

Configurer l'outil de surveillance en temps réel pour l'activité d'audit de l'administrateur dans Cisco Unified Communications Manager

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer l'outil de surveillance en temps réel (RTMT) pour afficher et auditer l'activité en temps réel dans Cisco Unified Communications Manager (CUCM).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration CUCM
- Configuration du suivi CUCM
- Navigation RTMT

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Solutions Cisco Unified Communications Manager
- Outil de surveillance en temps réel

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Pour CUCM, le journal d'audit des applications prend en charge les mises à jour de configuration pour les interfaces CUCM telles que Communications Manager Administration, Cisco Unified RTMT, Cisco Unified Communications Manager CDR Analysis and Reporting et Cisco Unified Servicability.

Pour le service IM and Presence, le journal d'audit des applications prend en charge les mises à jour de configuration pour les interfaces IM et Presence telles que Cisco Unified Communications Manager IM and Presence Administration, Cisco Unified IM and Presence Real-Time Monitoring Tool et Cisco Unified IM and Presence Servicability.

Pour Cisco Unity Connection, le journal d'audit des applications prend en charge les mises à jour de configuration pour les interfaces Cisco Unity Connection, l'administration Cisco Unity Connection, la facilité de maintenance Cisco Unity Connection, Cisco Personal Communications Assistant et les clients qui utilisent les API (Connection REST Application Programming Interfaces).

Configuration

Suivez ces étapes afin de configurer la capacité du journal d'audit et d'afficher la piste d'audit à partir de RTMT.

Étape 1. Activer le journal d'audit. Accédez à **Cisco Unified Serviceability > Tools > Audit Log Configuration** et activez ces paramètres

- Activer le journal d'audit
- Activer la purge
- Activer la rotation du journal
- Journalisation détaillée de l'audit (les journaux d'audit détaillés fournissent les mêmes éléments que les journaux d'audit standard, mais incluent également des modifications de configuration. Par exemple, le journal d'audit inclut les éléments qui ont été ajoutés, mis à jour et supprimés, y compris les valeurs modifiées.)

Note: Vous devez activer ces services, **Service d'audit des services réseau** et **Service réseau Surveillance des partitions du journal Cisco**

Astuce : Lorsque la rotation du journal est désactivée (non cochée), le journal d'audit ignore le paramètre Nombre maximal de fichiers.

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*

Étape 2. Vous pouvez désormais utiliser RTMT pour afficher les journaux d'audit. Ouvrez et connectez-vous à Cisco RTMT. Accédez à **System > Tools > AuditLog Viewer** et sélectionnez le noeud à partir duquel vous souhaitez surveiller l'activité.

Étape 3. Sélectionnez **Journaux AuditApp** et dans la liste de sélection, puis choisissez le fichier .log souhaité. Un affichage des événements du fichier journal sélectionné s'affiche.

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

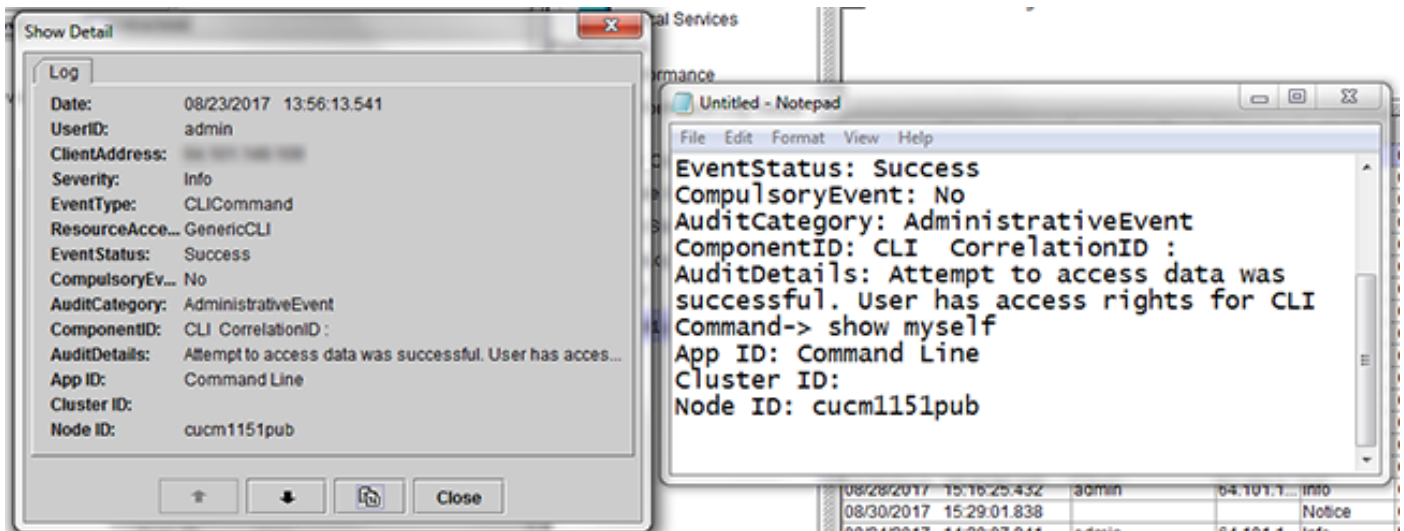
- AuditApp Logs
 - Archive
 - Audit00000012.log
- Cisco Unified OS Logs

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

Étape 4. Sélectionnez deux fois l'entrée souhaitée pour afficher d'autres détails sur l'événement. Dans cet exemple, nous avons une piste d'audit de commande CLI qui indique que la commande **show my** a été exécutée sur le noeud, **cucm1151pub**. Sélectionnez l'icône avec une image de page double pour copier les détails de l'alerte qui peuvent être collés ailleurs.



Conseil : cochez la case **Actualisation automatique** pour activer les mises à jour dynamiques pour les entrées de journal dans la Visionneuse AuditLog.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [Paramètres de configuration du journal d'audit](#)