감사 로그

- 감사 로그, 1 페이지

감사 로그

감사 로깅을 통해 시스템에 대한 구성 변경 사항이 감사를 위해 개별 로그 파일에 기록됩니다.

감사 로깅 (표준)

감사 로깅이 활성화되어 있지만 세부 감사 로깅 옵션을 선택하지 않으면 시스템은 표준 감사 로깅을 위해 구성됩니다.

표준 감사 로깅을 통해 시스템에 대한 구성 변경 사항이 감사를 위해 개별 로그 파일에 기록됩니다. 서비스 가용성 GUI의 제어 센터 네트워크 서비스 아래에 표시되는 Cisco Audit Event Service는 사용자에 의해 또는 사용자 작업의 결과로 발생하는 시스템에 대한 구성 변경 사항을 모니터링 및 기록합니다.

서비스 가용성 GUI의 감사 로그 구성 창에 액세스하여 감사 로그에 대한 설정을 구성합니다.

표준 감사 로그에는 다음 부분이 포함되어 있습니다.

- 감사 로깅 프레임워크 - 프레임워크는 알람 라이브러리를 사용하여 감사 이벤트를 감사 로그에 기록하는 API로 구성됩니다. GenericAlarmCatalog.xml로 정의된 알람 카탈로그가 이러한 알람에 적용됩니다. 시스템 구성 요소마다 고유한 로깅이 제공됩니다.

  다음 예는 Unified Communications Manager 구성 요소에서 알람을 전송하는 데 사용할 수 있는 API를 표시합니다.

  ```
  User ID: CCMAdministratorClient IP Address: 172.19.240.207 Severity: 3
  EventType: ServiceStatusUpdated ResourceAccessed: CCMService EventStatus:
  Successful Description: CallManager Service status is stopped
  ```

- 감사 이벤트 로깅 - 감사 이벤트는 로깅해야 하는 이벤트를 나타냅니다. 다음 예는 샘플 감사 이벤트를 표시합니다.

```
CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3
EventType:ServiceStatusUpdated ResourceAccessed: CCMService
EventStatus:Successful Description: Call Manager Service status is stopped
App ID:Cisco Tomcat Cluster ID:StandAloneCluster Node ID:sa-cm1-3
```

팁 감사 이벤트 로깅은 기본적으로 중앙 집중식이고 활성화되어 있습니다. Syslog 감사라고 하는 알람 모니터에서 로그를 작성합니다. 기본적으로 로그는 회전하도록 구성되어 있습니다. AuditLogAlarmMonitor가 감사 이벤트를 쓸 수 없는 경우 AuditLogAlarmMonitor는이 오류를 syslog 파일에 중대한 오류로 기록합니다. 알림 관리자는 이 오류를 SeverityMatchFound 알림의 일부로 보고합니다. 이벤트 로깅이 실패하는 경우에도 실제 작업은 계속됩니다. 모든 감사 로그는 Cisco Unified Real-Time Monitoring Tool의 추적 및 로그 센트럴에서 수집, 보고 및 삭제됩니다.

Cisco 통합 서비스 가용성 표준 이벤트 로깅

Cisco 통합 서비스 가용성는 다음 이벤트를 기록합니다.

- 서비스 활성화, 비활성화, 시작 또는 중지.
- 추적 구성 및 알람 구성 변경.
- SNMP 구성의 변경.
- CDR 관리의 변경. (Cisco Unified Communications Manager만 해당)
- 서비스 가용성 보고서 아카이브의 보고서를 검토합니다. 이 로그는 리포터 노드에서 볼 수 있습니다. (Unified Communications Manager만 해당)

Cisco Unified Real-Time Monitoring Tool 표준 이벤트 로깅

Cisco Unified Real-Time Monitoring Tool는 감사 이벤트 알람을 사용하여 다음 이벤트를 기록합니다.

- 알림 구성
- 알림 일시 중지
- 이메일 구성
- 노드 알림 상태 설정
- 알림 추가
- 알림 작업 추가
- 알림 지우기
- 알림 활성화
- 알림 작업 제거
- 알림 제거

Unified Communications Manager 표준 이벤트 로깅

Cisco CDR Analysis and Reporting(CAR)에서 다음 이벤트에 대한 감사 로그를 생성합니다.

