 (System Administrator) ] ウィンドウの認証の最大遅延 (秒) 。
CUCA Response Time Max [ms]	指定された要求に応答するための tomcat サーバに対する最大時間 (ミリ秒単位) 。

## CUC Sessions: Web E-mail Access

CUC Sessions: Web E-mail Access オブジェクトは、Web 電子メールのアクセスセッション (IMAP) に関する情報を提供します。次の表には、CUC Sessions: Web E-mail Access カウンタについての情報が含まれます。

表 125 : CUC Sessions: Web E-mail Access

カウンタ	カウンタの説明
Messages Read - Total	Cisco Unity Connection の最後の再起動以降、読み取られた電子メール メッセージの合計数。
Session Duration Average [ms]	コール単位で測定されたすべての電子メール セッションの平均持続時間 (ミリ秒単位) 。
Session Duration Total [ms]	コール単位で測定されたすべてのメール セッションの合計持続時間 (ミリ秒単位) 。
Sessions - Current	アクティブな電子メール音声セッションの数。
Sessions - Total	Cisco Unity Connection の最後の再起動以降の電子メール音声セッションの合計数。

## CUC System Agent

CUC System Agent オブジェクトは、システムの定期的タスクに関する情報を記録します。次の表に、CUC System Agent カウンタに関する情報を示します。

カウンタ	カウンタの説明
Message Related Files Shredded Total	削除されたメッセージ関連ファイルの合計数。
Message Related Files Shredded Failed	削除に失敗したメッセージ関連ファイルの合計数
Total Number of Requests sent by HTTP[S]/CCI Link	リーダーにより送信された HTTP (S) 要求の累計数。
Total Number of successful response of HTTP[S]/CCI Requests	フィーダにより正常に処理された HTTP (S) 要求の累計数。
Total Number of failure response of HTTP[S]/CCI Requests	フィーダにより正常に処理されなかった HTTP (S) 要求の累計数。
Total Number of Directory Objects Successfully Processed	正常に処理されたディレクトリ オブジェクトの累計数。
Directory Objects Processed Successfully In Last One Minute	1分あたりの正常に処理されたディレクトリ オブジェクト。
Delete Request sent to Media Sense Total	Unity Connection の最後の再起動以降に MediaSense サーバに送信された削除要求の合計数。
Media Sense Timeout While Delete Total	Unity Connection の最後の再起動以降に MediaSense サーバに送信された削除要求への応答での接続タイムアウトの合計数。

# システム アラート

## AuthenticationFailed

認証では、ログイン時に送信されたユーザ ID とパスワードが検証されます。無効なユーザ ID および/またはパスワードが使用された場合、アラームが生成されます。

### デフォルト設定

表 126 : *AuthenticationFailed RTMT* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の頻度を越えた AuthenticationFailed イベントの数 最近 1 分間に 1 回
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## CiscoDRFFailure

このアラートは、障害回復フレームワーク (DRF) バックアップまたは復元処理でエラーが発生したときに生成されます。

## デフォルト設定

表 127 : CiscoDRFFailure RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 CiscoDRFFailure イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## CoreDumpFileFound

このアラートは、CoreDumpFileFound イベントが生成されたときに発生します。このアラートは、コア アンプ ファイルがシステムに存在することを示します。

## デフォルト設定

表 128 : CoreDumpFileFound RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効

値	デフォルト設定
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 CoreDumpFileFound イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Trace download Parameters	オフ
Enable Email	オン
Trigger Alert Action	デフォルト

## CpuPegging

CPU 使用率は、設定可能なしきい値に基づいてモニタされます。使用率が、設定されているしきい値を上回ると、このアラートが生成されます。

### デフォルト設定

表 129 : CpuPegging RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 99%
時間 (Duration)	値がしきい値を 60 秒間継続的に下回った場合または超えた場合にだけアラートをトリガーする
頻度 (Frequency)	30 分以内に最大 3 回のアラートをトリガーする

値	デフォルト設定
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## CriticalServiceDown

CriticalServiceDown アラートは、サービスのステータスがダウン状態の場合に生成されます（その他の状態の場合には生成されません）。

### デフォルト設定

表 130 : CriticalServiceDown RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 サービス ステータスが DOWN である
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Trace download Parameters	[Enable Trace Download] はオフになっている
Enable Email	オン
Trigger Alert Action	デフォルト



## DBChangeNotifyFailure

このアラートは、Cisco Database Notification サービスに問題が発生し、このサービスが停止する可能性がある場合に発生します。この状態は、データベース内でキューに入れられている変更通知要求が停止し、システムに加えられた変更内容が有効にならないことを示します。アラートが存在するノードで Cisco Database Layer Monitor が実行されているかどうかを確認します。実行されている場合、このサービスを再起動します。サービスを再起動してもこのアラートが安全な範囲に戻らない場合、**show tech notify** および **show tech dbstateinfo** の出力を収集し、対処方法についてシスコ テクニカル アシスタンス センター (TAC) までお問い合わせください。

### デフォルト設定

表 131 : *DBChangeNotifyFailure* RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 DBChangeNotify キューの遅延が 2 分を超えている
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	30 分以内に最大 1 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## DBReplicationFailure

このアラームは、Informix Dynamic Server (IDS) の複製に障害があることを示し、データベース管理者の介入を必要とします。



(注) DBReplicationFailure は、（従来の DBReplicationFailure アラームではなく）複製ステータス perfmon カウンタに基づいていることに注意してください。このアラートは、対応する複製ステータス perfmon カウンタの値が **3**（不正な複製）または **4**（複製の設定失敗）になったときにトリガーされます。

### デフォルト設定

表 132 : DBReplicationFailure RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 DBReplicationFailure が発生した
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	60 分以内に最大 1 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## DBReplicationTableOutOfSync

### デフォルト設定

表 133 : DBReplicationTableOutOfSync RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン

値	デフォルト設定
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 アラーム番号 888 の IDSReplicationFailure イベントが生成された。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	60 分以内に最大 1 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## HardwareFailure

このアラートは、ハードウェア障害イベント（ディスク ドライブの障害、電源の障害など）がトリガーされたときに発生します。

### デフォルト設定

表 134 : **HardwareFailure RTMT** アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 HardwareFailure イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする

値	デフォルト設定
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## LogFileSearchStringFound

このアラートは、LogFileSearchStringFound イベントが生成されたときに発生します。これは、検索文字列がログ ファイル中に見つかったことを示します。

### デフォルト設定

表 135 : LogFileSearchStringFound RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	警告
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 LogFileSearchStringFound イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## LogPartitionHighWaterMarkExceeded

このアラートは、ログパーティションの使用済みディスク領域のパーセンテージが、設定された上限を超えると発生します。このアラートが生成された場合、Log Partition Monitoring Tool (LPM) はログパーティション中のファイルを削除し（下限に達するまで）、ディスク領域が不足するのを防ぎます。



(注) LPM により、保持しておきたいファイルが削除される可能性があります。LogPartitionLowWaterMarkExceeded アラートを受信した場合はすぐに対処してください。

### デフォルト設定

表 136 : LogPartitionHighWaterMarkExceeded RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 ログパーティションの使用済みディスク領域が上限 (95%) を超えている
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## LogPartitionLowWaterMarkExceeded

このアラートは、LogPartitionLowWaterMarkExceeded イベントが生成されたときに発生します。これは、ログパーティションの使用済みディスク領域のパーセンテージが、設定されている下限を超えたことを示します。



(注) このアラートは早期に発生する警告であることに注意してください。管理者は、ディスク領域を空ける作業を開始する必要があります。RTMT/TLCを使用すると、トレースおよびログファイルの収集や、サーバからの削除を行うことができます。管理者は、再度下限を超えないように、トレース ファイルの数を調整することを推奨します。

## デフォルト設定

表 137 : *LogPartitionLowWaterMarkExceeded RTMT* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 ログ パーティションの使用済みディスク領域が下限 (90%) を超えている
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## LowActivePartitionAvailableDiskSpace

このアラートは、アクティブ パーティションの利用可能なディスク領域のパーセンテージが、設定されている値を下回ると発生します。

## デフォルト設定

表 138 : *LowActivePartitionAvailableDiskSpace RTMT* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 アクティブパーティションの利用可能ディスク領域が (4%) 未満である
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	30 分以内に最大 3 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## LowAvailableVirtualMemory

RTMT は、仮想メモリの使用率をモニタしています。メモリが少なくなると、LowAvailableVirtualMemory アラートが生成されます。

## デフォルト設定

表 139 : *LowAvailableVirtualMemory RTMT* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効

値	デフォルト設定
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 利用可能な仮想メモリが (30%) 未満である
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	30 分以内に最大 3 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## LowInactivePartitionAvailableDiskSpace

このアラートは、非アクティブパーティションの利用可能なディスク領域のパーセンテージが、設定されている値を下回ると発生します。

### デフォルト設定

表 140 : LowInactivePartitionAvailableDiskSpace RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 非アクティブパーティションの利用可能ディスク領域が (4%) 未満である
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	30 分以内に最大 3 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン



値	デフォルト設定
Trigger Alert Action	デフォルト

## LowSwapPartitionAvailableDiskSpace

このアラートは、スワップパーティションの利用可能ディスク領域が少ないことを示します。



(注)

スワップパーティションは仮想メモリの一部なので、スワップパーティションとして利用可能なディスク領域が不足すると仮想メモリも不足することになります。

### デフォルト設定

表 141 : LowSwapPartitionAvailableDiskSpace RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 スワップパーティションの利用可能ディスク領域が (10%) 未満である
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	30 分以内に最大 3 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## ServerDown

このアラートは、リモート ノードに到達できない場合に発生します。



- (注) Unified Communications Manager および IM and Presence Service : ServerDown アラートは、現在アクティブな AMC (プライマリ AMC、またはプライマリ AMC が使用不可の場合にはバックアップ AMC) がクラスタ内の別のサーバに到達できない場合に生成されます。このアラートは、サーバダウン状態以外に、ネットワーク接続の問題も示します。

### デフォルト設定

表 142 : ServerDown RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 ServerDown が発生した
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	60 分以内に最大 1 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## SparePartitionHighWaterMarkExceeded

このアラートは、SparePartitionHighWaterMarkExceeded イベントが生成されたときに発生します。このアラートは、予備パーティション内の使用済みディスク領域のパーセンテージが、設定されている上限を超えたことを示します。

