문제 해결 도구

이 섹션에서는 Unified Communications Manager 구성, 모니터링 및 문제 해결에 사용하는 도구 및 유틸리티를 설명하고, 동일한 데이터의 반복적인 테스트 및 수집을 방지하기 위해 정보 수집에 대한 일반적인 지침을 제공합니다.

참고 이 문서에 나열된 일부 URL 사이트에 액세스하려면 등록된 사용자여야 하며 로그인해야 합니다.

Cisco 통합 서비스 가용성 문제 해결 도구

Cisco 유니파이드 Serviceability에서 다양한 Unified Communications Manager 시스템을 모니터링하고 분석할 수 있는 다음과 같은 다양한 유형의 도구에 대한 자세한 내용은 *Cisco* 통합 서비스 가용성 관리 가이드를 참조하십시오.

표 *1:* 서비스 가용성 도구

용어	정의
Cisco Unified Real-Time Monitoring Tool(RTMT)	이 도구는 Unified Communications Manager 장치 및 성능 카운터에 대한 실시간 정보를 제공하며 추적을 수집할 수 있습니다. 성능 카운터는 시스템 또는 Unified Communications Manager에 따라 다릅니다. 개체는 특정 장치 또는 기능(예: Cisco Unified IP Phone 또는 Unified Communications Manager 시스템 성능)에 대한 카운터 같은 논리적 그룹을 구성합니다. 카운터는 시스템 성능에 대한 다양한 측면을 측정합니다. 카운터는 등록된 전화기 수, 시도된 통화 수 및 진행 중인 통화 수와 같은 통계를 측정합니다.
알람	관리자는 알람을 사용하여 런타임 상태 및 Unified Communications Manager 시스템의 상태를 얻습니다. 알람에는 설명 및 권장 작업 등 시스템 문제에 대한 정보가 포함되어 있습니다. 관리자는 알람 정의 데이터베이스에서 알람 정보를 검색합니다. 알람 정의에는 알람 및 권장 작업에 대한 설명이 포함되어 있습니다.
추적	관리자 및 Cisco 엔지니어가 추적 파일을 사용하여 Unified Communications Manager 서비스 문제에 대한 구체적인 정보를 얻습니다. Cisco 유니파이드 Serviceability는 구성된 추적 정보를 추적 로그 파일로 전송합니다. 두 가지 유형의 추적 로그 파일(SDI 및 SDL)이 있습니다. 모든 서비스에는 기본 추적 로그 파일이 포함됩니다. 시스템은 서비스에서 SDI(시스템 진단 인터페이스) 정보를 추적하고 런타임 이벤트 및 추적을 로그 파일로 기록합니다. SDL 추적 로그 파일에는 Cisco CallManager 및 Cisco CTIManager와 같은 서비스의 통화 처리 정보가 포함됩니다. 시스템에서 통화의 SDL(신호 디스트리뷰션 레이어)을 추적하고 상태 전환을 로그 파일에 기록합니다. 참고 대부분의 경우에는 Cisco TAC(Technical Assistance Center) 요청이 있을 때에만 SDL 추적을 수집합니다.
품질 보고서 도구	이 용어는 Cisco 유니파이드 Serviceability에서 음질 및 일반 문제 보고 유틸리티를 지정합니다.
서비스 가용성 커넥터	Cisco Webex 서비스 가용성 서비스는 Cisco 기술 지원 담당자가 인프라의 문제를 진단할 수 있는 속도를 높여줍니다. 이 서비스는 SR 케이스에서 진단 로그 및 정보의 찾기, 검색 및 저장 작업을 자동화합니다. 또한 이 서비스는 사용자 온-프레미스 장비와 관련된 문제를 효율적으로 식별하고 해결할 수 있도록 진단 서명에 대한 분석을 트리거합니다.

명령줄 인터페이스

CLI(명령줄 인터페이스)를 사용하여 기본 유지 보수 및 장애 복구를 위해 Unified Communications Manager 시스템에 액세스합니다. 유선 터미널(시스템 모니터 및 키보드)을 사용하거나 SSH 세션을 수행하여 시스템에 대한 액세스 권한을 얻습니다.

계정 이름 및 암호는 설치 시 생성됩니다. 설치 후에 암호를 변경할 수 있지만 계정 이름은 변경할 수 없습니다.

명령은 시스템에서 일부 기능을 수행하는 텍스트 명령을 나타냅니다. 명령은 독립 실행형이거나 필수 또는 선택적 인수나 옵션을 가질 수 있습니다.

수준은 명령 모음으로 구성됩니다. 예를 들어, show는 수준을 지정하는 반면, show status는 명령을 지정합니다. 각 수준 및 명령에는 연결된 권한 수준도 포함되어 있습니다. 충분한 권한 수준이 있는 경우에만 명령을 실행할 수 있습니다.

Unified Communications Manager CLI 명령에 대한 자세한 내용은 *Cisco Unified Solutions*용 명령줄 인터페이스 참조 설명서를 참조하십시오.

kernelDump 유틸리티

kernelDump 유틸리티를 사용하면 보조 서버를 요구하지 않고 영향을 받는 시스템에서 로컬로 크래시 덤프 로그를 수집할 수 있습니다.

Unified Communications Manager 클러스터에서 크래시 덤프 정보를 수집하기 전에 서버에서 kernelDump 유틸리티가 활성화되어 있어야 합니다.

참고 더 효율적인 문제 해결을 위해 Unified Communications Manager를 설치한 후 kernelDump 유틸리티가 활성화되어 있는지 확인하는 것이 좋습니다. 아직 수행하지 않은 경우, 지원되는 어플라이언스 릴리스에서 Unified Communications Manager를 업그레이드하기 전에 kernelDump 유틸리티를 활성화합니다.

중요 kernelDump 유틸리티를 활성화하거나 비활성화하면 노드를 재부팅해야 합니다. 재부팅이 허용되는 창 내에 있지 않은 경우에는 enable 명령을 실행하지 마십시오.

Cisco 통합 커뮤니케이션 운영 체제에 대한 CLI(명령줄 인터페이스)를 사용하여 kernelDump 유틸리티의 상태를 활성화, 비활성화 또는 확인할 수 있습니다.

다음 절차를 사용하여 커널 덤프 유틸리티를 활성화합니다.

유틸리티에서 수집한 파일을 사용하여 작업

kerneldump 유틸리티에서 충돌 정보를 보려면 *Cisco Unified Real-Time Monitoring Tool* 또는 CLI(명령줄 인터페이스)를 사용하십시오. *Cisco Unified Real-Time Monitoring Tool*를 사용하여 kerneldump 로그를 수집하려면 추적 및 로그 센트럴에서 파일 수집 옵션을 선택합니다. 시스템 서비스/애플리케이션 탭에서 Kerneldump 로그 확인란을 선택합니다. *Cisco Unified Real-Time Monitoring Tool* 사용에 대한 자세한 내용은 *Cisco Unified Real-Time Monitoring Tool* 관리 지침서를 참조하십시오.

