단순 네트워크 관리 프로토콜

SNMP(Simple Network Management Protocol) 지원

애플리케이션 레이어 프로토콜인 SNMP를 사용하면 노드, 라우터 등과 같은 네트워크 장치 간에 관리 정보를 교환하기 쉽습니다. TCP/IP의 일부로 SNMP를 사용하면 관리자가 네트워크 성능을 원격 관리하고 네트워크 문제를 찾아 해결하며 네트워크 확장을 계획할 수 있습니다.

서비스 가용성 GUI를 사용하여 V1, V2c 및 V3에 대한 커뮤니티 문자열, 사용자 및 알림 대상과 같은 SNMP 관련 설정을 구성합니다. 사용자가 구성하는 SNMP 설정은 로컬 노드에 적용됩니다. 그러나 시스템 구성에서 클러스터를 지원하는 경우 SNMP 구성 창의 "모든 노드에 적용" 옵션을 사용하여 클러스터의 모든 서버에 설정을 적용할 수 있습니다.

팁 Unified Communications Manager만 해당: Unified Communications Manager 6.0 이상을 업그레이드 중에는 Cisco Unified CallManager 또는 Unified Communications Manager 4.X에서 지정한 SNMP 구성 매개 변수가 마이그레이션되지 않습니다. Cisco 통합 서비스 가용성에서 SNMP 구성 절차를 다시 수행해야 합니다.

SNMP는 IPv4와 IPv6을 지원하며 CISCO-CCM-MIB에 IPv4와 IPv6 주소, 기본 설정 등에 대한 열과 저장소가 포함되어 있습니다.

SNMP 기본 사항

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

- 관리되는 장치 - SNMP 에이전트를 포함하고 관리되는 네트워크에 상주하는 네트워크 노드입니다. 관리되는 장치는 관리 정보를 수집 및 저장하고 SNMP를 사용하여 사용할 수 있게합니다.

  Unified Communications Manager 및 IM and Presence Service에만 해당: 클러스터를 지원하는 구성에서는 클러스터의 첫 번째 노드가 관리되는 장치의 역할을 합니다.

- 에이전트 - 관리되는 장치에 있는 네트워크 관리 소프트웨어 모듈입니다. 에이전트는 관리 정보에 대한 로컬 지식을 포함하고 이를 SNMP와 호환되는 형태로 변환합니다.

  마스터 에이전트 및 하위 에이전트 구성 요소는 SNMP를 지원하는 데 사용됩니다. 마스터 에이전트는 에이전트 프로토콜 엔진 역할을 하고 SNMP 요청과 관련된 인증, 권한 부여, 액세스 제어 및 프라이버시 기능을 수행합니다. 마찬가지로, 마스터 에이전트는 MIB-II와 관련된 MIB(Management Information Base) 변수를 일부 포함합니다. 마스터 에이전트는 하위 에이전트가 필요한 작업을 완료한 후에도 하위 에이전트를 연결 및 연결 해제합니다. SNMP 마스터 에이전트는 포트 161에서 수신하고, 벤더 MIB용 SNMP 패킷을 전달합니다.

  Unified Communications Manager 하위 에이전트는 로컬 Unified Communications Manager와 상호작용합니다. Unified Communications Manager 서브 에이전트는 SNMP 마스터 에이전트에 트랩 및 정보 메시지를 전송하고 SNMP 마스터 에이전트는 SNMP 트랩 수신기(알림 대상)와 통신합니다.

  IM and Presence Service 하위 에이전트는 로컬 IM and Presence Service와만 상호 작용합니다. IM and Presence Service 하위 에이전트는 SNMP 마스터 에이전트에 트랩 및 정보 메시지를 전송하고 SNMP 마스터 에이전트는 SNMP 트랩 수신기(알림 대상)와 통신합니다.

- NMS(네트워크 관리 시스템) - 네트워크 관리에 필요한 벌크 처리 및 메모리 리소스를 제공하는 SNMP 관리 애플리케이션(이 도구가 실행되는 PC와 함께)입니다. NMS는 관리되는 장치를 모니터링하고 제어하는 애플리케이션을 실행합니다. 다음과 같은 NMS가 지원됩니다.
  - CiscoWorks LAN Management Solution
  - HP OpenView
  - SNMP 및 Unified Communications Manager SNMP 인터페이스를 지원하는 타사 애플리케이션

SNMP Management Information Base

SNMP를 사용하면 계층 구조로 구성된 정보의 컬렉션인 MIB(Management Information Base)에 액세스할 수 있습니다. MIB는 개체 식별자로 식별되는 관리되는 개체를 구성합니다. 관리되는 장치의 특정 특성을 포함하는 MIB 개체는 하나 이상의 개체 인스턴스(변수)로 구성됩니다.

SNMP 인터페이스는 다음 Cisco 표준 MIB를 제공합니다.

- CISCO-CDP-MIB
- CISCO-CCM-MIB
- CISCO-SYSLOG-MIB
- CISCO-UNITY-MIB

다음 제한을 준수하십시오.

- Unified Communications Manager는 CISCO-UNITY-MIB를 지원하지 않습니다.
- Cisco Unity Connection은 CISCO-CCM-MIB를 지원하지 않습니다.
- IM and Presence Service는 CISCO-CCM-MIB 및 CISCO-UNITY-MIB를 지원하지 않습니다.

SNM) 확장 에이전트는 서버에 상주하며 서버에 알려진 장치에 대한 자세한 정보를 제공하는 CISCO-CCM-MIB를 노출합니다. 클러스터 구성의 경우 SNMP 확장 에이전트는 클러스터의 각 서버에 상주합니다. CISCO-CCM-MIB는 클러스터를 지원하는 구성에서 서버에 대한 장치 등록 상태, IP 주소, 설명 및 모델 유형과 같은 장치 정보를 제공합니다.

SNMP 인터페이스는 다음 산업 표준 MIB를 제공합니다.

- SYSAPPL-MIB
- MIB-II(RFC 1213)
- HOST-RESOURCES-MIB

CISCO-CDP-MIB

CDP 하위 에이전트를 사용하여 Cisco Discovery Protocol MIB, CISCO-CDP-MIB를 읽습니다. 이 MIB를 사용하면 SNMP 관리 장치에서 네트워크의 다른 Cisco 장치에 자신을 광고 하도록 할 수 있습니다.

CDP 하위 에이전트는 CDP-MIB를 구현합니다. CDP-MIB에는 다음과 같은 개체가 포함되어 있습니다.

- cdpInterfaceIfIndex
- cdpInterfaceMessageInterval
- cdpInterfaceEnable
- cdpInterfaceGroup
- cdpInterfacePort
- cdpGlobalRun
- cdpGlobalMessageInterval
- cdpGlobalHoldTime
- cdpGlobalLastChange
- Cdpgobdeviceid
- cdpGlobalDeviceIdFormat
- cdpGlobalDeviceIdFormatCpd

참고 CISCO-CDP-MIB는 CISCO-SMI, CISCO-TC, CISCO-VTP-MIB의 프레즌스에 의존합니다.

SYSAPPL-MIB

시스템 애플리케이션 에이전트를 사용하여 시스템에서 실행 중인 설치된 애플리케이션, 애플리케이션 구성 요소 및 프로세스와 같은 SYSAPPL-MIB로부터 정보를 가져올 수 있습니다.

시스템 애플리케이션 에이전트는 SYSAPPL-MIB의 다음 개체 그룹을 지원합니다.