## デフォルト設定

表 143 : SparePartitionHighWaterMarkExceeded RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 予備パーティションの使用済みディスク領域が上限 (95%) を超えている
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## SparePartitionLowWaterMarkExceeded

このアラートは、SparePartitionLowWaterMarkExceeded イベントが生成されたときに発生します。このアラートは、予備パーティションの使用済みディスク領域のパーセンテージが、下限しきい値を超えたことを示します。

## デフォルト設定

表 144 : SparePartitionLowWaterMarkExceeded RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)

値	デフォルト設定
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 予備パーティションの使用済みディスク領域が下限 (90%) を超えている
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## SyslogSeverityMatchFound

このアラートは、SyslogSeverityMatchFound イベントが生成されたときに発生します。このアラートは、一致する重大度を含む syslog メッセージが存在することを示します。

### デフォルト設定

表 145 : SyslogSeverityMatchFound RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 SyslogSeverityMatchFound イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする

値	デフォルト設定
スケジュール	毎日 24 時間
Syslog Severity Parameters	クリティカル (Critical)
Enable Email	オン
Trigger Alert Action	デフォルト

## SyslogStringMatchFound

このアラートは、SyslogStringMatchFound イベントが生成されたときに発生します。このアラートは、一致する検索文字列を含む syslog メッセージが存在することを示します。

### デフォルト設定

表 146 : SyslogStringMatchFound RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 SyslogStringMatchFound イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Syslog Alert Parameters	(検索文字列のテキスト ボックス)
Enable Email	オン
Trigger Alert Action	デフォルト

## SystemVersionMismatched

このアラートは、システムのバージョンが一致しない場合に発生します。

デフォルト設定

表 147: SystemVersionMismatched RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 SystemVersionMismatched が発生した
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	60 分以内に最大 1 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## TotalProcessesAndThreadsExceededThreshold

このアラートは、TotalProcessesAndThreadsExceededThreshold イベントが生成されたときに発生します。このアラートは、プロセスおよびスレッドの現在の合計数が、Cisco RIS Data Collector サービスパラメータに設定されている最大タスク数を超過していることを示します。この場合、プロセスがリークしているか、プロセスでスレッドリークが発生している可能性があります。

## デフォルト設定

表 148 : *TotalProcessesAndThreadsExceededThreshold RTMT* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 TotalProcessesAndThreadsExceededThreshold イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## 音声およびビデオ アラート

**BeginThrottlingCallListBLFSubscriptions**

このアラートは、BeginThrottlingCallListBLFSubscriptions イベントが生成されたときに発生します。これは、システムの過負荷を避けるために、Cisco Unified Communications Manager が CallList BLF サブスクリプションの制御を開始したことを示します。

## デフォルト設定

表 149 : *BeginThrottlingCallListBLFSubscriptions RTMT* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン

値	デフォルト設定
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 BeginThrottlingCallListBLFSubscriptions イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## CallAttemptBlockedByPolicy

### デフォルト設定

表 150 : CallAttemptBlockedByPolicy RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	警告
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 CallAttemptBlockedByPolicy イベントが生成された。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	30 分以内に最大 3 回のアラートをトリガーする



値	デフォルト設定
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## CallProcessingNodeCpuPegging

このアラートは、コール処理サーバの CPU 負荷率が、設定された時間で設定された割合を超えたときに発生します。

管理者が対処しない場合、特に CallManager サービスで、CPU の高い使用率が原因で Cisco Unified Communications Manager がクラッシュするおそれがあります。CallProcessingNodeCpuPegging アラートにより、クラッシュを未然に防ぐことができます。

CPU 使用率が急上昇する場合、CallProcessingNodeCpuPegging に加えて、CoreDumpFound アラーム、CriticalServiceDown アラーム、SDLLinkOutOfService アラーム、および NumberOfRegisteredPhonesDropped alarms アラームなどの他のアラームが発行される場合があります。



- (注) Cisco Unified Communications Manager の VMware インストール時に DRF バックアップや管理ツールの一括エクスポートなどのタスクを実行すると、CPU 使用率が急上昇する場合があります。一般に、CPU 使用率の急上昇の原因となるプロセスは、gzip および DRFLocal です。
- システムが CallProcessingNodeCpuPegging アラームを生成する場合は、システムの Open Virtualization Archive (OVA) テンプレートの仕様に従い、Cisco Unified Communications Manager で 7500 人のユーザをサポートするための vCPU を追加します。

### デフォルト設定

表 151 : CallProcessingNodeCpuPegging RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効

値	デフォルト設定
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 プロセッサの負荷が (90%) を超えている
時間 (Duration)	値がしきい値を 60 秒間継続的に下回った場合または超えた場合にだけアラートをトリガーする
頻度 (Frequency)	30 分以内に最大 3 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## CARSchedulerJobFailed

### デフォルト設定

表 152 : CARSchedulerJobFailed RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	エラー (Error)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 CARSchedulerJobFailed イベントが生成された。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## CARIDSEngineCritical

### デフォルト設定

表 153 : CARIDSEngineCritical RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 CARIDSEngineCritical イベントが生成された。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## CARIDSEngineFailure

### デフォルト設定

表 154 : CARIDSEngineFailure RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	エラー (Error)

値	デフォルト設定
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 CARIDSEngineFailure イベントが生成された。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## CDRAgentSendFileFailed

このアラートは、CDR Agent が Cisco Unified Communications Manager ノードから Cisco Unified Communications Manager クラスタ内の CDR リポジトリ ノードに CDR ファイルを送信できない場合に発生します。

### デフォルト設定

表 155 : CDRAgentSendFileFailed RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 CDRAgentSendFileFailed イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする

値	デフォルト設定
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## CDRFileDeliveryFailed

このアラートは、外部の課金サーバへの CDR ファイルの FTP 配信が失敗した場合に発生します。

### デフォルト設定

表 156 : CDRFileDeliveryFailed RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 CDRFileDeliveryFailed イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## CDRHighWaterMarkExceeded

このアラートは、CDR ファイルの上限を超えた場合に発生します。また、このアラートは、正常に配信された CDR ファイルのいくつかが消滅されたことも示します。

## デフォルト設定

表 157 : CDRHighWaterMarkExceeded RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 CDRHighWaterMarkExceeded イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## CDRMaximumDiskSpaceExceeded

このアラームは、CDR ファイルのディスク使用率が最大ディスク割り当てを超えたときに発生します。また、このアラームは、未配信のファイルがいくつか削除されたことも示します。

## デフォルト設定

表 158 : CDRMaximumDiskSpaceExceeded RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効

値	デフォルト設定
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 CDRMaximumDiskSpaceExceeded イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## CiscoElmNotConnected

### デフォルト設定

表 159 : *CiscoElmNotConnected RTMT* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	警告
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 CiscoElmNotConnected イベントが生成された。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## CiscoGraceTimeLeft

### デフォルト設定

表 160 : CiscoGraceTimeLeft RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	情報 (Informational)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 CiscoGraceTimeLeft イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## CiscoNoProvisionTimeout

### デフォルト設定

表 161 : CiscoNoProvisionTimeout RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	エラー (Error)



値	デフォルト設定
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 CiscoNoProvisionTimeout イベントが生成された。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## CiscoSystemInDemo

### デフォルト設定

表 162 : CiscoSystemInDemo RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	警告
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 CiscoSystemInDemo イベントが生成された。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間

値	デフォルト設定
Enable Email	オン
Trigger Alert Action	デフォルト

## CiscoSystemInOverage

### デフォルト設定

表 163 : CiscoSystemInOverage RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	警告
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 CiscoSystemInOverage イベントが生成された。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## CiscoSystemSecurityMismatch

### デフォルト設定

表 164 : CiscoSystemSecurityMismatch RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	警告
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 CiscoSystemSecurityMismatch イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## CodeYellow

AverageExpectedDelay カウンタは、着信メッセージを処理する現在の平均予測遅延を表します。値が Code Yellow Entry Latency サービスパラメータで指定されている値を超えた場合、CodeYellow アラームが生成されます。CodeYellow アラートは、トラブルシューティングの目的でトレースファイルをダウンロードするように設定できます。

### デフォルト設定

表 165 : CodeYellow RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン

値	デフォルト設定
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 Cisco CallManager CodeYellowEntry イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Trace download Parameters	[Enable Trace Download] はオフになっている
Enable Email	オン
Trigger Alert Action	デフォルト

## DDRBlockPrevention

このアラートは、アラーム番号 31 の `IDSReplicationFailure` アラームが発生したときにトリガーされます。このアラームは、サービスの拒否を避けるための予防的なプロシージャを呼び出します。このプロシージャはコール処理に影響を与えないので、このプロセス中に複製アラームを無視できます。

このプロシージャは、完了するまでに最大 60 分かかります。このプロシージャが完了したことを確認するには、各ノードの `RTMT` 複製ステータスが 2 になっていることを確認します。このプロセス中にシステムをリブートしないでください。

### デフォルト設定

表 166 : *DDRBlockPrevention RTMT* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)

値	デフォルト設定
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 アラーム番号 31 の IDSReplicationFailure アラームが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	60 分以内に最大 1 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## DDRDown

このアラートは、アラーム番号 32 の IDSReplicationFailure アラームが発生したときにトリガーされます。バックグラウンドで自動回復プロシージャが実行されるので、対処は必要ありません。

このプロシージャは、完了するまでに約15分かかります。このプロシージャが完了したことを確認するには、各ノードの RTMT 複製ステータスが 2 になっていることを確認します。

### デフォルト設定

表 167 : DDRDown RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 アラーム番号 32 の IDSReplicationFailure アラームが生成された
時間 (Duration)	すぐにアラートをトリガーする

値	デフォルト設定
頻度 (Frequency)	60 分以内に最大 1 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## EMCCFailedInLocalCluster

### デフォルト設定

表 168 : *EMCCFailedInLocalCluster RTMT* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	エラー (Error)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 EMCCFailedInLocalCluster イベントが生成された。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	30 分以内に最大 3 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## EMCCFailedInRemoteCluster

### デフォルト設定

表 169 : EMCCFailedInRemoteCluster RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	警告
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 EMCCFailedInRemoteCluster イベントが生成された。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	30 分以内に最大 3 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## ExcessiveVoiceQualityReports

このアラートは、設定されている時間間隔中に報告された Quality Report Tool (QRT) の回数が、設定されている値を超えたときに生成されます。デフォルトのしきい値は、60 分以内に 0 回です。