- 로더 예약
- 일별, 주별 및 월별 보고 일정
- 메일 매개 변수 구성
- 다이얼 계획 구성
- 게이트웨이 구성
- 시스템 환경설정 구성
- 자동 삭제 구성
- 기간, 시간 및 음성 품질에 대한 등급 엔진 구성
- QoS 구성
- 미리 작성된 보고서 구성에 대한 자동 생성/알림
- 알림 제한 구성

Cisco Unified CM 관리 표준 이벤트 로깅

Cisco Unified Communications Manager 관리의 다양한 구성 요소에 대해 다음과 같은 이벤트가 기록됩니다.

- 사용자 로깅(사용자 로그인 및 사용자 로그아웃)
- 사용자 역할 구성원 자격 업데이트(사용자 추가, 사용자 삭제, 사용자 역할 업데이트됨)
- 역할 업데이트(새 역할이 추가, 삭제 또는 업데이트됨)
- 장치 업데이트(전화기 및 게이트웨이)
- 서버 구성 업데이트(알람 또는 추적 구성, 서비스 매개 변수, 엔터프라이즈 매개 변수, IP 주소, 호스트 이름, 이더넷 설정 및 Unified Communications Manager 서버 추가 또는 삭제에 대한 변경 사항)

Cisco Unified Communications 자가 관리 포털 표준 이벤트 로깅

사용자 로깅(사용자 로그인 및 사용자 로그아웃) 이벤트는 Cisco Unified Communications 자가 관리 포털에 대해 기록됩니다.

명령줄 인터페이스 표준 이벤트 로깅

명령줄 인터페이스를 통해 실행된 모든 명령이 기록됩니다(Unified Communications Manager 및 Cisco Unity Connection 모두).

Cisco Unity Connection 관리 표준 이벤트 로깅

Cisco Unity Connection 관리는 다음 이벤트를 기록합니다.

- 사용자 로깅(사용자 로그인 및 사용자 로그아웃)
- 모든 구성 변경 사항(다음을 포함하되 이에 제한되지 않음: 사용자, 연락처, 통화 관리 개체, 네트워킹, 시스템 설정 및 전화 통신)
- 작업 관리(작업 활성화 또는 비활성화)
- 벌크 관리 도구(벌크 생성, 벌크 삭제)
- 사용자 정의 키패드 맵(맵 업데이트)

Cisco Personal Communications Assistant(Cisco PCA) 표준 이벤트 로깅

Cisco Personal Communications Assistant 클라이언트는 다음 이벤트를 기록합니다.

- 사용자 로깅(사용자 로그인 및 사용자 로그아웃)
- Messaging Assistant를 통해 이루어진 모든 구성 변경

Cisco Unity Connection 서비스 가용성 표준 이벤트 로깅

Cisco Unity Connection 서비스 가용성은 다음 이벤트를 기록합니다.

- 사용자 로깅(사용자 로그인 및 사용자 로그아웃)
- 모든 구성이 변경됩니다.
- 서비스 활성화, 비활성화, 시작 또는 중지.

대표 상태 전송 **API** 이벤트 로깅을 사용하는 **Cisco Unity Connection** 클라이언트

대표 상태 전송(REST) API를 사용하는 Cisco Unity Connection 클라이언트는 다음 이벤트를 기록합니다.

- 사용자 로깅(사용자 API 인증).
- Cisco Unity Connection 프로비저닝 인터페이스를 이용하는 API 통화.

Cisco Unified IM and Presence Serviceability 표준 이벤트 로깅

Cisco Unified IM and Presence Serviceability는 다음 이벤트를 기록합니다.

- 서비스 활성화, 비활성화, 시작 또는 중지
- 추적 구성 및 알람 구성 변경
- SNMP 구성의 변경
- 서비스 가용성 보고서 아카이브의 모든 보고서 검토(이 로그는 리포터 노드에서 볼 수 있음)

Cisco Unified IM and Presence 실시간 모니터링 도구 표준 이벤트 로깅

Cisco Unified IM and Presence 실시간 모니터링 도구는 감사 이벤트 알람을 사용하여 다음 이벤트를 기록합니다.

- 알림 구성
- 알림 일시 중지
- 이메일 구성
- 노드 알림 상태 설정
- 알림 추가
- 알림 작업 추가
- 알림 지우기
- 알림 활성화
- 알림 작업 제거
- 알림 제거

Cisco IM and Presence 관리 표준 이벤트 로깅

다음 이벤트는 Cisco Unified Communications Manager IM and Presence 관리의 다양한 구성 요소에 대해 기록됩니다.