- sysApplInstallPkg
- sysApplRun
- sysApplMap
- sysApplInstallElmt
- sysApplElmtRun

표 *1: SYSAPPL-MIB* 명령

명령	설명
장치 관련 쿼리	
sysApplInstallPkgVersion	소프트웨어 제조업체가 애플리케이션 패키지에 할당한 버전 번호를 제공합니다.
sysApplElmPastRunUser	프로세스 소유자의 로그인 이름(예: root)을 제공합니다.
메모리, 스토리지 및 CPU 관련 쿼리	
sysApplElmPastRunMemory	이 프로세스가 종료되기 전에 할당된 실제 시스템 메모리의 총 양을 kb 단위로 제공합니다.
sysApplElmtPastRunCPU	이 프로세스에 사용된 총 시스템 CPU 리소스의 마지막으로 알려진 100분의 1초 수를 제공합니다. 참고 다중 프로세서 시스템에서 이 값은 실제(벽면 시계) 시간의 100분의 1초에 100분의 1초 이상씩 증가할수 있습니다.

sysApplInstallElmtCurSizeLow	현재 파일 크기 모듈로(modulo) 2^32 바이트를 제공합니다. 예를 들어, 총 크기가 4,294,967,296 바이트인 파일의 경우 이 변수의 값은 0입니다. 총 크기가 4,294,967,295 바이트인 파일의 경우 이 변수는 4,294,967,295가 됩니다.
sysApplInstallElmtSizeLow	설치된 파일 크기 모듈로(modulo) 2^32 바이트를 제공합니다. 이것은 설치 직후 디스크에 있는 파일의 크기입니다. 예를 들어, 총 크기가 4,294,967,296 바이트인 파일의 경우 이 변수의 값은 0입니다. 총 크기가 4,294,967,295 바이트인 파일의 경우 이 변수는 4,294,967,295가 됩니다.
sysApplElmRunMemory	현재 이 프로세스에 할당된 실제 시스템 메모리의 총 양을 kb 단위로 제공합니다.
sysApplElmRunCPU	이 프로세스에 사용된 총 시스템 CPU 리소스의 100분의 1초 수를 제공합니다. 참고 다중 프로세서 시스템에서 이 값은 실제(벽면 시계) 시간의 100분의 1초에 100분의 1초 이상씩 증가했을 수 있습니다.
프로세스 관련 쿼리	
sysApplElmtRunState	실행 중인 프로세스의 현재 상태를 제공합니다. 가능한 값은 실행 중(1), 실행 가능(2) 상태이지만 CPU 같은 리소스 대기 중, 이벤트 대기 중(3), 종료 중(4) 또는 기타(5)입니다.
sysApplElmtRunNumFiles	프로세스에서 현재 연 일반 파일 수를 제공합니다. 전송 연결(소켓)은 이 값의 계산에 포함되어서는 안 되며 시스템 특정 특수 파일 유형이어서는 안 됩니다.
sysApplElmtRunTimeStarted	프로세스가 시작된 시간을 제공합니다.
sysApplElmtRunMemory	현재 이 프로세스에 할당된 실제 시스템 메모리의 총 양을 kb 단위로 제공합니다.
sysApplElmtPastRunInstallID	설치된 요소 테이블에 인덱스를 제공합니다. 이 개체의 값은 이 항목이 이전에 실행된 프로세스를 나타내는 애플리케이션 요소에 대한 sysApplInstallElmtIndex와 동일한 값입니다.

sysApplElmtPastRunUser	프로세스 소유자의 로그인 이름(예: root)을 제공합니다.
sysApplElmtPastRunTimeEnded	프로세스가 종료된 시간을 제공합니다.
sysApplElmtRunUser	프로세스 소유자의 로그인 이름(예: root)을 제공합니다.
sysApplRunStarted	애플리케이션이 시작된 날짜 및 시간을 제공합니다.
sysApplElmtRunCPU	이 프로세스에 사용된 총 시스템 CPU 리소스의 100분의 1초 수를 제공합니다. 참고 다중 프로세서 시스템에서 이 값은 실제(벽면 시계) 시간의 100분의 1초에 100분의 1초 이상씩 증가했을 수 있습니다.
소프트웨어 구성 요소 관련 쿼리	
sysApplInstallPkgProductName	제조업체가 소프트웨어 애플리케이션 패키지에 할당한 이름을 제공합니다.
sysApplElmtRunParameters	프로세스에 대한 시작 매개 변수를 제공합니다.
sysApplElmtRunName	프로세스의 전체 경로 및 파일 이름을 제공합니다. 예를 들어 '/opt/MYYpkg/bin/myyproc'은 실행 경로가 'opt/MYYpkg/bin/myyproc'인 프로세스 'myyproc'에 대해 반환됩니다.
sysApplInstallElmtName	애플리케이션에 포함되어 있는 이 요소의 이름을 제공합니다.
sysApplElmtRunUser	프로세스 소유자의 로그인 이름(예: root)을 제공합니다.

sysApplInstallElmtPath	이 요소가 설치된 디렉터리에 대한 전체 경로를 제공합니다. 예를 들어, '/opt/EMPuma/bin' 디렉터리에 설치된 요소에 대한 값은 '/opt/EMPuma/bin'입니다. 대부분의 애플리케이션 패키지에는 패키지에 포함된 요소에 대한 정보가 포함됩니다. 또한 일반적으로 요소는 패키지 설치 디렉터리 아래 하위 디렉터리에 설치됩니다. 요소 경로 이름이 패키지 정보 자체에 포함되지 않은 경우에는 일반적으로 하위 디렉터리를 검색하여 경로를 결정할 수 있습니다. 해당 위치에 요소가 설치되어 있지 않고 다른 정보를 에이전트 구현에 사용할 수 없는 경우 경로를 알 수 없으며 null이 반환됩니다.
sysApplMapInstallPkgIndex	이 개체의 값을 제공하고 이 프로세스가 속해 있는 애플리케이션에 대해 설치된 소프트웨어 패키지를 식별합니다. 프로세스의 상위 애플리케이션을 확인할 수 있는 경우 이 개체의 값은 이 프로세스를 포함하는 설치된 애플리케이션에 해당하는 sysApplInstallPkgTable의 항목에 대한 sysApplInstallPkgIndex 값과 동일합니다. 그러나 상위 애플리케이션을 확인할 수 없는 경우(예: 프로세스가 설치된 특정 애플리케이션에 속하지 않는 경우) 이 개체의 값은 '0'이고, 이 프로세스는 애플리케이션, 그런 다음 설치된 소프트웨어 패키지로 다시 연결될 수 없다는 것을 알 수 있습니다.
sysApplElmtRunInstallID	sysApplInstallElmtTable에 인덱스를 제공합니다. 이 개체의 값은 이 항목이 실행 중인 인스턴스를 나타내는 애플리케이션 요소에 대한 sysApplInstallElmtIndex와 동일한 값입니다. 이 프로세스를 설치된 실행 파일과 연결할 수 없는 경우 값은 '0'이어야 합니다.

