



ツールおよびレポート

- [サービスアビリティ レポートのアーカイブ, 1 ページ](#)
- [CDR Repository Manager, 24 ページ](#)
- [監査ログ, 32 ページ](#)
- [ロケーション \(Locations\) , 43 ページ](#)

サービスアビリティ レポートのアーカイブ

Cisco Serviceability Reporter サービスは、特定のレポートについて統計情報のサマリーを表示するグラフを含む、日報を生成します。Reporter は、ログに記録された情報に基づいてレポートを 1 日 1 回生成します。

Serviceability GUI を使用して、[ツール (Tools)] > [サービスアビリティ レポートのアーカイブ (Serviceability Reports Archive)] からレポートを表示します。レポートを表示する前に、Cisco Serviceability Reporter サービスをアクティブ化する必要があります。サービスをアクティブ化した後、レポートの生成に最大 24 時間かかる場合があります。

レポートには、前日の 24 時間のデータが含まれます。レポート名に追加されるサフィックスは、Reporter がレポートを生成した日付を表します。たとえば、AlertRep_mm_dd_yyyy.pdf です。[サービスアビリティ レポートのアーカイブ (Serviceability Reports Archive)] ウィンドウでは、この日付を使用して該当する日付だけのレポートを表示します。レポートは、前日のタイムスタンプを持つログファイルにあるデータから生成されます。システムは、現在の日付と過去 2 日間のログファイルを対象にデータを収集します。

レポートに表示される時刻にはサーバの「システム時刻」が反映されます。

レポートの生成中にサーバからログ ファイルを取得できます。



(注) Cisco Unified Reporting Web アプリケーションは、1つの出力にデータのスナップショットビューを提供し、データチェックを実行します。また、生成されたレポートをアーカイブすることもできます。詳細については、『Cisco Unified Reporting Administration Guide』を参照してください。

サービスアビリティ レポートのアーカイブのクラスタ構成に関する考慮事項

この項は、Cisco Unified Communications Manager および IM and Presence Service だけに適用されません。

- Cisco Serviceability Reporter は最初のサーバでのみアクティブなため、Reporter は常に、他のサーバではなく、最初のサーバでのみレポートを生成します。
- レポートに表示される時刻には最初のサーバの「システム時刻」が反映されます。最初のサーバとそれに続くサーバが異なるタイムゾーンにある場合は、最初のサーバの「システム時刻」がレポートに表示されます。
- クラスタ内のサーバ ロケーション間のタイムゾーンの差は、レポート用にデータが収集されるときに考慮されます。
- レポートの生成時に、個々のサーバまたはクラスタ内のすべてのサーバからログファイルを選択できます。
- Cisco Unified Reporting Web アプリケーションの出力やデータチェックには、アクセス可能なすべてのサーバからのクラスタ データが含まれます。

Serviceability Reporter のサービス パラメータ

Cisco Serviceability Reporter は次のサービス パラメータを使用します。

- RTMT Reporter Designated Node : RTMT Reporter が動作する指定ノードを指定します。このデフォルトは、Cisco Serviceability Reporter サービスが最初にアクティブ化されたサーバの IP アドレスです。

Cisco Unified Communications Manager のみ : Serviceability Reporter サービスは CPU を大量に消費するため、非コール処理ノードを指定することを推奨します。

- Report Generation Time : 午前 0 時以降の分数を指定します。レポートは最新日のこの時刻に生成されます。最小値は 0 で、最大値は 1439 です。
- Report Deletion Age : レポートがディスクに保持される日数を指定します。指定した期間を経過したレポートは削除されます。最小値は 0 で、最大値は 30 です。



ヒント

レポートをディセーブルにするには、Report Deletion Age サービス パラメータの値を 0 に設定します。

サービス パラメータ設定に関する詳細については、次のガイドを参照してください。

- Cisco Unified Communications Manager のみ：『*System Configuration Guide for Cisco Unified Communications Manager*』
- Connection のみ：『*System Administration Guide for Cisco Unity Connection*』



(注)

Cisco Unified Communications Manager のみ：ノードがネットワークから完全に削除され、Cisco Unified Communications Manager Administration のサーバリストに表示されない場合、ログファイルにそのノードのデータが含まれている場合でも、Reporter はレポートを生成するときそのノードを含めません。

デバイス統計レポート

デバイス統計レポートは、IM and Presence Service および Cisco Unity Connection には適用されません。

デバイス統計レポートでは、次の折れ線グラフが表示されます。

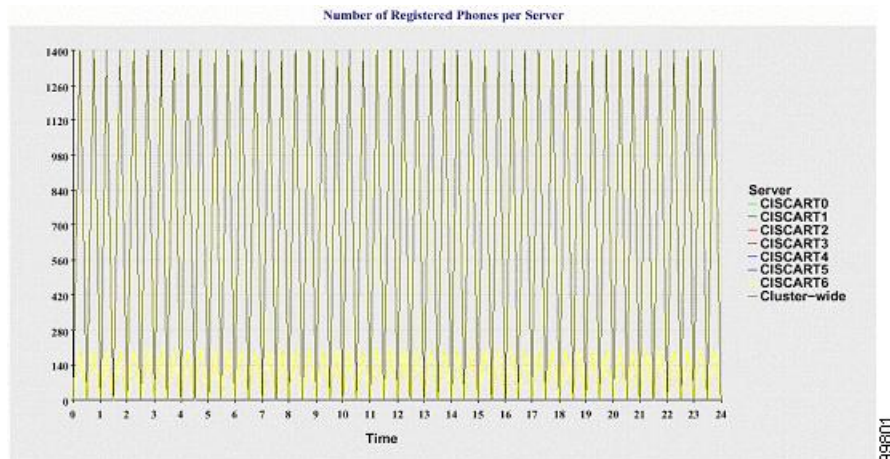
- サーバごとの登録済み電話機の数
- クラスタ内の H.323 ゲートウェイの数
- クラスタ内のトランクの数

サーバごとの登録済み電話機の数

折れ線グラフには、Cisco Unified Communications Manager の各サーバ（および Cisco Unified Communications Manager クラスタ構成内のクラスタ）の登録済み電話機の数が表示されます。グラフの各線はデータが利用できるサーバのデータを表し、クラスタ全体のデータを示す線がさらに 1 本あります（Cisco Unified Communications Manager クラスタのみ）。グラフ内の各データ値は、15 分の間に登録された電話機の平均数を表します。サーバにデータが表示されない場合、そのサーバを表す線は生成されません。登録済み電話機について、サーバ（または Cisco Unified Communications Manager クラスタ構成内のすべてのサーバ）のデータが存在しない場合、グラフは生成されません。メッセージ「利用可能なデバイス統計レポートのデータがありません (No data for Device Statistics report available)」が表示されます。

次の図は、Cisco Unified Communications Manager のクラスタ構成内の Cisco Unified Communications Manager サーバごとの登録済み電話機の数を表す折れ線グラフの例を示しています。

図 1: サーバごとの登録済み電話機の数を示す折れ線グラフ

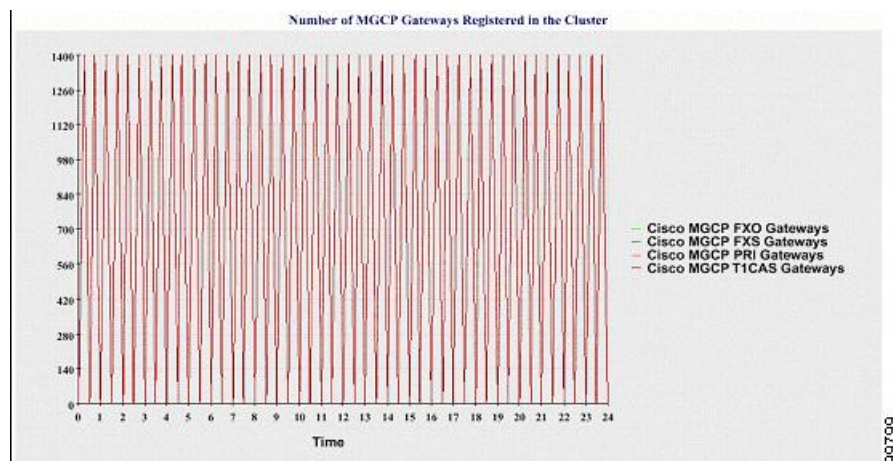


クラスタ内の登録済み MGCP ゲートウェイの数

折れ線グラフには、登録済み MGCP FXO、FXS、PRI、T1CAS ゲートウェイの数が表示されます。各線は、Cisco Unified Communications Manager サーバ（または Cisco Unified Communications Manager クラスタ構成のクラスタ）のデータのみ表しています。つまり、4 本の線は各ゲートウェイ タイプのサーバ（またはクラスタ全体）の詳細を示します。グラフ内の各データ値は、15 分の間に登録された MGCP ゲートウェイの平均数を表します。あるゲートウェイに関するデータがサーバ（またはクラスタ内のすべてのサーバ）に存在しない場合、そのゲートウェイのデータを表す線は生成されません。すべてのゲートウェイに関するデータがサーバ（またはクラスタ内のすべてのサーバ）に存在しない場合、グラフは生成されません。

次の図は、Cisco Unified Communications Manager クラスタ構成における、クラスタごとの登録済みゲートウェイの数を表す折れ線グラフの例を示しています。

図 2: クラスタごとの登録済みゲートウェイの数を示す折れ線グラフ

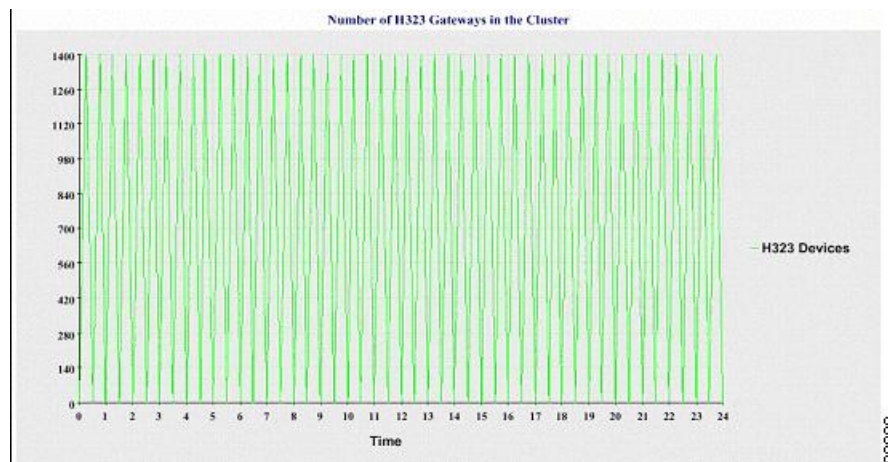


クラスタ内の H.323 ゲートウェイの数

折れ線グラフには、H.323 ゲートウェイの数が表示されます。1本の線により、H.323 ゲートウェイの詳細（または Cisco Unified Communications Manager クラスタ構成のクラスタ全体の詳細）が示されます。グラフ内の各データ値は、15分間での H.323 ゲートウェイの平均数を表します。サーバ（またはクラスタ内のすべてのサーバ）の H.323 ゲートウェイに関するデータが存在しない場合、グラフは生成されません。

次の図は、Cisco Unified Communications Manager クラスタ構成のクラスタごとの H.323 ゲートウェイの数を表す折れ線グラフの例を示しています。

図 3: クラスタごとの登録済み H.323 ゲートウェイの数を示す折れ線グラフ

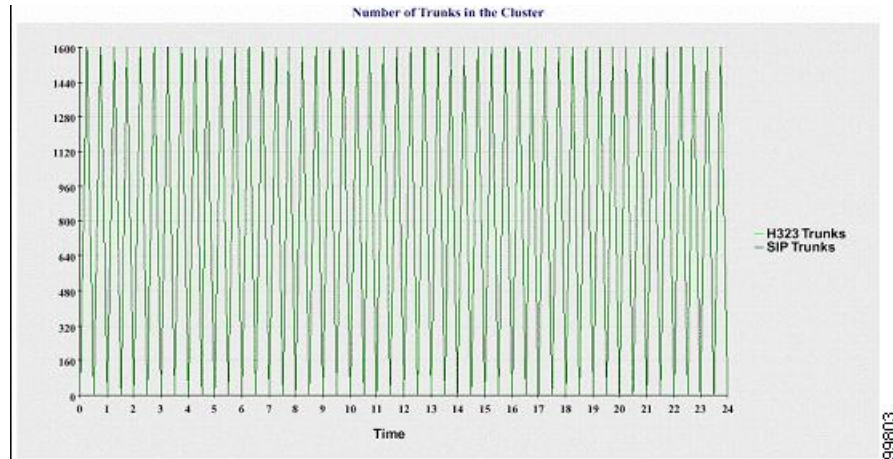


クラスタ内のトランクの数

折れ線グラフには、H.323 および SIP トランクの数が表示されます。2本の線により、H.323 トランクおよび SIP トランクの詳細（または Cisco Unified Communications Manager クラスタ構成のクラスタ全体の詳細）が示されます。グラフ内の各データ値は、15分間での H.323 および SIP トランクの平均数を表します。サーバ（またはクラスタ内のすべてのサーバ）の H.323 トランクに関するデータが存在しない場合、H.323 トランクのデータを表す線は生成されません。サーバ（またはクラスタ内のすべてのサーバ）の SIP トランクに関するデータが存在しない場合、SIP トランクのデータを表す線は生成されません。トランクに関するデータがまったく存在しない場合、グラフは生成されません。

次の図は、Cisco Unified Communications Manager クラスタ構成のクラスタごとのトランクの数を表す折れ線グラフの例を示します。

図 4: クラスタごとのトランクの数を示す折れ線グラフ



サーバ（またはクラスタ内の各サーバ）には、ファイル名パターン DeviceLog_mm_dd_yyyy_hh_mm.csv に一致するログファイルが格納されています。ログファイルには次の情報が格納されています。

- サーバ（または Cisco Unified Communications Manager クラスタ内の各サーバ）上の登録済み電話機の数
- サーバ（または Cisco Unified Communications Manager クラスタ内の各サーバ）上の登録済み MGCP FXO、FXS、PRI、および T1CAS ゲートウェイの数
- サーバ（または Cisco Unified Communications Manager クラスタ内の各サーバ）上の登録済み H.323 ゲートウェイの数
- SIP トランクと H.323 トランクの数