- 관리자 로깅(관리, OS 관리, 재해 복구 시스템 및 보고 등 IM and Presence 인터페이스에 대한 로그인 및 로그아웃)
- 사용자 역할 구성원 자격 업데이트(사용자 추가, 사용자 삭제, 사용자 역할 업데이트됨)
- 역할 업데이트(새 역할이 추가, 삭제 또는 업데이트됨)
- 장치 업데이트(전화기 및 게이트웨이)
- 서버 구성 업데이트(알람 또는 추적 구성, 서비스 매개 변수, 엔터프라이즈 매개 변수, IP 주소, 호스트 이름, 이더넷 설정 및 IM and Presence 서버 추가 또는 삭제 변경)

IM and Presence 애플리케이션 표준 이벤트 로깅

다음 이벤트는 IM and Presence 애플리케이션의 다양한 구성 요소에 의해 기록됩니다.

- IM 클라이언트(사용자 로그인, 사용자 로그아웃 및 실패한 로그인 시도)에 대한 최종 사용자 로그온
- IM 채팅방에서 사용자 입력 및 종료
- IM 채팅방 만들기 및 소멸

명령줄 인터페이스 표준 이벤트 로깅

명령줄 인터페이스를 통해 실행된 모든 명령이 기록됩니다.

감사 로깅(자세히)

세부 감사 로깅은 표준(기본) 감사 로그에 저장되지 않은 추가 구성 수정 사항을 기록하는 선택적 기능입니다. 표준 감사 로그에 저장된 모든 정보 외에도 세부 감사 로그에는 수정된 값을 포함하여 추가, 업데이트 및 삭제된 구성 항목이 포함됩니다. 세부 감사 로깅은 기본적으로 비활성화되어 있지만 감사 로그 구성 창에서 활성화할 수 있습니다.

감사 로그 유형

시스템 감사 로그

시스템 감사 로그는 Linux OS 사용자의 생성, 수정 또는 삭제, 로그 변조, 파일 또는 디렉터리 권한에 대한 변경 등의 작업을 추적합니다. 이 유형의 감사 로그는 수집된 데이터 양이 많아 기본적으로 비활성화됩니다. 이 기능을 활성화하려면 CLI를 사용하여 utils auditd를 수동으로 활성화해야 합니다. 시스템 감사 로그 기능을 활성화한 후 실시간 모니터링 도구에서 추적 및 로그 센트럴을 통해 선택한 로그를 수집, 확인, 다운로드 또는 삭제할 수 있습니다. 시스템 감사 로그는 `vos-audit.log`의 형식을 취합니다.

이 기능을 활성화하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Solutions*용 명령줄 인터페이스 설명서를 참조하십시오. 실시간 모니터링 도구에서 수집된 로그에 액세스하는 방법에 대한 자세한 내용은 *Cisco Unified Cisco Unified Real-Time Monitoring Tool* 관리 설명서를 참조하십시오.

애플리케이션 감사 로그

애플리케이션 감사 로그는 사용자가 수행했거나 사용자 작업의 결과로 시스템에 대한 구성 변경 사항을 모니터링하고 기록합니다.

참고 애플리케이션 감사 로그(Linux auditd)는 CLI를 통해서만 활성화하거나 비활성화할 수 있습니다. 실시간 모니터링 도구를 통한 vos-audit.log 수집 외에는 이 유형의 감사 로그에 대한 설정을 변경할 수 없습니다.

데이터베이스 감사 로그

데이터베이스 감사 로그는 로그인과 같은 Informix 데이터베이스에 대한 액세스와 관련된 모든 활동을 추적합니다.

감사 로그 구성 작업 흐름

감사 로깅을 구성하려면 다음 작업을 완료하십시오.

프로시저

	명령 또는 동작	목적
단계 1	감사 로깅 설정, 7 페이지	감사 로그 구성 창에서 감사 로그 구성을 설정합니다. 원격 감사 로깅을 사용할지 여부와 세부 감사 로깅 옵션을 사용할지 여부를 구성할 수 있습니다.
단계 2	원격 감사 로그 전송 프로토콜 구성, 8 페이지	(선택 사항) 원격 감사 로깅이 구성된 경우 전송 프로토콜을 구성합니다. 정상 작동 모드의 시스템 기본값은 UDP이지만, TCP 또는 TLS를 구성할 수도 있습니다.
단계 3	경고 알림을 위한 전자 메일 서버 구성, 9 페이지	(선택 사항) RTMT에서 이메일 알림을 위한 이메일 서버를 설정합니다.
단계 4	이메일 알림 활성화, 9 페이지	(선택 사항) 다음 이메일 알림 중 하나를 설정합니다. • TCP를 사용하여 구성된 원격 감사 로깅이 있는 경우 **TCPRemoteSyslogDeliveryFailed** 알림에 대한 이메일 알림을 설정합니다. • TLS를 사용하여 구성된 원격 감사 로깅이 있는 경우 **TLSRemoteSyslogDeliveryFailed** 알림에 대한 이메일 알림을 설정합니다.
단계 5	플랫폼 로그에 대해 원격 감사 로깅 구성, 9 페이지	플랫폼 감사 로그 및 원격 서버 로그에 대한 원격 감사 로깅을 설정합니다. 이러한 유형의 감사 로그의 경우 FileBeat 클라이언트 및 외부 logstash 서버를 구성해야 합니다.

