

Herramienta del monitoreo en tiempo real de la configuración para auditoría la actividad Admin en el administrador de las Comunicaciones unificadas de Cisco

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar la herramienta del monitoreo en tiempo real (RTMT) para ver y para auditoría la actividad en tiempo real en el administrador de las Comunicaciones unificadas de Cisco (CUCM).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- La administración CUCM
- Configuración de la traza CUCM
- RTMT navegación

Componentes Utilizados

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

- Administrador de las Comunicaciones unificadas de Cisco
- Herramienta del monitoreo en tiempo real

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese

de que usted entienda el impacto potencial del comando any.

Antecedentes

Para CUCM que el registro de auditoría de la aplicación soporta las actualizaciones de la configuración para las interfaces CUCM tales como administración del administrador de comunicaciones, Cisco unificó RTMT, análisis CDR del administrador de las Comunicaciones unificadas de Cisco e información y utilidad unificada Cisco.

Para IM y la presencia mantenga las actualizaciones de la configuración de los soportes del registro de auditoría de la aplicación para IM y las interfaces de la presencia tales como administrador de las Comunicaciones unificadas de Cisco IM y la administración de la presencia, Cisco unificó IM y la herramienta y Cisco del monitoreo en tiempo real de la presencia unificaron IM y la utilidad de la presencia.

Para el Cisco Unity Connection el registro de auditoría de la aplicación soporta las actualizaciones de la configuración para las interfaces del Cisco Unity Connection, la administración del Cisco Unity Connection, la utilidad del Cisco Unity Connection, Asistente de comunicaciones personales de Cisco y los clientes que utilizan las interfaces programadas de la aplicación del RESTO de la conexión (API).

Configurar

Siga los siguientes pasos para configurar la capacidad del registro de auditoría y ver el rastro de auditoría de RTMT.

Paso 1. Registro de auditoría del permiso. Navegue a **Cisco unificó la utilidad > las herramientas > la configuración del registro de auditoría** y habilitan estos parámetros

- Habilite el registro de auditoría
- Habilite la purga
- Habilite la rotación del registro
- Registro de auditoría detallado (los registros de auditoría detallados proporcionan los mismos elementos que los registros de auditoría regulares, pero también incluyen los cambios de configuración. Por ejemplo, el registro de auditoría incluye los elementos que fueron agregados, puestos al día, y borrados, incluyendo los valores modificados.)

Nota: Usted debe habilitar estos servicios, el **servicio del evento de auditoría del servicio de red** y **monitorear de las divisiones del registro de Cisco del servicio de red**

Consejo: Cuando se inhabilita la rotación del registro (desmarcado), el registro de auditoría ignora el máximo no de la determinación de los 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 usted puede utilizar RTMT para ver los registros de auditoría. Ábrase y inicie sesión a Cisco RTMT. Navegue a **Sytem > a las herramientas > al Visualizador de AuditLog** y seleccione el nodo del cual usted quisiera monitorear la actividad.

Paso 3. Seleccione los **registros de AuditApp** y de la lista de la selección y elija el archivo deseado de .log. Le presentan con vistas a los eventos para el archivo del 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

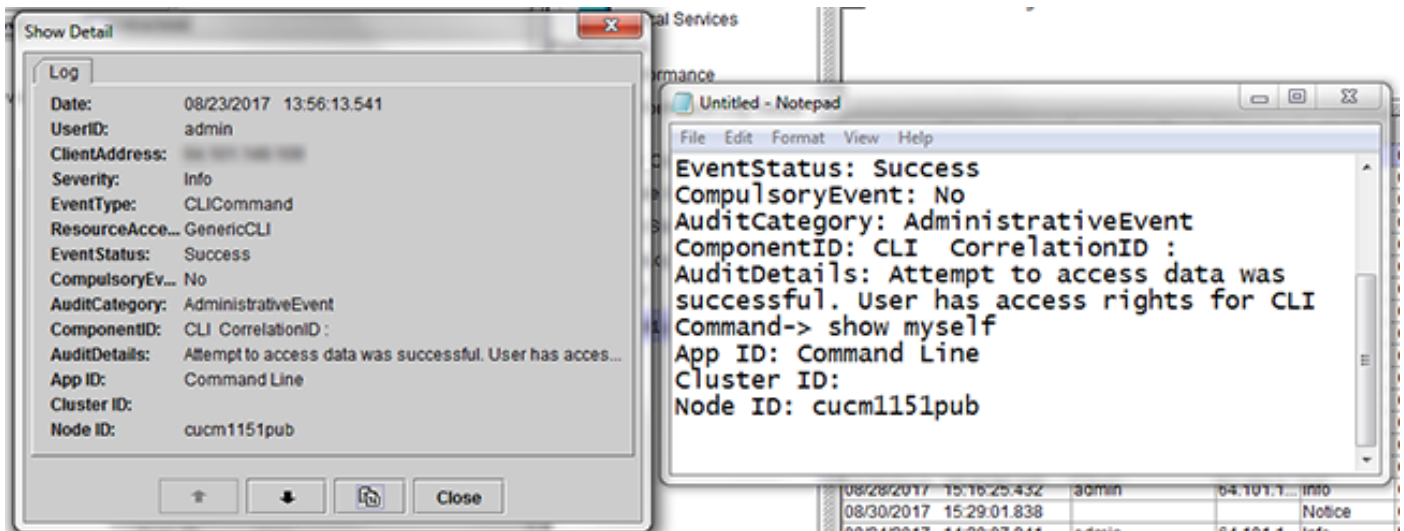
- AuditApp Logs
 - Archive
 - Audit00000012.log
- Cisco Unified OS Logs

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 Find Save

System Summary AuditLog Viewer

Paso 4. Seleccione la entrada deseada dos veces para ver más lejos los detalles del evento. En este ejemplo tenemos un rastro de auditoría del comando CLI que indique que realizaron al comando **show mismo** en el nodo, **cucm1151pub**. Seleccione el icono con la imagen doble de la página para copiar los detalles alertas que se pueden pegar a otra parte.



Consejo: Seleccione el checkbox para el **auto restauran** para habilitar las actualizaciones dinámicas a las entradas de registro dentro del Visualizador de AuditLog.

Verificación

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

Troubleshooting

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

Información Relacionada

- [Ajustes de la configuración del registro de auditoría](#)