サーバ統計レポート

サーバ統計レポートでは、次の折れ線グラフが表示されます。

- サーバごとの CPU のパーセンテージ
- サーバごとのメモリ使用率のパーセンテージ
- サーバごとの最大パーティションのハードディスク使用率のパーセンテージ

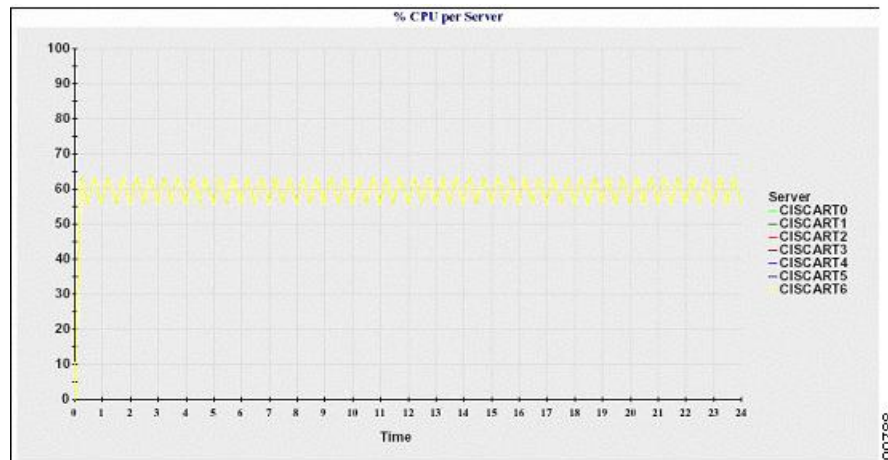
クラスタ固有の統計情報は、Cisco Unified Communications Manager および IM and Presence Service によってのみサポートされます。

サーバごとの CPU のパーセンテージ

折れ線グラフには、サーバ（またはクラスタ内の各サーバ）の CPU 使用率のパーセンテージが表示されます。グラフの折れ線は、データが利用できるサーバのデータを表します（または、クラスタ内のサーバごとに 1 本の折れ線）。グラフ内の各データ値は、15 分間の平均 CPU 使用率を表します。サーバ（またはクラスタ内のいずれかのサーバ）のデータが存在しない場合、そのサーバを表す線は生成されません。生成する線がない場合は、Reporter はグラフを作成しません。メッセージ「サーバ統計レポートのデータがありません (No data for Server Statistics report available)」が表示されます。

次の図は、Cisco Unified Communications Manager のクラスタ構成でサーバごとの CPU 使用率のパーセンテージを表す折れ線グラフの例を示します。

図 5: サーバごとの CPU のパーセンテージを示す折れ線グラフ

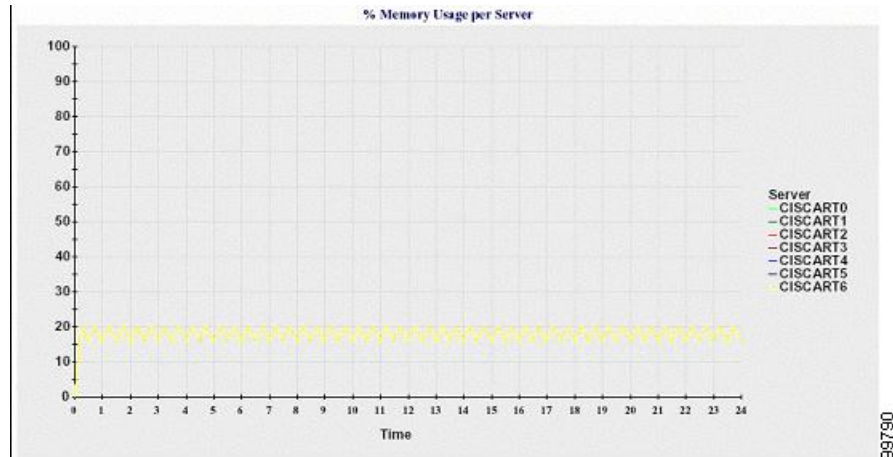


サーバごとのメモリ使用率のパーセンテージ

折れ線グラフには、Cisco Unified Communications Manager サーバのメモリ使用率のパーセンテージ (%MemoryInUse) が表示されます。Cisco Unified Communications Manager クラスタ構成では、データが利用できるクラスタ内のサーバごとに 1 本の線があります。グラフ内の各データ値は、15 分間の平均メモリ使用率を表します。データが存在しない場合はグラフが生成されません。クラスタ構成でいずれかのサーバのデータが存在しない場合、Reporter はそのサーバを表す線を生成しません。

次の図は、クラスタ構成で Cisco Unified Communications Manager サーバあたりのメモリ消費率を示す線グラフの例を示します。

図 6: サーバごとのメモリ使用率のパーセンテージを示す折れ線グラフ

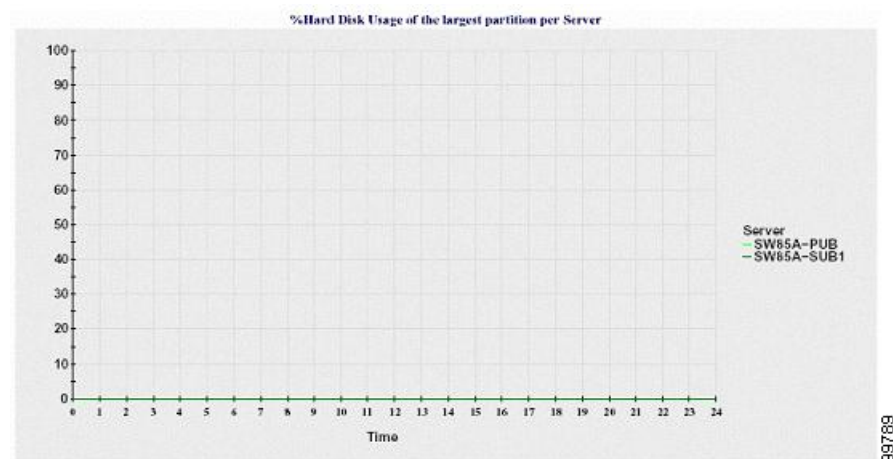


サーバごとの最大パーティションのハードディスク使用率のパーセンテージ

折れ線グラフには、サーバまたはクラスタ構成の各サーバ上の最大パーティションのディスク領域使用率のパーセンテージ (%DiskSpaceInUse) が表示されます。グラフ内の各データ値は、15分間の平均ディスク使用率を表します。データが存在しない場合はグラフが生成されません。クラスタ構成でいずれかのサーバのデータが存在しない場合、Reporter はそのサーバを表す線を生成しません。

次の図は、Cisco Unified Communications Manager のクラスタ構成でサーバごとの最大パーティションのハードディスク使用率のパーセンテージを表す折れ線グラフの例を示します。

図 7: サーバごとの最大パーティションのハードディスク使用率のパーセンテージを示す折れ線グラフ



サーバ（またはクラスタ構成内の各サーバ）には、ファイル名パターン `ServerLog_mm_dd_yyyy_hh_mm.csv` に一致するログファイルが格納されています。ログファイルには次の情報が格納されています。

- サーバ（またはクラスタ内の各サーバ）での CPU 使用率
- サーバ（またはクラスタ内の各サーバ）でのメモリ使用率（%MemoryInUse）
- サーバ（またはクラスタの各サーバ）の最大パーティションのハードディスク使用率（%DiskSpaceInUse）

サービス統計レポート

サービス統計レポートは、IM and Presence Service および Cisco Unity Connection をサポートしていません。

サービス統計レポートでは、次の折れ線グラフが表示されます。

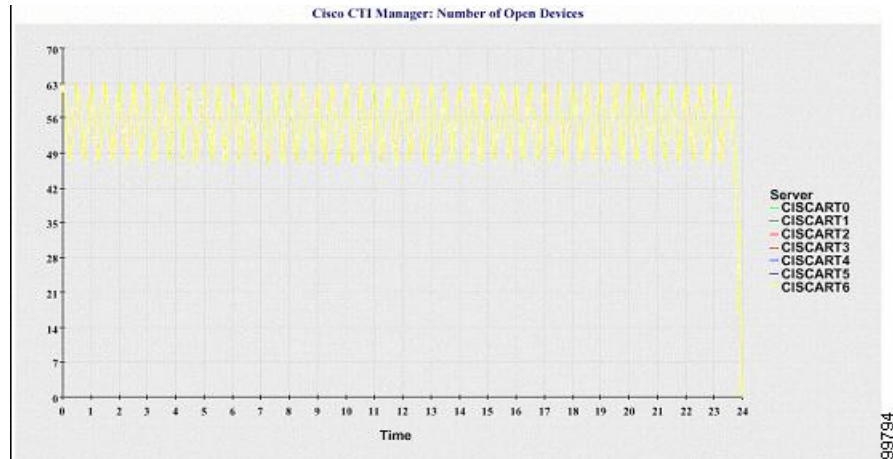
- Cisco CTI Manager : オープン デバイスの数
- Cisco CTI Manager : オープン回線の数
- Cisco TFTP : 要求の数
- Cisco TFTP : 中断された要求の数

Cisco CTI Manager : オープン デバイスの数

折れ線グラフには、CTI Manager（または Cisco Unified Communications Manager クラスタ構成内の各 CTI Manager）の CTI オープン デバイスの数が表示されます。各折れ線グラフは、サービスがアクティブなサーバ（または Cisco Unified Communications Manager のクラスタ内の各サーバ）のデータを表します。グラフ内の各データ値は、15 分間の CTI オープン デバイスの平均数を表します。データが存在しない場合はグラフが生成されません。Cisco Unified Communications Manager クラスタ構成でいずれかのサーバのデータが存在しない場合、Reporter はそのサーバを表す線を生成しません。メッセージ「利用可能なサービス統計レポートのデータがありません（No data for Service Statistics report available）」が表示されます。

次の図は、Cisco Unified Communications Manager のクラスタ構成で Cisco CTI Manager あたりのオープン デバイスを表す折れ線グラフの例を示します。

図 8 : Cisco CTI Manager : オープン デバイスの数を示す折れ線グラフ

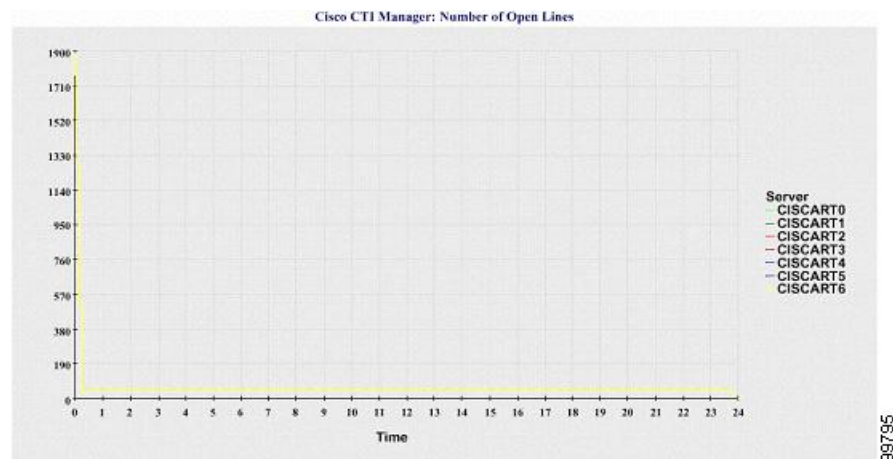


Cisco CTI Manager : オープン回線の数

折れ線グラフには、CTI Manager（または Cisco Unified Communications Manager クラスタ構成内の CTI Manager ごと）の CTI オープン回線の数が表示されます。グラフの折れ線は、Cisco CTI Manager サービスがアクティブなサーバのデータを表します（または Cisco Unified Communications Manager クラスタ構成内のサーバごとに 1 本の線）。グラフ内の各データ値は、15 分間の CTI オープン回線の平均数を表します。データが存在しない場合はグラフが生成されません。Cisco Unified Communications Manager クラスタ構成でいずれかのサーバのデータが存在しない場合、Reporter はそのサーバを表す線を生成しません。

次の図は、Cisco Unified Communications Manager のクラスタ構成内の Cisco CTI Manager ごとのオープン回線の数を表す折れ線グラフの例を示します。

図 9 : Cisco CTI Manager : オープン回線の数示す折れ線グラフ

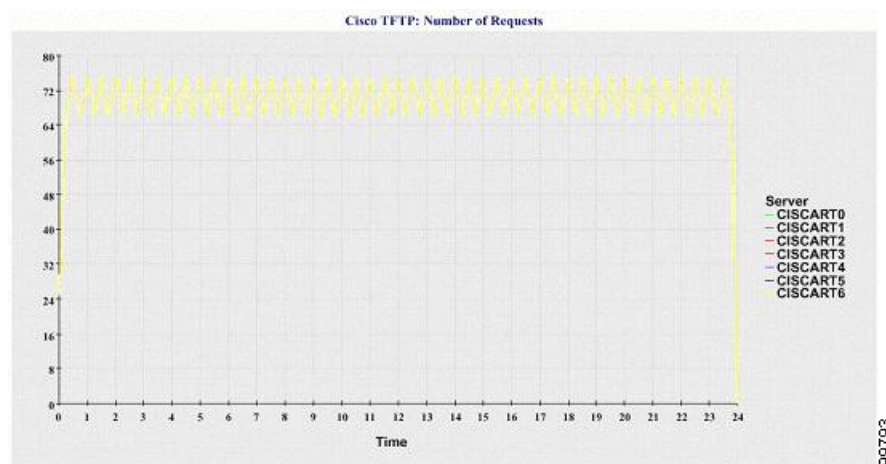


Cisco TFTP : 要求の数

折れ線グラフには、TFTP サーバ（または Cisco Unified Communications Manager クラスタ構成内の TFTP サーバごと）の Cisco TFTP 要求の数が表示されます。グラフの折れ線は、Cisco TFTP サービスがアクティブなサーバのデータを示します（または Cisco Unified Communications Manager クラスタ内のサーバごとに 1 本の線）。グラフ内の各データ値は、15 分間の TFTP 要求の平均数を表します。データが存在しない場合はグラフが生成されません。Cisco Unified Communications Manager クラスタ構成でいずれかのサーバのデータが存在しない場合、Reporter はそのサーバを表す線を生成しません。