CLI를 사용하여 kerneldump 로그를 수집하려면 충돌 디렉터리의 파일에 대한 "file" CLI 명령을 사용합니다. 이러한 항목은 "activelog" 파티션 아래에 있습니다. 로그 파일 이름은 kerneldump 클라이언트의 IP 주소로 시작하여 파일을 만든 날짜로 끝납니다. file 명령에 대한 자세한 내용은 *Cisco Unified Solutions*용 명령줄 인터페이스 설명서를 참조하십시오.

Kerneldump 유틸리티 활성화

이 절차를 사용하여 kerneldump 유틸리티를 활성화합니다. 커널 충돌이 발생하는 경우 유틸리티는 충돌을 수집하고 덤프하는 메커니즘을 제공합니다. 로컬 서버 또는 외부 서버에 로그를 덤프하도록 유틸리티를 구성할 수 있습니다.

프로시저

단계 **1** 명령줄 인터페이스에 로그인합니다.

단계 **2** 다음 중 하나를 완료합니다.

- 로컬 서버에서 커널 충돌을 덤프하려면 `utils os kernelcrash enable` CLI 명령을 실행합니다.
- 외부 서버에 커널 충돌을 덤프하려면 외부 서버의 IP 주소를 사용하여 `utils os kerneldump ssh enable <ip_address>` CLI 명령을 실행합니다.

단계 **3** 서버를 재부팅합니다.

예

참고 kerneldump 유틸리티를 비활성화해야 하는 경우에는 `utils os kernelcrash disable` CLI 명령을 실행하여 코어 덤프에 대한 로컬 서버를 비활성화하고 `utils os kerneldump ssh disable < ip_address >` CLI 명령을 사용하여 외부 서버에서 유틸리티를 비활성화할 수 있습니다.

다음에 수행할 작업

Real Time Monitoring Tool에서 이메일 경고를 구성하여 코어 덤프에 대해 알려줍니다. 자세한 내용은 핵심 덤프에 대한 이메일 경고 활성화을 참조하십시오.

kerneldump 유틸리티 및 문제 해결에 관한 자세한 내용은 *Cisco Unified Communications Manager*용 문제 해결 설명서를 참조하십시오.

핵심 덤프에 대한 이메일 경고 활성화

이 절차를 사용하여 핵심 덤프가 발생할 때마다 관리자에게 이메일을 보낼 수 있도록 실시간 모니터링 도구를 구성할 수 있습니다.

프로시저

단계 **1** 시스템 > 도구 > 알림 > 알림 센트럴을 선택합니다.

단계 **2** **CoreDumpFileFound** 알림을 마우스 오른쪽 버튼으로 클릭하고 알림 속성 설정을 선택합니다.

단계 **3** 마법사 프롬프트에 따라 기본 설정 기준을 설정합니다.

a) 알림 속성**:** 이메일 알림 팝업에서 이메일 활성화가 선택되어 있는지 확인하고 구성을 클릭하여 관리자에게 이메일을 보낼 기본 알림 작업을 설정합니다.

b) 프롬프트에 따라 수신자 이메일 주소를 추가합니다. 이 알림이 트리거되면 기본 동작은 이 주소로 이메일을 전송합니다.

c) 저장을 클릭합니다.

단계 **4** 기본 이메일 서버를 설정합니다.

a) 시스템 > 도구 > 알림 > 이메일 서버 구성을 선택합니다.

b) 이메일 서버 설정을 입력합니다.

c) 확인을 클릭합니다.

네트워크 관리

Unified Communications Manager 원격 서비스 가용성에 대한 네트워크 관리 도구를 사용합니다.

- 시스템 로그 관리
- Cisco Discovery Protocol 지원
- SNMP(Simple Network Management Protocol) 지원

자세한 내용은 이러한 네트워크 관리 도구에 대한 섹션에 제공된 URL의 설명서를 참조하십시오.

시스템 로그 관리

Cisco 시스템 로그 분석은 다른 네트워크 관리 시스템에 맞게 조정될 수 있지만, RME(Resource Manager Essentials)와 함께 패키지된 Cisco 시스템 로그 분석은 Cisco 장치에서 시스템 로그 메시지를 관리하는 최상의 방법을 제공합니다.

Cisco 시스템 로그 분석기는 여러 애플리케이션에 대한 시스템 로그의 공통된 저장 및 분석을 제공하는 Cisco 시스템 로그 분석의 구성 요소로 사용됩니다. 기타 주요 구성 요소인 시스템 로그 분석기 수집기에서 Unified Communications Manager 서버로부터 로그 메시지를 수집합니다.

이러한 두 Cisco 애플리케이션은 함께 작동하여 Cisco 통합 커뮤니케이션 솔루션에 대한 중앙 집중식 시스템 로깅 서비스를 제공합니다.

RME 설명서는 *http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml* URL을 참조하십시오.

Cisco Discovery Protocol 지원

Cisco Discovery Protocol Support를 사용하면 Unified Communications Manager 서버를 검색하고 해당 서버를 관리할 수 있습니다.

RME 설명서는 *http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml* URL을 참조하십시오.

SNMP(Simple Network Management Protocol) 지원

NMS(네트워크 관리 시스템)는 네트워크 장치 간에 관리 정보를 교환하기 위해 업계 표준 인터페이스인 SNMP를 사용합니다. TCP/IP 프로토콜의 일부로 SNMP를 사용하면 관리자가 네트워크 성능을 원격 관리하고 네트워크 문제를 찾아 해결하며 네트워크 확장을 계획할 수 있습니다.

SNMP 관리 네트워크는 관리되는 장치, 에이전트 및 네트워크 관리 시스템의 세 가지 핵심 구성 요소로 이루어집니다.

- 관리되는 장치는 SNMP 에이전트를 포함하고 관리되는 네트워크에 상주하는 네트워크 노드를 나타냅니다. 관리되는 장치는 관리 정보를 수집 및 저장하고 SNMP를 사용하여 사용할 수 있게 합니다.
- 에이전트는 관리되는 장치에 있는 네트워크 관리 소프트웨어입니다. 에이전트는 관리 정보에 대한 로컬 지식을 포함하고 이를 SNMP와 호환되는 형태로 변환합니다.
- 네트워크 관리 시스템은 SNMP 관리 애플리케이션과 해당 애플리케이션이 실행되는 시스템으로 구성됩니다. NMS는 관리되는 장치를 모니터링하고 제어하는 애플리케이션을 실행합니다. NMS는 네트워크 관리에 필요한 벌크 처리 및 메모리 리소스를 제공합니다. 다음 NMS는 Unified Communications Manager와 호환성을 공유합니다.
  - CiscoWorks 공통 서비스 소프트웨어
  - HP OpenView
  - SNMP 및 Unified Communications Manager SNMP 인터페이스를 지원하는 타사 애플리케이션

스니퍼 추적

일반적으로 문제 정보를 포함하는 VLAN 또는 포트(CatOS, Cat6K-IOS, XL-IOS)를 확장하도록 구성된 Catalyst 포트에 랩톱이나 기타 스니퍼 장착 장치를 연결하여 스니퍼 추적을 수집합니다. 사용할 수 있는 빈 포트가 없는 경우에는 스위치와 장치 사이에 삽입된 허브에 스니퍼 장착 장치를 연결합니다.