감사 로깅 설정

시작하기 전에

원격 감사 로깅은 각 클러스터 노드와 원격 syslog 서버 간에 원격 syslog 서버 및 구성된 IPSec을 설정하고 그 사이에 있는 게이트웨이에 대한 연결을 포함해야 합니다. IPSec 구성은 *Cisco IOS* 보안 구성 설명서를 참조하십시오.

프로시저

단계 1 Cisco 통합 서비스 가용성에서 도구 > 감사 로그 구성을 선택합니다.

단계 **2** 서버 드롭다운 메뉴에서 클러스터의 서버를 선택하고 이동을 클릭합니다.

단계 **3** 모든 클러스터 노드를 기록하려면 모든 노드에 적용 확인란을 선택합니다.

단계 **4** 서버 이름 필드에 원격 syslog 서버의 IP 주소 또는 FQDN(Fully Qualified Domain Name)을 입력합니다.

단계 **5** (선택 사항) 수정된 항목과 수정된 값을 포함하여 구성 업데이트를 기록하려면 세부 감사 로깅 확인란을 선택합니다.

단계 **6** 감사 로그 구성 창의 나머지 필드를 완료합니다. 필드 및 해당 설명에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **7** 저장을 클릭합니다.

다음에 수행할 작업

원격 감사 로그 전송 프로토콜 구성, 8 페이지

원격 감사 로그 전송 프로토콜 구성

이 절차를 사용하여 원격 감사 로그에 대한 전송 프로토콜을 변경합니다. 시스템 기본값은 UDP이지만 로 다시 구성할 수 있습니다. TCP 또는 TLS

프로시저

단계 **1** 명령줄 인터페이스에 로그인합니다.

단계 **2** **utils remotesyslog show protocol** 명령을 실행하여 구성된 프로토콜을 확인합니다.

단계 **3** 이 노드의 프로토콜을 변경해야 하는 경우 다음을 수행합니다.

- TCP를 구성하려면 **utils remotesyslog set protocol tcp** 명령을 실행합니다.
- UDP를 구성하려면 **utils remotesyslog set protocol udp** 명령을 실행합니다.
- TLS를 구성하려면 **utils remotesyslog set protocol tls** 명령을 실행합니다.

  TLS 연결을 설정하려면, 보안 인증서를 syslog 서버에서 Unified Communications Manager 및 IM and Presence Service의 tomcat 신뢰 저장소로 업로드해야 합니다.

  참고 Common Criteria 모드에서는 엄격한 호스트 이름 확인이 구현됩니다. 따라서 인증서와 일치하는 FQDN(Fully Qualified Domain Name)을 사용하여 서버를 구성해야 합니다.

단계 **4** 프로토콜을 변경한 경우 노드를 다시 시작합니다.

단계 **5** 모든 Unified Communications Manager 및 IM and Presence Service 클러스터 노드에서 이 절차를 반복합니다.

다음에 수행할 작업

경고 알림을 위한 전자 메일 서버 구성, 9 페이지

경고 알림을 위한 전자 메일 서버 구성

이 절차를 사용하여 알림 공지를 위한 이메일 서버를 설정합니다.

프로시저

단계 **1** 실시간 모니터링 도구의 시스템 창에서 중앙 알림을 클릭합니다.
단계 **2** 시스템 > 도구 > 알림 > 이메일 서버 구성을 선택합니다.
단계 **3** 메일 서버 구성 팝업에서 메일 서버에 대한 세부 정보를 입력합니다.
단계 **4** 확인을 클릭합니다.

다음에 수행할 작업

이메일 알림 활성화, 9 페이지

이메일 알림 활성화

TCP 또는 TLS가 구성된 원격 감사 로깅이 있는 경우 이 절차를 사용하여 이메일 알림을 설정하여 전송 실패를 알립니다.