次の図は、TFTP サーバごとの Cisco TFTP 要求の数を表す折れ線グラフの例を示します。

図 10 : Cisco TFTP : 要求の数を示す折れ線グラフ

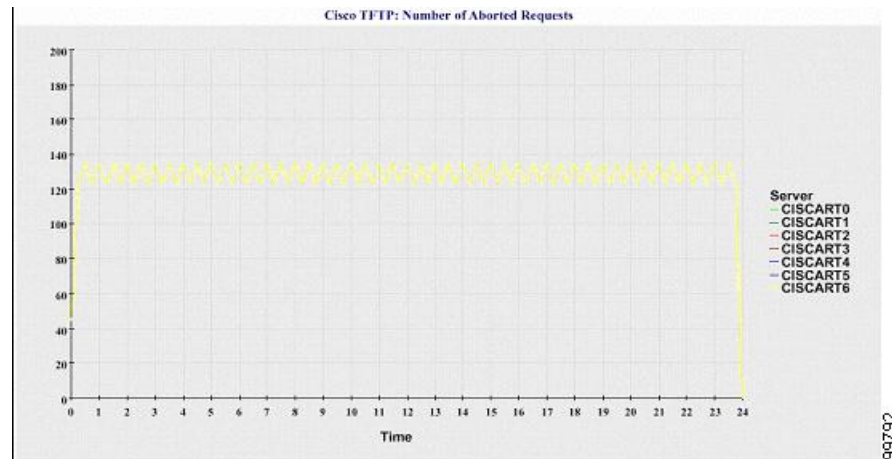


Cisco TFTP : 中断された要求の数

折れ線グラフには、TFTP サーバ（または Cisco Unified Communications Manager クラスタ構成内の TFTP サーバごと）の中断された Cisco TFTP 要求の数が表示されます。グラフの折れ線は、Cisco TFTP サービスがアクティブなサーバのデータを示します（または Cisco Unified Communications Manager クラスタ内のサーバごとに 1 本の線）。グラフ内の各データ値は、15 分間の中断された TFTP 要求の平均を表します。データが存在しない場合はグラフが生成されません。Cisco Unified Communications Manager クラスタ構成でいずれかのサーバのデータが存在しない場合、Reporter はそのサーバを表す線を生成しません。

次の図は、TFTP サーバごとに中断された Cisco TFTP 要求の数を表す折れ線グラフの例を示します。

図 11: *Cisco TFTP*: 中断された要求の数を表す折れ線グラフ



サーバ（または Cisco Unified Communications Manager クラスタ内の各サーバ）には、ファイル名パターン ServiceLog_mm_dd_yyyy_hh_mm.csv に一致するログ ファイルが格納されています。ログ ファイルには次の情報が格納されています。

- 各 CTI Manager : オープン デバイスの数
- 各 CTI Manager : オープン回線の数
- 各 Cisco TFTP サーバ : TotalTftpRequests
- 各 Cisco TFTP サーバ : TotalTftpRequestsAborted

コール アクティビティ レポート

コールアクティビティ レポートは、IM and Presence Service および Cisco Unity Connection をサポートしていません。

コールアクティビティ レポートでは、次の折れ線グラフが表示されます。

- クラスタの Cisco Unified Communications Manager コールアクティビティ
- クラスタの H.323 ゲートウェイ コールアクティビティ
- クラスタの MGCP ゲートウェイ コールアクティビティ
- MGCP ゲートウェイ
- クラスタのトランク コールアクティビティ

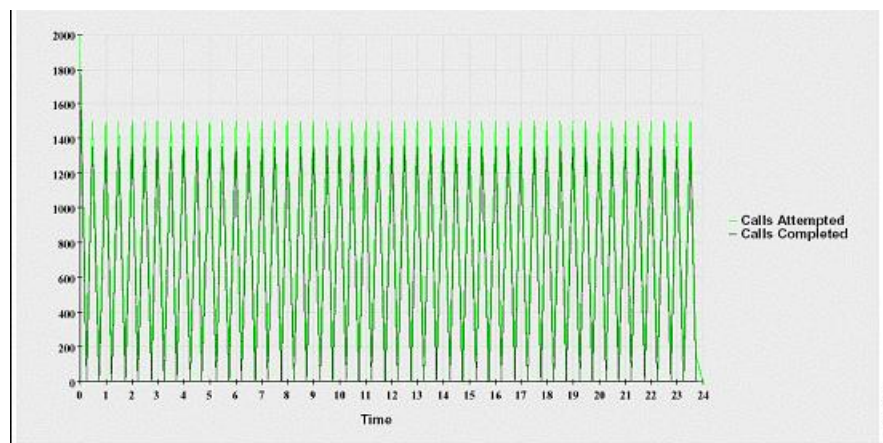
クラスタの Cisco Unified Communications Manager コール アクティビティ

折れ線グラフには、試行された Cisco Unified Communications Manager コールと完了したコールの数が表示されます。Cisco Unified Communications Manager クラスタ構成では、折れ線グラフにはクラスタ全体の試行されたコールと完了したコールの数が表示されます。グラフは2本の線で構成され、1本は試行されたコールの数、もう1本は完了したコールの数を示します。Cisco Unified Communications Manager クラスタ構成の場合、各線はクラスタ値を表します。これは（データが利用できる）クラスタ内のすべてのサーバの値の合計です。グラフ内の各データ値は、15分の間に試行されたコールと完了したコールの総数を表します。

完了した Cisco Unified Communications Manager コールのデータが存在しない場合、完了したコールのデータを表す線は生成されません。試行された Cisco Unified Communications Manager コールのデータが存在しない場合、試行されたコールのデータを表す線は生成されません。Cisco Unified Communications Manager クラスタ構成では、クラスタ内のサーバに関するデータが存在しない場合、そのサーバで試行されたコールと完了したコールを表す線は生成されません。Cisco Unified Communications Manager コール アクティビティのデータがまったく存在しない場合、グラフは生成されません。メッセージ「利用可能なコールアクティビティレポートのデータがありません (No data for Call Activities report available)」が表示されます。

次の図は、Cisco Unified Communications Manager クラスタの試行されたコールと完了したコールを表す折れ線グラフを示しています。

図 12：クラスタの Cisco Unified Communications Manager コール アクティビティを示す折れ線グラフ



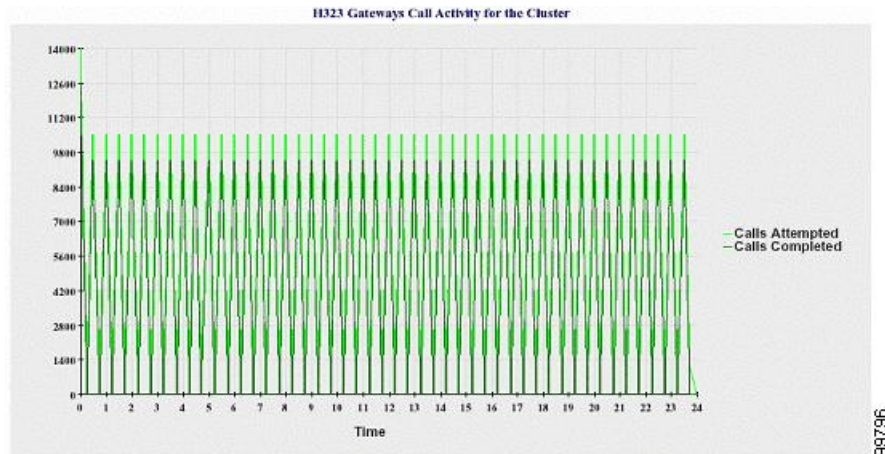
クラスタの H.323 ゲートウェイ コール アクティビティ

折れ線グラフには、H.323 ゲートウェイの試行されたコールと完了したコールの数が表示されます。Cisco Unified Communications Manager クラスタ構成では、折れ線グラフにはクラスタ全体の試行されたコールと完了したコールの数が表示されます。グラフは2本の線で構成され、1本は試行されたコールの数、もう1本は完了したコールの数を示します。Cisco Unified Communications Manager クラスタ構成の場合、各線はクラスタ値を表します。これは（データが利用できる）クラスタ内のすべてのサーバの値の合計と同じ値です。グラフ内の各データ値は、15分の間に試行されたコールと完了したコールの総数を表します。完了した H.323 ゲートウェイ コールのデータが存在しない場合、完了したコールのデータを表す線は生成されません。試行された H.323 ゲー

トウェイ コールのデータが存在しない場合、試行されたコールのデータを表す線は生成されません。Cisco Unified Communications Manager クラスタ構成では、クラスタ内のサーバに関するデータが存在しない場合、そのサーバで試行されたコールと完了したコールを表す線は生成されません。H.323 ゲートウェイ コールアクティビティのデータがまったく存在しない場合、グラフは生成されません。

次の図は、Cisco Unified Communications Manager クラスタの H.323 ゲートウェイ コールアクティビティを表す折れ線グラフを示しています。

図 13: クラスタの H.323 ゲートウェイ コールアクティビティを示す折れ線グラフ

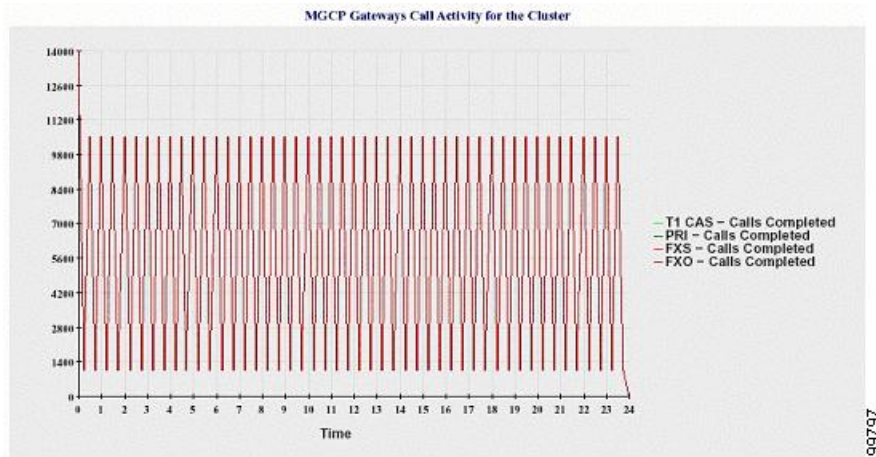


クラスタの MGCP ゲートウェイ コールアクティビティ

折れ線グラフには、MGCPFXO、FXS、PRI、およびTICASゲートウェイの1時間に完了したコールの数が表示されます。Cisco Unified Communications Manager クラスタ構成では、グラフにはCisco Unified Communications Manager クラスタ全体の完了したコールの数が表示されます。グラフは最大4本の線で構成され、完了したコールの数が（データが利用できる）ゲートウェイタイプごとに示されます。グラフ内の各データ値は、15分の間に完了したコールの総数を表します。ゲートウェイのデータが存在しない場合、その特定のゲートウェイについて完了したコールのデータを表す線は生成されません。すべてのゲートウェイに関してデータが存在しない場合、グラフは生成されません。

次の図は、Cisco Unified Communications Manager クラスタの MGCP ゲートウェイ コール アクティビティを表す折れ線グラフを示しています。

図 14: クラスタの MGCP ゲートウェイ コール アクティビティを示す折れ線グラフ

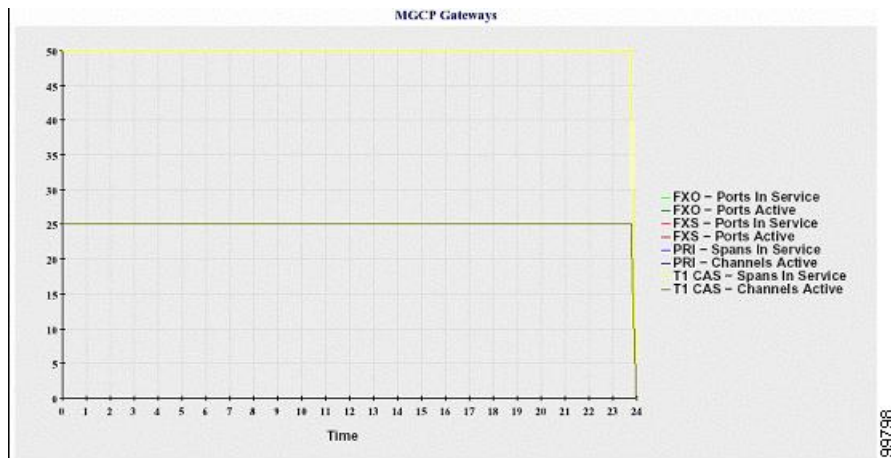


MGCP ゲートウェイ

折れ線グラフには、MGCP FXO ゲートウェイと FXS ゲートウェイの稼働中のポートおよびアクティブポートの数、および PRI ゲートウェイと TICAS ゲートウェイの稼働中のスパンまたはアクティブチャンネルの数が表示されます。Cisco Unified Communications Manager クラスタ構成の場合、グラフには Cisco Unified Communications Manager クラスタ全体のデータが表示されます。グラフは 8 本の線で構成され、MGCP FXO および FXS の稼働中のポートの数に 2 本、MGCP FXO および FXS のアクティブポートの数に 2 本割り当てられています。残りの 4 本は、PRI および TICAS ゲートウェイの稼働中のスパンとアクティブチャンネルの数を示しています。Cisco Unified Communications Manager クラスタ構成の場合、各線はクラスタ値を表します。これは（データが利用できる）クラスタ内のすべてのサーバの値の合計です。グラフ内の各データ値は、15 分間での稼働中のポートの総数、アクティブポートの数、稼働中のスパンの数、またはアクティブチャンネルの数を表します。すべてのサーバについて、ゲートウェイ（MGCP PRI、T1CAS）の稼働中のスパンまたはアクティブチャンネルの数に関するデータが存在しない場合、そのゲートウェイのデータを表す線は生成されません。