팁 TAC 엔지니어에 의한 추적 읽기 및 해석에 도움이 되도록 하려면 TAC에서 널리 사용되는 Sniffer Pro 소프트웨어를 사용하는 것이 좋습니다.

IP 전화기, 게이트웨이, Unified Communications Manager 등과 같이 관련된 모든 장비의 IP/MAC 주소를 사용할 수 있습니다.

디버그

debug특권 EXEC 명령의 출력은 프로토콜 상태 및 네트워크 활동과 관련된 다양 한 인터 네트워킹 이벤트에 대한 진단 정보를 제공합니다.

디버그 출력을 파일로 캡처할 수 있도록 터미널 에뮬레이터 소프트웨어(예: 하이퍼터미널)를 설정합니다. 하이퍼터미널에서 전환을 클릭한 다음 텍스트 캡처를 클릭하고 적절한 옵션을 선택합니다.

IOS 음성 게이트웨이 디버그를 실행하기 전에 **servicetimestampsdebugdatetimemsec**가 게이트웨이에서 전역으로 구성되어 있는지 확인합니다.

참고 작업 시간 중에 라이브 환경에서 디버깅을 수집하지 않도록 하십시오.

가능하면 근무 시간이 아닐 때 디버깅을 수집하십시오. 라이브 환경에서 디버그를 수집해야 하는 경우에는 로깅 콘솔 없음 및 로깅 버퍼링됨을 구성합니다. 디버그를 수집하려면 **show log**를 사용하십시오.

일부 디버그는 시간이 오래 걸릴 수 있으므로 콘솔 포트(기본 로깅 콘솔) 또는 버퍼(로깅 버퍼)에서 직접 수집합니다. 텔넷 세션을 통해 디버그를 수집하면 장치 성능에 영향을 줄 수 있고, 결과를 다시 수집해야 하는 불완전한 디버그일 수 있습니다.

디버그를 중지하려면 **no debug all** 또는 **undebug all** 명령을 사용하십시오. **show debug** 명령을 사용하여 디버그가 꺼져 있는지 확인합니다.

Cisco 보안 텔넷

Cisco 보안 텔넷을 사용하면 Cisco Service 엔지니어(CSE) 투명 방화벽이 사이트의 Unified Communications Manager노드에 액세스할 수 있습니다. 강력한 암호화를 사용하면 *Cisco* 보안 텔넷을

사용하여 특별한 텔넷 클라이언트가 Cisco 시스템에서 방화벽 뒤에 있는 텔넷 데몬에 연결되도록 할 수 있습니다. 이 보안 연결을 사용하면 방화벽을 수정할 필요 없이 Unified Communications Manager 노드의 원격 모니터링 및 문제 해결을 수행할 수 있습니다.

참고 Cisco는 사용자의 허가가 있는 경우에만 이 서비스를 제공합니다. 프로세스를 시작하는 데 도움이 되도록 사이트에 네트워크 관리자가 있는지 확인해야 합니다.

패킷 캡처

이 섹션에는 패킷 캡처에 대한 정보가 포함되어 있습니다.

관련 항목

패킷 캡처 개요, 8 페이지
패킷 캡처를 위한 구성 검사 목록, 9 페이지
표준 패킷 스니퍼 액세스 제어 그룹에 최종 사용자 추가 , 9 페이지
패킷 캡처 서비스 매개 변수 구성, 10 페이지
전화기 구성 창에서 패킷 캡처 구성, 10 페이지
게이트웨이 및 트렁크 구성 창에서 패킷 캡처 구성, 11 페이지
패킷 캡처 구성 설정, 13 페이지
캡처된 패킷 분석, 15 페이지

패킷 캡처 개요

암호화를 활성화한 후에 미디어 및 TCP 패킷을 검사하는 타사 문제 해결 도구가 작동하지 않으므로 Unified Communications Manager를 사용하여 다음 작업을 수행하여 문제가 발생하는지 확인해야 합니다.

- Unified Communications Manager와 장치[Cisco Unified IP Phone (SIP 및 SCCP), Cisco IOS MGCP 게이트웨이, H.323 게이트웨이, H.323/H.245/H.225 트렁크 또는 SIP 트렁크]에서 교환되는 메시지에 대한 패킷을 분석합니다.
- 장치 간에 SRTP(Secure Real Time Protocol) 패킷을 캡처합니다.
- 메시지에서 미디어 암호화 키 자료를 추출하고 장치 간의 미디어를 해독합니다.

팁 동시에 여러 장치에 대해 이 작업을 수행하면 CPU 사용량이 많아지고 및 통화 처리 중단이 발생할 수 있습니다. 통화 처리 중단을 최소화할 수 있는 경우 이 작업을 수행하는 것이 좋습니다.

자세한 내용은 Cisco Unified Communications Manager 보안 설명서를 참조하십시오.

패킷 캡처를 위한 구성 검사 목록

관련 데이터의 압축을 풀고 분석하려면 다음 작업이 포함됩니다.

절차

1. 표준 패킷 스니퍼 사용자 그룹에 최종 사용자를 추가합니다.
2. Cisco Unified Communications Manager Administration의 서비스 매개 변수 구성 창에서 패킷 캡처 서비스 매개 변수를 구성합니다. 예를 들어 패킷 캡처 활성화 서비스 매개 변수를 구성합니다.
3. 전화기, 게이트웨이 또는 트렁크 구성 창에서 장치별로 패킷 캡처 설정을 구성합니다.

참고 이 작업이 네트워크에서 높은 CPU 사용량을 유발할 수 있으므로 많은 장치에 대해 동시에 패킷 캡처를 사용하도록 설정하지 않는 것이 좋습니다.

4. 영향을 받는 장치 사이에서 스니퍼 추적을 사용하여 SRTP 패킷을 캡처합니다. 스니퍼 추적 도구를 지원하는 설명서를 참조하십시오.
5. 패킷을 캡처한 후에는 패킷 캡처 활성화 서비스 매개 변수를 False로 설정합니다.
6. 패킷을 분석하는 데 필요한 파일을 수집합니다.
7. Cisco 기술 지원 센터(TAC)는 패킷을 분석합니다. 이 작업을 수행하려면 TAC에 직접 문의하십시오.

관련 항목

표준 패킷 스니퍼 액세스 제어 그룹에 최종 사용자 추가 , 9 페이지
캡처된 패킷 분석, 15 페이지
게이트웨이 및 트렁크 구성 창에서 패킷 캡처 구성, 11 페이지
전화기 구성 창에서 패킷 캡처 구성, 10 페이지
패킷 캡처 서비스 매개 변수 구성, 10 페이지
패킷 캡처 구성 설정, 13 페이지

표준 패킷 스니퍼 액세스 제어 그룹에 최종 사용자 추가

표준 패킷 스니퍼 사용자 그룹에 속하는 최종 사용자는 패킷 캡처를 지원하는 장치에 대한 패킷 캡처 모드 및 패킷 캡처 기간 설정을 구성할 수 있습니다. 사용자가 표준 패킷 스니퍼 액세스 제어 그룹에 없는 경우 사용자는 패킷 캡처를 시작할 수 없습니다.

