

Cisco Unified Communications Managerの管理者アクティビティを監査するためのリアルタイムモニタリングツールの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Cisco Unified Communications Manager(CUCM)のリアルタイムアクティビティを表示および監査するようにReal Time Monitoring Tool(RTMT)を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- CUCM の管理
- CUCMトレースの設定
- RTMTナビゲーション

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Unified Communications Manager
- リアルタイム監視ツール

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

CUCMの場合、アプリケーション監査ログは、Communications Manager Administration、Cisco Unified RTMT、Cisco Unified Communications Manager CDR Analysis and Reporting、Cisco Unified ServiceabilityなどのCUCMインターフェイスの設定更新をサポートします。

IM and Presenceサービスの場合、アプリケーション監査ログは、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インターフェイスの設定更新をサポートします。

Cisco Unity Connectionの場合、アプリケーション監査ログは、Cisco Unity Connectionインターフェイス、Cisco Unity Connection Administration、Cisco Unity Connection Serviceability、Cisco Personal Communications Assistant、およびConnection REST Application Programming Interfaces(API)を使用するクライアントの設定更新をサポートします。

設定

次の手順に従って、監査ログ機能を設定し、RTMTから監査証跡を表示します。

ステップ1：監査ログを有効にします。[Cisco Unified Serviceability] > [Tools] > [Audit Log Configuration]に移動し、これらのパラメータを有効にします

- 監査ログの有効化
- ページの有効化
- ログのローテーションの有効化
- 詳細な監査ログ(詳細な監査ログは、通常の監査ログと同じ項目を提供しますが、設定変更も含まれます。たとえば、監査ログには、変更された値を含む、追加、更新、および削除された項目が含まれます)。

注：これらのサービス、Network Service Audit Event Service、およびNetwork Service Cisco Log Partitions Monitoringを有効にする必要があります

ヒント：ログのローテーションが無効(オフ)の場合、監査ログは[ファイルの最大数]設定を無視します。

Audit Log Configuration

 Save  Set to Default

Status:

 Ready

Select Server

Server*

Apply to All Nodes

Application Audit Log Settings

Filter Settings

- Enable Audit Log
- Enable Purging
- Enable Log Rotation
- Detailed Audit Logging

Remote Syslog

Server Name¹

Remote Syslog Audit Event Level

Output Settings

Maximum No. of Files*

Maximum File Size (MB)*

Notification Settings

Warning Threshold for Approaching Log Rotation Overwrite (%)*

Database Audit Log Filter Settings

Enable Audit Log

Debug Audit Level

Output Settings

Enable Audit Log Rotation

Maximum No. of Files*

No. of Files Deleted on Log Rotation*

ステップ2:RTMTを使用して監査ログを表示できます。Cisco RTMTを開いてログインします。[システム]>[ツール]>[AuditLog Viewer]に移動し、アクティビティを監視するノードを選択します。

ステップ3:[AuditApp Logs]を選択し、選択リストから目的の.logファイルを選択します。選択したログファイルのイベントが表示されます。

File System Voice/Video AnalysisManager IM and Presence Edit Window Application Help