sysApplRunCurrentState	실행 중인 애플리케이션 인스턴스의 현재 상태를 제공합니다. 가능한 값은 실행 중(1), 실행 가능(2) 상태이지만 CPU 같은 리소스 대기 중, 이벤트 대기 중(3), 종료 중(4) 또는 기타(5)입니다. 이 값은 이 애플리케이션 인스턴스의 실행 중인 요소에 대한 평가, (sysApplElmRunState 참조) 및 sysApplInstallElmtRole에 정의된 역할을 기반으로합니다. 하나 이상의 REQUIRED 요소가 더 이상 실행되고 있지 않은 경우에는 에이전트 구현에서 애플리케이션 인스턴스가 종료 중인 것으로 감지될 수 있습니다. 대부분의 에이전트 구현은 두 번째 내부 폴링이 완료될 때까지 기다린 후 애플리케이션 인스턴스를 종료 중으로 표시하기 전에 REQUIRED 요소를 시작할 시스템 시간을 제공합니다.
sysApplInstallPkgDate	이 소프트웨어 애플리케이션을 호스트에 설치한 날짜 및 시간을 제공합니다.
sysApplInstallPkgVersion	소프트웨어 제조업체가 애플리케이션 패키지에 할당한 버전 번호를 제공합니다.
sysApplInstallElmtType	설치된 애플리케이션에 속하는 요소의 유형을 제공합니다.
날짜/시간 관련 쿼리	
sysApplElmtRunCPU	이 프로세스에 사용된 총 시스템 CPU 리소스의 100분의 1초 수입니다. 참고 다중 프로세서 시스템에서 이 값은 실제(벽면 시계) 시간의 100분의 1초에 100분의 1초 이상씩 증가했을 수 있습니다.
sysApplInstallPkgDate	이 소프트웨어 애플리케이션을 호스트에 설치한 날짜 및 시간을 제공합니다.
sysApplElmtPastRunTimeEnded	프로세스가 종료된 시간을 제공합니다.
sysApplRunStarted	애플리케이션이 시작된 날짜 및 시간을 제공합니다.

MIB-II

MIB2 에이전트를 사용하여 MIB-II로부터 정보를 얻습니다. MIB2 에이전트는 RFC 1213에 정의된 변수(예: 인터페이스, IP 등)에 대한 액세스를 제공하고 다음 개체 그룹을 지원합니다.

- 시스템
- 인터페이스
- at
- ip
- icmp
- tcp
- udp
- SNMP

표 ***2: MIB-II*** 명령

명령	설명
장치 관련 쿼리	
sysName	이 관리되는 노드에 관리적으로 할당된 이름을 제공합니다. 규칙에 따라 이 이름은 노드의 FQDN(Fully Qualified Domain Name)입니다. 이름을 알 수 없는 경우 이 값은 길이가 0인 문자열입니다.
sysDescr	엔터티에 대한 텍스트 설명을 제공합니다. 이 값에는 시스템 하드웨어 유형, 소프트웨어 운영 체제 및 네트워킹 소프트웨어의 전체 이름 및 버전 ID가 포함되어야 합니다.
SNMP 진단 쿼리	
sysName	이 관리되는 노드에 관리적으로 할당된 이름을 제공합니다. 규칙에 따라 이 이름은 노드의 FQDN(Fully Qualified Domain Name)입니다. 이름을 알 수 없는 경우 이 값은 길이가 0인 문자열입니다.
sysUpTime	시스템의 네트워크 관리 부분이 마지막으로 다시 초기화된 이후 경과한 시간(1/100초)을 제공합니다.
SNMPInTotalReqVars	유효한 SNMP Get 요청 및 Get-Next PDU를 수신한 결과로 SNMP 프로토콜 엔터티에서 성공적으로 검색한 총 MIB 개체 수를 제공합니다.
SNMPOutPkts	SNMP 엔터티에서 전송 서비스로 전달된 총 SNMP 메시지 수를 제공합니다.

sysServices	이 엔터티가 제공할 수 있는 서비스 집합을 나타내는 값을 제공합니다. 값은 합계입니다. 이 합계는 처음에 0 값을 사용합니다. 그런 다음, 1에서 7 범위의 각 레이어 L에 대해 이 노드가 트랜잭션을 수행하고 (L - 1)로 상승한 2가 합계에 추가됩니다. 예를 들어, 애플리케이션 서비스를 제공하는 호스트인 노드 값은 4 (2^(3-1))입니다. 반면에, 애플리케이션 서비스를 제공하는 호스트인 노드 값은 72 (2^(4-1) + 2^(7-1))입니다. 참고 인터넷 프로토콜 제품군의 컨텍스트에서 레이어 1 물리적(예: 리피터), 레이어 2 데이터 링크/서브 네트워크(예: 브리지), 레이어 3 인터넷(IP 지원), 레이어 4 종단 간(TCP 지원), 레이어 7 애플리케이션(SMTP 지원)을 계산합니다. OSI 프로토콜을 포함하는 시스템의 경우 레이어 5 및 6을 계산할 수도 있습니다.
SNMPEnableAuthenTraps	SNMP 엔터티가 authenticationFailure 트랩을 생성할 수 있는지 여부를 나타냅니다. 이 개체의 값은 모든 구성 정보를 무시합니다. 따라서 이는 모든 authenticationFailure 트랩이 비활성화될 수 있는 수단을 제공합니다. 참고 Cisco에서는 이 개체가 네트워크 관리 시스템을 다시 초기화하는 동안 일정하게 유지되도록 비휘발성 메모리에 저장하는 것이 좋습니다.
Syslog 관련 쿼리	
SNMPEnabledAuthenTraps	SNMP 엔터티가 authenticationFailure 트랩을 생성할 수 있는지 여부를 나타냅니다. 이 개체의 값은 모든 구성 정보를 무시합니다. 따라서 이는 모든 authenticationFailure 트랩이 비활성화될 수 있는 수단을 제공합니다. 참고 Cisco에서는 이 개체가 네트워크 관리 시스템을 다시 초기화하는 동안 일정하게 유지되도록 비휘발성 메모리에 저장하는 것이 좋습니다.
날짜/시간 관련 쿼리	

sysUpTime	시스템의 네트워크 관리 부분이 마지막으로 다시 초기화된 이후 경과한 시간(1/100초)을 제공합니다.

HOST-RESOURCES MIB

호스트 리소스 에이전트를 사용하여 HOST-RESOURCES-MIB에서 값을 가져옵니다. 호스트 리소스 에이전트는 저장소 리소스, 프로세스 테이블, 장치 정보 및 설치된 소프트웨어 베이스와 같은 호스트 정보에 대한 SNMP 액세스를 제공합니다. 호스트 리소스 에이전트는 다음 개체 그룹을 지원합니다.

- hrSystem
- hrStorage
- hrDevice
- hrSWRun
- hrSWRunPerf
- hrSWInstalled

표 ***3: HOST-RESOURCES MIB*** 명령

명령	설명
장치 관련 쿼리	
hrFSMountPoint	이 파일 시스템 루트의 경로 이름을 제공합니다.
hrDeviceDescr	장치 제조업체 및 개정을 포함하여 이 장치에 대한 텍스트 설명을 제공하고, 선택적으로 일련 번호를 제공합니다.
hrStorageDescr	저장소의 유형 및 인스턴스에 대한 설명을 제공합니다.
메모리, 스토리지 및 CPU 관련 쿼리	
hrMemorySize	호스트에 포함된 물리적 읽기/쓰기 주 메모리(일반적으로 RAM)의 양을 제공합니다.
hrStorageSize	저장소의 크기를 hrStorageAllocationUnits 단위로 제공합니다. 이 개체는 해당 작업이 적절하고 기본 시스템에서 가능한 경우 저장 영역의 크기에 대한 원격 구성을 허용하도록 쓸 수 있습니다. 예를 들어, 버퍼 풀에 할당된 주 메모리의 양과 가상 메모리에 할당된 디스크 공간을 수정할 수 있습니다.
프로세스 관련 쿼리	