표준 패킷 스니퍼 액세스 제어 그룹에 최종 사용자를 추가하는 방법을 설명하는 다음 절차는 Cisco Unified Communications Manager 관리 지침서에 설명된 대로 최종 사용자를 Cisco Unified Communications Manager Administration에서 구성한 것으로 가정합니다.

절차

1. Cisco Unified Communications Manager 관리 지침서에 설명된 대로 액세스 제어 그룹을 찾습니다.
2. 찾기/나열 창이 표시 되 면 표준 패킷 스니퍼 사용자 링크를 클릭합니다.
3. 그룹에 추가 버튼을 클릭합니다.
4. Cisco Unified Communications Manager 관리 지침서의 설명에 따라 최종 사용자를 추가합니다.
5. 사용자를 추가한 후 저장을 클릭합니다.

패킷 캡처 서비스 매개 변수 구성

패킷 캡처에 대한 매개 변수를 구성하려면 다음 절차를 수행합니다.

절차

1. Unified Communications Manager에서 시스템 > 서비스 매개 변수를 선택합니다.
2. 서버 드롭다운 목록 상자에서 Cisco CallManager 서비스를 활성화한 활성 서버를 선택합니다.
3. 서비스 드롭다운 목록 상자에서 **Cisco CallManager(**활성**)** 서비스를 선택합니다.
4. TLS 패킷 캡처 구성 창으로 스크롤하고 패킷 캡처 설정을 구성합니다.

팁 서비스 매개 변수에 대한 정보를 보려면 매개 변수 이름을 클릭하거나 창에 표시되는 물음표를 클릭합니다.

참고 패킷 캡처가 발생하려면 패킷 캡처 활성화 서비스 매개 변수를 True로 설정해야 합니다.

5. 변경 사항을 적용하려면 저장을 클릭합니다.
6. 계속해서 패킷 캡처를 구성할 수 있습니다.

관련 항목

게이트웨이 및 트렁크 구성 창에서 패킷 캡처 구성, 11 페이지
전화기 구성 창에서 패킷 캡처 구성, 10 페이지

전화기 구성 창에서 패킷 캡처 구성

서비스 매개 변수 창에서 패킷 캡처를 활성화한 후에는 Cisco Unified Communications Manager Administration의 전화기 구성 창에서 장치별로 패킷 캡처를 구성할 수 있습니다.

패킷 캡처를 전화기별로 활성화하거나 비활성화할 수 있습니다. 패킷 캡처의 기본 설정은 없음입니다.

주의 이 작업이 네트워크에서 높은 CPU 사용량을 유발할 수 있으므로 많은 전화기에 대해 동시에 패킷 캡처를 사용하도록 설정하지 않는 것이 좋습니다.

패킷을 캡처하지 않으려거나 작업을 완료한 경우 패킷 캡처 활성화 서비스 매개 변수를 False로 설정합니다.

전화기에 대해 패킷 캡처에 대한 매개 변수를 구성하려면 다음 절차를 수행합니다.

절차

1. 패킷 캡처 설정을 구성하기 전에 패킷 캡처 구성과 관련된 주제를 참조하십시오.
2. Cisco Unified Communications Manager 시스템 구성 설명서에 설명된 대로 SIP 또는 SCCP 전화기를 찾습니다.
3. 전화기 구성 창이 표시되면 패킷 캡처 구성 설정에 설명된 대로 문제 해결 설정을 구성합니다.
4. 구성을 완료한 후에 저장을 클릭합니다.
5. 재설정 대화 상자에서 확인을 클릭합니다.

팁 Cisco Unified Communications Manager Administration에 장치를 재설정하라는 메시지가 표시되지만 패킷을 캡처하기 위해 장치를 재설정할 필요는 없습니다.

추가 단계

영향을 받는 장치 사이에서 스니퍼 추적을 사용하여 SRTP 패킷을 캡처합니다.

패킷을 캡처한 후에는 패킷 캡처 활성화 서비스 매개 변수를 False로 설정합니다.

관련 항목

캡처된 패킷 분석, 15 페이지
패킷 캡처를 위한 구성 검사 목록, 9 페이지

게이트웨이 및 트렁크 구성 창에서 패킷 캡처 구성

다음 게이트웨이및 트렁크는 Unified Communications Manager에서 패킷 캡처를 지원합니다.

- Cisco IOS MGCP 게이트웨이
- H.323 게이트웨이
- H.323/H.245/H.225 트렁크
- SIP 트렁크

팁 이 작업이 네트워크에서 높은 CPU 사용량을 유발할 수 있으므로 많은 장치에 대해 동시에 패킷 캡처를 사용하도록 설정하지 않는 것이 좋습니다.

패킷을 캡처하지 않으려거나 작업을 완료한 경우 패킷 캡처 활성화 서비스 매개 변수를 False로 설정합니다.

게이트웨이 또는 트렁크 구성 창에서 패킷 캡처 설정을 구성하려면 다음 절차를 수행합니다.

절차

1. 패킷 캡처 설정을 구성하기 전에 패킷 캡처 구성과 관련된 주제를 참조하십시오.
2. 다음 작업 중 하나를 수행합니다.
   - Cisco Unified Communications Manager 시스템 구성 설명서에 설명된 대로 Cisco IOS MGCP 게이트웨이를 찾습니다.
   - Cisco Unified Communications Manager 시스템 구성 설명서에 설명된 대로 H.323 게이트웨이를 찾습니다.
   - Cisco Unified Communications Manager 시스템 구성 설명서에 설명된 대로 H.323/H.245/H.225 트렁크를 찾습니다.
   - Cisco Unified Communications Manager 시스템 구성 설명서에 설명된 대로 SIP 트렁크를 찾습니다.
3. 구성 창이 표시되면 패킷 캡처 모드 및 패킷 캡처 기간 설정을 찾습니다.

팁 Cisco IOS MGCP 게이트웨이를 찾은 경우 Cisco Unified Communications Manager 관리 지침서에 설명된 대로 Cisco IOS MGCP 게이트웨이에 대한 포트를 구성했는지 확인합니다. Cisco IOS MGCP 게이트웨이에 대한 패킷 캡처 설정은 엔드포인트 ID에 대한 게이트웨이 구성 창에 표시됩니다. 이 창에 액세스하려면 음성 인터페이스 카드의 엔드포인트 ID를 클릭합니다.

4. 패킷 캡처 구성 설정에 설명된 대로 문제 해결 설정을 구성합니다.
5. 패킷 캡처 설정을 구성한 후에는 저장을 클릭합니다.
6. 재설정 대화 상자에서 확인을 클릭합니다.

팁 Cisco Unified Communications Manager Administration에 장치를 재설정하라는 메시지가 표시되지만 패킷을 캡처하기 위해 장치를 재설정할 필요는 없습니다.

추가 단계

영향을 받는 장치 사이에서 스니퍼 추적을 사용하여 SRTP 패킷을 캡처합니다.

패킷을 캡처한 후에는 패킷 캡처 활성화 서비스 매개 변수를 False로 설정합니다.