### デフォルト設定

表 170 : ExcessiveVoiceQualityReports RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン

値	デフォルト設定
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 品質レポートの回数が最近 60 分間で 0 回を超えている
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## ILSHubClusterUnreachable

### デフォルト設定

表 171 : ILSHubClusterUnreachable RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	アラート (Alert)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 リモート ILS サーバとの接続を確立できない。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする



値	デフォルト設定
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## ILSPwdAuthenticationFailed

### デフォルト設定

表 172 : *ILSPwdAuthenticationFailed RTMT* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	アラート (Alert)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 リモート クラスタでの ILS によるパスワード認証の失敗。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## ILSTLSAuthenticationFailed

### デフォルト設定

表 173 : *ILSTLSAuthenticationFailed RTMT* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	アラート (Alert)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 リモート クラスタで ILS への TLS 障害が発生した。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## IMEDistributedCachelnactive

このアラームは、Cisco Unified Communications Manager が Cisco IME サーバに接続を試行したものの、IME 分散キャッシュがアクティブでない場合に生成されます。

Cisco IME サーバの証明書がプロビジョニングされていることと、IME 分散キャッシュがアクティブ化されていることを CLI を使用して確認します。

### デフォルト設定

表 174 : *IMEDistributedCachelnactive* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン

値	デフォルト設定
重大度 (Severity)	エラー (Error)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 非アクティブな IME 分散キャッシュ
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## IMEOverQuota

このアラートは、この Cisco IME サービスを使用する Cisco Unified Communications Manager サーバが、IME 分散キャッシュに対してパブリッシュされたダイヤルイン (DID) 数の割り当てを超えたことを示します。アラートには、Cisco IME サーバの名前に加え、現在およびターゲットの割り当て値が含まれます。

この Cisco IME サービスを使用するすべての Cisco Unified Communications Manager サーバで DID プレフィックスが正しくプロビジョニングされていることを確認します。

プレフィックスが正しくプロビジョニングされている場合は、Cisco IME サービスの容量を超えています。サービスをもう 1 つ設定し、異なる Cisco IME サービス上の Cisco IME クライアントインスタンス (Cisco Unified Communications Manager) に DID プレフィックスを分割する必要があります。

### デフォルト設定

表 175: IMEOverQuota アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	アラート (Alert)

値	デフォルト設定
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 VAP 割り当て超過
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## IMEQualityAlert

このアラートは、IP ネットワーク品質の問題によってかなりの数の Cisco IME コールが PSTN にフェールバックされたか、コールが確立されなかったことを Cisco Unified Communications Manager が特定したときに生成されます。このアラートは次の 2 種類のイベントによってトリガーされます。

- 現在アクティブな多数の Cisco IME コールがすべてフェールバックを要求した、または PSTN にフェールバックされた場合。
- 直近の多数のコールの試行が PSTN に送信されたが、IP 上に確立されなかった場合。

このアラートを受信したときは、IP 接続を確認します。IP 接続に問題がない場合、CDR、CMR、およびファイアウォールのログを確認し、コールが PSTN にフェールバックされた理由または IP 上に確立されなかった理由を判別します。

### デフォルト設定

表 176 : *IMEQualityAlert* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	エラー (Error)

値	デフォルト設定
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 Cisco IME リンク品質の問題
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## InsufficientFallbackIdentifiers

このアラートは、同一のフォールバック DID を使用する現在進行中の Cisco IME コールが多すぎて、Cisco Unified Communications Manager が処理している新しい Cisco IME コールに割り当てる DTMF デジタルシーケンスが足りないときに生成されます。新しいコールは継続しますが、音声品質が低下しても PSTN にフォールバックすることができません。

このアラームが生成された場合、このコールに関連付けるフォールバック プロファイルを確認します。Cisco Unified Communications Manager の管理ページでプロファイルを確認し、[**関連 DTMF 番号のフォールバック番号 (Fallback Number of Correlation DTMF Digits)**] フィールドの現在の設定を調べます。このフィールドの値を 1 つ上げて、新しい値によってこれらのアラートが解消されるかどうかを確認します。一般に、このパラメータは十分大きい値にする必要があり、このプロファイルに関連付ける登録数に対して作成された Cisco IME 同時コール数が、この登録数を指数とする 10 の累乗の値よりも常にずっと低くなるようにします。たとえば、このフォールバック プロファイルに関連付けるパターンの Cisco IME 同時コール数が常に 10,000 未満である場合、この値を 5 に設定する (10 の 5 乗は 100,000) ことで、Cisco Unified Communications Manager からこのアラートが生成されなくなります。

ただし、この値を大きくすると、フォールバックに要する時間が若干長くなります。このため、[**関連 DTMF 番号のフォールバック番号 (Fallback Number of Correlation DTMF Digits)**] フィールドの値は、このアラートが生成されない程度に大きい値を設定する必要があります。

DTMF デジタルフィールドの値を大きくする代わりに、異なるフォールバック DID を持つ別のフォールバック プロファイルを追加して、より少ない数の登録パターンをそのフォールバック プロファイルに関連付けることができます。この方法を使用すると、より少ない桁数を使用できます。

## デフォルト設定

表 177 : *InsufficientFallbackIdentifiers* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	エラー (Error)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 フォールバック ID を割り当てることができない
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	1 分以内に最大 1 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## IMEServiceStatus

このアラートは、特定の Cisco IME クライアント インスタンス (Cisco Unified Communications Manager) の Cisco IME サービスに対する接続の全体的な健全性を示します。アラートは次の状態を示します。

- 0 : 不明。Cisco IME サービスがアクティブ化されていないことを示している可能性があります。
- 1 : 健全。Cisco Unified Communications Manager が Cisco IME クライアント インスタンスのプライマリおよびバックアップサーバ (設定されている場合) への接続を正常に確立したことを示します。
- 2 : 動作不良。Cisco IME はアクティブ化されているが、Cisco IME サーバとのハンドシェイク手順を正常に完了していないことを示します。このカウンタの値はプライマリ IME サーバとセカンダリ IME サーバの両方のハンドシェイク ステータスを反映していることに注意してください。

## デフォルト設定

表 178 : *IMServiceStatus* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 VAP 接続の問題
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	60 分ごとに最大 1 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## InvalidCredentials

このアラートは、Cisco Unified Communications Manager で設定されたユーザ名とパスワードが Cisco IME サーバで設定されたものと一致しないために、Cisco Unified Communications Manager が Cisco IME サーバに接続できないことを示します。

アラートには、Cisco IME サーバへの接続に使用されたユーザ名とパスワードに加え、ターゲット Cisco IME サーバの IP アドレスおよび名前が含まれます。このアラートを解決するには、Cisco IME サーバにログインし、設定されているユーザ名およびパスワードが Cisco Unified Communications Manager で設定されているユーザ名およびパスワードと一致することを確認します。

## デフォルト設定

表 179 : *InvalidCredentials* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン

値	デフォルト設定
重大度 (Severity)	アラート (Alert)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 Cisco IME サーバへのクレデンシャルが失敗した
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## LocationOutOfResource

このアラートは、LocationOutOfResource イベントの回数が、設定されている時間間隔中に、設定されているしきい値を超えたときに発生します。これは、ロケーションまたはリンクの音声、ビデオ、またはイマーシブ帯域幅のいずれか、またはすべてが使い尽くされたことを示します。

### デフォルト設定

表 180 : LocationOutOfResource アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	警告
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーします： LocationOutOfResource イベントが 60 秒以内に 5 回生成された
時間 (Duration)	すぐにアラートをトリガーする



値	デフォルト設定
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## MaliciousCallTrace

これは、Cisco Unified Communications Manager に迷惑呼が存在することを示します。迷惑呼の識別 (MCID) 機能が呼び出されます。

### デフォルト設定

表 181 : *MaliciousCallTrace RTMT* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 迷惑呼トレースが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## MediaListExhausted

このアラートは、MediaListExhausted イベントの回数が、設定されている時間間隔中に、設定されているしきい値を超えたときに発生します。このアラートは、メディア リストで定義されている使用可能なメディア リソースがすべて使用中であることを示します。デフォルトの値は、60 分以内に 0 回です。

### デフォルト設定

表 182 : MediaListExhausted RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	警告
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 MediaListExhausted イベントの回数が最近 60 分間で 0 回を超えている
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## MgcpDChannelOutOfService

このアラートは、メディア ゲートウェイ コントロール プロトコル (BRI) D チャネルがアウトオブサービスのままである場合にトリガーされます。

## デフォルト設定

表 183 : *MgcpDChannelOutOfService RTMT* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 MGCP DChannel がアウト オブ サービスである
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## NumberOfRegisteredDevicesExceeded

このアラートは、NumberOfRegisteredDevicesExceeded イベントが生成されたときに発生します。

## デフォルト設定

表 184 : *NumberOfRegisteredDevicesExceeded RTMT* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効

値	デフォルト設定
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 NumberOfRegisteredDevicesExceeded イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## NumberOfRegisteredGatewaysDecreased

このアラートは、クラスタに登録されたゲートウェイの数が、連続したポーリング間で減少したときに発生します。

### デフォルト設定

表 185 : NumberOfRegisteredGatewaysDecreased RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 登録されたゲートウェイの数が減少した
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン

値	デフォルト設定
Trigger Alert Action	デフォルト

## NumberOfRegisteredGatewaysIncreased

このアラートは、クラスタに登録されたゲートウェイの数が、連続したポーリング間で増加したときに発生します。

### デフォルト設定

表 186 : *NumberOfRegisteredGatewaysIncreased* RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 登録されたゲートウェイの数が増加した
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## NumberOfRegisteredMediaDevicesDecreased

このアラートは、クラスタに登録されたメディア デバイスの数が、連続したポーリング間で減少したときに発生します。

## デフォルト設定

表 187 : *NumberOfRegisteredMediaDevicesDecreased* RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 登録されたメディア デバイスの数が減少した
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## NumberOfRegisteredMediaDevicesIncreased

このアラートは、クラスタに登録されたメディア デバイスの数が、連続したポーリング間で増加したときに発生します。

## デフォルト設定

表 188 : *NumberOfRegisteredMediaDevicesIncreased* RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 登録されたメディア デバイスの数が増加した
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする

値	デフォルト設定
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## NumberOfRegisteredPhonesDropped