프로시저

단계 **1** 실시간 모니터링 도구의 시스템 영역에서 중앙 알림을 클릭합니다.
단계 **2** 중앙 알림 창에서

- TCP를 사용한 원격 감사 로깅이 있는 경우 **TCPRemoteSyslogDeliveryFailed**를 선택합니다.
- TLS를 사용한 원격 감사 로깅이 있는 경우 **TLSRemoteSyslogDeliveryFailed**를 선택합니다.

단계 **3** 시스템 > 도구 > 알림 > 알림 작업 구성을 선택합니다.
단계 **4** 알림 작업 팝업에서 기본값을 선택하고 편집을 클릭합니다.
단계 **5** 알림 작업 팝업에서 수신자를 추가합니다.
단계 **6** 팝업 창에 이메일 알림을 보낼 주소를 입력하고 확인을 클릭합니다.
단계 **7** 알림 작업 팝업에서 수신자 아래 주소가 나타나는지, 활성화 확인란이 선택되었는지 확인합니다.
단계 **8** 확인을 클릭합니다.

플랫폼 로그에 대해 원격 감사 로깅 구성

이 작업을 완료하여 플랫폼 감사 로그, 원격 지원 로그 및 벌크 관리 csv 파일에 대한 원격 감사 로깅 지원을 추가합니다. 이러한 유형의 로그에 대해 FileBeat 클라이언트 및 logstash 서버가 사용됩니다.

시작하기 전에

외부 logstash 서버를 설정했는지 확인합니다.

프로시저

	명령 또는 동작	목적
단계 1	Logstash 서버 정보 구성, 10 페이지	IP 주소, 포트 및 파일 유형과 같은 외부 logstash 서버 세부 정보를 사용하여 FileBeat 클라이언트를 구성합니다.
단계 2	FileBeat 클라이언트 구성, 10 페이지	원격 감사 로깅을 위해 FileBeat 클라이언트를 활성화합니다.

Logstash 서버 정보 구성

이 절차를 사용하여 외부 logstash 서버 정보(예: IP 주소, 포트 번호 및 다운로드 가능 파일 유형)를 사용하여 FileBeat 클라이언트를 구성합니다.

시작하기 전에

외부 logstash 서버를 설정했는지 확인합니다.

프로시저

단계 1 명령줄 인터페이스에 로그인합니다.

단계 2 **utils FileBeat configure** 명령을 실행합니다.

단계 3 프롬프트에 따라 logstash 서버 세부 정보를 구성합니다.

FileBeat 클라이언트 구성

이 절차를 사용하여 플랫폼 감사 로그, 원격 지원 로그 및 벌크 관리 csv 파일을 업로드하는 데 사용되는 FileBeat 클라이언트를 활성화하거나 비활성화할 수 있습니다.

프로시저

단계 1 명령줄 인터페이스에 로그인합니다.

단계 2 **utils filebeat status** 명령을 실행하여 FileBeat 클라이언트가 활성화되었는지 확인합니다.

단계 3 다음 명령 중 하나를 실행합니다.

- 클라이언트를 활성화하려면 **utils filebeat enable** 명령을 실행합니다.
- 클라이언트를 비활성화하려면 **utils filebeat disable** 명령을 실행합니다.

참고 TCP는 기본 전송 프로토콜입니다.

단계 **4** (선택 사항) TLS를 전송 프로토콜로 사용하려면 다음을 수행합니다.

- TLS를 전송 프로토콜로 활성화하려면 **utils FileBeat tls enable** 명령을 실행합니다.
- TLS를 전송 프로토콜로 비활성화하려면 **utils FileBeat tls disable** 명령을 실행합니다.

참고 TLS를 사용하려면 logstash 서버에서 Unified Communications Manager 및 IM and Presence Service의 tomcat 신뢰 저장소로 보안 인증서를 업로드해야 합니다.

단계 **5** 각 노드에서 이 절차를 반복합니다.

모든 노드에서 동시에 이러한 명령을 실행하지 마십시오.

감사 로그 구성 설정

시작하기 전에

감사 역할이 있는 사용자만 감사 로그 설정을 변경할 수 있습니다. 기본적으로 Unified Communications Manager의 경우 CCMAdministrator는 새로 설치하고 업그레이드한 후 감사 역할을 소유합니다. CCMAdministrator는 Cisco Unified Communications Manager 관리의 사용자 그룹 구성 창에서 감사 권한이 있는 모든 사용자를 표준 감사 사용자 그룹에 할당할 수 있습니다. 이렇게 하려면 표준 감사 사용자 그룹에서 CCMAdministrator를 제거할 수 있습니다.