관련 항목

캡처된 패킷 분석, 15 페이지
패킷 캡처를 위한 구성 검사 목록, 9 페이지

패킷 캡처 구성 설정

다음 표에서는 게이트웨이, 트렁크 및 전화기에 대한 패킷 캡처를 구성할 때 패킷 캡처 모드 및 패킷 캡처 기간 설정에 대해 설명합니다.

설정	설명
패킷 캡처 모드	이 설정은 암호화 문제를 해결하기 위해서만 존재합니다. 패킷을 캡처하면 CPU 사용량이 많아지거나 통화 처리가 중단될 수 있습니다. 드롭다운 목록 상자에서 다음 옵션 중 하나를 선택합니다. • 없음 - 기본 설정으로 사용되는 이 옵션은 패킷 캡처가 발생하지 않음을 나타냅니다. 패킷 캡처를 완료한 후 Unified Communications Manager는 패킷 캡처 모드를 없음으로 설정합니다. • 배치 처리 모드 - Unified Communications Manager이 해독되었거나 암호화되지 않은 메시지를 파일로 작성하고 각 파일이 시스템에서 암호화됩니다. 매일 시스템에서 새 암호화 키를 사용하여 새 파일을 생성합니다. Unified Communications Manager은 7일 동안 파일을 저장하며, 파일을 암호화하는 데 사용한 키 또한 안전한 위치에 저장합니다. Unified Communications Manager는 파일을 PktCap 가상 디렉터리에 저장합니다. 단일 파일에는 타임스탬프, 소스 IP 주소, 소스 IP 포트, 대상 IP 주소, 패킷 프로토콜, 메시지 길이 및 메시지가 있습니다. TAC 디버깅 도구에서는 HTTPS, 관리자 사용자 이름 및 암호, 그리고 캡처된 패킷이 포함된 단일의 암호화된 파일을 요청하도록 지정된 날짜를 사용합니다. 마찬가지로, 도구는 암호화된 파일의 암호를 해독하기 위한 키 정보를 요청합니다. 팁 TAC를 연결하기 전에 영향을 받는 장치 사이에서 스니퍼 추적을 사용하여 SRTP 패킷을 캡처해야 합니다.

설정	설명
패킷 캡처 지속 시간	이 설정은 암호화 문제를 해결하기 위해서만 존재합니다. 패킷을 캡처하면 CPU 사용량이 많아지거나 통화 처리가 중단될 수 있습니다. 이 필드에서는 패킷 캡처 세션 하나에 할당한 최대 시간(분)을 세션을 지정합니다. 범위는 0~300분이며 기본 설정은 0입니다. 패킷 캡처를 시작하려면 필드에 0 이외의 다른 값을 입력합니다. 패킷 캡처가 완료되면 값 0이 표시됩니다.

관련 항목

게이트웨이 및 트렁크 구성 창에서 패킷 캡처 구성, 11 페이지
전화기 구성 창에서 패킷 캡처 구성, 10 페이지

캡처된 패킷 분석

Cisco 기술 지원 센터(TAC)는 디버깅 도구를 사용하여 패킷을 분석합니다. TAC를 연결하기 전에 영향을 받는 장치 사이에서 스니퍼 추적을 사용하여 SRTP 패킷을 캡처합니다. 다음 정보를 수집한 후에는 직접 TAC에 문의하십시오.

- 패킷 캡처 파일—**https://<IP address or server name>/pktCap/pktCap.jsp?file=mm-dd-yyyy.pkt**, 여기서 서버를 탐색하여 월, 일 및 연도(mm-dd-yyyy)로 패킷 캡처 파일을 찾습니다.
- 파일에 대한 키—**https://<IP address or server name>/pktCap/pktCap.jsp?key=mm-dd-yyyy.pkt**, 여기서 서버를 탐색하여 월, 일 및 연도(mm-dd-yyyy)로 키를 찾습니다.
- 표준 패킷 스니퍼 사용자 그룹에 속한 최종 사용자의 사용자 이름 및 암호

자세한 내용은 Cisco Unified Communications Manager 보안 설명서의 내용을 참조하십시오.

일반적인 문제 해결 작업, 도구 및 명령

이 섹션에서는 루트 액세스가 비활성화된 Unified Communications Manager 서버를 문제 해결하는 데 도움이 되는 명령 및 유틸리티에 대한 빠른 참조를 제공합니다. 다음 표에서는 여러 가지 시스템 문제를 해결하기 위한 정보를 수집하는 데 사용할 수 있는 CLI 명령 및 GUI 선택 사항에 대한 요약을 제공합니다.

표 *2: CLI* 명령 및 *GUI* 선택 사항 요약

정보	**Linux** 명령	서비스 가용성 **GUI** 도구	**CLI** 명령
CPU 사용량	위쪽	RTMT 보기 탭으로 이동하고 서버 > **CPU** 및 메모리를 선택합니다.	프로세서 CPU 사용량: show perf query class Processor 모든 프로세스에 대한 프로세스 CPU 사용량: show perf query counter Process "% CPU Time" 개별 프로세스 카운터 세부 정보(CPU 사용량 포함) show perf query instance <Process task_name>
프로세스 상태	ps	RTMT 보기 탭으로 이동하고 서버 > 프로세스를 선택합니다.	show perf query counter Process "Process Status"
디스크 사용량	df/du	RTMT 보기 탭으로 이동하고 서버 > 디스크 사용량 을 선택합니다	show perf query counter Partition"% Used" 또는 show perf query class Partition
메모리	free	RTMT 보기 탭으로 이동하고 서버 > **CPU** 및 메모리를 선택합니다.	show perf query class Memory
네트워크 상태	netstats		show network status
서버 재부팅	reboot	서버에서 플랫폼 웹 페이지에 로그인 서버 > 현재 버전으로 이동	utils system restart
추적/로그 수집	Sftp, ftp	RTMT 도구 탭으로 이동하고 추적 > 추적 및 로그 센트럴 을 선택합니다	파일 나열: file list 파일 다운로드: file get 파일 보기: file view

다음 표에서는 이러한 문제를 해결하는 데 사용할 수 있는 일반적인 문제 및 도구 목록을 제공합니다.

표 ***3: CLI*** 명령 및 ***GUI*** 선택과 관련된 일반적인 문제 해결

작업	**GUI** 도구	**CLI** 명령
데이터베이스 액세스	none	관리자로 로그인하고 다음 표시 **show** 중 하나를 사용합니다. • show tech database • show tech dbinuse • show tech dbschema • show tech devdefaults • show tech gateway • show tech locales • show tech notify • show tech procedures • show tech routepatterns • show tech routeplan • show tech systables • show tech table • show tech triggers • show tech version • show tech params* SQL 명령을 실행하려면 **run** 명령을 사용합니다. • run sql <sql 명령>
디스크 공간 확보 참고 로그 파티션에서 파일만 삭제할 수 있습니다.	RTMT 클라이언트 애플리케이션을 사용하여 도구 탭으로 이동하고 추적 및 로그 센트럴 > 파일 수집을 선택합니다. 기준을 선택하여 수집할 파일을 선택한 다음 파일 삭제 옵션을 선택합니다. 이렇게 하면 PC에 파일을 다운로드한 후 Unified Communications Manager 서버에서 파일이 삭제됩니다.	file delete

작업	**GUI** 도구	**CLI** 명령
코어 파일 보기	코어 파일은 볼 수 없습니다. 그러나 RTMT 애플리케이션을 사용하고 추적 및 로그 센트럴 > 크래시 덤프 수집을 선택하여 코어 파일을 다운로드할 수 있습니다.	utils core [옵션]
Unified Communications Manager 서버 재부팅	서버의 플랫폼에 로그인하고 재시작 > 현재 버전으로 이동합니다.	utils system restart
추적에 대한 디버그 수준 변경	`https://<server_ipaddress>:8443/ccmservice/`의 *Cisco Unity Connection* 서비스 가용성 관리에 로그인하고추적 > 구성을 선택합니다.	set trace enable [Detailed, Significant, Error, Arbitrary, Entry_exit, State_Transition, Special] [syslogmib, cdpmib, dbl, dbnotify]
netstats 보기	none	show network status

문제 해결 팁

Unified Communications Manager의 문제를 해결할 때 다음 팁이 도움이 될 수 있습니다.