次の図は、MGCP ゲートウェイを表す折れ線グラフを示しています。

図 15: MGCP ゲートウェイを示す折れ線グラフ

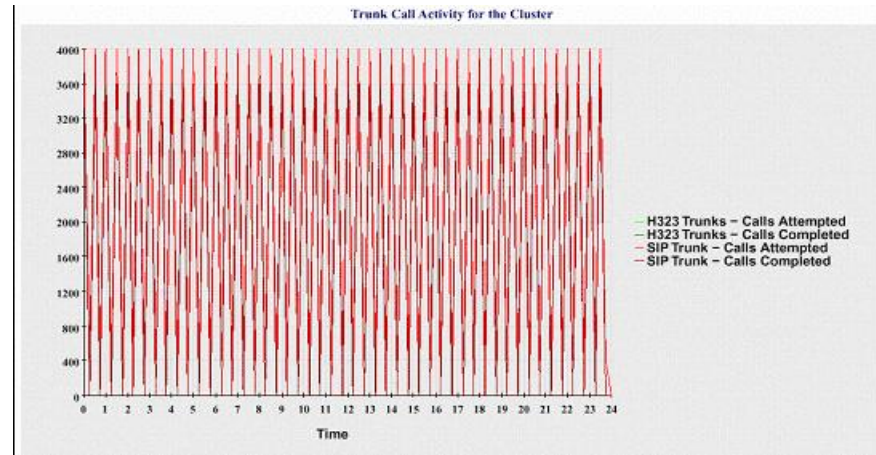


クラスタのトランクコールアクティビティ

折れ線グラフには、SIP トランクと H.323 トランクの 1 時間に完了したコールと試行されたコールの数が表示されます。Cisco Unified Communications Manager クラスタ構成の場合、グラフには Cisco Unified Communications Manager クラスタ全体の完了したコールと試行されたコールの数が表示されます。グラフは 4 本の線で構成され、2 本は（データが利用できる）SIP および H.323 トランクの完了したコールの数、もう 2 本は試行されたコールの数を示します。Cisco Unified Communications Manager クラスタ構成の場合、各線はクラスタ値を表します。これは（データが利用できる）クラスタ内のすべてのノードの値の合計です。グラフ内の各データ値は、15 分の間に完了したコールの総数または試行されたコールの数を表します。トランクのデータが存在しない場合、その特定のトランクについて完了したコールまたは試行されたコールを表す線は生成されません。両方のトランクタイプに関してデータが存在しない場合、グラフは生成されません。

次の図は、Cisco Unified Communications Manager クラスタのトランク コール アクティビティを表す折れ線グラフを示しています。

図 16: クラスタのトランク コール アクティビティを示す折れ線グラフ



サーバ（または Cisco Unified Communications Manager クラスタ構成内の各サーバ）には、ファイル名パターン CallLog_mm_dd_yyyy_hh_mm.csv に一致するログファイルが格納されています。ログファイルには次の情報が格納されています。

- Cisco Unified Communications Manager（または Cisco Unified Communications Manager クラスタ内の各サーバ）の試行されたコールおよび完了したコール
- H.323 ゲートウェイ（または Cisco Unified Communications Manager クラスタ内の各サーバのゲートウェイ）の試行されたコールおよび完了したコール
- MGCP FXO、FXS、PRI、T1CAS ゲートウェイ（または Cisco Unified Communications Manager クラスタ内の各サーバのゲートウェイ）の完了したコール
- （Cisco Unified Communications Manager クラスタ内の各サーバの）MGCP FXO ゲートウェイと FXS ゲートウェイの稼働中のポートおよびアクティブポート、および PRI ゲートウェイと T1CAS ゲートウェイの稼働中のスパンおよびアクティブチャンネル
- H.323 トランクと SIP トランクの試行されたコールおよび完了したコール

アラート サマリー レポート

アラート サマリー レポートには、その日に生成されたアラートの詳細が表示されます。

クラスタ固有の統計情報は、Cisco Unified Communications Manager および IM and Presence Service でのみサポートされます。

サーバごとのアラートの数

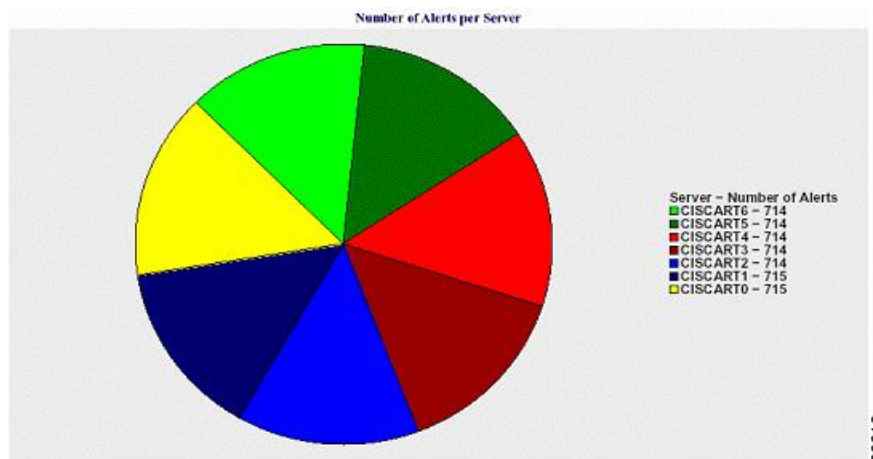
クラスタ内のノードごとのアラートの数が円グラフに表示されます。グラフには、生成されたアラートのサーバ全体の詳細が表示されます。円グラフの各領域は、クラスタの特定のサーバに対

して生成されたアラートの数を表しています。グラフには、クラスタ内のサーバ（Reporterによってその日にアラートが生成されたサーバ）と同じ数の領域が含まれます。あるサーバのデータがない場合、そのサーバを表すチャートの領域はありません。すべてのサーバのデータが存在しない場合はグラフが生成されません。メッセージ「その日はアラートが生成されませんでした（No alerts were generated for the day）」が表示されます。

Cisco Unity Connection のみ：円グラフには、サーバのアラート数が示されます。グラフには、生成されたアラートのサーバ全体の詳細が表示されます。サーバのデータが存在しない場合はグラフが生成されません。メッセージ「その日はアラートが生成されませんでした（No alerts were generated for the day）」が表示されます。

次のグラフは、Cisco Unified Communications Manager クラスタ内のサーバごとのアラート数を表す円グラフの例を示しています。

図 17: サーバごとのアラート数を示す円グラフ

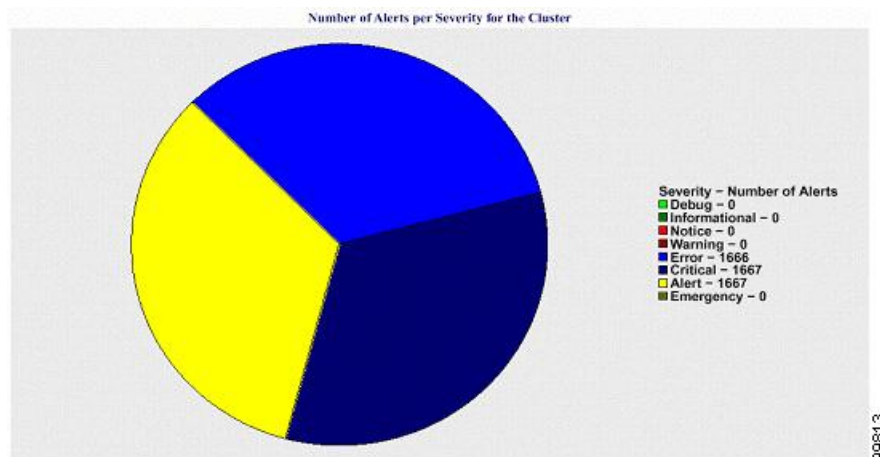


クラスタの重大度ごとのアラート数

アラートの重大度ごとのアラート数が円グラフに表示されます。グラフには、生成されたアラートの重大度の詳細が表示されます。円グラフの各領域は、生成された特定の重大度タイプのアラートの数を表します。グラフには、（Reporterによってその日に生成されたアラートの）重大度と同じ数の領域が含まれます。ある重大度のデータがない場合、その重大度を表すチャートの領域はありません。データが存在しない場合はグラフが生成されません。

次のグラフは、Cisco Unified Communications Manager クラスタの重大度ごとのアラート数を表す円グラフの例を示しています。

図 18: クラスタの重大度ごとのアラート数を表す円グラフ

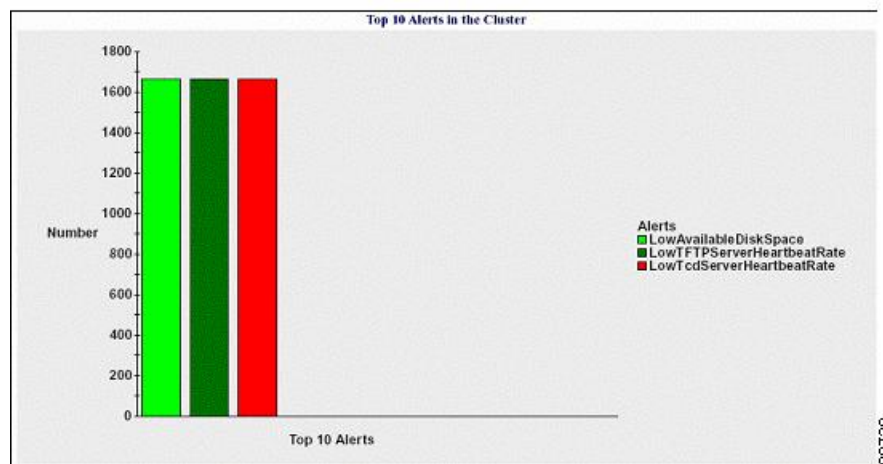


クラスタ内の上位 10 のアラート

特定のアラート タイプのアラート数が棒グラフに表示されます。グラフには、アラートタイプに基づいて生成されたアラートの詳細が表示されます。それぞれの折れ線は、そのアラートタイプのアラートの数を表します。グラフには、アラート数が多いものから順に、最初の 10 個のアラートの詳細のみが表示されます。特定のアラートタイプのデータがない場合、そのアラートを表す折れ線はありません。アラートタイプのデータがない場合はグラフが生成されません。

次のグラフは、Cisco Unified Communications Manager クラスタ内の上位 10 のアラートを表す棒グラフの例を示しています。

図 19: クラスタ内の上位 10 のアラートを表す棒グラフ



サーバ（またはクラスタ内の各サーバ）には、ファイル名パターン `AlertLog_mm_dd_yyyy_hh_mm.csv` に一致するログファイルが格納されています。ログファイルには次の情報が格納されています。

- 時刻：アラートが発生した時刻
- アラート名：わかりやすい名前
- ノード名：アラートが発生したサーバ
- モニタ対象オブジェクト：モニタされるオブジェクト
- 重大度：アラートの重大度

パフォーマンス保護レポート

パフォーマンス保護レポートは、IM and Presence Service および Cisco Unity Connection をサポートしていません。

パフォーマンス保護レポートには、特定のレポートの統計情報を表示するさまざまなグラフで構成される要約が表示されます。Reporter は、ログに記録された情報に基づいてレポートを 1 日 1 回生成します。

パフォーマンス保護レポートは、過去 7 日間のデフォルト モニタリング オブジェクトに関する傾向分析情報を提供します。この情報により、Cisco Intercompany Media Engine に関する情報を追跡できます。レポートには、Cisco IME クライアントの総コール数およびフォールバック コール率を示す Cisco IME クライアント コール アクティビティ グラフが表示されます。

パフォーマンス保護レポートは、次のグラフで構成されます。

- Cisco Unified Communications Manager コール アクティビティ
- 登録済み電話機および MGCP ゲートウェイの数
- システム リソースの使用率
- デバイスとダイヤル プランの数量

Cisco Unified Communications Manager コール アクティビティ

折れ線グラフには、試行されたコールと完了したコールの数の 1 時間ごとの増減率がアクティブコール数として表示されます。Cisco Unified Communications Manager のクラスタ構成では、クラスタ内の各サーバのデータについてグラフが作成されます。グラフは 3 本の線で構成され、それぞれ試行されたコールの数、完了したコールの数、およびアクティブコールを示します。コールアクティビティのデータが存在しない場合、Reporter はグラフを生成しません。

登録済み電話機および MGCP ゲートウェイの数

折れ線グラフには、登録済み電話機および MGCP ゲートウェイの数が表示されます。Cisco Unified Communications Manager のクラスタ構成の場合、グラフにはクラスタ内の各サーバのデータが表示されます。グラフは 2 本の線で構成され、1 本は登録済み電話機の数、もう 1 本は MGCP ゲー

トウェイの数を示します。電話機または MGCP ゲートウェイのデータがない場合、Reporter はグラフを生成しません。

システム リソースの使用率

折れ線グラフには、サーバ（または Cisco Unified Communications Manager クラスタ構成のクラスタ全体）の CPU 負荷率とメモリ使用率（バイト）が表示されます。グラフは 2 本の線で構成され、1 本は CPU 負荷、もう 1 本はメモリ使用率を示します。Cisco Unified Communications Manager のクラスタでは、各線はクラスタ値を表します。これは（データが利用できる）クラスタ内のすべてのサーバの値の平均です。電話機または MGCP ゲートウェイのデータがない場合、Reporter はグラフを生成しません。

デバイスとダイヤル プランの数量

2つのテーブルに、デバイスの数およびダイヤルプランコンポーネントの数に関する Cisco Unified Communications Manager データベースの情報が表示されます。デバイステーブルは、IP フォン、Cisco Unity Connection ポート、H.323 クライアント、H.323 ゲートウェイ、MGCP ゲートウェイ、MOH リソース、および MTP リソースの数を示します。ダイヤルプランテーブルは、電話番号と回線、ルートパターン、およびトランスレーションパターンの数を示します。

サービスアビリティ レポートのアーカイブのセットアップの概要

次の手順では、サービスアビリティ レポートのアーカイブ機能を設定する方法について説明します。

手順

-
- ステップ 1 Cisco Serviceability Reporter サービスをアクティブ化します。
 - ステップ 2 Cisco Serviceability Reporter サービスのパラメータを設定します。
 - ステップ 3 Cisco Serviceability Reporter サービスが生成するレポートを表示します。
-

関連トピック

[機能サービスのアクティブ化](#)

[Serviceability Reporter のサービス パラメータ](#)、(2 ページ)

サービスアビリティ レポートのアーカイブのセットアップ

Cisco Serviceability Reporter サービスは、Cisco Unified Serviceability の日次レポートを生成します。各レポートには、特定のレポートの統計を示すさまざまなチャートを構成する要約が表示されます。Reporter は、ログに記録された情報に基づいてレポートを 1 日 1 回生成します。

ここでは、[サービスアビリティ レポートのアーカイブ (Serviceability Reports Archive)] ウィンドウの使用方法について説明します。

はじめる前に

Cisco Serviceability Reporter サービスをアクティブ化します。このサービスをアクティブ化すると、CPU に高い負荷がかかります。サービスをアクティブ化した後、レポートの生成に最大 24 時間かかる場合があります。