IM and Presence Service의 경우 관리자는 새로 설치 및 업그레이드 후 감사 역할을 담당하며 감사 권한이 있는 사용자를 표준 감사 사용자 그룹에 할당할 수 있습니다.

Cisco Unity Connection의 경우 설치 중에 생성된 애플리케이션 관리 계정에 감사 관리자 역할이 있으며 역할에 다른 관리 사용자를 할당할 수 있습니다. 이 계정에서 감사 관리자 역할을 제거할 수도 있습니다.

표준 감사 로그 구성 역할은 감사 로그를 삭제하고 Cisco Unified Real-Time Monitoring Tool, IM and Presence 실시간 모니터링 도구, 추적 수집 도구, 실시간 모니터링 도구(RTMT), 알림 구성, 제어 센터 - 서비스 가용성 사용자 인터페이스의 네트워크 서비스, RTMT 프로파일 저장, 서비스 가용성 사용자 인터페이스의 감사 구성 및 감사 추적이라고 하는 리소스에 대한 읽기/업데이트 액세스 기능을 제공합니다.

표준 감사 로그 구성 역할은 감사 로그를 삭제하고 Cisco Unified RTMT, 추적 수집 도구, RTMT 알림 구성, 제어 센터 - Cisco 통합 서비스 가용성, RTMT 프로파일 저장, Cisco 통합 서비스 가용성의 감사 구성 및 감사 추적이라고 하는 리소스에 대한 읽기/업데이트 액세스 기능을 제공하는 것입니다.

Cisco Unity Connection의 감사 관리자 역할은 Cisco Unified RTMT에서 감사 로그를 보고, 다운로드하고, 삭제할 수 있는 기능을 제공합니다.

Unified Communications Manager의 역할, 사용자 및 사용자 그룹에 대한 자세한 내용은 *Cisco Unified Communications Manager* 관리 설명서를 참조하십시오.

Cisco Unity Connection에서 역할 및 사용자에 대한 자세한 내용은 *Cisco Unity Connection* 관련 사용자 이동, 추가 및 변경 설명서를 참조하십시오.

IM and Presence의 역할, 사용자 및 사용자 그룹에 대한 자세한 내용은 *Unified Communications Manager* 에서 *IM and Presence Service* 구성 및 관리를 참조하십시오.

다음 표에서는 Cisco 통합 서비스 가용성 감사 로그 구성 창에서 구성할 수 있는 설정에 대해 설명합니다.

표 ***1:*** 감사 로그 구성 설정

필드	설명
서버 선택	
서버	감사 로그를 구성할 서버(노드)를 선택합니다. 그런 다음 이동을 클릭합니다.
모든 노드에 적용	감사 로그 구성을 클러스터의 모든 노드에 적용하려면 모든 노드에 적용 확인란을 선택합니다.
애플리케이션 감사 로그 설정	

필드	설명
감사 로그 활성화	이 확인란을 선택하면 애플리케이션 감사 로그에 대한 감사 로그가 생성됩니다. Unified Communications Manager의 경우 애플리케이션 감사 로그는 Unified Communications Manager 사용자 인터페이스(예: Cisco Unified Communications Manager 관리,Cisco Unified RTMT, Cisco Unified Communications Manager CDR 분석 및 보고, Cisco 통합 서비스 가용성)에 대한 구성 업데이트를 지원합니다. IM and Presence Service의 경우 애플리케이션 감사 로그는 IM and Presence사용자 인터페이스(예: Cisco Unified Communications Manager IM and Presence 관리, Cisco Unified IM and Presence 실시간 모니터링 도구, Cisco Unified IM and Presence Serviceability)에 대한 구성 업데이트를 지원합니다. Cisco Unity Connection의 경우 애플리케이션 감사 로그는 Cisco Unity Connection 사용자 인터페이스(Cisco Unity Connection 관리, Cisco Unity Connection Serviceability, Cisco Personal Communications Assistant 및 Connection REST API를 사용하는 클라이언트 포함)에 대한 구성 업데이트를 지원합니다. 이 설정은 기본적으로 활성화된 것으로 표시됩니다. 참고 네트워크 서비스 감사 이벤트 서비스가 실행되고 있어야합니다.