팁 Unified Communications Manager의 릴리스 노트에서 알려진 문제를 확인합니다. 릴리스 노트는 알려진 문제에 대한 설명 및 해결 방법을 제공합니다.

팁 장치가 등록된 위치를 파악합니다.

각 Unified Communications Manager 로그는 로컬로 파일을 추적합니다. 전화기 또는 게이트웨이가 특정 Unified Communications Manager에 등록된 경우 통화가 시작되면 해당 Unified Communications Manager에서 통화 처리가 완료됩니다. 문제를 디버깅하려면 해당 Unified Communications Manager에서 추적을 캡처해야 합니다.

일반적인 실수는 가입자 서버에 등록되었지만 게시자 서버에서 추적을 캡처하는 장치를 포함하는 것입니다. 이러한 추적 파일은 거의 비어 있습니다(분명히 서로 간에 통화는 없는 것임).

또 다른 일반적인 문제는 장치 1을 CM1에 등록하고 장치 2를 CM2에 등록하는 것입니다. 장치 1이 장치 2에 전화를 걸 경우 통화 추적은 CM1에서 발생하고, 장치 2가 장치 1에 전화를 걸면 CM2에서 추적이 발생합니다. 양방향 통화 문제를 해결하는 경우 두 Unified Communications Manager의 두 추적 모두에서 문제 해결에 필요한 모든 정보를 수집해야 합니다.

팁 문제의 대략적인 시간을 파악합니다.

여러 통화가 발생했을 수 있으므로 통화의 대략적인 시간을 알고 있으면 TAC가 신속하게 문제를 찾을 수 있습니다.

활성 통화 중에 **i** 또는 **?** 버튼을 두 번 눌러 Cisco Unified IP Phone 79xx에서 전화 통계를 얻을 수 있습니다.

문제를 재현하고 정보를 생성하는 테스트를 실행하는 경우 문제를 이해하는 데 중요한 다음 데이터를 알고 있어야 합니다.

- 호출한 번호/호출된 번호
- 특정 시나리오에 관련된 기타 번호
- 통화 시간

참고 문제 해결을 위해서는 모든 장비의 시간 동기화가 중요하다는 점을 기억하십시오.

문제를 재현하는 경우 파일의 수정 날짜와 타임스탬프를 확인하여 해당 시간대에 대한 파일을 선택해야 합니다. 적절한 추적을 수집하는 가장 좋은 방법은 문제를 재현한 다음 가장 최근 파일을 신속하게 찾아서 Unified Communications Manager 서버에서 복사하는 것입니다.

팁 로그 파일을 덮어쓰지 않도록 저장합니다.

잠시 후 파일을 덮어씁니다. 파일이 기록되고 있는지 확인하는 유일한 방법은 메뉴 모음에서 보기 > 새로 고침을 선택하고 파일의 날짜 및 시간을 확인하는 것입니다.

시스템 기록 로그

이 시스템 기록 로그는 초기 시스템 설치, 시스템 업그레이드, Cisco 옵션 설치 및 DRS 백업과 DRS 복원에 대한 간략한 개요와 스위치 버전 및 재부팅 기록을 제공하기 위한 중앙 위치를 제공합니다.

관련 항목

시스템 기록 로그 개요, 19 페이지
시스템 기록 로그 필드, 20 페이지
시스템 기록 로그 액세스, 21 페이지

시스템 기록 로그 개요

시스템 기록 로그는 간단한 ASCII 파일인 **system-history.log**로 존재하며 데이터베이스에서 데이터가 유지 관리되지 않습니다. 과도하게 커지지 않으므로 시스템 기록 파일은 회전되지 않습니다.

시스템 기록 로그는 다음과 같은 기능을 제공합니다.

- 서버에 초기 소프트웨어 설치를 기록합니다.
- 모든 소프트웨어 업그레이드의 성공, 실패 또는 취소(Cisco 옵션 파일 및 패치)를 기록합니다.
- 수행되는 모든 DRS 백업 및 복원을 기록합니다.
- CLI 또는 GUI를 통해 발생한 스위치 버전의 모든 호출을 기록합니다.
- CLI 또는 GUI를 통해 발생한 재시작 및 종료에 대한 모든 호출을 기록합니다.
- 시스템의 모든 부팅을 기록합니다. 다시 시작 또는 종료 항목과 관련되지 않은 경우 부팅은 수동 재부팅, 전원 사이클 또는 커널 비상의 결과입니다.
- 초기 설치 이후 또는 기능 사용 가능 시간 이후 시스템 기록을 포함하는 단일 파일을 유지 관리합니다.
- 설치 폴더에 있습니다. **file** 명령 또는 Real Time Monitoring Tool을 사용하여 CLI에서 로그에 액세스할 수 있습니다.

시스템 기록 로그 필드

로그에는 제품 이름, 제품 버전 및 커널 이미지에 대한 정보가 포함된 일반 헤더가 표시됩니다. 예를 들어:

==========

제품 이름 - Unified Communications Manager

제품 버전 - 7.1.0.39000-9023

커널 이미지 - 2.6.9-67.EL

==========

각 시스템 기록 로그 항목에는 다음 필드가 포함되어 있습니다.

타임스탬프 사용자 *ID* 작업 설명 시작/결과

시스템 기록 로그 필드에는 다음 값이 포함될 수 있습니다.