hrSWRunName	제조업체, 개정 및 일반적으로 알려진 이름을 포함하여 실행 중인 소프트웨어에 대한 텍스트 설명을 제공합니다. 이 소프트웨어가 로컬로 설치된 경우 해당 hrSWInstalledName에 사용된 것과 동일한 문자열이어야 합니다.
hrSystemProcesses	이 시스템에서 현재 로드되었거나 실행 중인 프로세스 컨텍스트 수를 제공합니다.
hrSWRunIndex	호스트에서 실행되는 각 소프트웨어 부분에 대한 고유한 값을 제공합니다. 가능하면 시스템의 고유한 고유 식별 번호를 사용합니다.
소프트웨어 구성 요소 관련 쿼리	
hrSWInstalledName	제조업체, 개정, 일반적으로 알려진 이름 및 선택적으로 일련 번호를 포함하여 설치된 이 소프트웨어 부분에 대한 텍스트 설명을 제공합니다.
hrSWRunPath	이 소프트웨어를 로드한 장기 저장소(예: 디스크 드라이브)의 위치에 대한 설명을 제공합니다.
날짜/시간 관련 쿼리	
hrSystemDate	호스트 로컬 날짜 및 시간을 제공합니다.
hrFSLastPartialBackupDate	이 파일 시스템의 일부가 백업용으로 다른 저장 장치에 복사된 마지막 날짜를 제공합니다. 이 정보는 백업이 정기적으로 수행되고 있는지 확인하는 데 유용합니다. 이 정보를 알 수 없는 경우 이 변수에는(16진수) '00 00 01 01 00 00 00 00'으로 인코딩되는 0000년 1월 1일 00:00:00.0에 해당하는 값이 있습니다.

CISCO-SYSLOG-MIB

Syslog는 모든 시스템 메시지를 추적하고 중요한 정보를 통해 기록합니다. 이 MIB를 사용하면 네트워크 관리 애플리케이션에서 syslog 메시지를 SNMP 트랩으로 수신할 수 있습니다.

Cisco Syslog 에이전트는 다음 MIB 개체와 함께 트랩 기능을 지원합니다.

- clogNotificationsSent
- clogNotificationsEnabled
- clogMaxSeverity
- clogMsgIgnores
- clogMsgDrops

참고 CISCO-SYSLOG-MIB는 CISCO-SMI MIB가 존재하는지 여부에 따라 달라집니다.

표 *4: CISCO-SYSLOG-MIB* 명령

명령	설명
Syslog 관련 쿼리	
clogNotificationEnabled	장치에서 syslog 메시지를 생성하는 경우 clogMessageGenerated 알림을 보낼지 여부를 나타냅니다. 알림을 비활성화해도 syslog 메시지가 clogHistoryTable에 추가되는 것은 방지되지 않습니다.
clogMaxSeverity	처리할 syslog 심각도 수준을 나타냅니다. 에이전트는 이 값보다 심각도 값이 큰 모든 syslog 메시지를 무시합니다. 참고 심각도 숫자 값은 심각도가 감소하면 증가합니다. 예를 들어 오류(4)는 디버그(8) 보다 심각합니다.

CISCO-CCM-MIB/CISCO-CCM-CAPABILITY MIB

CISCO-CCM-MIB는 Unified Communications Manager 및 이 Unified Communications Manager 노드에 표시되는 전화기, 게이트웨이 등과 같은 연결된 장치에 대한 동적(실시간) 및 구성된(정적) 정보를 모두 포함합니다. SNMP(Simple Network Management Protocol) 테이블에는 IP 주소, 등록 상태 및 모델 유형과 같은 정보가 포함되어 있습니다.

SNMP는 IPv4와 IPv6을 지원하며 CISCO-CCM-MIB에 IPv4와 IPv6 주소, 기본 설정 등에 대한 열과 저장소가 포함되어 있습니다.

참고 Unified Communications Manager는 Unified Communications Manager 시스템에서 이 MIB를 지원합니다. IM and Presence Service 및 Cisco Unity Connection은 이 MIB를 지원하지 않습니다.

CISCO-CCM-MIB 및 MIB 정의에 대한 지원 목록을 보려면 다음 링크로 이동하십시오.

ftp://ftp.cisco.com/pub/MIBs/supportlists/callmanager/callmanager-supportlist.html

Unified Communications Manager 릴리스 전반에 걸쳐 사용되지 않는 개체를 포함하여 MIB 종속성 및 MIB 내용을 보려면 다음 링크로 이동하십시오. http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&mibName=CISCO-CCM-CAPABILITY

동적 테이블은 Cisco CallManager 서비스가 실행 중인 경우(또는 Unified Communications Manager 클러스터 구성의 경우에는 로컬 Cisco CallManager 서비스)에만 채워집니다. Cisco CallManager SNMP Service가 실행 중일 때는 정적 테이블이 채워집니다.

표 *5: Cisco-CCM-MIB* 동적 테이블

테이블	목차
ccmTable	이 테이블은 로컬 Unified Communications Manager의 버전 및 설치 ID를 저장합니다. 이 테이블에는 로컬 Unified Communications Manager가 알고 있지만 버전 세부 정보에 대해 "알 수 없는" 것으로 표시되는 클러스터의 모든 Unified Communications Manager에 대한 정보도 저장됩니다. 로컬 Unified Communications Manager가 다운된 경우 버전 및 설치 ID 값을 제외하고 테이블은 빈 상태로 유지됩니다.
ccmPhoneFailed, ccmPhoneStatusUpdate, ccmPhoneExtn, ccmPhone, ccmPhoneExtension	Cisco Unified IP 전화기의 경우 ccmPhoneTable의 등록된 전화기 수는 Unified Communications Manager/RegisteredHardware 전화기 perfmon 카운터와 일치해야 합니다. ccmPhoneTable에는 등록되었거나, 등록되지 않았거나, 거부된 Cisco Unified IP 전화기에 대한 항목이 하나씩 포함됩니다. CcmPhoneExtnTable은 ccmPhoneTable 및 ccmPhoneExtnTable의 항목을 관련하여 결합된 인덱스 ccmPhoneIndex 및 ccmPhoneExtnIndex를 사용합니다.
ccmCTIDevice, ccmCTIDeviceDirNum	CcmCTIDeviceTable은 각 CTI 장치를 하나의 장치로 저장합니다. CTI 경로 포인트 또는 CTI 포트의 등록 상태에 따라, Unified Communications Manager MIB의 ccmRegisteredCTIDevices, ccmUnregisteredCTIDevices 및 ccmRejectedCTIDevices 카운터가 업데이트됩니다.
ccmSIPDevice	CCMSIPDeviceTable은 각 SIP 트렁크를 하나의 장치로 저장합니다.

