Konfigurieren des Echtzeit-Überwachungstools zur Überwachung der Admin-Aktivität in Cisco Unified Communications Manager

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie das Real Time Monitoring Tool (RTMT) so konfigurieren, dass Echtzeitaktivitäten in Cisco Unified Communications Manager (CUCM) angezeigt und überwacht werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- CUCM-Administration
- CUCM-Trace-Konfiguration
- RTMT-Navigation

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Unified Communications Manager
- Echtzeit-Überwachungs-Tool

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Für CUCM unterstützt das Anwendungs-Audit-Protokoll Konfigurationsaktualisierungen für CUCM-Schnittstellen wie Communications Manager Administration, Cisco Unified RTMT, Cisco Unified Communications Manager CDR Analysis and Reporting sowie Cisco Unified Serviceability.

Für IM- und Presence-Services unterstützt das Anwendungs-Audit-Protokoll Konfigurationsaktualisierungen für IM- und Presence-Schnittstellen wie Cisco Unified Communications Manager IM and Presence Administration, Cisco Unified IM and Presence Real-Time Monitoring Tool und Cisco Unified IM and Presence Serviceability.

Für Cisco Unity Connection unterstützt das Anwendungs-Audit-Protokoll Konfigurationsaktualisierungen für Cisco Unity Connection-Schnittstellen, Cisco Unity Connection Administration, Cisco Unity Connection Serviceability, Cisco Personal Communications Assistant und Clients, die die Connection REST Application Programming Interfaces (APIs) verwenden.

Konfigurieren

Befolgen Sie diese Schritte, um die Prüfprotokollfunktion zu konfigurieren und den Prüfpfad von RTMT anzuzeigen.

Schritt 1: Aktivieren des Überwachungsprotokolls. Navigieren Sie zu **Cisco Unified Serviceability > Tools > Audit Log Configuration**, und aktivieren Sie diese Parameter.

- Audit-Protokoll aktivieren
- Löschen aktivieren
- Rotation von Protokolldateien aktivieren
- Detaillierte Audit-Protokollierung (Detaillierte Audit-Protokolle stellen dieselben Elemente bereit wie reguläre Audit-Protokolle, enthalten aber auch Konfigurationsänderungen. Beispielsweise enthält das Überwachungsprotokoll Elemente, die hinzugefügt, aktualisiert und gelöscht wurden, einschließlich der geänderten Werte.)

  Hinweis: Sie müssen diese Dienste, den **Network Service Audit Event Service** und **Network Service Cisco Log Partitions Monitoring** aktivieren.

  Tipp: Wenn die Protokollrotation deaktiviert ist (nicht aktiviert), ignoriert das Überwachungsprotokoll die Einstellung Maximale Anzahl von Dateien.

Audit Log Configuration

💾 Save 🔧 Set to Default

Status:
ⓘ Ready

Select Server
Server* `cucm1151pub--CUCM Voice/Video ▾` `Go`
☐ Apply to All Nodes

Application Audit Log Settings
Filter Settings
　☑ Enable Audit Log
　☑ Enable Purging
　☑ Enable Log Rotation
　☑ Detailed Audit Logging

Remote Syslog
　Server Name[1] `_____`　　Remote Syslog Audit Event Level `Debug ▾`

Output Settings
　Maximum No. of Files* `250`
　Maximum File Size (MB)* `2`

Notification Settings
　Warning Threshold for Approaching Log Rotation Overwrite (%)* `80`

Database Audit Log Filter Settings
　☑ Enable Audit Log　　Debug Audit Level `Database Updates ▾`

Output Settings
　☑ Enable Audit Log Rotation
　Maximum No. of Files* `40`
　No. of Files Deleted on Log Rotation* `20`

`Save` `Set to Default`

Schritt 2: Sie können nun RTMT verwenden, um Überwachungsprotokolle anzuzeigen. Öffnen und melden Sie sich bei Cisco RTMT an. Navigieren Sie zu **System > Tools > AuditLog Viewer** und wählen Sie den Knoten aus, von dem Sie die Aktivität überwachen möchten.

Schritt 3: Wählen Sie **AuditApp Logs** und dann aus der Auswahlliste die gewünschte Protokolldatei aus. Es wird eine Ansicht der Ereignisse für die ausgewählte Protokolldatei angezeigt.

Schritt 4: Wählen Sie zweimal den gewünschten Eintrag aus, um weitere Veranstaltungsdetails anzuzeigen. In diesem Beispiel gibt es einen CLI-Befehlsüberwachungspfad, der anzeigt, dass der Befehl **show me** auf knoten **cucm1151pub** ausgeführt wurde. Wählen Sie das Symbol mit einem doppelseitigen Bild aus, um die Alarmdetails zu kopieren, die an eine andere Stelle eingefügt werden können.
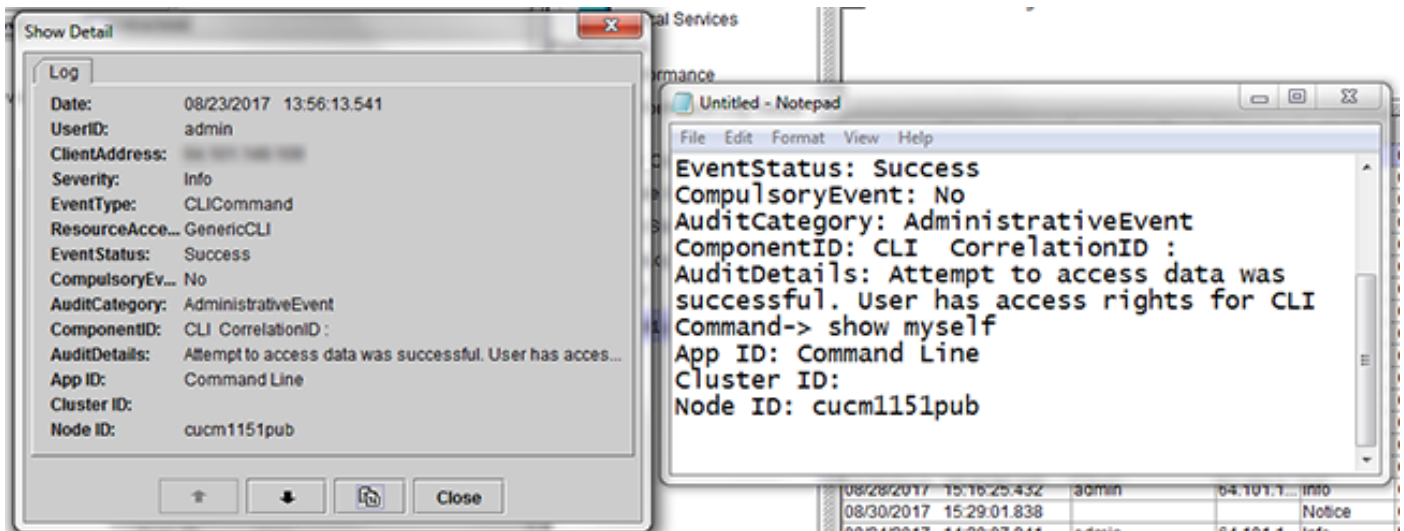
Tipp: Aktivieren Sie das Kontrollkästchen für **automatische Aktualisierung**, um dynamische Aktualisierungen von Protokolleinträgen in der AuditLog Viewer zu aktivieren.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- [Konfigurationseinstellungen für das Audit-Protokoll](#)