Cisco Unified Communications Manager の場合のみ：このサービスはコール処理を行わないサーバでアクティブ化することを推奨します。

手順

-
- ステップ 1** [ツール (Tools)] > [サービスアビリティ レポートのアーカイブ (Serviceability Reports Archive)] を選択します。
[サービスアビリティ レポートのアーカイブ (Serviceability Reports Archive)] ウィンドウにレポートを確認できる月と年が表示されます。
- ステップ 2** [年月 (Month-Year)] ペインから、レポートを表示する月と年を選択します。
選択した月に対応する日の一覧が表示されます。
- ステップ 3** レポートを表示するには、レポートが生成された日に対応するリンクをクリックします。
選択した日のレポート ファイルが表示されます。
- ステップ 4** 特定の PDF レポートを表示するには、表示したいレポートのリンクをクリックします。
ヒント ブラウザでノード名を使用して Cisco Unified Serviceability を表示した場合は、レポートを表示する前に Cisco Unified Serviceability にログインする必要があります。
ネットワークでネットワーク アドレス変換 (NAT) を使用しているときに NAT の内側にあるサービスアビリティ レポートにアクセスする場合は、ブラウザの URL に NAT に関連付けられたプライベートネットワークの IP アドレスを入力します。NAT の外側にあるレポートにアクセスする場合は、パブリック IP アドレスを入力すると、NAT によってプライベート IP アドレスに適切に変換/マッピングされます。
PDF レポートを表示するには、Acrobat Reader をインストールしてください。Acrobat Reader をダウンロードするには、[サービスアビリティ レポートのアーカイブ (Serviceability Reports Archive)] ウィンドウの下部にあるリンクをクリックします。
ウィンドウが開き、選択したレポートの PDF ファイルが表示されます。
-

サービスアビリティ レポートのアーカイブへのアクセス

サービスアビリティ レポートのアーカイブのアクティブ化

手順

- ステップ 1 [ツール (Tools)]>[サービスのアクティベーション (Service Activation)]を選択します。
- ステップ 2 [サーバ (Server)]リストボックスで、必要なサーバを選択し、[移動 (Go)]を選択します。
- ステップ 3 [パフォーマンスおよびモニタリング サービス (Performance and Monitoring services)]ペインに移動します。
- ステップ 4 [Cisco Serviceability Reporter サービス (Cisco Serviceability Reporter service)]チェックボックスをオンにして、[Save (保存)]を選択します。
- ステップ 5 [ツール (Tools)]>[コントロールセンターの機能サービス (Control Center - Feature Services)]を選択します。
- ステップ 6 [サーバ (Server)]リストボックスで、必要なサーバを選択し、[移動 (Go)]を選択します。
- ステップ 7 [パフォーマンスおよびモニタリング サービス (Performance and Monitoring services)]に移動し、Cisco Serviceability Reporter を探します。
- ステップ 8 Cisco Serviceability Reporter のステータスが[起動済み (Started)]かつ[アクティブ化 (Activated)]になっていることを確認します。 Cisco Serviceability Reporter が動作していない場合は、Cisco Serviceability Reporter を選択し、[開始 (Start)]を選択します。

次の作業

ブラウザでサーバ名を入力して Cisco Unified IM and Presence Serviceability を開いた場合は、レポートを表示する前に Cisco Unified IM and Presence Serviceability にサインインする必要があります。

Cisco Unified IM and Presence Serviceability サービスは、他のノードでサービスを有効にした場合でも、必ず最初のノードでレポートを生成します。

サービスアビリティ レポートのアーカイブへのアクセス

はじめる前に

Cisco Serviceability Reporter サービスをアクティブ化します。 サービスをアクティブ化した後、レポートの生成に最大 24 時間かかる場合があります。

手順

- ステップ 1** [ツール (Tools)] > [サービスアビリティ レポートのアーカイブ (Serviceability Reports Archive)] を選択します。
- ステップ 2** [年月 (Month-Year)] セクションで、レポートを表示する月と年を選択します。
- ステップ 3** レポートが生成された日に対応するリンクを選択し、必要なレポートを表示します。
- ステップ 4** 表示するレポートのリンクを選択し、特定の PDF レポートを表示します。
[トレースフィルタ設定 (Trace Filter Settings)] 領域のデバイスに関するセクションは、IM and Presence には関係しません。
- ヒント** ブラウザでサーバ名を入力して Cisco Unified IM and Presence Serviceability を開いた場合は、レポートを表示する前に Cisco Unified IM and Presence Serviceability にサインインする必要があります。

CDR Repository Manager

この項の内容は、IM and Presence Service には適用されません。

[CDRの管理設定 (CDR Management Configuration)] ウィンドウを使用して、呼詳細レコード (CDR) ファイルと呼管理レコード (CMR) ファイルに割り当てるディスク領域の容量、ファイルを削除するまでの保存日数、および CDR の送信先となる最大 3 つの課金アプリケーションサーバを設定します。 CDR Repository Manager サービスは、CDR ファイルと CMR ファイルが正常に送信されるか、[CDRの管理設定 (CDR Management Configuration)] ウィンドウで課金アプリケーションサーバが変更または削除されるか、ファイルが保存期間を過ぎて削除されるまで、[CDRの管理設定 (CDR Management Configuration)] ウィンドウに設定されている課金サーバに対して、これらのファイルの送信を繰り返し試行します。



- (注) [エンタープライズパラメータ設定 (Enterprise Parameters Configuration)] ウィンドウにアクセスするには、Cisco Unified Communications Manager Administration を開き、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] の順に選択します。 **CDR File Time Interval** パラメータは、CDR データを収集する際の間隔を指定します。たとえば、この値を 1 に設定すると、各ファイルには 1 分間の CDR データ (有効になっている場合は CDR と CMR) が含まれます。外部課金サーバと CAR データベースは、この間隔が経過するまで各ファイルのデータを受信しません。そのため、このパラメータに設定する間隔を決める際には、どのくらい早く CDR データにアクセスする必要があるかを考慮してください。たとえば、このパラメータを 60 に設定すると、各ファイルには 60 分間のデータが含まれますが、60 分が経過し、レコードが CAR データベースに書き込まれ、CDR ファイルが設定済みの課金サーバに送信されるまで、そのデータは使用できません。デフォルト値は 1 です。最小値は 1 で、最大値は 1440 です。この必須フィールドの測定単位は分です。

CDR Agent と CDR Repository Manager の両方により、CDR File Time Interval に依存しない間隔でファイルが処理されます。CDR Repository Manager は、課金アプリケーション サーバに既存のすべての CDR ファイルを送信し、6 秒間スリープしてから送信する新しいファイルを確認して、この 6 秒間隔の動作を継続して行います。宛先（外部課金アプリケーション サーバ）が応答しない場合、スリープ間隔の 2 倍の長さ（12 秒）でプロセスが再試行されます。配信が失敗するたびにスリープ時間が倍増し（6、12、24、48 秒というように）、これは 2 分間に達するまで続きます。それ以降は配信が成功するまで 2 分間隔になります。配信が成功すると、自動的に 6 秒間隔に戻ります。

ユーザは、6 秒の処理間隔および障害時に倍増するスリープ間隔を設定できません。ユーザが設定できるのは、**CDR File Time Interval** エンタープライズ パラメータだけです。最初のファイル配信失敗後はアラートは送信されません。デフォルトでは、任意の課金アプリケーションサーバにファイルを配信する Cisco CDR Repository Manager サービスが 2 回目に配信に失敗した後に、CDRFileDeliveryFailed アラートが生成されます。電子メールを送信したり、ポケットベルなどで通知するようにアラートを設定できます。アラートの設定の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』の「Working with Alerts」の章を参照してください。

それ以降に課金アプリケーション サーバにファイルを配信できなかった場合は、CDRFileDeliveryFailureContinues の syslog アラームが生成されます。

CDR Agent はほぼ同じように動作します。まず、パブリッシャに既存のすべての CDR ファイルを送信します。送信する追加ファイルがない場合、CDR Agent は 6 秒間スリープしてから新しいファイルを確認します。配信が失敗するとすぐにスリープ間隔が 1 分間に変更され、配信が成功するまで 1 分間隔になります。ファイルの配信が成功すると、6 秒間隔に戻ります。

CDR Agent が最初にファイル配信に失敗した後は、アラートは送信されません。デフォルトでは、CDR Agent が 2 回目に配信に失敗した後に、CDRAgentSendFileFailed アラートが生成されます。電子メールを送信したり、ポケットベルなどで通知するようにアラートを設定できます。アラートの設定の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』の「Working with Alerts」の章を参照してください。

それ以降にファイルを配信できなかった場合は、CDRAgentSendFileFailedContinues の syslog アラームが生成されます。

ファイル転送タイマーを起動または再起動する必要がある場合は、[Cisco Unified Serviceability] ウィンドウに移動し、[ツール (Tools)] > [コントロールセンター (Control Center)] > [ネットワーク サービス (Network Services)] を選択すると、Cisco CDR Repository Manager または CDR Agent プロセスを再開できます。

High Water Mark パラメータに基づいてファイルの削除を有効にすると、CDR Repository Manager サービスは、CDR ファイルと CMR ファイルが使用するディスク領域の容量をモニタします。ディスク使用率が設定されている上限を超えると、ディスク領域が下限値に達するか、正常に配信されたファイルがすべて削除されるまで、すべての宛先に正常に配信され、（CAR がアクティブな場合は）CAR データベースにロードされた CDR ファイルおよび CMR ファイルがパーージされます。正常に配信されたファイルがすべて削除された後もディスク使用率が上限を超えている場合は、ディスク使用率が設定されているディスク割り当て量を超えていない限り、それ以上ファイルは削除されません。ディスク使用率が設定されているディスク割り当て量を超える場合は、

ファイルが保存期間内であるかどうか、または正常に配信されたかどうかに関係なく、ディスク使用率が上限を下回るまで、最も古いファイルからパージされます。



(注) High Water Mark パラメータに基づくファイルの削除を有効にするかどうかに関係なく、ディスク使用率が設定されているディスク割り当て量を超える場合は、CDR Repository Manager サービスによって、ディスク使用率が上限を下回るまで、最も古いファイルから CDR ファイルおよび CMR ファイルが削除されます。

Cisco Log Partition Monitoring Tool サービスは、CDR Repository Manager に配信されていない CDR フラット ファイルおよび CMR フラット ファイルのディスク使用率をモニタします。

Cisco Unified Communications Manager のみ：サーバのログパーティションのディスク使用率が設定されている上限を超過し、サービスによって他のログファイルとトレースファイルがすべて削除されている場合は、ログパーティションモニタ サービスによって、CDR Repository Manager に配信されていない後続ノードの CDR/CMR ファイルが削除されます。

ログパーティションモニタリングの詳細については、『Cisco Unified Real-Time Monitoring Tool Administration Guide』を参照してください。

一般パラメータのセットアップ

CDR のディスク使用およびファイル保存パラメータを設定するには、次の手順を実行します。

手順

-
- ステップ 1** [ツール (Tools)] > [CDR管理 (CDR Management)] を選択します。
[CDR管理 (CDR Management)] ウィンドウが表示されます。
- ステップ 2** 変更する CDR Manager 一般パラメータ値をクリックします。
- ステップ 3** 適切な CDR Repository Manager 一般パラメータの設定を入力します。
- ステップ 4** [Update (更新)] をクリックします。
- ヒント** いつでも [デフォルトの設定 (Set Default)] をクリックしてデフォルト値を指定できます。デフォルトの設定後、[更新 (Update)] をクリックしてデフォルト値を保存します。
-

関連トピック

[一般パラメータの設定, \(27 ページ\)](#)

一般パラメータの設定

次の表では、[CDRの管理設定 (CDR Management Configuration)] ウィンドウの [一般パラメータ (General Parameters)] セクションでの設定について説明します。

表 1: *CDR Repository Manager* の一般パラメータの設定

フィールド	説明
ディスク割り当て (MB) (Disk Allocation (MB))	<p>CDR および CMR フラット ファイル ストレージに割り当てる数値をメガバイトで選択します。</p> <p>デフォルトのディスクの割り当てと範囲は、サーバのハードドライブのサイズによって変わります。</p> <p>(注) CAR データベースの最大サイズは、Cisco Unified Communications Manager サーバの場合は 6 GB です。</p> <p>ディスク使用率が CDR ファイルに割り当てられた最大ディスク容量を超えると、システムによって CDRMaximumDiskSpaceExceeded アラートが生成され、正常に処理されたファイル (課金サーバに送信され、CAR にロードされたもの) がすべて削除されます。ディスク使用率が依然として割り当てられているディスク容量を超えている場合は、ディスク使用率の上限を下回るまで、未配信ファイルと保存期間内のファイルが最も古いものから削除されます。</p> <p>大規模なシステムで十分なディスク領域が割り当てられていない場合は、CAR Scheduler が CAR データベースにファイルをロードする前に、システムによって CDR ファイルと CMR ファイルが削除される場合があります。たとえば、CAR Scheduler が 1 日に 1 回実行されるよう設定した場合に、ディスク割り当ての設定が 1 日に生成される CDR ファイルおよび CMR ファイルを保存するには不十分な大きさであると、これらのファイルが CAR データベースにロードされる前にシステムによって削除されます。</p>