필드	설명
제거 활성화	LPM(로그 파티션 모니터)은 제거 활성화 옵션을 확인하여 감사 로그 제거가 필요한 지 여부를 결정합니다. 이 확인란을 선택하면 공통 파티션 디스크 사용량이 상위 워터마크 위에 있을 때마다 LPM이 RTMT에서 모든 감사 로그 파일을 제거합니다. 그러나 확인란의 선택을 취소하여 제거를 비활성화할 수 있습니다. 제거가 비활성화된 경우 디스크가 가득찰 때까지 감사 로그의 수가 계속 커집니다. 이 작업으로 인해 시스템이 중단될 수 있습니다. 제거 활성화 확인란을 선택 취소할 때 제거가 비활성화되는 위험을 설명하는 메시지입니다. 이 옵션은 활성 파티션의 감사 로그에 사용할 수 있습니다. 감사 로그가 비활성 파티션에 있는 경우 디스크 사용량이 상위 워터마크 위에 있을 때 감사 로그가 비워집니다. RTMT에서 추적 및 로그 센트럴 > 감사 로그를 선택하여 감사 로그에 액세스할 수 있습니다. 참고 네트워크 서비스 Cisco Log Partition Monitoring Tool가 실행되고 있어야합니다.
로그 로테이션 활성화	시스템은 이 옵션을 읽어 감사 로그 파일을 로테이션해야 하는지 또는 새 파일을 생성해야 하는지 여부를 결정합니다. 최대 파일 수는 5000을 초과할 수 없습니다. 로테이션 활성화 확인란을 선택하면 최대 파일 수에 도달한 후에 시스템에서 가장 오래된 감사 로그 파일을 덮어쓰기 시작합니다. 팁 로그 로테이션이 비활성화(선택 취소)되면 감사 로그에서 최대 파일 수 설정을 무시합니다.
세부 감사 로깅	이 확인란을 선택하면 시스템에서 세부 감사 로그를 사용할 수 있습니다. 세부 감사 로그는 일반 감사 로그와 동일한 항목을 제공하지만 구성 변경 사항도 포함합니다. 예를 들어 감사 로그에는 수정된 값을 포함하여 추가, 업데이트 및 삭제된 항목이 포함됩니다.

필드	설명
서버 이름	syslog 메시지를 수락하는 데 사용할 원격 syslog 서버의 이름 또는 IP 주소를 입력합니다. 서버 이름을 지정하지 않은 경우 Cisco 통합 서비스 가용성는 Syslog 메시지를 전송하지 않습니다. Unified Communications Manager 노드는 다른 서버에서 syslog 메시지를 허용하지 않으므로 Unified Communications Manager 노드를 대상으로 지정하지 마십시오. 이는 IM and Presence Service에만 적용됩니다.
원격 Syslog 감사 이벤트 수준	원격 syslog 서버에 대해 원하는 syslog 메시지 심각도를 선택합니다. 심각도 수준이 선택된 모든 syslog 메시지는 원격 syslog로 전송됩니다. 이는 IM and Presence Service에만 적용됩니다.
최대 파일 수	로그에 포함시킬 최대 파일 수를 입력합니다. 기본 설정은 250입니다. 최대 수는 5000을 지정합니다.
최대 파일 크기	감사 로그의 최대 파일 크기를 입력합니다. 파일 크기 값은 1MB에서 10MB 사이여야 합니다. 1에서 10 사이의 숫자를 지정해야 합니다.

필드	설명
근접 로그 로테이션 덮어쓰기에 대한 경고 임계값(%)	감사 로그를 덮어쓰게되는 수준에 도달하면 시스템에서 알림을 받을 수 있습니다. 이 필드를 사용하여 시스템에서 알림을 전송하는 임계값을 설정합니다. 예를 들어, 2MB 250개 파일의 기본 설정을 사용하고 경고 임계값이 80%인 경우, 시스템은 감사 로그 200개 파일(80%)이 누적되면 알람을 전송합니다. 감사 기록을 유지하려는 경우에는 RTMT를 사용하여 시스템에서 로그를 덮어쓰기 전에 로그를 검색할 수 있습니다. RTMT는 수집한 후에 파일을 삭제하는 옵션을 제공합니다. 1에서 99% 사이의 값을 입력합니다. 기본값은 80%입니다. 이 필드를 설정할 때 로그 로테이션 활성화 옵션도 선택해야 합니다. 참고 감사 로그에 할당된 총 디스크 공간은 최대 파일 수에 최대 파일 크기를 곱한 값입니다. 디스크의 감사 로그 크기가 할당된 총 디스크 공간의 이 비율을 초과하는 경우 시스템은 알림 센트럴에서 알람을 발생시킵니다.
데이터베이스 감사 로그 필터 설정	
감사 로그 활성화	이 확인란을 선택하면 Unified Communications Manager 및 Cisco Unity Connection 데이터베이스에 대한 감사 로그가 생성됩니다. 이 설정을 디버그 감사 수준 설정과 함께 사용하여 데이터베이스의 특정 항목에 대한 로그를 만들 수 있습니다.