테이블	목차
ccmH323Device	CcmH323DeviceTable에는 Unified Communications Manager가 정보(클러스터 구성의 경우에는 로컬 Unified Communications Manager)를 포함하는 H.323 장치의 목록이 포함되어 있습니다. H.323 전화기 또는 H.323 게이트웨이의 경우 ccmH.323DeviceTable은 각 H.323 장치에 대해 하나의 항목을 포함합니다. (H.323 전화기 및 게이트웨이는 Unified Communications Manager에 등록되지 않습니다. Unified Communications Manager는 표시된 H.323 전화기 및 게이트웨이의 통화를 처리할 준비가 되면 H.323Started 알람을 생성합니다. 시스템은 H.323 트렁크 정보의 일부로 게이트키퍼 정보를 제공합니다.
ccmVoiceMailDevice, ccmVoiceMailDirNum	Cisco uOne, ActiveVoice의 경우 ccmVoiceMailDeviceTable에는 각 음성 메시징 장치에 대한 항목이 하나씩 포함됩니다. 등록 상태를 기준으로 Cisc MIB의 ccmRegisteredVoiceMailDevices, ccmUnregisteredVoiceMailDevices 및 ccmRejectedVoiceMailDevices 카운터가 업데이트됩니다.
ccmGateway	CcmRegisteredGateways, ccmUnregistered 게이트웨이 및 ccmRejectedGateways는 등록된 게이트웨이 장치 또는 포트의 수, 등록되지 않은 게이트웨이 장치 또는 포트의 수 및 거부된 게이트웨이 장치 또는 포트의 수를 각각 추적합니다. Unified Communications Manager는 장치 또는 포트 수준에서 알람을 생성합니다. CallManager 알람을 기반으로 하는 ccmGatewayTable은 장치 또는 포트 수준 정보를 포함합니다. 등록되거나 등록되지 않았거나 거부된 장치 또는 포트에는 ccmGatewayTable에 하나의 항목이 있습니다. FXS 포트 2개와 T1 포트 1개를 사용하는 VG200에는 ccmGatewayTable에 세 개의 항목이 있습니다. CcmActiveGateway 및 ccmInActiveGateway 카운터는(등록되지 않거나 거부된) 게이트웨이 장치 또는 포트를 사용하여 활성(등록됨) 및 분실된 연락처의 수를 추적합니다. 등록 상태를 기준으로 ccmRegisteredGateways, ccmUnregisteredGateways 및 ccmRejectedGateways 카운터가 업데이트됩니다.

테이블	목차
ccmMediaDeviceInfo	이 테이블에는 한 번 이상 로컬 Unified Communications Manager에 등록을 시도한 모든 미디어 장치의 목록이 포함되어 있습니다.
ccmGroup	이 테이블에는 Unified Communications Manager 클러스터의 Unified Communications Manager 그룹이 포함되어 있습니다.
ccmGroupMapping	이 테이블은 클러스터의 모든 Unified Communications Manager를 Unified Communications Manager 그룹에 매핑합니다. 로컬 Unified Communications Manager 노드가 다운되면 테이블은 비어 있는 상태로 유지됩니다.

표 ***6: CISCO-CCM-MIB*** 정적 테이블

테이블	콘텐츠
ccmProductType	이 테이블에는 전화기 유형, 게이트웨이 유형, 미디어 장치 유형, H.323 장치 유형, CTI 장치 유형, 음성 메시징 장치 유형 및 SIP 장치 유형을 포함하여 Unified Communications Manager(또는 Unified Communications Manager 클러스터 구성의 경우)에서 지원되는 제품 유형 목록이 포함되어 있습니다.
ccmRegion, ccmRegionPair	ccmRegionTable에는 CCN(Cisco Communications Network) 시스템에서 지리적으로 구분된 모든 지역의 목록이 포함되어 있습니다. ccmRegionPairTable에는 Unified Communications Manager 클러스터에 대한 지리적 지역 쌍 목록이 포함되어 있습니다. 지리적 지역 쌍은 소스 지역과 대상 지역에 의해 정의됩니다.
ccmTimeZone	테이블에는 Unified Communications Manager 클러스터에 있는 모든 표준 시간대 그룹의 목록이 포함되어 있습니다.
ccmDevicePool	테이블에는 Unified Communications Manager 클러스터의 모든 장치 풀 목록이 포함되어 있습니다. 장치 풀은 지역, 날짜/시간 그룹 및 Unified Communications Manager 그룹에 의해 정의됩니다.

참고 CISCO-CCM-MIB의 '"ccmAlarmConfigInfo" 및 "ccmQualityReportAlarmConfigInfo" 그룹은 설명된 알림과 관련된 구성 매개 변수를 정의합니다.

CISCO-UNITY-MIB

CISCO-UNITY-MIB는 연결 SNMP 에이전트를 사용하여 Cisco Unity Connection에 대한 정보를 가져옵니다.

CISCO-UNITY-MIB 정의를 보려면 다음 링크로 이동하고 **SNMP V2 MIB**를 클릭합니다.

http://www.cisco.com/public/sw-center/netmgmt/cmtk/MIBs.shtml

참고 Cisco Unity Connection은 이 MIB를 지원합니다. Unified Communications Manager 및 IM and Presence Service는 이 MIB를 지원하지 않습니다.

Connection SNMP 에이전트는 다음 개체를 지원합니다.

표 ***7: CISCO-UNITY-MIB*** 개체

개체	설명
ciscoUnityTable	이 테이블은 호스트 이름 및 버전 번호와 같은 Cisco Unity Connection 서버에 대한 일반 정보를 포함합니다.
ciscoUnityPortTable	이 테이블은 Cisco Unity Connection 음성 메시징 포트에 대한 일반 정보를 포함합니다.
일반 Unity 사용 정보 개체	이 그룹에는 Cisco Unity Connection 음성 메시징 포트의 용량과 사용률에 대한 정보가 포함되어 있습니다.

SNMP 구성 요구 사항

시스템에서 기본 SNMP 구성은 제공하지 않습니다. MIB 정보에 액세스하려면 설치 후 SNMP 설정을 구성해야 합니다. Cisco는 SNMP V1, V2c 및 V3 버전을 지원합니다.

SNMP 에이전트는 커뮤니티 이름 및 인증 트랩에 보안을 제공합니다. MIB 정보에 액세스하려면 커뮤니티 이름을 구성해야 합니다. 다음 표에서는 필수 SNMP 구성 설정을 제공합니다.

표 ***8: SNMP*** 구성 요구 사항

구성	**Cisco** 통합 서비스 가용성 페이지
V1/V2c 커뮤니티 문자열	**SNMP** > **V1/V2c** > 커뮤니티 문자열

구성	**Cisco** 통합 서비스 가용성 페이지
V3 커뮤니티 문자열	**SNMP** > **V3** > 사용자
시스템 연락처 및 MIB2에 대한 위치	**SNMP** > **SystemGroup** > **MIB2** 시스템 그룹
트랩 대상(V1/V2c)	**SNMP** > **V1/V2c** > 알림 대상
트랩 대상(V3)	**SNMP** > **V3** > 알림 대상

SNMP 버전 1 지원

SMI(관리 정보) 구조의 사양 내에서 작동하는 SNMP의 초기 구현 SNMPv1(SNMP 버전 1)은 UDP(사용자 데이터그램 프로토콜) 및 IP(인터넷 프로토콜)와 같은 프로토콜을 통해 작동합니다.

SNMPv1 SMI는 테이블 형식 개체(즉, 여러 변수가 포함된 개체)의 인스턴스를 그룹화하는 데 사용되는 고도로 구조화된 테이블(MIB)을 정의합니다. 테이블에는 인덱스되는 0개 이상의 행이 포함되어 있으므로 SNMP에서 지원되는 명령을 사용하여 전체 행을 검색하거나 변경할 수 있습니다.

SNMPv1을 사용하는 경우에는 NMS가 요청을 발행하고 관리되는 장치가 응답을 반환합니다. 에이전트는 트랩 작업을 사용하여 NMS에게 중요한 이벤트를 비동기적으로 알립니다.

서비스 가용성 GUI에서는 **V1/V2c** 구성 창에서 SNMPv1 지원을 구성합니다.