Real Time Monitoring Tool For Cisco Unified Communications Solutions

System

AuditLog Viewer Select a Node cucm1151pub.ad.erleite.com Auto Refresh

Logs

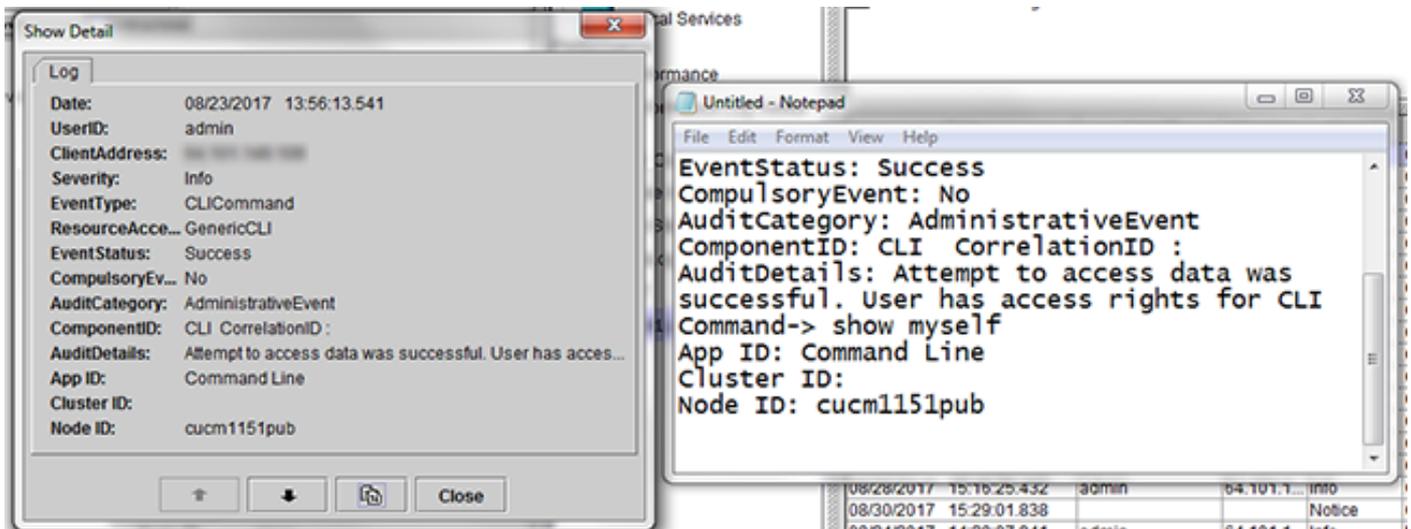
- AuditApp Logs
 - Archive
 - Audit00000012.log
- Cisco Unified OS Logs

Date	UserID	ClientAd...	Severity ▾	EventType	Re
08/24/2017 16:37:04.752	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/24/2017 16:37:06.257	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/24/2017 16:37:17.131	admin	64.101.1...	Error	UserLogging	Cisco SOAP Serve
08/24/2017 16:40:31.716	admin	64.101.1...	Error	UserLogging	Cisco Trace Collec
08/25/2017 15:18:37.030	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/25/2017 15:18:38.314	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/25/2017 15:18:48.385	admin	64.101.1...	Error	UserLogging	Cisco SOAP Serve
08/25/2017 15:20:04.751	admin	64.101.1...	Error	UserLogging	Cisco Trace Collec
08/28/2017 15:09:15.698		64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 15:09:15.751		64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 15:09:28.996	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 15:09:29.053	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 15:09:48.575	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 15:09:48.720	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 15:11:32.090	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 15:11:32.142	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 15:14:27.341	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 15:14:28.661	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 15:14:38.874	admin	64.101.1...	Error	UserLogging	Cisco SOAP Serve
08/28/2017 16:33:50.695	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 16:33:51.944	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 16:34:01.460	admin	64.101.1...	Error	UserLogging	Cisco SOAP Serve
08/29/2017 13:25:12.187	admin	10.201.2...	Error	UserLogging	Apache-Axis2
08/29/2017 13:50:16.272	admin	10.201.2...	Error	UserLogging	Apache-Axis2

Refresh Clear Filter Find Save

System Summary AuditLog Viewer

ステップ4：イベントの詳細を表示するには、目的のエントリを2回選択します。この例では、コマンドshow myeがノードcucm1151pubで実行されたことを示すCLIコマンド監査証跡があります。別の場所に貼り付けることができるアラートの詳細をコピーするには、二重ページの画像が付いたアイコンを選択します。



ヒント：[自動更新]のチェックボックスをオンにすると、AuditLog Viewer内のログエントリに対する動的な更新が有効になります。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- [監査ログの構成設定](#)