フィールド	説明
上限(%) (High Water Mark (%))	<p>このフィールドには、CDR ファイルおよびCMR ファイルに割り当てられるディスク容量の最大割合を指定します。たとえば、[ディスク割り当て (Disk Allocation)]フィールドから 2000 メガバイトを選択し、[上限(%) (High Water Mark (%))]フィールドから 80% を選択した場合、上限は 1600 メガバイトになります。上限の割合に加えて、CAR データベースの CDR 数は 1 つの Cisco Unified Communications Manager サーバで 2,000,000 レコードを超えることはできません。</p> <p>ディスク使用率が指定した割合を超えた場合、または CDR の総数が上限を超えた場合で、[HWMに基づく CDRまたはCMRファイルの削除の無効化 (Disable CDR/CMR Files Deletion Based on HWM)]チェックボックスがオフにされている場合には、正常に処理された CDR ファイルおよびCMR ファイル (課金サーバに送信され、CAR にロードされたもの) が、最も古いファイルから自動的に消去され、ディスク使用率が[下限(%) (Low Water Mark (%))]ドロップダウンリスト ボックスで指定した量になるまで減らされます。</p> <p>ディスク使用率が依然として下限または上限を超えている場合、ディスク使用率がディスク割り当ての値を超えていなければ、未配信のファイルまたはアンロードされたファイルは削除されません。</p> <p>[HWMに基づく CDRまたはCMRファイルの削除の無効化 (Disable CDR/CMR Files Deletion Based on HWM)]チェックボックスをオンにした場合は、CDR と CMR がこのフィールドで指定した割合に基づいて削除されることはありません。</p> <p>(注) CDR のディスク領域が上限を超えると、システムによって CDRHWMExceeded アラートが生成されます。</p>
下限(%) (Low Water Mark (%))	<p>このフィールドには、常に使用可能な CDR ファイルおよびCMR ファイルに割り当てるディスク容量の割合を指定します。たとえば、[ディスク割り当て (Disk Allocation)]フィールドから 2000 メガバイトを選択し、[下限(%) (Low Water Mark (%))]フィールドから 40% を選択した場合、下限は 800 メガバイトになります。</p>
CDR または CMR ファイルの保持期間(日数) (CDR / CMR Files Preservation Duration (Days))	<p>CDR ファイルおよび CMR ファイルを保持する日数を選択します。CDR Repository Manager は保持期間を過ぎたファイルを削除します。</p> <p>(注) CDRMaximumDiskSpaceExceeded アラームが繰り返し発生する場合は、ディスク割り当てを増やすか、または保持日数を短くしてください。</p>

フィールド	説明
HWMに基づく CDRまたはCMR ファイルの削除の無効化 (Disable CDR/CMR Files Deletion Based on HWM)	<p>(注) 上限のパラメータに基づく削除を有効化しているかどうかに関係なく、ディスク使用率が設定されているディスク割り当て、最大データベースサイズ、またはインストール環境の最大レコード数を超過した場合は、ディスク使用率が上限を下回るまで CDR Repository Manager サービスによって CDR ファイルおよび CMR ファイルが古いものから削除されます。</p> <p>ディスク使用率が [上限(%) (High Water Mark (%))] フィールドで指定した割合を超えた場合でも CDR と CMR を削除したくない場合は、このチェックボックスをオンにします。デフォルトではこのチェックボックスはオフにされているため、ディスク使用率が上限を超過するとシステムによって CDR と CMR が削除されます。</p>
CDR Repository Managerのホスト名 (CDR Repository Manager Host Name)	このフィールドには、CDR Repository Manager サーバのホスト名が一覧されます。
CDR Repository Managerのホストアドレス (CDR Repository Manager Host Address)	このフィールドには、CDR Repository Manager サーバの IP アドレスが一覧されます。

アプリケーション課金サーバのセットアップ

CDR の送信先となるアプリケーション課金サーバを設定するには、次の手順を使用します。最大 3 台の課金サーバを設定できます。

手順

ステップ 1 [ツール (Tools)] > [CDRの管理設定 (CDR Management Configuration)] の順に選択します。
[CDR の管理設定 (CDR Management Configuration)] ウィンドウが表示されます。

ステップ 2 次のいずれかの作業を実行します。

- 新しいアプリケーション課金サーバを追加するには、[新規追加 (Add New)] ボタンをクリックします。
- 既存のアプリケーション課金サーバを更新するには、サーバのホスト名/IPアドレスをクリックします。

ステップ 3 アプリケーション課金サーバのパラメータ設定を入力します。

ステップ 4 [追加 (Add)] または [更新 (Update)] をクリックします。

関連トピック

[アプリケーション課金サーバのパラメータ設定, \(30 ページ\)](#)

アプリケーション課金サーバのパラメータ設定

次の表に、[CDRの管理設定 (CDR Management Configuration)] ウィンドウの [課金アプリケーションサーバのパラメータ (Billing Application Server Parameters)] セクションで使用可能な設定について説明します。

表 2: アプリケーション課金サーバのパラメータ設定

フィールド	説明
ホスト名/IP アドレス (Host Name/IP Address)	<p>CDR の送信先となるアプリケーション課金サーバのホスト名または IP アドレスを入力します。</p> <p>このフィールドの値を変更すると、新しい宛先に未配信のファイルを送信するかどうかを尋ねるプロンプトが表示されます。</p> <p>次のいずれかの作業を実行します。</p> <ul style="list-style-type: none"> 新しいサーバにファイルを配信する場合は、[はい (Yes)] をクリックします。 未配信ファイルを送信せずにサーバのホスト名/IP アドレスを変更するには、[いいえ (No)] をクリックします。CDR 管理サービスによって CDR および CMR ファイルは正常に配信されたものとしてマークされます。
ユーザ名 (User Name)	アプリケーション課金サーバのユーザ名を入力します。
プロトコル (Protocol)	設定済みの課金サーバへ CDR ファイルを送信するために使用するプロトコルを FTP または SFTP から選択します。

フィールド	説明
ディレクトリパス (Directory Path)	<p>CDRの送信先となるアプリケーション課金サーバ上のディレクトリパスを入力します。指定するパスは、アプリケーション課金サーバで動作しているオペレーティングシステムによって、「/」または「\」で終了する必要があります。</p> <p>(注) FTPユーザにディレクトリに対する書き込み権限があることを確認します。</p>
パスワード (Password)	<p>アプリケーション課金サーバへのアクセスに使用するパスワードを入力します。</p>
障害時に再送 (Resend on Failure)	<p>[障害時に再送 (Resend on Failure)] ボックスをオンにすると、FTP または SFTP 接続が復旧した後に古い CDR および CMR ファイルを課金サーバに送信するように CDRM に通知されます。ボックスをオンにすると、Resend on Failure フラグが True に設定されます。チェックボックスをチェックしない場合、Resend on Failure フラグが False に設定されます。</p> <p>さまざまなシナリオが発生する可能性があります。課金サーバの Resend on Failure フラグが True に設定されている場合、すべての CDR ファイルが課金サーバに移動されます。Resend On Failure フラグが False に設定されている場合、課金サーバのシャットダウン中に生成された CDR ファイルが処理済みのフォルダに移動されますが、課金サーバには移動されません。Resend on Failure フラグが最初に True に設定された後で何度か変更された場合、[障害時に再送 (Resend on Failure)] ボックスがオンになるたびに CDR ファイルが課金サーバに移動されます。</p>
新しいキーの生成 (Generate New Key)	<p>新しいキーを生成し、SFTPサーバへの接続をリセットするには、[リセット (Reset)] ボタンをクリックします。</p>

アプリケーション課金サーバの削除

アプリケーション課金サーバを削除するには、次の手順を使用します。

手順

- ステップ 1** [ツール (Tools)] > [CDR管理 (CDR Management)] を選択します。
 [CDR の管理設定 (CDR Management Configuration)] ウィンドウが表示されます。

- ステップ 2** 削除するアプリケーション課金サーバの隣にあるチェックボックスをオンにして、[選択項目の削除 (Delete Selected)] をクリックします。
このサーバを削除すると、このサーバにまだ送信されていない CDR ファイルまたは CMR ファイルがこのサーバに送信されず、正常に送信されたファイルとして処理されることを示すメッセージが表示されます。
- ヒント** サーバを削除するとき、システムはそのサーバに送信されないファイルに対して CDRFileDeliveryFailed アラートを生成しません。
- ステップ 3** 削除を完了するには、[OK] をクリックします。
-

監査ログ

監査ログを使用すると、監査用の別のログ ファイルにシステムの設定変更が記録されます。

監査ロギング

監査ログを使用すると、監査用の別のログ ファイルにシステムの設定変更が記録されます。Serviceability GUI の [コントロールセンター - ネットワーク サービス (Control Center - Network Services)] の下に表示される Cisco Audit Event Service により、ユーザが行った、またはユーザの操作によって発生したシステムへの設定変更がモニタされ、ログに記録されます。

監査ログの設定を行うには、Serviceability GUI の [監査ログの設定 (Audit Log Configuration)] ウィンドウにアクセスします。

監査ログの構成は次のとおりです。

- **監査ロギングフレームワーク** : このフレームワークは、監査ログに監査イベントを書き込むためにアラーム ライブラリを使用する API で構成されます。GenericAlarmCatalog.xml として定義されたアラームカタログがこれらのアラームに適用されます。各種システムコンポーネントで独自のロギングが提供されます。

次に、アラームを送信するために Cisco Unified Communications Manager のコンポーネントが使用できる API の例を示します。

```
User ID: CCMAAdministratorClient IP Address: 172.19.240.207
Severity: 3
EventType: ServiceStatusUpdated
ResourceAccessed: CCMSERVICE
EventStatus: Successful
Description: CallManager Service status is stopped
```

- **監査イベントロギング** : 監査イベントとは、記録する必要があるあらゆるイベントを指します。次に、監査イベントの例を示します。

```
CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
UserID:CCMAAdministrator Client IP Address:172.19.240.207 Severity:3
EventType:ServiceStatusUpdated ResourceAccessed: CCMSERVICE
```



```
EventStatus:Successful Description: Call Manager Service status is
stopped App ID:Cisco Tomcat Cluster ID:StandAloneCluster Node
ID:sa-cml-3
```

**ヒント**

監査イベントのロギングは、デフォルトでは一元的に管理され、有効化されることに注意してください。Syslog Audit と呼ばれるアラーム モニタによってログが書き込まれます。デフォルトでは、ログはローテーションされるように設定されています。AuditLogAlarmMonitor が監査イベントを書き込むことができない場合、AuditLogAlarmMonitorはこのエラーを重大なエラーとしてsyslog ファイルに記録します。Alert Manager は、SeverityMatchFound アラートの一部としてこのエラーを報告します。イベント ロギングが失敗した場合も実際の動作は継続されます。監査ログはすべて、Cisco Unified Real-Time Monitoring Tool の Trace and Log Central から収集、表示、および削除されます。

Cisco Unified Serviceability のイベント ロギング

Cisco Unified Serviceability では次のイベントがログに記録されます。

- サービスのアクティブ化、非アクティブ化、起動、または停止。
- トレース設定およびアラーム設定の変更。
- SNMP 設定の変更。
- CDR 管理の変更（Cisco Unified Communications Manager のみ）。
- サービスアビリティ レポートのアーカイブのレポートの参照。このログは、レポート用ノードで表示されます（Cisco Unified Communications Manager のみ）。

Cisco Unified Real-Time Monitoring Tool のイベント ロギング

Cisco Unified Real-Time Monitoring Tool では、監査イベントアラームを含む次のイベントがログに記録されます。

- アラートの設定
- アラートの中断
- 電子メールの設定
- ノードアラート ステータスの設定
- アラートの追加
- アラートの追加アクション
- アラートのクリア
- アラートのイネーブル化
- アラートの削除アクション
- アラートの削除

Cisco Unified Communications Manager CDR Analysis and Reporting のイベント ロギング

Cisco Unified Communications Manager CDR Analysis and Reporting (CAR) では、次のイベントに関する監査ログが作成されます。

- ローダのスケジューリング
- 日次、週次、月次レポートのスケジューリング
- メールパラメータの設定
- ダイアルプラン設定
- ゲートウェイの設定
- システムプリファレンスの設定
- 自動消去の設定
- 接続時間、時刻、および音声品質の評価エンジンの設定
- QoS の設定
- 事前生成レポートの自動生成/アラートの設定
- 通知限度の設定

Cisco Unified Communications Manager Administration のイベント ロギング

Cisco Unified Communications Manager Administration のさまざまなコンポーネントについて、次のイベントがログに記録されます。

- ユーザのログイン/ログアウト
- ユーザのロールメンバーシップの更新 (ユーザの追加、ユーザの削除、またはユーザのロールの更新)
- ロールの更新 (新しいロールの追加、削除、または更新)
- デバイスの更新 (電話機およびゲートウェイ)
- サーバ設定の更新 (アラームまたはトレースの設定、サービスパラメータ、エンタープライズパラメータ、IP アドレス、ホスト名、イーサネット設定の変更、および Cisco Unified Communications Manager サーバの追加または削除)

Cisco Unified Communications Manager Administration のイベント ロギング

Cisco Unified Communications Manager Administration のさまざまなコンポーネントについて、次のイベントがログに記録されます。

- ユーザのログイン/ログアウト
- ユーザのロールメンバーシップの更新 (ユーザの追加、ユーザの削除、またはユーザのロールの更新)
- ロールの更新 (新しいロールの追加、削除、または更新)

- デバイスの更新（電話機およびゲートウェイ）
- サーバ設定の更新（アラームまたはトレースの設定、サービスパラメータ、エンタープライズパラメータ、IP アドレス、ホスト名、イーサネット設定の変更、および Cisco Unified Communications Manager サーバの追加または削除）

Cisco Unified Communications Manager ユーザ オプションのロギング

Cisco Unified Communications Manager ユーザ オプションについて、ユーザのロギング（ユーザのログインとログアウト） イベントがログに記録されます。

コマンドライン インターフェイスのイベントロギング

コマンドライン インターフェイスで実行されたすべてのコマンドがログに記録されます（Cisco Unified Communications Manager と Cisco Unity Connection の両方）。

Cisco Unity Connection Administration のイベント ロギング

Cisco Unity Connection Administration では次のイベントがログに記録されます。

- ユーザのログイン/ログアウト
- すべての設定変更（ユーザ、連絡先、コール管理オブジェクト、ネットワーク、システム設定、テレフォニーなど）
- タスク管理（タスクの有効化/無効化）
- 一括管理ツール（一括作成、一括削除）
- カスタム キーパッド マップ（マップの更新）

Cisco Personal Communications Assistant (Cisco PCA)

Cisco Personal Communications Assistant クライアントでは次のイベントがログに記録されます。

- ユーザのログイン/ログアウト
- Messaging Assistant で行われたすべての設定変更

Cisco Unity Connection Serviceability のイベント ロギング

Cisco Unity Connection Serviceability では次のイベントがログに記録されます。

- ユーザのログイン/ログアウト。
- すべての設定変更。
- サービスのアクティブ化、非アクティブ化、開始、または停止。

Representational State Transfer API を使用する Cisco Unity Connection クライアントのイベント ロギング

Representational State Transfer (REST) API を使用する Cisco Unity Connection クライアントでは次のイベントがログに記録されます。

- ユーザのログイン (ユーザの API 認証)。
- Cisco Unity Connection プロビジョニング インターフェイスを使用する API 呼び出し。