このアラートは、クラスタに登録された電話機の数、連続したポーリング間で、設定されている割合を超えて減少したときに発生します。

### デフォルト設定

表 189 : NumberOfRegisteredPhonesDropped RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 クラスタに登録された電話機の数 (10%) 減少した
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## RecordingCallSetupFail

デフォルト設定

表 190 : RecordingCallSetupFail RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	エラー (Error)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 RecordingCallSetupFail イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	30 分以内に最大 3 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## RecordingGatewayRegistrationRejected

デフォルト設定

表 191 : RecordingGatewayRegistrationRejected RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	エラー (Error)



値	デフォルト設定
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 RecordingGatewayRegistrationRejected イベントが生成された。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	30 分以内に最大 3 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## RecordingGatewayRegistrationTimeout

### デフォルト設定

表 192 : RecordingGatewayRegistrationTimeout RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	エラー (Error)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 生成された RecordingGatewayRegistrationTimeout イベント。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	30 分以内に最大 3 回のアラートをトリガーする
スケジュール	毎日 24 時間

値	デフォルト設定
Enable Email	オン
Trigger Alert Action	デフォルト

## RecordingGatewaySessionFailed

デフォルト設定

表 193 : RecordingGatewaySessionFailed RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	エラー (Error)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 RecordingGatewaySessionFailed イベントが生成された。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	30 分以内に最大 3 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## RecordingResourcesNotAvailable

デフォルト設定

表 194 : *RecordingResourcesNotAvailable* RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	警告
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 生成された RecordingGatewayRegistrationTimeout イベント。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	30 分以内に最大 3 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## RecordingSessionTerminatedUnexpectedly

デフォルト設定

表 195 : *RecordingSessionTerminatedUnexpectedly* RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	エラー (Error)

値	デフォルト設定
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 RecordingCallSetupFail イベントが生成された。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	30 分以内に最大 3 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## RTMTSessionsExceedsThreshold

### デフォルト設定

表 196 : RTMTSessionsExceedsThreshold RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	アラート (Alert)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 ast セッションの数が 250 を超える場合。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間

値	デフォルト設定
Enable Email	オン
Trigger Alert Action	デフォルト

## RouteListExhausted

このアラートは、RouteListExhausted イベントの回数が、設定されている時間間隔中に、設定されているしきい値を超えたときに発生します。このアラートは、ルートリストで定義されている使用可能なチャンネルがすべて使用中であることを示します。デフォルトの値は、60 分以内に 0 回です。

### デフォルト設定

表 197 : RouteListExhausted RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	警告
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 RouteListExhausted の回数が最近 60 分間で 0 回を超えている
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## SDLLinkOutOfService

このアラートは、SDLLinkOutOfService イベントが生成されたときに発生します。このイベントは、ローカル Cisco Unified Communications Manager がリモート Cisco Unified Communications Manager と通信できないことを示します。このイベントは通常、ネットワーク エラーか、リモート Cisco Unified Communications Manager が実行されていないことを示します。

### デフォルト設定

表 198 : SDLLinkOutOfService RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 SDLLinkOutOfService イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## TCPSetupToIMEFailed

このアラートは、Cisco Unified Communications Manager が Cisco IME サーバへの TCP 接続を確立できないときに発生します。このアラートは一般に、Cisco IME サーバの IP アドレスとポートが Cisco Unified Communications Manager Administration で正しく設定されていない場合か、イントラネット接続の問題が存在するために接続が確立されない場合に発生します。

アラートの Cisco IME サーバの IP アドレスとポートが有効であることを確認します。問題が解決しない場合は、Cisco Unified Communications Manager サーバと Cisco IME サーバ間の接続をテストします。

## デフォルト設定

表 199 : TCPSSetupToIMEFailed アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 Cisco IME サーバへの接続に失敗した
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## TLSConnectionToIMEFailed

このアラートは、Cisco IME サービスによって提示された証明書の期限が切れていたか、証明書が Cisco Unified Communications Manager CTL になかったために、Cisco IME サービスへの TLS 接続を確立できなかったときに発生します。

Cisco IME サービス証明書が Cisco Unified Communications Manager に設定されていることを確認します。

## デフォルト設定

表 200 : TLSConnectionToIMEFailed アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	アラート (Alert)

値	デフォルト設定
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 Cisco IME サービスへの TLS 障害が発生した
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## UserInputFailure

### デフォルト設定

表 201 : UserInputFailure RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	警告
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 UserInputFailure イベントが生成された。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	30 分以内に最大 3 回のアラートをトリガーする
スケジュール	毎日 24 時間



値	デフォルト設定
Enable Email	オン
Trigger Alert Action	デフォルト

## IM and Presence Service アラート

### CTIGWUserNotLicenced

#### アラートの説明

このアラートは、ユーザには有効なライセンスがないため、認証できないことを示します。

#### Unified RTMT のデフォルトしきい値

適用なし

#### 推奨処置

Cisco CTI ゲートウェイ アプリケーションのライセンスとユーザ設定を確認します。

### CTIGWQBFailedRequest

#### アラートの説明

このアラートは、Cisco CTI ゲートウェイ アプリケーションが、要求に対して失敗応答を受信したことを示します。

#### Unified RTMT のデフォルトしきい値

適用なし

#### 推奨処置

Cisco RTMT を使用して、Cisco SIP プロキシ サービスのトレース ログ ファイルで詳細なエラー メッセージを確認してください。

### CTIGWModuleNotEnabled

#### アラートの説明

このアラートは、Cisco CTI ゲートウェイ アプリケーションが、設定が不十分であるかまたはイネーブルでないことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco Cisco Unified Communications Manager IM and Presence CTI の [ゲートウェイ設定 (Gateway Settings) ] ページを使用して、Cisco CTI ゲートウェイ アプリケーションを設定し、イネーブルにします。

## CTIGWSystemError

### アラートの説明

このアラートは、Cisco CTI ゲートウェイ アプリケーションシステムのエラーを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco RTMT を使用して、Cisco SIP プロキシ サービスのトレース ログ ファイルで詳細なエラー メッセージを確認してください。

## CTIGWUserNotAuthorized

### アラートの説明

このアラートは、不正なデバイスまたは回線 DN が原因で、ユーザが承認されなかったことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

ユーザのデバイス設定および MOC 設定を確認します。

## CTIGWProviderFailedToOpen

### タイプ (Type)

IM and Presence Service

### アラートの説明

このアラートは、CTI プロバイダーが設定エラーが原因で開けなかったことを示します。

### Unified RTMT のデフォルトしきい値

該当なし。

#### 推奨処置

Administration GUI の [CTI 設定 (CTI Settings)] ページで、Cisco Unified Communications Manager のアドレスとアプリケーションのユーザ クレデンシヤルを確認します。

## DuplicateDirectoryURI

### アラートの説明

このアラートは、ディレクトリ URIIM アドレス スキームが設定されている時、同じディレクトリ URI 値が割り当てられているクラスタ間展開内に複数のユーザが設定されていることを示します。

### Unified RTMT のデフォルトしきい値

適用なし

#### 推奨処置

ただちに処置をして問題を修正してください。各ユーザは一意のディレクトリ URI が割り当てられる必要があります。影響を受けるユーザが、クラスタ間ピアに配置されている場合があります。

## DuplicateUserid

### アラートの説明

このアラートは、クラスタ間展開内の別のクラスタで、1 人以上のユーザに重複ユーザ ID が割り当てられていることを示します。

### Unified RTMT のデフォルトしきい値

適用なし

#### 推奨処置

ただちに処置をして問題を修正してください。各ユーザは一意のユーザ ID が割り当てられる必要があります。影響を受けるユーザが、クラスタ間ピアに配置されている場合があります。

## ESPSocketError

### アラートの説明

このアラートは、バインディング エラー（ソケット アドレス取得の失敗など）によって発生するネットワーク ソケット エラーを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco RTMT を使用して、Cisco SIP プロキシ サービスのトレース ログ ファイルで詳細なエラー メッセージを確認してください。

## ESPCreateLockFailed

### アラートの説明

このアラートは、ロック ファイルが作成されていないことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco RTMT を使用して、Cisco SIP プロキシ サービスのトレース ログ ファイルで詳細なエラー メッセージを確認してください。

## ESPConfigError

### アラートの説明

このアラートは、Cisco SIP プロキシ サービスのコンフィギュレーション ファイル エラーを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco Config Agent サービスが実行されていることを確認します。このサービスは、プロキシ コンフィギュレーション ファイルの書き込みに使用します。

## ESPSharedMemAllocFailed

### アラートの説明

このアラートは、テーブルの初期化を試みている間に、Cisco SIP Proxy サービスが共有メモリのセグメントを割り当てられなかったことを示しています。

### Unified RTMT のデフォルトしきい値

N/A

### 推奨処置

Unified RTMT を使用して、システムの共有メモリを検査し、Cisco SIP Proxy サービスのトレース ログ ファイルでエラー メッセージの詳細情報を確認して、Cisco TAC に連絡してください。

## ESPSharedMemSetPermFailed

### アラートの説明

このアラートは、テーブルの初期化を試みている間に、Cisco SIP Proxy サービスが共有メモリのセグメントに権限を設定できなかったことを示しています。

### Unified RTMT のデフォルトしきい値

N/A

### 推奨処置

Unified RTMT を使用して、システムの共有メモリを検査し、Cisco SIP Proxy サービスのトレース ログ ファイルでエラー メッセージの詳細情報を確認して、Cisco TAC に連絡してください。

## EspConfigAgentHighCPUUtilization

### アラートの説明

このアラートは、CPU 使用率が設定されたしきい値を超えたことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Unified RTMT を使用して、Cisco SIP プロキシ サービスのトレース ログ ファイルで詳細なエラー メッセージを確認してください。

## ESPMallocFailure

### アラートの説明

このアラートは、メモリの割り当てに失敗したことを示します。サーバに軽度のメモリ問題があるか、またはメモリ問題がないことを示す場合があります。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Unified RTMT を使用して、Cisco SIP プロキシ サービスのトレース ログ ファイルで詳細なエラーメッセージを確認してください。

## ESPRegistryError

### アラートの説明

このアラートは、リソース制限を超えたため SIP レジストリに登録を追加することができないことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco RTMT を使用して、Cisco SIP プロキシ サービスのトレース ログ ファイルで詳細なエラーメッセージを確認してください。