- 타임스탬프 - *mm/dd/yyyy hh:mm:ss* 형식으로 서버의 로컬 시간과 날짜를 표시합니다.
- 사용자 *ID* - 작업을 호출하는 사용자의 사용자 이름을 표시합니다.
- 작업 - 다음 작업 중 하나를 표시합니다.
  - 설치
  - Windows 업그레이드
  - 설치 중 업그레이드
  - 업그레이드
  - Cisco 옵션 설치

- 버전 전환
- 시스템 재시작
- 종료
- 부팅
- DRS 백업
- DRS 복원

- 설명 - 다음 메시지 중 하나를 표시합니다.
  - 버전: 기본 설치, Windows 업그레이드, 설치 중 업그레이드 및 업그레이드 작업의 경우 표시됩니다.
  - *Cisco* 옵션 파일 이름: Cisco 옵션 설치 작업의 경우 표시됩니다.
  - 타임스탬프: DRS 백업 및 DRS 복원 작업의 경우 표시됩니다.
  - 활성 버전에서 비활성 버전으로: 버전 전환 작업의 경우 표시됩니다.
  - 활성 버전: 시스템 재시작, 종료 및 부팅 작업의 경우 표시됩니다.
- 결과 - 다음과 같은 결과를 표시합니다.
  - 시작
  - 성공 또는 실패
  - 중단

다음은 시스템 기록 로그의 샘플입니다.

```
admin:file dump install system-history.log======================================
 Product Name - Cisco Unified Communications Manager Product Version -
6.1.2.9901-117 Kernel Image - 2.4.21-47.EL.cs.3BOOT
======================================= 07/25/2008 14:20:06 | root: Install
6.1.2.9901-117 Start 07/25/2008 15:05:37 | root: Install 6.1.2.9901-117 Success
07/25/2008 15:05:38 | root: Boot 6.1.2.9901-117 Start 07/30/2008 10:08:56 | root:
 Upgrade 6.1.2.9901-126 Start 07/30/2008 10:46:31 | root: Upgrade 6.1.2.9901-126
 Success 07/30/2008 10:46:43 | root: Switch Version 6.1.2.9901-117 to
6.1.2.9901-126 Start 07/30/2008 10:48:39 | root: Switch Version 6.1.2.9901-117
to 6.1.2.9901-126 Success 07/30/2008 10:48:39 | root: Restart 6.1.2.9901-126 Start
 07/30/2008 10:51:27 | root: Boot 6.1.2.9901-126 Start 08/01/2008 16:29:31 | root:
 Restart 6.1.2.9901-126 Start 08/01/2008 16:32:31 | root: Boot 6.1.2.9901-126
Start
```

시스템 기록 로그 액세스

CLI 또는 RTMT를 사용하여 시스템 기록 로그에 액세스할 수 있습니다.

CLI 사용

CLI **file** 명령을 사용하여 시스템 기록 로그에 액세스할 수 있습니다. 예를 들면 다음과 같습니다.

- **file view install system-history.log**
- **file get install system-history.log**

CLI **file** 명령에 대한 자세한 내용은 *Cisco Unified Solutions*용 명령줄 인터페이스 참조 설명서를 참조하십시오.

RTMT 사용

RTMT를 사용하여 시스템 기록 로그에 액세스할 수도 있습니다. 추적 및 로그 센트럴 탭에서 설치 로그 수집을 선택합니다.

RTMT 사용에 대한 자세한 내용은 *Cisco Unified Real-Time Monitoring Tool* 관리 지침서를 참조하십시오.

감사 로깅

중앙 집중식 감사 로깅을 통해 Unified Communications Manager 시스템에 대한 구성 변경 사항이 감사를 위해 개별 로그 파일에 기록됩니다. 감사 이벤트는 로깅해야 하는 이벤트를 나타냅니다. 다음 Unified Communications Manager 구성 요소는 감사 이벤트를 생성합니다.

- Cisco Unified Communications Manager Administration
- Cisco 유니파이드 Serviceability
- *Unified Communications Manager CDR Analysis and Reporting*
- *Cisco Unified Real-Time Monitoring Tool*
- *Cisco Unified Communications* 운영 체제
- 재해 복구 시스템
- 데이터베이스
- 명령줄 인터페이스
- 원격 지원 계정 활성화됨(기술 지원 팀에서 CLI 명령을 실행함)

*Cisco Business Edition 5000*에서 다음 Cisco Unity Connection 구성 요소는 감사 이벤트도 생성합니다.

- Cisco Unity Connection 관리
- *Cisco Personal Communications Assistant*(Cisco PCA)
- Cisco Unity Connection 서비스 가용성
- Cisco Unity Connection REST(Representational State Transfer) API를 사용하는 클라이언트