필드	설명
디버그 감사 수준	이 설정을 사용하여 로그에서 감사할 데이터베이스 항목을 선택할 수 있습니다. 드롭다운 목록 상자에서 다음 옵션 중 하나를 선택합니다. 각 감사 로그 필터 수준은 누적된다는 점에 유의하십시오. • 스키마 - 감사 로그 데이터베이스의 설정에 대한 변경 사항을 추적합니다(예: 데이터베이스 테이블의 열 및 행). • 관리 작업 - Unified Communications Manager 시스템에 대한 모든 관리 변경 사항(예: 시스템 유지 관리에 대한 변경 사항)과 모든 스키마 변경 사항을 추적합니다. 팁 대부분의 관리자는 관리 작업 설정을 비활성화 상태로 둡니다. 감사를 원하는 사용자의 경우 데이터베이스 업데이트 수준을 사용합니다. • 데이터베이스 업데이트 - 모든 스키마 변경 사항과 모든 관리 작업 변경 사항을 데이터베이의 모든 변경 내용에 대해 추적합니다. • 데이터베이스 읽기 - 모든 스키마 변경, 관리 작업 변경 및 데이터베이스 업데이트 변경 사항을 비롯하여 시스템에 대한 모든 읽기를 추적합니다. 팁 Unified Communications Manager, IM and Presence Service 또는 Cisco Unity Connection 시스템을 신속하게 확인하려는 경우에만 데이터베이스 읽기 수준을 선택합니다. 이 수준은 상당한 양의 시스템 리소스를 사용하며 짧은 시간 동안만 사용해야 합니다.
감사 로그 로테이션 활성화	시스템은 이 옵션을 읽어 데이터베이스 감사 로그 파일을 로테이션해야 하는지 또는 새 파일을 생성해야 하는지 여부를 결정합니다. 감사 로테이션 활성화 옵션 확인란을 선택하면 최대 파일 수에 도달한 후에 시스템에서 가장 오래된 감사 로그 파일을 덮어쓰기 시작합니다. 이 설정 확인란을 선택 취소하면 감사 로그는 최대 파일 수 설정을 무시합니다.

필드	설명
최대 파일 수	로그에 포함시킬 최대 파일 수를 입력합니다. 최대 파일 수에 입력하는 값이 로그 로테이션에서 삭제된 파일 수 설정에 입력하는 값보다 큰지 확인합니다. 4(최소)에서 40(최대) 사이의 숫자를 입력할 수 있습니다.
로그 로테이션에서 삭제된 파일 수	데이터베이스 감사 로그 로테이션이 발생하는 경우 시스템에서 삭제할 수 있는 최대 파일 수를 입력합니다. 이 필드에 입력할 수 있는 최소값은 1입니다. 최대값은 최대 파일 수 설정에 입력하는 값보다 2 작은 수입니다. 예를 들어, 최대 파일 수 필드에 40을 입력하는 경우 로그 로테이션에서 삭제된 파일 수에 입력할 수 있는 가장 높은 숫자는 38입니다.
기본값으로 설정	기본값으로 설정 버튼은 기본값을 지정합니다. 세부 문제 해결을 위해 다른 수준으로 설정해야 하는 경우가 아니면 감사 로그를 기본 모드로 설정하는 것이 좋습니다. 기본값으로 설정 옵션은 로그 파일에 사용되는 디스크 공간을 최소화합니다.

주의 이 기능을 활성화하면, 특히 디버그 감사 수준이 데이터베이스 업데이트 또는 데이터베이스 읽기로 설정된 경우 데이터베이스 로깅이 짧은 기간에 많은 양의 데이터를 생성할 수 있습니다. 이로 인해 사용량이 많은 시간 동안 성능에 심각한 영향을 미칠 수 있습니다. 일반적으로 데이터베이스 로깅을 비활성화하는 것이 좋습니다. 데이터베이스의 변경 내용을 추적하기 위해 로깅을 활성화해야 하는 경우 데이터베이스 업데이트 수준을 사용하여 짧은 시간 동안만 이 작업을 수행하는 것이 좋습니다. 마찬가지로, 관리 로깅은 특히 데이터베이스 항목을 폴링하는 경우(예: 데이터베이스에서 250개 장치 열기) 웹 사용자 인터페이스의 전반적인 성능에 영향을 미칩니다.