SNMP 버전 2c 지원

SNMPv1과 마찬가지로, SNMPv2c는 관리 정보(SMI) 구조의 사양 내에서 작동합니다. MIB 모듈에는 상호 관련된 관리 개체에 대한 정의가 포함되어 있습니다. SNMPv1에서 사용되는 작업은 SNMPv2에 사용되는 것과 유사합니다. 예를 들어, SNMPv2 트랩 작업은 SNMPv1에 사용된 것과 동일한 기능을 제공하지만 다른 메시지 형식을 사용하고 SNMPv1 트랩을 대체합니다.

SNMPv2c의 알림 작업을 사용하면 하나의 NMS가 다른 NMS로 트랩 정보를 전송하고 NMS로부터 응답을 받을 수 있습니다.

서비스 가용성 GUI에서는 **V1/V2c** 구성 창에서 SNMPv2c 지원을 구성합니다.

SNMP 버전 3 지원

SNMP 버전 3은 인증(요청을 진짜 소스에서 수신하는지 확인), 프라이버시(데이터 암호화), 인증(사용자가 요청된 작업을 허용하는지 확인) 및 액세스 제어(사용자에게 요청된 개체에 대한 액세스 권한이 있음)와 같은 보안 기능을 제공합니다. SNMP 패킷이 네트워크에 노출되지 않도록 하려면 SNMPv3을 사용하여 암호화를 구성할 수 있습니다.

참고 릴리스 12.5(1)SU1부터는 Unified Communications Manager에서 MD5 또는 DES 암호화 방법이 지원되지 않습니다. 인증 프로토콜로 SHA 또는 AES 중 하나를 선택하면서 SNMPv3 사용자를 추가할 수 있습니다.

SNMPv1 및 v2와 같은 커뮤니티 문자열을 사용하는 대신에 SNMPv3이 SNMP 사용자를 사용합니다.

서비스 가용성 GUI에서는 **V3** 구성 창에서 SNMPv3 지원을 구성합니다.

SNMP 서비스

다음 테이블에 있는 서비스는 SNMP 작업을 지원합니다.

참고 SNMP 마스터 에이전트는 MIB 인터페이스에 대한 기본 서비스 역할을 합니다. Cisco CallManager SNMP 서비스를 수동으로 활성화해야 합니다. 설치 후에 다른 모든 SNMP 서비스를 실행해야 합니다.

표 *9: SNMP* 서비스

MIB	서비스	창
CISCO-CCM-MIB	Cisco CallManager SNMP 서비스	**Cisco** 통합 서비스 가용성 > 도구 > 제어 센터 - 기능 서비스. 서버를 선택한 다음 성능 및 모니터링 범주를 선택합니다.
SNMP 에이전트	SNMP 마스터 에이전트	**Cisco** 통합 서비스 가용성 > 도구 > 제어 센터 - 네트워크 서비스. 서버를 선택한 다음 플랫폼 서비스 범주를 선택합니다. **Cisco Unified IM and Presence** 서비스 가능성도구 > 제어 센터 - 네트워크 서비스 서버를 선택한 다음 플랫폼 서비스 범주를 선택합니다.
CISCO-CDP-MIB	Cisco CDP 에이전트	
SYSAPPL-MIB	시스템 애플리케이션 에이전트	
MIB-II	MIB2 에이전트	
HOST-RESOURCES-MIB	호스트 리소스 에이전트	
CISCO-SYSLOG-MIB	Cisco Syslog Agent	
하드웨어 MIB	기본 에이전트 어댑터	
CISCO-UNITY-MIB	연결 SNMP 에이전트	**Cisco Unity Connection Serviceability** > 도구 > 서비스 관리**.** 서버를 선택한 다음 기본 서비스 범주를 선택합니다.

⚠

주의 네트워크 관리 시스템이 더 이상 Unified Communications Manager 또는 Cisco Unity Connection 네트워크를 모니터링하지 않으므로 SNMP 서비스를 중지하면 데이터가 손실될 수 있습니다. 기술 지원팀이 사용자에게 지시하지 않는 한 서비스를 중지하지 마십시오.

SNMP 커뮤니티 문자열 및 사용자

SNMP 커뮤니티 문자열은 보안을 제공하지 않지만, MIB 개체에 대한 액세스를 인증하고 포함된 암호로 작동합니다. SNMPv1 및 v2c에 대해서만 SNMP 커뮤니티 문자열을 구성합니다.

SNMPv3은 커뮤니티 문자열을 사용하지 않습니다. 대신, 버전 3은 SNMP 사용자를 사용합니다. 이러한 사용자는 커뮤니티 문자열과 동일한 용도로 사용되지만, 사용자는 암호화 또는 인증을 구성할 수 있으므로 보안을 제공합니다.

서비스 가용성 GUI에서 기본 커뮤니티 문자열 또는 사용자가 존재하지 않습니다.

SNMP 트랩 및 알림

SNMP 에이전트는 중요한 시스템 이벤트를 식별하기 위해 트랩 또는 알림 형태로 NMS에게 알림을 전송합니다. 트랩은 대상에서 확인을 수신하지 않지만, 알림은 확인을 수신합니다. 서비스 가용성 GUI의 SNMP 알림 대상 구성 창을 사용하여 알림 대상을 구성합니다.

참고 Unified Communications Manager는 Unified Communications Manager 및 IM and Presence Service 시스템에서 SNMP 트랩을 지원합니다.

SNMP 알림의 경우, 해당 트랩 플래그가 활성화되면 시스템에서 트랩을 즉시 전송합니다. syslog 에이전트의 경우 알람 및 시스템 수준 로그 메시지가 로그를 위해 syslog 데몬에 전송됩니다. 그리고 일부 표준 타사 애플리케이션에서는 로그 메시지를 syslog 데몬에 전송하여 로깅할 수 있습니다. 이러한 로그 메시지는 syslog 파일에 로컬로 기록되고 SNMP 트랩/알림으로 변환 됩니다.

다음 목록은 구성된 트랩 대상으로 전송되는 Unified Communications Manager SNMP 트랩/통지 메시지를 포함합니다.

- Unified Communications Manager 실패
- 전화기 실패
- 전화기 상태 업데이트
- 게이트웨이 실패
- 미디어 리소스 목록이 모두 사용됨
- 경로 목록이 모두 사용됨
- 게이트웨이 레이어 2 변경
- 품질 보고서
- 장난 전화
- Syslog 메시지 생성됨

팁 알림 대상을 구성하기 전에 필요한 SNMP 서비스가 활성화되어 실행 중인지 확인합니다. 커뮤니티 문자열/사용자에 대한 권한을 올바르게 구성했는지 확인합니다.

서비스 가용성 GUI에서 **SNMP** > **V1/V2** > 알림 대상 또는 **SNMP** > **V3** > 알림 대상을 선택하여 SNMP 트랩 대상을 구성합니다.

다음 표에서는 NMS(네트워크 관리 시스템)에서 구성하는 트랩/알림 매개 변수에 대한 정보를 제공합니다. NMS를 지원하는 SNMP 제품 설명서에 설명된 대로, NMS에 적절한 명령을 실행하여 테이블의 값을 구성할 수 있습니다.

참고 테이블에 나열된 모든 매개 변수는 마지막 두 매개 변수를 제외하고 CISCO-CCM-MIB의 일부입니다. 마지막 2 개, clogNotificationsEnabled 및 clogMaxSeverity는 ISCO-SYSLOG-MIB의 일부를 구성합니다.