Cisco Unified IM and Presence Serviceability のイベント ロギング

Cisco Unified IM and Presence Serviceability では次のイベントがログに記録されます。

- サービスのアクティブ化、非アクティブ化、起動、または停止
- トレース設定およびアラーム設定の変更
- SNMP 設定の変更
- サービスアビリティ レポートのアーカイブ内のレポートの参照 (このログは、レポート用ノードで表示されます)

Cisco Unified IM and Presence Real-Time Monitoring Tool のイベント ロギング

Cisco Unified IM and Presence Real-Time Monitoring Tool では、監査イベント アラームを含む次のイベントがログに記録されます。

- アラートの設定
- アラートの中断
- 電子メールの設定
- ノードアラート ステータスの設定
- アラートの追加
- アラートの追加アクション
- アラートのクリア
- アラートのイネーブル化
- アラートの削除アクション
- アラートの削除

Cisco Unified Communications Manager IM and Presence Administration のイベント ロギング

Cisco Unified Communications Manager IM and Presence Administration のさまざまなコンポーネントについて、次のイベントがログに記録されます。

- 管理者のロギング (Administration、OS Administration、Disaster Recovery System、Reporting などの IM and Presence のインターフェイスへのログインおよびログアウト)

- ユーザのロールメンバーシップの更新（ユーザの追加、ユーザの削除、またはユーザのロールの更新）
- ロールの更新（新しいロールの追加、削除、または更新）
- デバイスの更新（電話機およびゲートウェイ）
- サーバ設定の更新（アラームまたはトレースの設定、サービスパラメータ、エンタープライズパラメータ、IP アドレス、ホスト名、イーサネット設定の変更、および IM and Presence サーバの追加または削除）

IM and Presence アプリケーションのイベント ロギング

IM and Presence アプリケーションのさまざまなコンポーネントでは、次のイベントがログに記録されます。

- IM クライアントへのエンドユーザのログイン（ユーザのログイン/ログアウト、およびログイン試行の失敗）
- IM チャットルームへのユーザの入室および退室
- IM チャットルームの作成と破棄

コマンドラインインターフェイスのイベント ロギング

コマンドライン インターフェイスで実行されたすべてのコマンドがログに記録されます。

システム監査ログ

システム監査ログでは、Linux OS ユーザの作成、変更、削除、ログの改ざん、およびファイルまたはディレクトリの権限に対するあらゆる変更をトレースします。このタイプの監査ログは、収集されるデータが大量になるためにデフォルトでディセーブルになっています。この機能を有効にするには、CLI を使用して手動で `utils auditd` を有効にします。システム監査ログ機能をイネーブルにすると、Real-Time Monitoring Tool の [Trace & Log Central] を使用して、選択したログの収集、表示、ダウンロード、削除を実行できます。システム監査ログは `vos-audit.log` という形式になります。

この機能をイネーブルにする方法については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。Real-Time Monitoring Tool から収集したログを操作する方法については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

アプリケーション監査ログ

アプリケーション監査ログは、ユーザによる、またはユーザ操作の結果発生したシステムへの設定変更をモニタし、記録します。

データベース監査ログ

データベース監査ログは、ログインなど、Informix データベースへのアクセスに関連するすべてのアクティビティを追跡します。

監査ログのセットアップ

Serviceability GUI を使用して監査ログを設定するには、次の手順を実行します。



(注) アプリケーションの監査ログ (Linux auditd) は、CLIからのみイネーブルまたはディセーブルにすることができます。このタイプの監査ログの設定は、Real-Time Monitoring Tool による vos-audit.log の収集以外は変更できません。

手順

-
- ステップ 1** [ツール (Tools)] > [監査ログの設定 (Audit Log Configuration)] を選択します。
[監査ログの設定 (Audit Log Configuration)] ウィンドウが表示されます。
- ステップ 2** 監査ログ設定を行います。
- ステップ 3** [保存 (Save)] をクリックします。
ヒント [デフォルトに設定 (Set to Default)] をクリックすると、いつでもデフォルト値を指定できます。デフォルトの設定後、[保存 (Save)] をクリックしてデフォルト値を保存します。
-

関連トピック

[監査ログの構成時の設定, \(38 ページ\)](#)

監査ログの構成時の設定

はじめる前に

監査ロールを割り当てられたユーザだけが監査ログの設定を変更できることに注意してください。Cisco Cisco Unified Communications Manager の場合、デフォルトでは、新規インストールまたはアップグレードの後で、CCMAdministrator に監査ロールが与えられます。CCMAdministrator は、Cisco Cisco Unified Communications Manager Administration の [ユーザグループ設定 (User Group Configuration)] ウィンドウで標準監査ユーザグループに監査権限を持つユーザを割り当てることができます。その後必要であれば、標準監査ユーザグループから CCMAdministrator を削除できます。

IM and Presence Serviceの場合、新規インストールまたはアップグレードの後で管理者に監査ロールが与えられ、監査権限を持つ任意のユーザを標準監査ユーザグループに割り当てることができます。

Cisco Unity Connection の場合、インストール時に作成されたアプリケーション管理アカウントが Audit Administrator ロールに割り当てられます。このアカウントは、他の管理者ユーザをこのロールに割り当てることができます。このアカウントから Audit Administrator ロールを削除することもできます。

Standard Audit Log Configuration ロールには、監査ログを削除する権限と、Cisco Unified Real-Time Monitoring Tool、IM and Presence Real-Time Monitoring Tool、Trace Collection Tool、Real-Time Monitoring Tool (RTMT) アラート設定、Serviceability ユーザインターフェイスのコントロールセンター-ネットワークサービス、RTMT プロファイルの保存、Serviceability ユーザインターフェイスの監査設定、監査トレースというリソースへの読み取り/更新権限が与えられます。

Standard Audit Log Configuration ロールには、監査ログを削除する権限と、Cisco Unified RTMT、Trace Collection Tool、RTMT アラート設定、Cisco Unified Serviceability のコントロールセンター-ネットワークサービス、RTMT プロファイルの保存、Cisco Unified Serviceability の監査設定、監査トレースというリソースへの読み取り/更新権限が与えられます。

Cisco Unity Connection の Audit Administrator ロールに割り当てられたユーザは、Cisco Unified RTMT で監査ログを表示、ダウンロード、および削除できます。

Cisco Cisco Unified Communications Manager のロール、ユーザ、ユーザグループの詳細については、『Administration Guide for Cisco Unified Communications Manager』を参照してください。

Cisco Unity Connection のロールとユーザの詳細については、『User Moves, Adds, and Changes Guide for Cisco Unity Connection』を参照してください。

IM and Presence のロール、ユーザ、ユーザグループの詳細については、『Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager』を参照してください。

次の表に、Cisco Unified Serviceability の [監査ログの設定 (Audit Log Configuration)] ウィンドウで設定できる設定について説明します。

表 3: 監査ログの構成時の設定

フィールド	説明
サーバの選択 (Select Server)	
サーバ (Server)	監査ログを設定するサーバ (ノード) を選択し、[移動 (Go)] をクリックします。
すべてのノードに適用 (Apply to All Nodes)	クラスタのすべてのノードに監査ログ設定を適用する場合は、[すべてのノードに適用 (Apply to All Nodes)] チェックボックスをオンにします。
アプリケーション監査ログの設定 (Application Audit Log Settings)	

フィールド	説明
監査ログを有効にする (Enable Audit Log)	<p>このチェックボックスをオンにすると、監査ログがアプリケーション監査ログに対して作成されます。</p> <p>Cisco Cisco Unified Communications Manager の場合、アプリケーションの監査ログは Cisco Cisco Unified Communications Manager Administration、Cisco Unified RTMT、Cisco Cisco Unified Communications Manager CDR Analysis and Reporting、Cisco Unified Serviceability などの Cisco Cisco Unified Communications Manager ユーザ インターフェイスの設定更新をサポートします。</p> <p>IM and Presence Service の場合、アプリケーション監査ログは Cisco Cisco Unified Communications Manager IM and Presence Administration、Cisco Unified IM and Presence Real-Time Monitoring Tool、Cisco Unified IM and Presence Serviceability などの IM and Presence ユーザ インターフェイスの設定更新をサポートします。</p> <p>Cisco Unity Connection の場合、アプリケーション監査ログは Cisco Unity Connection Administration、Cisco Unity Connection Serviceability、Cisco Personal Communications Assistant、接続 REST API を使用するクライアントなどの Cisco Unity Connection ユーザ インターフェイスの設定更新をサポートします。</p> <p>この設定は、デフォルトで有効と表示されます。</p> <p>(注) ネットワーク サービス Audit Event Service が動作している必要があります。</p>
消去を有効にする (Enable Purging)	<p>Log Partition Monitor (LPM) は、[消去を有効にする (Enable Purging)] オプションを確認して監査ログを消去する必要があるかどうかを判断します。このチェックボックスをオンにすると、共通パーティションのディスク使用率が上限を超えるたびに LPM によって RTMT のすべての監査ログ ファイルが消去されます。ただし、このチェックボックスをオフにして消去を無効にすることができます。</p> <p>消去が無効の場合、監査ログの数は、ディスクがいっぱいになるまで増加し続けます。このアクションは、システムの中断を引き起こす可能性があります。[消去を有効にする (Enable Purging)] チェックボックスをオフにすると、消去の無効化のリスクを説明するメッセージが表示されます。このオプションは、アクティブパーティションの監査ログに使用可能なことに注意してください。監査ログが非アクティブパーティションにある場合、ディスク使用率が上限を上回ると消去されません。</p> <p>監査ログにアクセスするには、RTMT の [Trace & Log Central] > [監査ログ (Audit Logs)] を選択します。</p> <p>(注) ネットワーク サービス Cisco Log Partition Monitoring Tool が動作している必要があります。</p>

フィールド	説明
ログローテーションを有効にする (Enable Log Rotation)	<p>システムは、このオプションを読み取り、監査ログファイルをローテーションする必要があるか、または新しいファイルの作成を続行するかを判断します。ファイルの最大数は5000を超えることはできません。[ログローテーションを有効にする (Enable Log Rotation)] チェックボックスをオンにすると、監査ログファイルが最大数に達すると最も古いファイルが上書きされます。</p> <p>ヒント ログローテーションを無効 (オフ) にすると、監査ログは[最大ファイル数 (Maximum No. of Files)] 設定を無視します。</p>
サーバ名 (Server Name)	<p>Syslog メッセージ受信のために使用する、リモート Syslog サーバの名前または IP アドレスを入力します。サーバ名が指定されていない場合、Cisco Unified IM and Presence Serviceability は Syslog メッセージを送信しません。Cisco Cisco Unified Communications Manager ノードは別のサーバからの Syslog メッセージを受け入れないため、Cisco Cisco Unified Communications Manager ノードを宛先として指定しないでください。</p> <p>これは、IM and Presence Service にのみ適用されます。</p>
リモート Syslog 監査イベントレベル (Remote Syslog Audit Event Level)	<p>リモート Syslog サーバの、対象となる Syslog メッセージの重大度を選択します。選択した重大度以上のすべての Syslog メッセージが、リモート Syslog に送信されます。</p> <p>これは、IM and Presence Service にのみ適用されます。</p>
最大ファイル数 (Maximum No. of Files)	<p>ログに含めるファイルの最大数を入力します。デフォルト設定は 250 です。最大数は 5000 です。</p>
最大ファイルサイズ (Maximum File Size)	<p>監査ログの最大ファイルサイズを入力します。ファイルサイズの値は 1 ~ 10 MB にする必要があります。1 ~ 10 の間の数を指定します。</p>
データベース監査ログ フィルタ設定 (Database Audit Log Filter Settings)	
監査ログを有効にする (Enable Audit Log)	<p>このチェックボックスをオンにすると、監査ログが Cisco Cisco Unified Communications Manager および Cisco Unity Connection データベースに対して作成されます。[デバッグ監査レベル (Debug Audit Level)] の設定とともにこの設定を使用します。これにより、データベースの特定の側面に対してログを作成できます。</p>

フィールド	説明
デバッグ監査レベル (Debug Audit Level)	<p>この設定では、ログで監査するデータベースの側面を選択できます。ドロップダウンリストボックスから、次のオプションのいずれかを選択します。各監査ログフィルタレベルは累積的であることに注意してください。</p> <ul style="list-style-type: none"> • [スキーマ (Schema)] : 監査ログ データベースの設定の変更 (たとえば、データベース テーブルのカラムや行) を追跡します。 • [管理タスク (Administrative Tasks)] : Cisco Cisco Unified Communications Manager システムのすべての管理上の変更 (たとえば、システムを維持するための変更) 、および [スキーマ (Schema)] のすべての変更を追跡します。 ヒント ほとんどの管理者は [管理タスク (Administrative Tasks)] 設定を無効にしたままにします。監査が必要なユーザに対しては、[データベースの更新 (Database Updates)] レベルを使用します。 • [データベースの更新 (Database Updates)] : データベースのすべての変更、および [スキーマ (Schema)] のすべての変更と [管理タスク (Administrative Tasks)] のすべての変更を追跡します。 • [データベースの読み取り (Database Reads)] : システムのすべての読み取りと、[スキーマ (Schema)]、[管理タスク (Administrative Tasks)]、および [データベースの更新 (Database Updates)] のすべての変更を追跡します。 ヒント Cisco Cisco Unified Communications Manager、IM and Presence Service、または Cisco Unity Connection システムを簡単に確認する場合にのみ、[データベースの読み取り (Database Reads)] レベルを選択します。このレベルでは、大量のシステムリソースを消費するため、短時間だけ使用してください。
監査ログローテーションを有効にする (Enable Audit Log Rotation)	<p>システムはこのオプションを読み取り、データベースの監査ログ ファイルをローテーションする必要があるか、または新しいファイルの作成を続行するかどうかを判断します。[監査ログローテーションを有効にする (Enable Audit Log Rotation)] オプションのチェックボックスをオンにすると、監査ログ ファイルが最大数に達すると最も古いファイルが上書きされます。</p> <p>この設定のチェックボックスがオフの場合、監査ログでは [最大ファイル数 (Maximum No. of Files)] 設定は無視されます。</p>

