

Configurar la herramienta de supervisión en tiempo real para auditar la actividad de administrador en Cisco Unified Communications Manager

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar la herramienta de control en tiempo real (RTMT) para ver y auditar la actividad en tiempo real en Cisco Unified Communications Manager (CUCM).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Administración de CUCM
- Configuración de seguimiento de CUCM
- Navegación RTMT

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Unified Communications Manager
- Herramienta de supervisión en tiempo real

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Para CUCM, el registro de auditoría de la aplicación admite actualizaciones de configuración para interfaces de CUCM como Communications Manager Administration, Cisco Unified RTMT, Cisco Unified Communications Manager CDR Analysis and Reporting y Cisco Unified Serviceability.

Para IM and Presence Service, el registro de auditoría de la aplicación admite actualizaciones de configuración para interfaces de IM y presencia como Cisco Unified Communications Manager IM and Presence Administration, Cisco Unified IM and Presence Real-Time Monitoring Tool y Cisco Unified IM and Presence Serviceability.

Para Cisco Unity Connection, el registro de auditoría de la aplicación admite actualizaciones de configuración para las interfaces de Cisco Unity Connection, Cisco Unity Connection Administration, Cisco Unity Connection Serviceability, Cisco Personal Communications Assistant y los clientes que utilizan Connection REST Application Programming Interfaces (API).

Configurar

Siga estos pasos para configurar la capacidad de registro de auditoría y ver la pista de auditoría desde RTMT.

Paso 1. Habilitar registro de auditoría. Navegue hasta **Cisco Unified Serviceability > Tools > Audit Log Configuration** y habilite estos parámetros

- Activar registro de auditoría
- Habilitar depuración
- Activar rotación de registro
- Registro de auditoría detallado (los registros de auditoría detallados proporcionan los mismos elementos que los registros de auditoría habituales, pero también incluyen cambios de configuración. Por ejemplo, el registro de auditoría incluye elementos que se agregaron, actualizaron y eliminaron, incluidos los valores modificados.)

Nota: Debe habilitar estos servicios, **Servicio de eventos de auditoría de servicio de red** y **Servicio de red Supervisión de particiones de registro de Cisco**

Consejo: Cuando se desactiva la rotación de registros (sin marcar), el registro de auditoría ignora la configuración Número máximo de archivos.

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*

Paso 2. Ahora puede utilizar RTMT para ver registros de auditoría. Abra e inicie sesión en Cisco RTMT. Vaya a **System > Tools > AuditLog Viewer** y seleccione el nodo desde el que desea supervisar la actividad.

Paso 3. Seleccione **AuditApp Logs** y en la lista de selección y elija el archivo .log deseado. Se le presenta una vista de los eventos del archivo de registro seleccionado.

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 Clear Filter Find Save

System Summary
AuditLog Viewer

System Summary

Server

- CPU and Memory
- Process
- Disk Usage
- Critical Services

Performance

- Performance
- Performance Log Viewer

Tools

- Alert Central
- Trace & Log Central
- Job Status
- SysLog Viewer
- VLT
- AuditLog Viewer

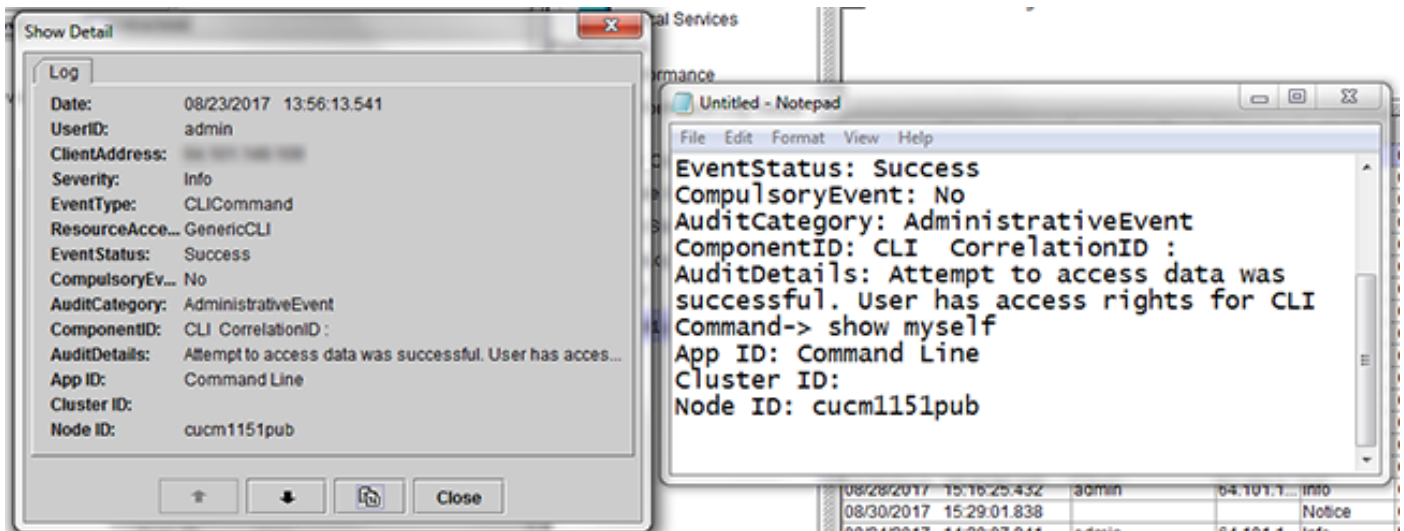
Voice/Video

AnalysisManager

IM and Presence

System Summary
 AuditLog Viewer

Paso 4. Seleccione dos veces la entrada deseada para ver más detalles del evento. En este ejemplo tenemos una pista de auditoría de comandos CLI que indica que el comando **show me** se realizó en el nodo, **cucm1151pub**. Seleccione el icono con una imagen de página doble para copiar los detalles de la alerta que se pueden pegar en otro lugar.



Sugerencia: Active la casilla de verificación **Actualización automática** para habilitar las actualizaciones dinámicas para registrar las entradas dentro del Visor de registros de auditoría.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- [Configuración de registro de auditoría](#)