

Configurar a ferramenta de monitoramento em tempo real para auditar a atividade do administrador no Cisco Unified Communications Manager

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como configurar a RTMT (Real Time Monitoring Tool) para visualizar e auditar atividades em tempo real no Cisco Unified Communications Manager (CUCM).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Administração do CUCM
- Configuração de rastreamento CUCM
- Navegação RTMT

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Unified Communications Manager
- Ferramenta de monitoramento em tempo 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Para o CUCM, o log de auditoria do aplicativo suporta atualizações de configuração para interfaces do CUCM, como Administração do Communications Manager, Cisco Unified RTMT, Análise e Relatório do CDR do Cisco Unified Communications Manager e Cisco Unified Serviceability.

Para o serviço IM e Presence, o log de auditoria do aplicativo suporta atualizações de configuração para interfaces IM e Presence, como o Cisco Unified Communications Manager IM and Presence Administration, Cisco Unified IM and Presence Real-Time Monitoring Tool e Cisco Unified IM and Presence Serviceability.

Para o Cisco Unity Connection, o registro de auditoria do aplicativo suporta atualizações de configuração para interfaces do Cisco Unity Connection, Cisco Unity Connection Administration, Cisco Unity Connection Serviceability, Cisco Personal Communications Assistant e clientes que usam as APIs (Interfaces de programação de aplicativos) do Connection REST.

Configurar

Siga estas etapas para configurar o recurso de log de auditoria e visualizar a trilha de auditoria da RTMT.

Etapa 1. Habilitar log de auditoria. Navegue até **Cisco Unified Serviceability > Tools > Audit Log Configuration** e ative esses parâmetros

- Ativar log de auditoria
- Ativar limpeza
- Ativar rotação de log
- Registro de auditoria detalhado (os registros de auditoria detalhados fornecem os mesmos itens dos registros de auditoria regulares, mas também incluem alterações de configuração. Por exemplo, o log de auditoria inclui itens que foram adicionados, atualizados e excluídos, incluindo os valores modificados.)


Note: Você deve habilitar esses serviços, o **Network Service Audit Event Service** e o **Network Service Cisco Log Partitions Monitoring**

Tip: Quando a rotação do log é desabilitada (desmarcada), o log de auditoria ignora a configuração Número máximo de arquivos.

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*

Etapa 2. Agora você pode usar RTMT para visualizar os Logs de Auditoria. Abra e faça login no Cisco RTMT. Navegue até **System > Tools > AuditLog Viewer** e selecione o nó do qual você deseja monitorar a atividade.

Etapa 3. Selecione **AuditApp Logs** e, na lista de seleção, escolha o arquivo .log desejado. Você verá uma exibição dos eventos do arquivo de log selecionado.

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.erteite.com** Auto Refresh

Logs

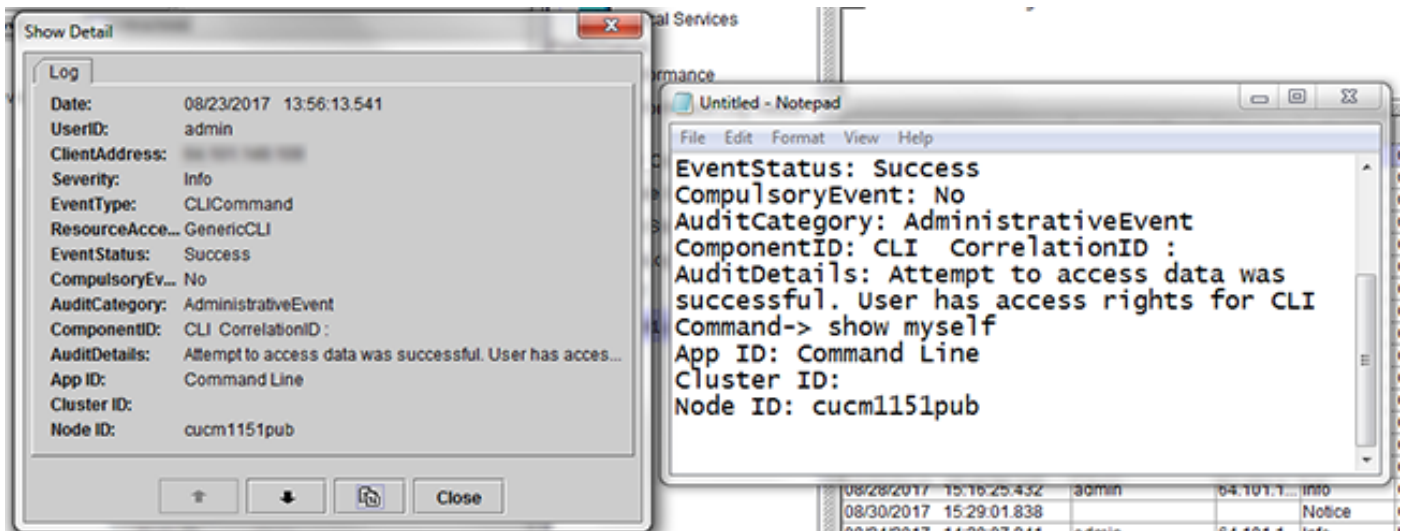
- AuditApp Logs
 - Archive
 - Audit00000012.log
- Cisco Unified OS Logs

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

Etapa 4. Selecione a entrada desejada duas vezes para ver mais detalhes do evento. Neste exemplo, temos uma trilha de auditoria de comando CLI que indica que o comando **show me** foi executado no nó, **cucm1151pub**. Selecione o ícone com imagem de página dupla para copiar os detalhes do alerta que podem ser colados em outro lugar.



Dica: marque a caixa de seleção de **Atualização automática** para ativar atualizações dinâmicas para registrar entradas no Visualizador de log de auditoria.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- [Configurações do log de auditoria](#)