フィールド	説明
最大ファイル数 (Maximum No. of Files)	ログに含めるファイルの最大数を入力します。[最大ファイル数 (Maximum No. of Files)] 設定に入力した値が、[ログローテーション時に削除されるファイル数 (No. of Files Deleted on Log Rotation)] 設定に入力した値を上回っていることを確認します。 4 (最小) ~ 40 (最大) の値を入力できます。
ログローテーション時に削除されるファイル数 (No. of Files Deleted on Log Rotation)	データベース監査ログのローテーションが発生したときにシステムが削除できるファイルの最大数を入力します。 このフィールドに入力できる最小値は1です。最大値は[最大ファイル数 (Max No. of Files)] 設定に入力した値よりも2低い数値です。たとえば、[最大ファイル数 (Max No. of Files)] フィールドに 40 を入力した場合、[ログローテーション時に削除されるファイル数 (No. of Files Deleted on Log Rotation)] フィールドに入力できる最大数は 38 です。



注意

有効になっている場合、特にデバッグ監査レベルが [データベースの更新 (Database Updates)] または [データベースの読み取り (Database Reads)] に設定されていると、データベース ロギングが短時間で大量のデータを生成する可能性があります。これにより、多用期間中に、パフォーマンスに重大な影響が発生する可能性があります。通常、データベース ロギングは無効のままにすることを推奨します。データベースの変更を追跡するためにロギングを有効にする必要がある場合には、[データベースの更新 (Database Updates)] レベルを使用して短時間のみの有効にすることを推奨します。同様に、特にデータベース エントリをポーリングする場合 (データベースから 250 台のデバイスを引き出す場合など)、管理ロギングは Web ユーザー インターフェイスの全体的なパフォーマンスに影響を与えます。

ロケーション (Locations)

この項の内容は、IM and Presence Service には適用されません。

ここでは、Cisco Unified Serviceability のロケーション機能 ([ツール (Tools)] > [ロケーション (Locations)]) について説明します。この機能を使用すると、管理者は企業内の設定済みロケーションの詳細を表示し、リンクおよびロケーション内の不一致を把握し、2つのロケーション間の有効なパスを確認し、ロケーションの切断されたグループを識別することができます。

ロケーション トポロジ

Cisco Unified Serviceability のロケーション トポロジは、企業で設定されているロケーションの詳細を提供します。ロケーション トポロジとは、ネットワーク内でのメディアのフローを表すモデル化されたトポロジを意味します。

よく用いられる用語とその定義を以下に示します。

アサーション

アサーションとは、クラスタで設定されているロケーション、リンクの帯域幅、および重みの値を意味します。アサートされた値は、別のクラスタに複製することができます。

不一致

不一致は、さまざまなクラスタ間でアサートされたロケーションの帯域幅の値やリンクの帯域幅、重みの値に違いがある場合に発生します。

有効なパス

有効なパスとは、2つのエンドロケーションを接続する一連の中間ロケーションであり、隣り合うロケーション間の各リンクには重みが割り当てられます。有効なパスは累積した重みが最も少ないものとして決定され、任意の2つのエンドロケーション間で帯域幅の差し引きに使用される唯一のパスです。

ロケーショントポロジの表示

Cisco Unified Serviceability のロケーショントポロジは、管理者がグラフィカルなロケーショントポロジを表形式で表示する上で役立ちます。管理者は、[検索 (Find)] フィルタを使用して必要なロケーションの名前をフィルタリングできます。ロケーショントポロジデータには、選択したロケーションのロケーション内の詳細やリンクの詳細が含まれます。

ここでは、Cisco Unified Serviceability でロケーショントポロジを検索して表示する方法について説明します。

手順

-
- ステップ 1** Cisco Unified Serviceability で、[ツール (Tools)] > [ロケーション (Locations)] > [トポロジ (Topology)] の順に選択します。
[ロケーショントポロジ (Locations Topology)] ウィンドウが表示されます。
- ステップ 2** [ロケーション名でロケーションを検索 (Find Locations Where Location Name)] ドロップダウンボックスから、フィルタ条件を選択します。
- ステップ 3** [ロケーション名でロケーションを検索 (Find Locations Where Location Name)] フィールドに検索文字列を入力し、[検索 (Find)] をクリックします。
(注) [ロケーション名でロケーションを検索 (Find Locations Where Location Name)] フィールドでは、大文字と小文字は区別されません。
選択したフィルタ条件でロケーションのリストが表示されます。
- ステップ 4** リスト内で任意のロケーションをクリックして展開し、ロケーション内の詳細とリンクの詳細を表示します。
ロケーション内の詳細には音声、ビデオ、イマーシブ帯域幅が含まれ、リンクの詳細には2つのロケーションを接続するリンクの詳細 (重み付け、音声、ビデオ、イマーシブ帯域幅など) が含まれます。

ヒント ロケーションのリストが長くなる場合は、複数のページになることがあります。別のページを表示するには、[ロケーショントポロジ (Locations Topology)] ウィンドウの下部にある適切なナビゲーションボタンをクリックするか、[ページ (Page)] フィールドにページ番号を入力します。ウィンドウに表示されるロケーションの数を変更するには、[ページあたりの行数 (Rows Per Page)] ドロップダウンボックスから別の値を選択します。

ヒント ロケーションが注意記号で強調表示されている場合は、不一致があることを意味します。この不一致の詳細を表示するには、[アサーションの詳細を表示 (View Assertion Details)] リンクをクリックします。

ステップ 5 任意のロケーションのアサーションの詳細を表示するには、展開した詳細セクションの下部にある [アサーションの詳細を表示 (View Assertion Details)] リンクをクリックします。
[アサーションの詳細 (Assertion Details)] ウィンドウが表示されます。

ステップ 6 [ロケーショントポロジ (Locations Topology)] ウィンドウに戻るには、[閉じる (Close)] をクリックします。

(注) ロケーショントポロジデータを XML 形式でダウンロードするには、[ロケーショントポロジ (Locations Topology)] ウィンドウの下部にある [トポロジのダウンロード (Download Topology)] または上部のツールバーにある [トポロジのダウンロード (Download Topology)] アイコンをクリックします。

XML 形式のトポロジデータの詳細については、『Cisco Unified Communications Manager XML Developers Guide』を参照してください。

アサーションの詳細の表示

次のアサーションの詳細を表示するには、Serviceability GUI を使用します。

- ロケーション内設定のアサーション：[クラスタでアサート (Asserted by Cluster)]、[オーディオ (Audio)]、[ビデオ (Video)]、[イマーシブ帯域幅 (Immersive bandwidth)] など、ロケーション内のアサーションの詳細が含まれます。[クラスタでアサート (Asserted by Cluster)] カラムには、特定のロケーションをアサートするすべてのクラスタの名前が表示されます。
- リンクのアサーション：[クラスタでアサート (Asserted by Cluster)]、[重み付け (Weight)]、[オーディオ (Audio)]、[ビデオ (Video)]、[イマーシブ帯域幅 (Immersive bandwidth)] など、2つのロケーションを接続するリンクのアサーションの詳細が含まれます。

手順

ステップ 1 [ツール (Tools)] > [ロケーション (Locations)] > [ロケーショントポロジ (Locations Topology)] の順に選択します。

ステップ 2 [ロケーショントポロジ (Locations Topology)] ウィンドウで、[アサーションの詳細を表示 (View Assertion Details)] リンクをクリックします。

ロケーションの不一致

[ロケーションの不一致 (Locations Discrepancy)] 画面には、さまざまなロケーション設定のアサーションにおける競合が表示されます。

次の詳細情報が表示されます。

- [リンク設定の不一致 (Link Configuration Discrepancy)] : 重み、音声、ビデオ、イマーシブ帯域幅などの、2つのロケーションを接続するリンクの不一致の詳細が表示されます。
- [ロケーション内設定の不一致 (Intralocation Configuration Discrepancy)] : 音声、ビデオ、イマーシブ帯域幅などの、ロケーション内の不一致の詳細が表示されます。

ロケーションの不一致の表示

ここでは、Cisco Unified Serviceability でロケーションの不一致を表示する方法について説明します。

手順

-
- ステップ 1** Cisco Unified Serviceability で、[ツール (Tools)] > [ロケーション (Locations)] > [不一致 (Discrepancy)] の順に選択します。
[ロケーションの不一致 (Location Discrepancy)] ウィンドウが表示されます。
- ステップ 2** リンク設定の不一致とロケーション内設定の不一致のリストが表示されます。
(注) [リンク設定の不一致 (Link Configuration Discrepancy)] セクションには、不一致が検出されたリンク名だけが表示されます。リンク名は、<Location Name 1> <--> <Location Name 2> の形式でリストされます。[ロケーション内設定の不一致 (Intralocation Configuration Discrepancy)] セクションには、不一致が検出されたロケーションの名前だけが表示されます。リスト内の要素は辞書順にソートされます。
不一致が検出されなかった場合、次のステータスメッセージが表示されます。
不一致が見つかりません (No discrepancies found)
- ステップ 3** リストで、リンク名またはロケーション名をクリックして展開し、異なるクラスタによってアサートされている設定の詳細を表形式で表示します。
下の行には、音声、ビデオ、イマーシブ帯域幅プールおよび重み付けのために考慮される有効値が表示されます (リンクの場合)。有効値と一致しない値は赤で強調表示されます。
(注) 有効値は、特定のカラムの最小値です。たとえば、音声帯域幅の有効値は [音声帯域幅 (Audio Bandwidth)] カラムの最小値です。
-

有効なパス

Cisco Unified Serviceability の [有効なパス (Effective Path)] 画面には、管理者が指定する 2 つのロケーション間で確立される音声、ビデオ、またはイマーシブ コールにメディアが使用する有効なパスの詳細が表示されます。この画面には、有効なパスの各リンクおよび内部ロケーションで使用可能な帯域幅と設定された帯域幅が表示されます。管理者は、コールの発信で帯域幅の問題が生じた場合に、このレポートを使用してリンクと内部ロケーションでの帯域幅の可用性を判断することができます。また、コールの発信時の帯域幅の問題を修復し、帯域幅の可用性が低い場所を検索するためにも Cisco Unified Serviceability の [有効なパス (Effective Path)] を使用できます。

Cisco Unified Serviceability の [有効なパス (Effective Path)] 画面には、選択した 2 つのロケーション間について次の詳細が表示されます。

- [クイックパスの概要 (Quick Path Overview)] : 累積的な重みと、有効なパス全体の設定済みおよび使用可能な音声、ビデオ、イマーシブ帯域幅の値の一部が表示されます。
- [詳細パスビュー (Detailed Path View)] : 有効なパスを構成するロケーションとリンクに対する音声、ビデオ、イマーシブ コールの重みと帯域幅の値 (使用可能および設定済み) が表示されます。発信元のロケーションが上位、宛先のロケーションが下位という順序で表形式で表示されます。



(注) レポートに表示される使用可能な帯域幅の値は、有効なパスを表示した時点での値です。Cisco Unified Real-Time Monitoring Tool ではリアルタイムの値を表示できます。

有効なパスの表示

手順

- ステップ 1** Cisco Unified Serviceability で、[ツール (Tools)] > [ロケーション (Locations)] > [有効なパス (Effective Path)] の順に選択します。
[有効なパス (Effective Path)] ウィンドウが表示されます。
- ステップ 2** [ロケーション (Locations)] ドロップダウン ボックスから、有効なパスが必要な任意の 2 つのロケーションを選択し、[検索 (Find)] をクリックします。
または、入力ボックスにロケーション名を入力し、一致するロケーション名が表示されたら、[検索 (Find)] をクリックします。

[クイックパスの概要 (Quick Path Overview)] セクションや [詳細パスビュー (Detailed Path View)] セクションなどの有効なパスに関する詳細が表示されます。選択した 2 つのロケーション間にパスが存在しない場合、次のステータス メッセージが表示されます。

<From_Location>と<To_Location>の間にパスが存在しません。(No path exists between <From_Location> and <To_Location>.)

切断されたグループ

Cisco Unified Serviceability の [切断されたグループ (Disconnected Groups)] 画面では、管理者がトポロジの一部であるロケーション間の切断を確認し、分析することができます。この画面には切断されたグループのロケーションの一覧が表示され、接続が必要なロケーションを管理者が理解するのに役立ちます。

トポロジ内での切断は、2つのロケーション間にリンクが設定されていないか、共有ロケーション名のスペルが間違っている場合に発生します。



(注) [切断されたグループ (Disconnected Groups)] 画面には、切断されたロケーションのグループだけが表示され、比較することができます。接続されたロケーションの詳細については、『*Administration Guide for Cisco Unified Communications Manager*』のロケーション設定に関するトピックを参照してください。

切断されたグループの表示

ここでは、Cisco Unified Serviceability で切断されたグループを表示する方法について説明します。

手順

Cisco Unified Serviceability で、[ツール (Tools)] > [ロケーション (Locations)] > [切断されたグループ (Disconnected Groups)] の順に選択します。

[切断されたグループ (Disconnected Groups)] 画面が表示されます。

以下の表に、[切断されたグループ (Disconnected Groups)] 画面に表示される設定の詳細を示します。

表 4: [切断されたグループ (Disconnected Groups)] 画面の設定

設定	説明
切断されたグループのリスト	
選択 (Select)	切断されたグループを選択して別の切断されたグループと比較する場合に、このボックスをオンにします。 注意 比較する際はグループを2つだけ選択できません。
グループ ID (Group ID)	選択したグループの自動生成された一意の ID 番号が表示されます。

設定	説明
説明 (Description)	グループ内の最初と最後のロケーションの名前が (アルファベット順に) 表示されます。 (注) 切断されたグループに1つのノードだけが存在する場合、そのノードの名前だけがここに表示されます。
ロケーションの数 (No of Locations)	グループ内のロケーションの数が表示されます。
選択したグループの比較 (Compare Selected Groups)	選択したグループを表示および比較するには、このボタンをクリックします。このボタンをクリックすると、選択したグループに関する詳細が表示されます。 選択したすべてのグループについて、そのグループに含まれるロケーションの名前と、ロケーションをアサートする対応するクラスタが表示されます。次の「選択したグループの比較ビュー」を参照してください。
選択したグループの比較ビュー	
ロケーション名 (Location Name)	グループに含まれているすべてのロケーションの名前がこのカラムに表示されます。
クラスタでアサート (Asserted by Cluster)	特定のロケーションをアサートするすべてのクラスタの名前がこのカラムに表示されます。

切断されたグループにロケーションが存在しない場合、次のステータスメッセージが表示されます。

切断されたグループのロケーションが見つかりません (No disconnected groups of locations found)



(注) 切断されたグループのリストは、どのカラムでもソートできます。デフォルトでは、グループは [ロケーションの数 (No of Locations)] カラムでソートされます。