## EspConfigAgentSharedMemoryStaticRouteError

### アラートの説明

このアラートは、Cisco Config Agent サービスが、共有メモリ内のスタティック ルートにアクセスできなかったことを示します。これは、システムのメモリが不足していることを示す場合があります。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco RTMT を使用して、システムの共有メモリが少なくなっていること、または使い尽くされていることを確認します。このアラームは、システムが過負荷になっているため、ユーザを IM and Presence Service クラスタ内の他のノードに再割り当てする必要があることを示す場合があります。ユーザを他のノードに再割り当てするには、Administration GUI の [トポロジ (Topology) ] ページを使用します。

## ESPStatsLogFileOpenFailed

### アラートの説明

このアラートは、Cisco SIP プロキシサービスのステータス ログ ファイルをオープンできなかったことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco RTMT を使用して、Cisco SIP プロキシサービスのトレース ログ ファイルで詳細なエラー メッセージを確認してください。

## ESPLoginError

### アラートの説明

このアラートは、ログイン データストアと通信中にエラーが発生したことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco RTMT を使用して、Cisco SIP プロキシサービスのトレース ログ ファイルで詳細なエラー メッセージを確認してください。

## EspConfigAgentProxyDomainNotConfigured

### アラートの説明

このアラートは、Cisco Config Agent サービスが設定されていないことを示します。Cisco Config Agent サービスでは、ACL を適切に生成するために、プロキシドメインを使用します。このサービスが設定されていないと、ルーティング障害が起きる場合があります。

**Unified RTMT のデフォルトしきい値**

適用なし

**推奨処置**

IM and Presence Service パブリッシャの [サービス パラメータ (Service Parameters) ] ドロップダウンメニューに移動します。[Cisco SIP Proxy] サービスを選択します。プロキシドメイン サービス パラメータとして IM and Presence Service ドメインを入力して保存します。

## EspConfigAgentNetworkRestored

**アラートの説明**

このアラートは、Cisco Config Agent ネットワークが復元されたことを示します。

**Unified RTMT のデフォルトしきい値**

適用なし

**推奨処置**

Cisco RTMT を使用して、システムの状態とネットワーク接続を確認してください。

## EspConfigAgentLocalDBAccessError

**アラートの説明**

このアラートは、Cisco Config Agent サービスでの IM and Presence Service のローカルデータベースの読み取りまたは書き込みが失敗したことを示します。

**Unified RTMT のデフォルトしきい値**

適用なし

**推奨処置**

Cisco RTMT を使用してシステムの状態を確認してください。A Cisco DB サービスが実行していることを確認してください。

## ESPConfigNotFound

**アラートの説明**

このアラートは、Cisco SIP プロキシ サービスのコンフィギュレーションファイルが見つからないことを示します。

**Unified RTMT のデフォルトしきい値**

適用なし



### 推奨処置

IM and Presence サーバに、コンフィギュレーション ファイル  
/usr/local/sip/conf/sipd.conf および  
/usr/local/sip/conf/dynamic.sipd.conf があることを確認してください。

## EspConfigAgentRemoteDBAccessError

### アラートの説明

このアラートは、Cisco Config Agent サービスが IM and Presence Service サービスのリモート データベースにアクセスできないことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

A Cisco DB が、アラートで指定されているノード上で実行されていることを確認してください。これらのエラーは一時的な場合があります。たとえば、Config Agent が、何らかの理由で使用できなくなっているリモート ノードにアクセスしようとしている場合です。そのような場合、このエラーが表示されることがあります。これは、インストールされていない、または使用可能でないノードにユーザを再割り当てすると起きる場合があります。

## ESPPassedParamInvalid

### アラートの説明

このアラートは、無効なパラメータが指定されていることを示します。パラメータが null であるために発行される場合もあります。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Unified RTMT を使用して、Cisco SIP プロキシ サービスのトレース ログ ファイルで詳細な エラー メッセージを確認してください。

## ESPSharedMemCreateFailed

### アラートの説明

このアラートは、テーブルの初期化を試みている間に、Cisco SIP Proxy サービスが共有メモリのセグメントを作成できなかったことを示しています。

**Unified RTMT のデフォルトしきい値**

N/A

**推奨処置**

Unified RTMT を使用して、システムの共有メモリを検査し、Cisco SIP Proxy サービスのトレース ログ ファイルでエラー メッセージの詳細情報を確認して、Cisco TAC に連絡してください。

## EspConfigAgentHighMemoryUtilization

**アラートの説明**

このアラートは、仮想メモリの使用率が設定されたしきい値を超えたことを示します。

**Unified RTMT のデフォルトしきい値**

適用なし

**推奨処置**

Unified RTMT を使用してメモリ使用率をモニタし、必要に応じてパフォーマンスを向上させるためにシステム負荷を減らしてください。

## ESP NAPTR Invalid Record

**アラートの説明**

このアラートは、NAPTR レコードの形式エラーを示します。

**Unified RTMT のデフォルトしきい値**

適用なし

**推奨処置**

Cisco RTMT を使用して、Cisco SIP プロキシ サービスのトレース ログ ファイルで詳細なエラー メッセージを確認してください。

## ESP Wrong IP Address

**アラートの説明**

このアラートは、無効な IP アドレスが入力されたことを示します。

**Unified RTMT のデフォルトしきい値**

適用なし

### 推奨処置

Cisco RTMT を使用して、Cisco SIP プロキシ サービスのトレース ログ ファイルで詳細なエラー メッセージを確認してください。

## EspConfigAgentNetworkOutage

### アラートの説明

このアラートは、Cisco Config Agent のネットワーク停止を示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco RTMT を使用して、システムの状態とネットワーク接続を確認してください。

## EspConfigAgentMemAllocError

### アラートの説明

このアラートは、Cisco Config Agent サービスがメモリを割り当てることができないことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Unified RTMT を使用して、システムの共有メモリが少なくなっていること、または使い尽くされていることを確認します。このアラームは、システムが過負荷になっているため、ユーザを IM and Presence Service クラスタ内の他のノードに再割り当てする必要があることを示す場合があります。ユーザを他のノードに再割り当てするには、IM and Presence Service Administration GUI の [トポロジ (Topology) ] ページを使用します。

## EspConfigAgentFileWriteError

### アラートの説明

このアラートは、Cisco Config Agent サービスがファイル システムに書き込むことができないことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco RTMT を使用して、ディスク容量が少なくなっていること、または使い尽くされていることを確認します。このアラームは、システムが過負荷になっているため、ユーザを IM and Presence Service クラスタ内の他のノードに再割り当てする必要があることを示す場合があります。ユーザを他のノードに再割り当てするには、IM and Presence Service Administration GUI の [トポロジ (Topology) ] ページを使用します。

## ESPVirtualProxyError

### アラートの説明

このアラートは Virtual\_Proxy\_Domain 関連のエラーを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco RTMT を使用して、Cisco SIP プロキシ サービスのトレース ログ ファイルで詳細なエラー メッセージを確認してください。

## ESPStopped

### アラートの説明

このアラートは、Cisco SIP Proxy サービスの子プロセスが停止したことを示します。

### Unified RTMT のデフォルトしきい値

N/A

### 推奨処置

管理者が手動でプロキシ サービスを停止しなかった場合、これは何らかの問題を示している可能性があります。Unified RTMT を使用して関連するアラームをチェックして、Cisco TAC に連絡してください。

## ESPWrongHostName

### アラートの説明

このアラートは、無効な IP アドレスまたは解決できないホスト名を示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco RTMT を使用して、Cisco SIP プロキシ サービスのトレース ログ ファイルで詳細なエラー メッセージを確認してください。

## ESPRoutingError

### アラートの説明

このアラートは、SIP ルート インターフェイス リソース制限の超過エラーを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco RTMT を使用して、Cisco SIP プロキシ サービスのトレース ログ ファイルで詳細なエラー メッセージを確認してください。

## InterclusterSyncAgentAXLConnectionFailed

### アラートの説明

このアラートは、リモートの IM and Presence Service クラスタへの認証に、Cisco Intercluster Sync Agent サービスが失敗したため、接続できないことを示します。

### Unified RTMT のデフォルトしきい値

該当なし。

### 推奨処置

AXL クレデンシャルが正しいことと、Cisco AXL Web サービスがリモートの IM and Presence Service クラスタで実行中かどうかを確認します。

## InterclusterSyncAgentPeerDuplicate

### アラートの説明

このアラートは、Cisco Intercluster Sync Agent サービスがリモートピアからのユーザ ロケーションデータの同期に失敗したことを示します。リモートピアは、ローカルクラスタ内にピアをすでに持つ IM and Presence Service クラスタに由来します。

### Unified RTMT のデフォルトしきい値

該当なし。

### 推奨処置

リモートピアのホスト名が、識別された既存のピアからのセカンダリノードでないことを確認します。新しいピアがセカンダリノードの場合は、このピアを IM and Presence Service Administration GUI の [クラスタ間詳細 (Inter-cluster details)] ページから削除します。また、システムトラブルシュータを実行して詳細を確認することもできます。

## ICSACertificateFingerPrintMisMatch

### アラートの説明

このアラートは、Cisco Intercluster Sync Agent サービスが、処理される証明書にフィンガープリントの不一致を検出したことを示します。

### Unified RTMT のデフォルトしきい値

N/A

### 推奨処置

ソースサーバの証明書と、このサーバにロードされる証明書を比較するために、IM and Presence Service の OS Administration GUI を使用します。問題の証明書を削除し、リロードする必要がある場合があります。

## ICSACertificateCASignedTrustCertFound

### アラートの説明

このアラートは、Cisco Intercluster Sync Agent サービスが署名済み CA 信頼証明書を検出したことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

無署名 CA 信頼証明書のみを許可するようにします。

## ICSACertificateValidationFailure

### アラートの説明

このアラートは、Cisco Intercluster Sync Agent サービスが、処理される証明書に認証エラーを検出したことを示します。

### Unified RTMT のデフォルトしきい値

N/A

### 推奨処置

ソース サーバの証明書と、このサーバにロードされる証明書を比較するために、IM and Presence Service の OS Administration GUI を使用します。問題の証明書を削除し、リロードする必要がある場合があります。

## InvalidDirectoryURI

### アラートの説明

このアラートは、ディレクトリ URIIM アドレス スキームが設定されているとき、展開内の 1 つ以上のユーザに空または無効なディレクトリ URI 値が割り当てられていることを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

