



アラート

- [Alert Central の表示 \(1 ページ\)](#)
- [アラートアクションのセットアップ \(8 ページ\)](#)
- [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 \(13 ページ\)](#)

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)]、[CallManager]、[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
- CriticalAuditEventGenerated
- CriticalServiceDown
- 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



(注) 監査イベントはアラートする価値がないため、CriticalAuditEventGenerated アラートをトリガーすることはできません。

関連トピック

[システムアラート](#)

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、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
- CodeYellow
- DDRBlockPrevention
- DDRDown
- EMCCFailedInLocalCluster
- EMCCFailedInRemoteCluster
- ExcessiveVoiceQualityReports
- ILSHubClusterUnreachable
- ILSPwdAuthenticationFailed
- ILSTLSAuthenticationFailed
- IMEDistributedCacheInactive
- IMEOverQuota

- IMQualityAlert
- IMServiceStatus
- InsufficientFallbackIdentifiers
- InvalidCredentials
- LocationOutOfResource
- MaliciousCallTrace
- MediaListExhausted
- MgcpcDChannelOutOfService
- NumberOfRegisteredDevicesExceeded
- NumberOfRegisteredGatewaysDecreased
- NumberOfRegisteredGatewaysIncreased
- NumberOfRegisteredMediaDevicesDecreased
- NumberOfRegisteredMediaDevicesIncreased
- NumberOfRegisteredPhonesDropped
- RouteListExhausted
- RTMTSessionExceedsThreshold
- SDLLinkOutOfService
- TCPSetupToIMEFailed
- TLSConnectionToIMEFailed
- UserInputFailure

関連トピック

[音声およびビデオ アラート](#)

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](#)

Cisco Unity Connection のアラート

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。これらのアラートは、Cisco Unity Connection と Cisco Business Edition 5000 にのみ適用されます。

- NoConnectionToPeer
- AutoFailoverSucceeded
- AutoFailoverFailed
- AutoFailbackSucceeded
- AutoFailbackFailed
- SbrFailed
- 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。
Cisco Business Edition 5000 は Cisco Unity Connection クラスタ設定をサポートしません。

関連トピック

[Cisco Unity Connection のアラート](#)

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 1: アラートアクションの設定

フィールド	説明	備考
アラートアクション 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	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 次のいずれかの操作を行います。

- a) クイック起動チャンネルで、次の操作を実行します。
 1. [System] をクリックします。
 2. ツリー階層で [ツール (Tools)] をダブルクリックします。
 3. [Alert Central] アイコンをクリックします。

- b) [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 次のいずれかの操作を行います。

- a) アラート プロパティを設定します。
- b) アラートを一時停止します。
- c) アラート通知の電子メールを設定します。
- d) アラート アクションを設定します。
- e) [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。
- f) 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。

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

ステップ 2 [シビラティ (重大度) (Severity)] リストチェックボックスで、通知の対象となるシビラティ (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 [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 2: 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"> 以上 (Over) : アラート通知がアクティブになる前にオンにします。[以上 (Over)] の値フィールドには、値を等しい値を入力します。 以下 (Under) : アラート通知がアクティブになる前にオンにします。[以下 (Under)] の値フィールドには、値を等しい値を入力します。 <p>ヒント これらのチェックボックスは、[頻度 (Frequency)] 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	

設定	説明
[絶対値 (Absolute)]、[差分 (Delta)]、[差分比率 (Delta Percentage)]	適用するオプション ボタンを選択します。 <ul style="list-style-type: none"> 絶対値 (Absolute) : 一部のカウンタ値は累積されるため、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 差分比率 (Delta Percentage) : カウンタ パフォーマンスの変
[期限 (Duration)] ペイン	
常に価値がある場合にのみアラートをトリガーする... (Trigger alert only when value constantly...) すぐにアラートをトリガーする	<ul style="list-style-type: none"> 常に価値がある場合にのみアラートをトリガーする... (Trigger alert only when value constantly...) 次の場合にアラートをトリガー：指定した秒数にわたって値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、秒数を入力します。 アラートをすぐにトリガー (Trigger alert immediately) : アラート通知を送信するときにアラート通知を送信する場合は、このオプション ボタンを選択します。
[頻度 (Frequency)] ペイン	
[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...)]	適用するオプション ボタンを選択します。 <ul style="list-style-type: none"> 各ポーリングでアラートをトリガー (Trigger alert on every poll) : アラート通知を送信する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 ボタンを選択して、送信するアラートの数とアラートを送信する間隔を入力します。 トリガーの間隔 (trigger up to...) : アラート通知を一定間隔で送信する場合は、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間隔を入力します。
[スケジュール (Schedule)] ペイン	
[24時間毎日 (24-hours daily)]、[開始/停止 (Start/Stop)]	適用するオプション ボタンを選択します。 <ul style="list-style-type: none"> 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。 開始/停止 (Start/Stop) : アラート通知を特定のタイムフレームで送信する場合は、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。オプション ボタンを選択して、開始時刻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。

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



重要 TLS モードを有効にする、認証モードを有効にする、ユーザー名、およびパスワードのフィールドは、リリース 14SU2 以降で導入されました。

手順

ステップ 1 [システム (System)] > [ツール (Tools)] > [アラート セントラル) 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 ウィザードの指示に従って優先条件を設定します。

- a) [アラート プロパティ: 電子メール通知 (Alert Properties: Email Notification)] ポップアップで、[電子メールの有効化 (Enable Email)] がオンになっていることを確認し、[設定 (Configure)] をクリックしてデフォルトのアラート アクションを設定します。これにより管理者に電子メールが送信されます。
- b) プロンプトに従って、受信者電子メールアドレスを [追加 (Add)] します。このアラートがトリガーされると、デフォルトのアクションは、このアドレスへの電子メールの送信になります。
- c) [保存 (Save)] をクリックします。

ステップ 4 デフォルトの電子メール サーバを設定します。

- a) [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。
- b) 電子メールアラートを送信する電子メールサーバーとポート情報を入力します。
- c) [送信するユーザー ID (Send User ID)] を入力します。
- d) [OK] をクリックします。

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。

翻訳について

このドキュメントは、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。