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
```

감사 이벤트에 대한 정보가 포함된 감사 로그는 일반 파티션에 기록됩니다. LPM(로그 파티션 모니터)은 추적 파일처럼 필요에 따라 이러한 감사 로그의 제거를 관리합니다. 기본적으로 LPM은 감사 로그를 제거하지만 감사 사용자는 Cisco 유니파이드 Serviceability의 감사 사용자 구성 창에서 이 설정을 변경할 수 있습니다. LPM은 공통 파티션 디스크 사용량이 임계값을 초과할 때마다 경고를 전송합니다. 그러나 경고에는 감사 로그 또는 추적 파일로 인해 디스크가 꽉 찼는지 여부에 대한 정보가 없습니다.

팁 감사 로깅을 지원하는 네트워크 서비스인 Cisco 감사 이벤트 서비스는 Cisco 유니파이드 Serviceability의 제어 센터에 - 네트워크 서비스에 표시됩니다. 감사 로그가 기록되지 않은 경우 Cisco 유니파이드 Serviceability에서 도구 > 제어 센터 - 네트워크 서비스를 선택하여 이 서비스를 중지하고 시작합니다.

모든 감사 로그는 *Cisco Unified Real-Time Monitoring Tool*의 추적 및 로그 센트럴에서 수집, 보고 및 삭제됩니다. 추적 및 로그 센트럴에서 RTMT의 감사 로그에 액세스합니다. 시스템 > 실시간 추적 > 감사 로그 > 노드로 이동합니다. 노드를 선택하면 다른 창에시스템 > **Cisco** 감사 로그가 표시됩니다.

RTMT에 표시되는 감사 로그 유형은 다음과 같습니다.

- 애플리케이션 로그
- 데이터베이스 로그
- 운영 체제 로그
- 원격 SupportAccEnabled 로그

애플리케이션 로그

RTMT의 AuditApp 폴더에 표시되는 애플리케이션 감사 로그는 Cisco Unified Communications Manager Administration, Cisco 유니파이드 Serviceability, *CLI*, *Cisco Unified Real-Time Monitoring Tool*(RTMT), 재해 복구 시스템 및 Cisco Unified CDR Analysis and Reporting(CAR)에 대한 구성 변경 사항을 제공합니다. *Cisco Business Edition 5000*의 경우 애플리케이션 감사 로그는 Cisco Unity Connection 관리, *Cisco Personal Communications Assistant*(Cisco PCA), Cisco Unity Connection 서비스 가용성 및 REST(Representational State Transfer) API를 사용하는 클라이언트에 대한 변경 사항을 기록합니다.

애플리케이션 로그는 기본적으로 활성화되어 있지만 도구 > 감사 로그 구성을 선택하여 Cisco 유니파이드 Serviceability에서 구성할 수 있습니다. 감사 로그 구성을 위해 구성할 수 있는 설정에 대한 설명은 *Cisco* 통합 서비스 가용성 관리 가이드를 참조하십시오.

Cisco 유니파이드 Serviceability에서 감사 로그를 비활성화하면 새 감사 로그 파일이 생성되지 않습니다.

팁 감사 역할이 있는 사용자만 감사 로그 설정을 변경할 수 있습니다. 기본적으로 CCMAdministrator는 새로 설치하고 업그레이드한 후 감사 역할을 소유합니다. CCMAdministrator는 CCMAdministrator가 감사 목적으로 생성하는 새 사용자에게 "표준 감사 사용자" 그룹을 할당할 수 있습니다. 그런 다음 감사 사용자 그룹에서 CCMAdministrator를 제거할 수 있습니다. "표준 감사 로그 구성" 역할은 감사 로그를 삭제하고 *Cisco Unified Real-Time Monitoring Tool*, 추적 수집 도구, RTMT 알림 구성, 제어 센터 - 네트워크 서비스 창, RTMT 프로파일 저장, 감사 구성 창 및 감사 추적이라고 하는 새로운 리소스에 대한 읽기/업데이트 액세스 기능을 제공하는 것입니다. *Cisco Business Edition 5000*에서 Cisco Unity Connection의 경우 설치 중에 생성된 애플리케이션 관리 계정에 감사 관리자 역할이 있으며 역할에 다른 관리 사용자를 할당할 수 있습니다.

Unified Communications Manager 구성된 최대 파일 크기에 도달할 때까지 하나의 애플리케이션 감사 로그 파일을 생성합니다. 그런 다음 새 애플리케이션 감사 로그 파일을 닫고 생성합니다. 시스템에서 로그 파일을 회전하도록 지정하는 경우 Unified Communications Manager는 구성된 수의 파일을 저장합니다. 일부 로깅 이벤트는 RTMT SyslogViewer를 사용하여 볼 수 있습니다.

다음과 같은 이벤트가 Cisco Unified Communications Manager Administration의 로그에 기록 됩니다.

- 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, Unified Communications Manager 서버 추가 또는 삭제에 대한 변경)

다음과 같은 이벤트가 Cisco 유니파이드 Serviceability의 로그에 기록 됩니다.

- 서비스 가용성 창에서 서비스 활성화, 비활성화, 시작 또는 중지
- 추적 구성 및 알람 구성 변경.
- SNMP 구성의 변경.
- CDR 관리의 변경.
- 서비스 가용성 보고서 아카이브의 보고서를 검토합니다. 리포터 노드에서 이 로그를 봅니다.

RTMT가 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 CDR Analysis and Reporting*에 대해 다음 이벤트가 기록됩니다.

- CDR 로더 일정 조정
- 일별, 주별 및 월별 사용자 보고서, 시스템 보고서 및 장치 보고서의 일정을 조정합니다.
- 메일 매개 변수 구성
- 다이얼 플랜 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

재해 복구 시스템에 대해 다음과 같은 이벤트가 기록됩니다.

- 백업 시작/실패
- 복원 시작/실패
- 백업 취소
- 백업 완료/실패
- 복원 완료/실패
- 백업 일정 저장/업데이트/삭제/활성화 또는 비활성화
- 백업용 대상 장치 저장/업데이트/삭제

*Cisco Business Edition 5000*의 경우 Cisco Unity Connection 관리에서는 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 Business Edition 5000*의 경우 Cisco PCA는 다음 이벤트를 기록합니다.

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

*Cisco Business Edition 5000*의 경우 Cisco Unity Connection 서비스 가용성은 다음 이벤트를 기록합니다.

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

*Cisco Business Edition 5000*의 경우 REST API를 사용하는 클라이언트는 다음 이벤트를 기록합니다.

- 사용자 로깅(사용자 API 인증).
- Cisco Unity Connection 프로비저닝 인터페이스(CUPI)를 이용하는 API 통화

데이터베이스 로그

RTMT의 informix 폴더에 표시되는 데이터베이스 감사 로그는 데이터베이스 변경 사항을 보고합니다. 기본적으로 활성화되지 않는 이 로그는 도구 > 감사 로그 구성을 선택하여 Cisco 유니파이드 Serviceability에서 구성됩니다. 감사 로그 구성에 대해 구성할 수 있는 설정에 대한 설명은 Cisco 유니파이드 Serviceability의 내용을 참조하십시오.

이 감사는 데이터베이스 변경 사항을 기록하고 애플리케이션 감사 로그 애플리케이션 구성이 변경되기 때문에 애플리케이션 감사와는 다릅니다. 데이터베이스 감사가 Cisco 유니파이드 Serviceability에서 활성화되지 않은 경우에는 informix 폴더가 RTMT에 표시되지 않습니다.

운영 체제 로그

RTMT의 vos 폴더에 표시되는 운영 체제 감사 로그는 운영 체제에 의해 트리거되는 이벤트를 보고합니다. 이 로그는 기본적으로 활성화되지 않습니다. **utils auditd** CLI 명령은 이벤트를 활성화, 비활성화 또는 상태를 제공합니다.

CLI에서 감사가 활성화되지 않은 경우에는 vos 폴더가 RTMT에 표시되지 않습니다.

CLI에 대한 자세한 내용은 *Cisco Unified Solutions*용 명령줄 인터페이스 설명서를 참조하십시오.

원격 지원 계정 활성화 로그

RTMT의 vos 폴더에 표시되는 원격 지원 계정 활성화 감사 로그는 기술 지원 팀이 실행한 CLI 명령을 보고합니다. 이 로그는 구성할 수 없으며, 기술 지원 팀에서 원격 지원 계정 설정을 활성화한 경우에만 로그가 생성됩니다.

Cisco Unified Communications Manager 서비스가 실행 중인지 확인

다음 절차를 사용하여 서버에서 활성 상태인 Cisco CallManager 서비스를 확인합니다.

절차

1. Cisco Unified Communications Manager Administration에서탐색 > **Cisco** 통합 서비스 가용성을 선택합니다.
2. 도구 > 서비스 활성화를 선택합니다.
3. 서버 열에서 원하는 서버를 선택합니다.

   선택하는 서버는 현재 서버 제목 옆에 표시되고, 구성된 서비스가 있는 일련의 상자가 표시됩니다.

   활성화 상태 열은 Cisco CallManager 회선에서 활성화 또는 비활성화 상태를 표시합니다.

   활성화됨 상태가 표시되면 지정된 Cisco 콜매니저 서비스는 선택한 서버에서 활성 상태로 유지됩니다.

   비활성화됨 상태가 표시되면 다음 단계를 계속합니다.
4. 원하는 Cisco 콜매니저 서비스에 대한 확인란을 선택합니다.
5. 업데이트 버튼을 클릭합니다.

   활성화 상태 열이 지정된 Cisco 콜매니저 서비스 회선에서 활성화도됨을 표시합니다.

   이제 지정된 서비스가 선택한 서버에 대해 활성화된 것으로 표시됩니다.

Cisco 콜매니저 서비스가 활성화되어 있고 서비스가 현재 실행 중인지 확인하려는 경우 다음 절차를 수행합니다.

절차

1. Cisco Unified Communications Manager Administration에서탐색 > **Cisco** 통합 서비스 가용성을 선택합니다.

   Cisco 통합 서비스 가용성 창이 표시됩니다.
2. 도구 > 제어 센터 - 기능 서비스를 선택합니다.
3. 서버 열에서 서버를 선택합니다.

선택하는 서버는 현재 서버 제목 옆에 표시되고, 구성된 서비스가 있는 상자가 표시됩니다.
상태 열에 선택한 서버에 대해 실행 중인 서비스가 표시됩니다.