ただちに処置をして問題を修正してください。影響を受けるユーザが、クラスタ間ピアに配置されている場合があります。

## LegacyCUPCLogin

### アラートの説明

このアラートは、Cisco Unified Personal Communicator のレガシークライアントが Cisco Client Profile Agent サービスにログインしようとしたことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco Unified Personal Communicator のレガシークライアントはサポートされないため、アップグレードする必要があります。

## NotInCucmServerListError

### アラートの説明

このアラートは、IM and Presence ノードが Cisco Unified Communications Manager パブリックのサーバリストに含まれていないため Cisco Sync Agent の起動に失敗したことを示します。

**Unified RTMT のデフォルトしきい値**

適用なし

**推奨処置**

IM and Presence ノードを Cisco Unified Communications Manager サーバのサーバリストに追加し、Cisco Sync Agent サービスを起動します。

## PEStateLocked

**アラートの説明**

このアラートは、管理上、Cisco Presence Engine サービスでトラフィック処理が禁止されていることを示します。

**Unified RTMT のデフォルトしきい値**

適用なし

**推奨処置**

このアラートは通知専用です。特に対処の必要はありません。

## PWSAboveCPULimit

**アラートの説明**

このアラートは、CPU 使用率が設定されたしきい値を超えたことが Cisco SIP Proxy サービスで実行中の Presence Web Service モジュールにより検出されたことを示します。この間、CPU 使用率が設定されたしきい値未満に低下するまで、新しい要求はブロックされます。

**Unified RTMT のデフォルトしきい値**

適用なし

**推奨処置**

Unified RTMT を使用して、Cisco SIP Proxy サービスのログの詳細を確認してください。

## PWSRequestLimitReached

**アラートの説明**

このアラートは、秒あたりの Cisco SIP Proxy サービス要求数の制限に到達したことを示します。

**Unified RTMT のデフォルトしきい値**

適用なし



### 推奨処置

着信要求のレートを抑制する必要がある場合があります。

## PEIDSQueryError

### アラートの説明

このアラートは、IM and Presence Service データベースのクエリーを実行中に Cisco Presence Engine サービスがエラーを検出したことを示します。

### Unified RTMT のデフォルトしきい値

N/A

### 推奨処置

都合のよいときに Cisco Presence Engine サービスを再起動します。問題が続く場合は、関連するエラー メッセージとログ ファイルを確認し、Cisco TAC にお問い合わせください。

## PEStateDisabled

### アラートの説明

このアラートは、Cisco Presence Engine サービスが使用できず、トラフィックを処理できないことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

ログ ファイルをチェックし、Unified RTMT を使用して Cisco Presence Engine サービスをモニタしてください。

## PELoadHighWaterMark

### アラートの説明

このアラートは、Cisco Presence Engine サービスが CPU 使用率しきい値を超えたことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco RTMT を使用して、次のアクティブ サブスクリプション カウンタを確認してください：ActiveSubscriptions、ActiveViews、SubscriptionActiveReceivedFromForeign、および SubscriptionActiveSentForeign。この状態が続く場合は、クラスタ内の別の IM and Presence Service ノードにユーザを移動することを検討することをお勧めします。

## PWSAboveSipSubscriptionLimit

### アラートの説明

このアラートは、サブスクリプションの数が設定された制限を超えたことが Cisco SIP Proxy サービスで実行中の Presence Web Service により検出されたことを示します。この間、Presence Web Service は、サブスクリプションの数が設定された制限を下回るようになるまで、新しい着信 SIP サブスクリプションをブロックします。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco RTMT を使用して、Cisco SIP Proxy サービスのログの詳細を確認してください。

## PEMemoryHighCondition

### アラートの説明

このアラートは、Cisco Presence Engine サービスがメモリしきい値に達したことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Unified RTMT を使用して、次のアクティブ サブスクリプション カウンタを確認してください：ActiveSubscriptions、ActiveViews、SubscriptionActiveReceivedFromForeign、および SubscriptionActiveSentForeign。この状態が続く場合は、クラスタ内の別の IM and Presence ノードに一部のユーザをオフロードします。

## PEsipSocketBindFailure

### アラートの説明

このアラートは、Cisco Presence Engine サービスが表示された設定済みインターフェイスに接続できないことを示します。このインターフェイスでは SIP トラフィックは処理できません。

### Unified RTMT のデフォルトしきい値

適用なし

#### 推奨処置

Cisco Presence Engine サービスのリッスン インターフェイスが IM and Presence Service Administration GUI の [アプリケーションリスナー (Application Listener) ] ページで正しく設定されていることを確認します。netstat を使用して他のプロセスが同じポートでリッスンしていないことを確認します。

## PEIDStoIMDBDatabaseSyncError

### アラートの説明

このアラートは、IM and Presence データベースと Cisco Presence Engine とデータベース サービス間の同期が失敗したことを示します (Cisco Login Datastore、Cisco Route Datastore、Cisco Presence Datastore、および Cisco SIP Registration Datastore)。

### Unified RTMT のデフォルトしきい値

N/A

#### 推奨処置

都合のよいときに Cisco Presence Engine サービスを再起動します。問題が続く場合は、関連するエラー メッセージとログ ファイルを確認し、Cisco TAC にお問い合わせください。

## PEIDSSubscribeError

### アラートの説明

このアラートは、Cisco Presence Engine サービスが IM and Presence Service データベース変更通知をサブスクライブできなかったを示します。

### Unified RTMT のデフォルトしきい値

N/A

#### 推奨処置

都合のよいときに Cisco Presence Engine サービスを再起動します。問題が続く場合は、関連するエラー メッセージとログ ファイルを確認し、Cisco TAC にお問い合わせください。

## PWSSCBFindFailed

### アラートの説明

このアラートは find\_scb() へのコールが SCB ルックアップに失敗したことを示す NULL を返したことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco RTMT を使用して、Cisco SIP プロキシ サービスのトレース ログ ファイルで詳細なエラー メッセージを確認してください。

## PEDatabaseError

### アラートの説明

このアラートは、データベースから情報を取得中に Cisco Presence Engine サービスでエラーが発生したことを示します。これは Cisco DB サービスに問題が生じていることを示している場合があります。

### Unified RTMT のデフォルトしきい値

N/A

### 推奨処置

Cisco DB サービスが実行されていることを確認します。Unified RTMT を使用して、Cisco Presence Engine サービス ログでエラーをチェックしてください。詳細については、Cisco TAC にお問い合わせください。

## PWSSCBInitFailed

### アラートの説明

このアラートは、SCB の初期化が失敗したことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco SIP プロキシ サービスを再起動します。

## PEWebDAVInitializationFailure

### アラートの説明

このアラートは、Cisco Presence Engine サービスが WebDAV ライブラリを初期化できなかったことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco Presence Engine サービスを再起動します。

## PEPeerNodeFailure

### アラートの説明

このアラートは、サブクラスタのピア ノードの Cisco Presence Engine サービスが失敗したことを示します。

### Unified RTMT のデフォルトしきい値

N/A

### 推奨処置

Cisco Presence Engine サービスが動作していることを確認するには、Cisco Unified Serviceability を使用します。詳細については、Cisco TAC にお問い合わせください。

## PEAutoRecoveryFailed

### アラートの説明

このアラートは、エラーを Cisco Presence Engine サービスの起動シーケンス中に発生したことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

このエラーは、設定に問題がある可能性があります。失敗メッセージで認識された問題を修正します。

## SRMFailover

### タイプ (Type)

IM and Presence Service

### アラートの説明

このアラートは、Server Recovery Manager が自動フェールオーバーを実行していることを示します。

### Unified RTMT のデフォルトしきい値

N/A

### 推奨処置

障害が発生したノードが起動しており、重要なサービスが実行されていることを確認します。

## SRMFailed

### アラートの説明

このアラートは、Server Recovery Manager が障害状態であることを示します。

### Unified RTMT のデフォルトしきい値

N/A

### 推奨処置

都合の良いときに Server Recovery Manager を再起動します。

## UASCBFindFailed

### アラートの説明

このアラートは find\_scb() へのコールが SCB ルックアップに失敗したことを示す NULL を返したことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco RTMT を使用して、Cisco SIP プロキシ サービスのトレース ログ ファイルで詳細なエラー メッセージを確認してください。

## UASCBGetFailed

### アラートの説明

このアラートは、`tchtable_acquire_tcb()` へのコールが SCB の取得または作成に失敗したことを示す NULL を返したことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco RTMT を使用して、Cisco SIP プロキシ サービスのトレース ログ ファイルで詳細なエラー メッセージを確認してください。

## XcpMFTDBConnectError

### アラートの説明

このアラートは、Cisco XCP データ アクセス レイヤが外部データベースに接続できなかったことを示します。

### Unified RTMT のデフォルトしきい値

N/A

### 推奨処置

システム トラブルシュータで詳細を確認してください。外部データベースが正常に動作していること、および外部データベース サーバとのネットワーク接続に問題があるかどうかについても確認します。

## XcpMFTExtFsMountError

### アラートの説明

このアラートは、Cisco XCP File Transfer Manager で外部ファイル サーバとの接続が失われたことを示します。

### Unified RTMT のデフォルトしきい値

N/A

### 推奨処置

External File Server Troubleshooter で詳細を確認してください。外部ファイル サーバが正常に動作していること、または外部ファイル サーバとのネットワーク接続に問題があるかどうかについても確認します。

## XcpMFTExtFsFreeSpaceWarn

### アラートの説明

このアラートは、Cisco XCP File Transfer Manager が外部ファイル サーバの空きディスク領域が少ないことを検出したことを示します。

### Unified RTMT のデフォルトしきい値

残っているファイル サーバのディスク容量が 10% 未満である。

### 推奨処置

アラートはディスク領域を 15% 以上に上げることでクリアされます。ファイル転送に使われるパーティションから不要なファイルを削除して、外部ファイル サーバの領域を解放します。

## XcpDBConnectError

### アラートの説明

Cisco XCP データ アクセス レイヤが DB に接続できませんでした。これはローカルまたは外部のデータベースがダウンしているか、または外部データベースへのネットワーク接続が失われたことを示す場合があります。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

システム トラブルシュータで詳細を確認してください。外部データベースが正常に動作していること、および外部データベース サーバとのネットワーク接続に問題があるかどうかについても確認します。

## XcpCmStartupError

### アラートの説明

このアラートは、XCP Connection Manager サービスが起動に失敗したことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