IM and Presence Service의 경우, NMS에 clogNotificationsEnabled 및 clogMaxSeverity 트랩/알림 매개 변수만 구성합니다.

표 ***10: Cisco Unified Communications Manager*** 트랩/알림 구성 매개 변수

매개 변수명	기본값	생성된 트랩	구성 권장 사항
ccmCallManagerAlarmEnable	True	ccmCallManagerFailed ccmMediaResourceListExhausted ccmRouteListExhausted ccmTLSConnectionFailure	기본 사양을 유지합니다.
ccmGatewayAlarmEnable	True	ccmGatewayFailed ccmGatewayLayer2Change Cisco Unified Communications Manager 관리에서 Cisco ATA 186 장치를 전화기로 구성할 수 있지만, Unified Communications Manager가 Cisco ATA 장치에 대한 SNMP 트랩을 전송하면 게이트웨이 유형 트랩(예: ccmGatewayFailed)이 전송됩니다.	없음 기본값은 이 트랩을 활성화로 지정합니다.
ccmPhoneStatusUpdateStorePeriod ccmPhoneStatusUpdateAlarmInterval	1800 0	ccmPhoneStatusUpdate	ccmPhoneStatusUpdateAlarmInterval을 30과 3600 사이의 값으로 설정합니다.
ccmPhoneFailedStorePeriod ccmPhoneFailedAlarmInterval	1800 0	ccmPhoneFailed	ccmPhoneFailedAlarmInterval을 30과 3600 사이의 값으로 설정합니다.
ccmMaliciousCallAlarmEnable	True	ccmMaliciousCall	없음 기본값은 이 트랩을 활성화로 지정합니다.

매개 변수명	기본값	생성된 트랩	구성 권장 사항
ccmQualityReportAlarmEnable	True	이 트랩은 Cisco Extended Functions 서비스가 활성화되어 서버에서 실행 중인 경우 또는 로컬 Unified Communications Manager 서버에서 클러스터 구성(Unified Communications Manager에만 해당)의 경우에만 생성됩니다. ccmQualityReport	없음 기본값은 이 트랩을 활성화로 지정합니다.
clogNotificationsEnabled	False	clogMessageGenerated	트랩 생성을 활성화하려면 clogNotificationsEnable를 True로 설정합니다.
clogMaxSeverity	경고	clogMessageGenerated	ClogMaxSeverity를 경고로 설정하면 애플리케이션에서 최소 알림 심각도 수준이 있는 syslog 메시지를 생성할 때 SNMP 트랩이 생성됩니다.

SFTP 서버 지원

내부 테스트의 경우 Cisco에서 제공하고 Cisco TAC에서 지원하는 Cisco Prime Collaboration Deployment(PCD)의 SFTP 서버를 사용합니다. SFTP 서버 옵션에 대한 요약은 다음 표를 참조하십시오.

표 ***11: SFTP*** 서버 지원

SFTP 서버	지원 설명
Cisco Prime Collaboration Deployment의 SFTP 서버	이 서버는 Cisco에서 제공 및 테스트하고 Cisco TAC에서 완벽하게 지원하는 유일한 SFTP 서버입니다. 버전 호환성은 Emergency Responder 및 Cisco Prime Collaboration Deployment 버전에 따라 달라집니다. 버전(SFTP) 또는 Emergency Responder를 업그레이드하기 전에 버전이 호환되는지 확인하기 위해 Cisco Prime Collaboration Deployment 관리 설명서를 참조하십시오.

SFTP 서버	지원 설명
기술 파트너의 SFTP 서버	이러한 서버는 타사에서 제공하고 타사에서 테스트했습니다. 버전 호환성은 타사 테스트에 따라 다릅니다. SFTP 제품을 업그레이드하거나 Unified Communications Manager를 업그레이드할 경우 기술 파트너가 페이지에서 버전 호환성 여부를 참조하십시오. https://marketplace.cisco.com
다른 타사의 SFTP 서버	이러한 서버는 타사에서 제공하고 Cisco TAC에서 공식 지원하지 않습니다. 버전 호환성은 SFTP 버전 및 Emergency Responder 버전의 호환성을 위해 최대한 노력합니다. 참고 이러한 제품은 Cisco에서 테스트하지 않았으므로 기능을 보증할 수 없습니다. Cisco TAC는 이러한 제품을 지원하지 않습니다. SFTP 솔루션을 완벽하게 테스트하고 지원하기 위해 Cisco Prime Collaboration Deployment 또는 기술 파트너를 이용합니다.

SNMP 구성 작업 흐름

이러한 작업을 완료하여 단순한 네트워크 관리 프로토콜을 구성합니다. 작업으로 구성할 SNMP 버전은 다양할 수 있다는 것을 알아야 합니다. SNMP V1, V2c 또는 V3 중에서 선택할 수 있습니다.

시작하기 전에

SNMP 네트워크 관리 시스템을 설치하고 구성합니다.

프로시저

	명령 또는 동작	목적
단계 1	SNMP 서비스 활성화, 24 페이지	필수 SNMP 서비스가 실행 중인지 확인합니다.
단계 2	SNMP 버전에 따라 다음 작업 중 하나를 완료합니다. • SNMP 커뮤니티 문자열 구성, 25 페이지 • SNMP 사용자 구성, 27 페이지	SNMP V1 또는 V2의 경우 커뮤니티 문자열을 구성합니다. SNMP V3의 경우 SNMP 사용자를 구성합니다.
단계 3	원격 SNMP 엔진 ID 가져오기, 31 페이지	SNMP V3의 경우 알림 대상 구성에 필요한 원격 SNMP 엔진의 주소를 가져옵니다.

	명령 또는 동작	목적
		참고 이 절차는 SNMP V3에 반드시 필요하지만, SNMP V1 또는 V2c에는 선택 사항입니다.
단계 4	SNMP 알림 대상 구성, 31 페이지	모든 SNMP 버전의 경우 SNMP 트랩 및 알림에 대한 알림 대상을 구성합니다.
단계 5	MIB2 시스템 그룹 구성, 36 페이지	MIB-II 시스템 그룹에 대한 시스템 연결 및 시스템 위치를 구성합니다.
단계 6	CISCO-SYSLOG-MIB 트랩 매개 변수, 37 페이지	CISCO-SYSLOG-MIB에 대한 트랩 설정을 구성합니다.
단계 7	CISCO-CCM-MIB 트랩 매개 변수, 38 페이지	Unified Communications Manager만 해당: CISCO-CCM-MIB에 대한 트랩 설정을 구성합니다.
단계 8	SNMP 마스터 에이전트 다시 시작, 38 페이지	SNMP 구성을 완료한 후에는 SNMP 마스터 에이전트를 다시 시작합니다.
단계 9	SNMP 네트워크 관리 시스템에서 Unified Communications Manager 트랩 매개 변수를 구성합니다.	

SNMP 서비스 활성화

이 절차를 사용하여 SNMP 서비스가 작동 중인지 확인합니다.

프로시저

단계 1 Cisco 통합 서비스 가용성에 로그인합니다.

단계 2 **Cisco SNMP Master Agent** 네트워크 서비스가 실행 중인지 확인합니다. 서비스는 기본적으로 켜져 있습니다.

a) 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.
b) 게시자 노드를 선택하고 이동을 클릭합니다.
c) **Cisco SNMP Master Agent** 서비스가 실행되고 있는지 확인합니다.