CM のログ ファイルで詳細情報を確認します。



## XcpSIPFedCmComponentConnectError

### アラートの説明

このアラートは、Cisco XCP SIP Federation Connection Manager が Cisco XCP ルータへの接続に失敗したためにシャットダウンしていることを示しています。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco XCP SIP Federation Connection Manager ログ ファイルで詳細情報を確認します。

## XcpTxtConfGearError

### アラートの説明

このアラートは、XCP Text Conference Manager (TC) サービスが設定されたコンポーネントをロードできなかったことを示します。これにより、サービスが期待どおりに開始または動作できなくなる可能性があります。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

詳細については、XCP Text Conference ログ ファイルを確認します。

## XCPConfigMgrConfigurationFailure

### アラートの説明

このアラートは、Cisco XCP Config Manager が正常に XCP 設定を更新できなかったことを示しています。

### Unified RTMT のデフォルトしきい値

N/A

### 推奨処置

根本原因については Cisco XCP Config Manager のログを確認します。Cisco TAC に連絡して、サポートを受けてください。

## XcpWebCmComponentConnectError

### アラートの説明

このアラートは、Cisco XCP Web Connection Manager が Cisco XCP ルータへの接続に失敗したためにシャットダウンしていることを示しています。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco XCP Web Connection Manager のログ ファイルで詳細情報を確認します。

## XcpXMPPFedCmStartupError

## XcpXMPPFedCmComponentConnectError

### アラートの説明

このアラートは、Cisco XCP XMPP Federation Connection Manager が Cisco XCP ルータへの接続に失敗したためにシャットダウンしていることを示しています。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco XCP XMPP Federation Connection Manager ログ ファイルで詳細情報を確認します。

## XcpSIPFedCmStartupError

### アラートの説明

このアラートは、Cisco XCP SIP Federation Connection Manager サービスが起動に失敗したことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco XCP SIP Federation Connection Manager ログ ファイルで詳細情報を確認します。

## XcpCmXmppdError

### アラートの説明

このアラートは、XCP Connection Manager (CM) サービスで XMPP インターフェイスにエラーがあることを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

CM のログ ファイルで詳細情報を確認します。

## XcpCmPauseSockets

### アラートの説明

このアラートは、優れた XCP の内部パケットまたはデータベース要求が設定された上限に達したことを示します。クライアント接続は、保留中の要求がしきい値を下回るまで一時停止されます。ユーザには、問題が解決されるまで遅延が発生します。解決前に設定されたタイムアウトに達した場合、ユーザは接続解除される可能性があります。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

詳細については XCP ルータ ログ ファイルを確認します。XCP Connection Manager からのタイムアウトによるクライアントの切断をモニタします。

## XcpThirdPartyComplianceConnectError

### アラートの説明

このアラートは、Cisco XCP ルータがサードパーティ製のコンプライアンスサーバに接続できないことを示します。これは、ネットワークの問題やサードパーティ製コンプライアンスサーバの設定またはライセンス問題が原因である可能性があります。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

これは、IM and Presence Service で IM が中断される重大なエラーです。サードパーティ製コンプライアンス サーバへのネットワーク接続とサードパーティ製コンプライアンス サーバの設定（ライセンスを含む）を確認します。IM サービスを復元するには、接続失敗の原因が特定されるまで管理 GUI の [コンプライアンス設定（Compliance Settings）] オプションを [未設定（Not Configured）] に設定します。

## XCPConfigMgrJabberRestartRequired

### アラートの説明

このアラートは、バッファ サイズが原因でシステムが停止した後に、Cisco XCP Config Manager が XCP XML ファイルを再生成したことを示します。変更を適用するために、Cisco XCP ルータを再起動する必要があります。

### Unified RTMT のデフォルトしきい値

N/A

### 推奨処置

Cisco XCP ルータを再起動します（そのほうが便利な場合）。

## XcpTxtConfDBConnectError

### アラートの説明

このアラートは、Cisco XCP テキスト会議のデータ アクセス レイヤが外部データベースに接続できなかったことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

詳細についてシステム トラブルシューティング ツールを確認します。外部データベースが正常に動作していること、および外部データベース サーバとのネットワーク接続に問題があるかどうかについても確認します。

## XcpMdnsStartError

### アラートの説明

このアラートは、XCP ルータが Multicast Domain Name Service (MDNS) の起動に失敗したことを示します。これにより、クラスタ内の他のルータに接続障害を引き起こす可能性があります。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

詳細については XCP ルータ ログ ファイルを確認します。

## XCPConfigMgrR2RPasswordEncryptionFailed

### アラートの説明

このアラートは、Cisco XCP Config Manager が、クラスタ間およびルータ間の設定に関連付けられたパスワードを暗号化できなかったことを示します。

### Unified RTMT のデフォルトしきい値

N/A

### 推奨処置

Cisco XCP Config Manager を再起動し、次に Cisco XCP ルータを再起動します（そのほうが便利な場合）。

## XcpCmComponentConnectError

### アラートの説明

このアラートは、Cisco XCP Connection Manager が Cisco XCP ルータへの接続に失敗したためにシャットダウンしていることを示しています。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco XCP Connection Manager のログ ファイルで詳細情報を確認します。

## XcpWebCmStartupError

### アラートの説明

このアラートは、Cisco XCP Web Connection Manager サービスが起動に失敗したことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco XCP Web Connection Manager のログ ファイルで詳細情報を確認します。

## XCPConfigMgrR2RRequestTimedOut

### アラートの説明

このアラートは、Cisco XCP Config Manager が XCP ルータに R2R 構成要求を送信したが、XCP ルータが許可された時間内に要求を承認しなかったことを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco XCP Config Manager を再起動し、次に XCP ルータを再起動します。

## XcpWebCmHttpdError

### アラートの説明

このアラートは、Cisco XCP Web Connection Manager サービスで HTTP インターフェイスにエラーがあることを示します。

### Unified RTMT のデフォルトしきい値

適用なし

### 推奨処置

Cisco XCP Web Connection Manager のログ ファイルで詳細情報を確認します。

## XCPCongMgrHostNameResolutionFailed

### アラートの説明

このアラートは、Cisco XCP Config Manager で、Cisco XCP ルータがそのノードに接続することを許可するために DNS 名を解決することができなかったことを示します。

### Unified RTMT のデフォルトしきい値

N/A

### 推奨処置

ローカル クラスタとリモート クラスタの両方のすべてのホスト名と FQDN の DNS 解決可能性を確認します。DNS が解決可能になった後、Cisco XCP Config Manager を再起動し、次に Cisco XCP ルータを再起動します。

## XcpSIPGWStackResourceError

### アラートの説明

このアラートは、サポートされる同時 SIP Federation サブスクリプションまたは SIP Federation IM セッションが最大数に到達し、Cisco XCP SIP Federation Connection Manager に追加のサブスクリプションまたは IM セッションを処理するために必要なリソースがないことを示しています。

### Unified RTMT のデフォルトしきい値

N/A

### 推奨処置

Cisco XCP SIP Federation Connection Manager に事前に割り当てられた SIP スタック メモリのサービス パラメータを増やします。注：この設定を変更する場合は、使用可能なメモリがあることを確認します。十分なメモリがない場合は、ハードウェア能力の制限に到達している可能性があります。

## Intercompany Media Engine アラート

### BannedFromNetwork

このアラートは、ネットワーク管理者がネットワーク（IME 分散キャッシング）でこの Cisco IME サーバを禁止して、この Cisco IME サービスを全体的または部分的に操作不能にしたことを示します。ネットワーク管理者がサーバを禁止することはまれですが、ネットワークへの悪質な

攻撃にサーバが使用されていることが検出された場合は禁止します。エラー中にこのアラートを受け取った場合は、すぐに TAC に問い合わせてください。

### デフォルト設定

表 202 : *BannedFromNetwork* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	アラート (Alert)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 Cisco IME サービスがネットワークから禁止された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## IMEDistributedCacheCertificateExpiring

このアラートは、IME 分散キャッシュで使用される証明書が期限切れになるまでの残りの日数を示します。証明書は期限切れになる前に置き換える必要があります。

### デフォルト設定

表 203 : *IMEDistributedCacheCertificateExpiring* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	警告



値	デフォルト設定
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 Cisco IME の分散キャッシュ証明書の期限切れが迫っている。14 日間。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	1440 分以内に最大 1 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## IMEDistributedCacheFailure

このカウンタは、IME 分散キャッシュの健全性を示します。値ゼロ（赤色）は、IME 分散キャッシュに次のような重大な問題が発生していることを示します。

- ネットワークが分割された後で、Cisco IME が問題を解決できない。この場合、検証に失敗する場合があります。
- Cisco IME サービスがネットワークにまったく接続されておらず、ブートストラップサーバに到達できない。

値 1（黄色）は、Cisco IME ネットワークで軽微な問題が発生していることを示します。たとえば、ブートストラップサーバ間の接続の問題や Cisco IME ネットワークのその他の問題などです。このカウンタが 1 になった原因を示す可能性のあるすべてのアラームを調べてください。値 2 は、IME 分散キャッシュが正常に動作し、システムは健全であると見なされることを示します。

### デフォルト設定

表 204 : *IMEDistributedCacheFailure* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	アラート (Alert)

値	デフォルト設定
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 IME 分散キャッシュの異常状態 1 : ネットワークで軽微な問題が発生 0 : ネットワークに問題が発生
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	60 分以内にアラートを 1 回トリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## IMESdILinkOutOfService

このアラートは、Cisco IME サービスと Cisco AMC Service や Cisco CallManager Service などの Cisco IME Config Manager サービスとの通信が切断されたことを示します。

このアラートは通常、（メンテナンスのために意図的に、または接続障害が原因で意図せずに）このいずれかのサービスが停止したことを示します。

### デフォルト設定

表 205 : *IMESdILinkOutOfService* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効

値	デフォルト設定
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 SDLLinkOOS イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## InvalidCertificate

このアラートは、管理者が Cisco IME サーバで IME 分散キャッシュを有効化したものの、有効な証明書の設定を省略したか、不正な証明書を設定したことを示します。

### デフォルト設定

表 206 : *InvalidCertificate* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	アラート (Alert)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 無効な証明書が設定された。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン

値	デフォルト設定
Trigger Alert Action	デフォルト

## InvalidCredentials

このアラートは、Cisco Unified Communications Manager で設定されたユーザ名とパスワードが Cisco IME サーバで設定されたものと一致しないために、Cisco Unified Communications Manager が Cisco IME サーバに接続できないことを示します。

アラートには、Cisco IME サーバへの接続に使用されたユーザ名とパスワードに加え、ターゲット Cisco IME サーバの IP アドレスおよび名前が含まれます。このアラートを解決するには、Cisco IME サーバにログインし、設定されているユーザ名およびパスワードが Cisco Unified Communications Manager で設定されているユーザ名およびパスワードと一致することを確認します。

### デフォルト設定

表 207 : *InvalidCredentials* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	エラー (Error)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 無効または不一致のクレデンシャル。
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## MessageOfTheDay

Cisco IME ネットワークの管理者がユーザ宛のメッセージを保有している場合、Cisco IME サービスによりこのアラートが生成されます。

### デフォルト設定

表 208 : *MessageOfTheDay* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	通知 (Notice)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 ネットワーク管理者からのメッセージ
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	1440 分以内に最大 1 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## SWUpdateRequired

Cisco IME サーバは、Cisco IME サーバソフトウェアの新規バージョンが必要な場合、このアラートを生成します。このアラートはアップグレードを実行するまで繰り返されます。ソフトウェアアップデートに関するより多くの情報を取得するには、シスコの Web サイトに移動します。重要なアップデートはこのアラートを受信してから数日中にインストールする必要があります。

これらのアップグレードはセキュリティ脆弱性か主な機能上の停止に対応します。場合によっては、重大なアップグレードをすぐに適用されない場合、Cisco IME サーバがネットワークに接続できなくなる可能性があります。

## デフォルト設定

表 209 : *SWUpdateRequired* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	警告
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 ソフトウェア アップグレードが必要になった
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	60 分以内に最大 1 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## TicketPasswordChanged

Cisco IME サーバは、管理者が検証チケットの生成に使用されるパスワードを変更する場合、このアラートを生成します。

権限のある管理者がパスワードを変更したことを確認します。不正な変更は、Cisco IME サービスの管理インターフェイスのセキュリティが破られていることを示す場合があります。不正な変更が行われたと判断した場合は、それ以上の不正アクセスを防止するために、Cisco IME サーバの管理パスワードをただちに更新します。管理パスワードを変更するには、Cisco IME サーバ CLI で **set password admin** と入力します。

## デフォルト設定

表 210 : *TicketPasswordChanged* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン

値	デフォルト設定
重大度 (Severity)	通知 (Notice)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 チケットパスワードが変更された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## ValidationsPendingExceeded

このアラートは、Cisco IME サーバ上の保留中の検証の数を示します。この数は、Cisco IME サーバ上の作業のバックログのインジケータを提供します。

### デフォルト設定

表 211 : **ValidationsPendingExceeded** アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on the following servers	一覧表示されたサーバで有効
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 Cisco IME の保留中の検証が 100 を超えた
時間 (Duration)	すぐにアラートをトリガーする

値	デフォルト設定
頻度 (Frequency)	60 分以内に最大 1 回のアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## Cisco Unity Connection アラート

### NoConnectionToPeer

(Cisco Unity Connection クラスタ構成のみ) このアラートは、Cisco Unity Connection クラスタ サーバが相互に通信できない場合 (たとえば、ネットワーク接続が失われた場合) に生成されます。

#### デフォルト設定

表 212 : NoConnectionToPeer RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on following server(s)	[有効 (Enabled) ]
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 NoConnectionToPeer イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト



## AutoFailoverSucceeded

(Cisco Unity Connection クラスタ設定) : このアラートは次の条件で生成されます。

- (プライマリ ステータスのサーバで重大な障害が発生した場合などに) セカンダリ ステータスのサーバが、ステータスを自動的にプライマリに変更した場合に、ボイスメッセージング機能とクラスタのデータベースを処理する責任を負う。このアラートは、次のイベントが発生したことを通知します。
  - 最初にプライマリ ステータスだったサーバで重大な障害が発生した。
  - 最初にセカンダリ ステータスだったサーバのステータスがプライマリになり、すべてのコールを正常に処理している。
- 機能を停止していたサーバ (前述) がオンラインに復帰し、両方のサーバがボイスメッセージング機能と複製の処理の責任を共有するように、サーバのステータスが自動的に変更された。

### デフォルト設定

表 213 : *AutoFailoverSucceeded* RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	情報 (Informational)
Enable/Disable this alert on following server(s)	[有効 (Enabled) ]
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 AutoFailoverSucceeded イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## AutoFailoverFailed

(Cisco Unity Connection クラスタ設定) : このアラートは次の条件で生成されます。

- (プライマリ ステータスのサーバで重大な障害が発生した場合などに) セカンダリ ステータスのサーバがステータスを自動的にプライマリに変更しようとしたが、サーバステータスの自動変更が失敗して、セカンダリ ステータスのサーバがセカンダリ ステータスを保持している。
- 機能を停止した (たとえば重大な障害が発生した) サーバがオンラインに復帰しない。クラスタ内で 1 台のサーバだけが機能している。

### デフォルト設定

表 214 : AutoFailoverFailed RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	エラー (Error)
Enable/Disable this alert on following server(s)	[有効 (Enabled) ]
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 AutoFailoverFailed イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## AutoFailbackSucceeded

(Cisco Unity Connection クラスタ設定) このアラートは、プライマリ ステータスのサーバの機能停止の原因となった問題 (これにより、セカンダリ ステータスのサーバのステータスがプライマリに変更された) が解決され、両方のサーバが再度オンラインになった場合に生成されます。次

に、機能を停止していたサーバがプライマリ ステータスになり、もう一方のサーバがセカンダリ ステータスになるように、両方のサーバは自動的にステータスを変更します。

### デフォルト設定

表 215 : *AutoFailbackSucceeded RTMT* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	情報 (Informational)
Enable/Disable this alert on following server(s)	[有効 (Enabled) ]
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 AutoFailbackSucceeded イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## AutoFailbackFailed

(Cisco Unity Connection クラスタ設定) : このアラートは、パブリッシャ ノードがオンラインでなく、プライマリ ステータスのサーバが状態を自動的に変更できなかった場合に発生します。

### デフォルト設定

表 216 : *AutoFailbackFailed RTMT* アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	エラー (Error)

値	デフォルト設定
Enable/Disable this alert on following server(s)	[有効 (Enabled) ]
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 AutoFailbackFailed イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## SbrFailed (スプリットブレイン解決の失敗)

Cisco Unity Connection クラスタが設定されているとき、2 台のサーバが相互に通信できない場合、両方とも同時にプライマリステータス (“スプリットブレイン”状態) になり、ボイスメッセージング機能処理し、メッセージを各自のメッセージストアに保存しますが、複製は実行しません。ユーザは、メッセージを取得できますが、これらのメッセージが取得されたことを認識するのは 1 台のサーバだけです。

サーバの両方が相互に通信できるとき、各ユーザ メールボックスの正しい内容と状態を決定することによってこのスプリットブレイン状態が解決されます。

- 受信した新しいメッセージかどうか。
- 新しいメッセージの MWI がすでに送信済みかどうか。
- どのメッセージを再生したか。
- どのメッセージが削除されたか。

スプリットブレイン状態の解決に失敗した場合、このアラートが発生します。

### デフォルト設定

表 217 : SbrFailed RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン

値	デフォルト設定
重大度 (Severity)	情報 (Informational)
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 SbrFailed イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## DiskConsumptionCloseToCapacityThreshold

このアラートは、Cisco Unity Connection サーバ上のハードディスク使用量が Cisco Unity Connection Administration の [システム設定 (System Settings)] > [詳細設定 (Advanced)] > [ディスク容量 (Disk Capacity)] ウィンドウで指定したパーセンテージまであと 10 パーセントのところに到達すると生成されます。たとえば、容量のしきい値の制限が 95% の場合、使用率が 85% になると、アラートがトリガーされます。

### デフォルト設定

表 218 : DiskConsumptionCloseToCapacityThreshold RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	エラー (Error)
Enable/Disable this alert on following server(s)	[有効 (Enabled)]
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 DiskConsumptionCloseToCapacityThreshold イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする

値	デフォルト設定
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## DiskConsumptionExceedsCapacityThreshold

このアラートは、Cisco Unity Connection サーバ上のハードディスク使用量が Cisco Unity Connection Administration の [システム設定 (System Settings)] > [詳細設定 (Advanced)] > [ディスク容量 (Disk Capacity)] ウィンドウで指定したパーセンテージの制限に到達するか、または超えた場合に生成されます。

### デフォルト設定

表 219 : DiskConsumptionExceedsCapacityThreshold RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	エラー (Error)
Enable/Disable this alert on following server(s)	[有効 (Enabled)]
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 DiskConsumptionExceedsCapacityThreshold イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## LicenseExpirationWarning

Cisco Unity Connection は、ユーザやポートなど、複数の機能のライセンスを提供します。システムは、これらのライセンスを適用します。お客様が期間限定ライセンスを使用して特定機能を使用する場合、このライセンスには有効期限が設定されます。ライセンスの有効期限が来る前に、システムによりメッセージが送信されて、このアラートが発生します。ログには、ライセンスの有効期限までの日数が表示されます。

### デフォルト設定

表 220 : LicenseExpirationWarning RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	クリティカル (Critical)
Enable/Disable this alert on following server(s)	[有効 (Enabled) ]
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 LicenseExpirationWarning イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト

## LicenseExpired

Cisco Unity Connection は、ユーザやポートなど、複数の機能のライセンスを提供します。システムは、これらのライセンスを適用します。お客様が期間限定ライセンスを使用して特定機能を使用する場合、このライセンスには有効期限が設定されます。ライセンスの期限が来ると、ライセンスが無効になり、このアラートが発生します。

## デフォルト設定

表 221 : LicenseExpired RTMT アラートのデフォルト設定

値	デフォルト設定
Enable Alert	オン
重大度 (Severity)	情報 (Informational)
Enable/Disable this alert on following server(s)	[有効 (Enabled) ]
しきい値 (Threshold)	次の条件が満たされたときにアラートをトリガーする。 LicenseExpired イベントが生成された
時間 (Duration)	すぐにアラートをトリガーする
頻度 (Frequency)	ポーリングごとにアラートをトリガーする
スケジュール	毎日 24 時間
Enable Email	オン
Trigger Alert Action	デフォルト