단계 3 **Cisco Call Manager SNMP** 서비스를 시작합니다.

a) 제어 센터 > 서비스 활성화를 선택합니다.
b) 서버 드롭다운에서 게시자 노드를 선택하고 이동을 클릭합니다.
c) **Cisco CALL Manager SNMP** 서비스가 실행 중인지 확인합니다. 실행 중이 아니면 해당 확인란을 선택하고 저장을 클릭합니다.

다음에 수행할 작업

SNMP V1 또는 V2c를 구성하는 경우 SNMP 커뮤니티 문자열 구성, 25 페이지.

SNMP V3을 구성하는 경우 SNMP 사용자 구성, 27 페이지.

SNMP 커뮤니티 문자열 구성

SNMP V1 또는 V2c를 배포하는 경우 이 절차를 사용하여 SNMP 커뮤니티 문자열을 설정합니다.

참고 이 절차는 SNMP V1 또는 V2c에 필요합니다. SNMP V3의 경우 커뮤니티 문자열 대신 SNMP 사용자를 구성합니다.

프로시저

단계 **1** Cisco 통합 서비스 가용성에서 **SNMP** > **V1/V2c** > 커뮤니티 문자열을 선택합니다.

단계 **2** 서버를 선택하고 찾기 를 클릭하여 기존 커뮤니티 문자열을 검색합니다. 선택적으로 검색 매개 변수를 입력하여 특정 커뮤니티 문자열을 찾을 수 있습니다.

단계 **3** 다음 중 하나를 수행합니다.

- 기존 SNMP 커뮤니티 문자열을 편집하려면 문자열을 선택합니다.
- 새 커뮤니티 문자열을 추가하려면 새로 추가를 클릭합니다.

참고 기존 커뮤니티 문자열을 삭제하려면 문자열을 선택하고 선택한 항목 삭제를 클릭합니다. 사용자를 삭제한 후에는 Cisco SNMP Master Agent를 다시 시작합니다.

단계 **4** 커뮤니티 문자열 이름을 입력합니다.

단계 **5** **SNMP** 커뮤니티 문자열 구성 창에서 필드를 완성합니다. 필드 및 해당 설정에 대한 도움말은 커뮤니티 문자열 구성 설정, 26 페이지의 내용을 참조하십시오.

단계 **6** 액세스 권한 드롭다운에서 이 커뮤니티 문자열에 대한 권한을 구성합니다.

단계 **7** 이러한 설정이 모든 클러스터 노드에 적용되도록 하려면 모든 노드에 적용 확인란을 선택합니다.

단계 **8** 저장을 클릭합니다.

단계 **9** 확인을 클릭하여 SNMP 마스터 에이전트 서비스를 다시 시작하고 변경 사항을 적용합니다.

다음에 수행할 작업

SNMP 알림 대상 구성, 31 페이지

커뮤니티 문자열 구성 설정

다음 표에서는 커뮤니티 문자열 구성 설정을 설명합니다.

표 ***12:*** 커뮤니티 문자열 구성 설정

필드	설명
서버	커뮤니티 문자열 찾기의 절차를 수행할 때 서버 선택을 지정했기 때문에 커뮤니티 문자열 구성 창에서 이 설정이 읽기 전용으로 표시됩니다. 커뮤니티 문자열에 대한 서버를 변경하려면 커뮤니티 문자열 찾기 절차를 수행합니다.
커뮤니티 문자열	커뮤니티 문자열 이름을 입력합니다. 이 이름은 최대 32자로 구성되고 영문자, 하이픈(-) 및 밑줄(_) 조합이 포함될 수 있습니다. 팁 외부인이 파악하기 어려운 커뮤니티 문자열 이름을 선택합니다. 커뮤니티 문자열을 편집할 때 커뮤니티 문자열의 이름을 변경할 수 없습니다.
모든 호스트에서 SNMP 패킷 수락	모든 호스트에서 SNMP 패킷을 수락하려면 이 버튼을 클릭합니다.
다음 호스트의 SNMP 패킷만 수락	특정 호스트에서 SNMP 패킷을 수락하려면 라디오 버튼을 클릭합니다. 호스트 이름//IPv4/IPv6 주소 필드에 SNMP 패킷을 수락할 IPv4 또는 IPv6 주소를 입력하고 삽입을 클릭합니다. IPv4 주소는 점으로 구분된 십진수 형식입니다. 예를 들어 10.66.34.23. IPv6 주소는 콜론으로 구분된 16진수 형식입니다. 예를 들어 2001:0db8:85a3:0000:0000:8a2e:0370:7334 또는 2001:0db8:85a3::8a2e:0370:7334. SNMP 패킷을 수락할 각 주소에 대해 이 과정을 반복합니다. 주소를 삭제하려면 호스트 IPv4/IPv6 주소 목록 상자에서 해당 주소를 선택하고제거를 클릭합니다.

필드	설명
액세스 권한	드롭다운 목록 상자의 다음 목록에서 적절한 액세스 수준을 선택합니다. 읽기 전용 커뮤니티 문자열은 MIB 개체의 값만 읽을 수 있습니다. **ReadWrite** 커뮤니티 문자열은 MIB 개체의 값을 읽고 쓸 수 있습니다. **ReadWriteNotify** 커뮤니티 문자열은 MIB 개체의 값을 읽고 쓰고, 트랩에 대한 MIB 개체 값을 전송하고 메시지를 알릴 수 있습니다. **NotifyOnly** 커뮤니티 문자열은 트랩에 대한 MIB 개체 값만 전송하고 메시지를 알릴 수 있습니다. **ReadNotifyOnly** 커뮤니티 문자열은 MIB 개체의 값을 읽을 수 있고 트랩 및 알림 메시지에 대한 값을 전송할 수도 있습니다. 없음 커뮤니티 문자열은 트랩 정보를 읽거나 쓰거나 전송할 수 없습니다. 팁 트랩 구성 매개 변수를 변경하려면 NotifyOnly, ReadNotifyOnly 또는 ReadWriteNotify 권한을 사용하여 커뮤니티 문자열을 구성합니다. IM and Presence Service는 ReadNoticyOnly를 지원하지 않습니다.
모든 노드에 적용	커뮤니티 문자열을 클러스터의 모든 노드에 적용하려면이 확인란을 선택합니다. 이 필드는 Unified Communications Manager 및 IM and Presence Service 클러스터에만 적용됩니다.

SNMP 사용자 구성

SNMP V3을 배포하는 경우 이 절차를 사용하여 SNMP 사용자를 설정합니다.

참고 이 절차는 SNMP V3에만 필요합니다. SNMP V1 또는 V2c의 경우 대신 커뮤니티 문자열을 구성합니다.

프로시저

단계 **1** Cisco 통합 서비스 가용성에서 **SNMP** > **V3** > 사용자를 선택합니다.

단계 **2** 서버를 선택하고 찾기 를 클릭하여 기존 SNMP 사용자를 검색합니다. 선택적으로 검색 매개 변수를 입력하여 특정 사용자를 찾을 수 있습니다.

단계 **3** 다음 중 하나를 수행합니다.

- 기존 SNMP 사용자를 편집하려면 사용자를 선택합니다.
- 새 SNMP 사용자를 추가하려면 새로 추가를 클릭합니다.

참고 기존 사용자를 삭제하려면 사용자를 선택하고 선택한 항목 삭제를 클릭합니다. 사용자를 삭제한 후에는 Cisco SNMP Master Agent를 다시 시작합니다.

단계 **4** **SNMP** 사용자 이름을 입력합니다.

단계 **5** SNMP 사용자 구성 설정을 입력합니다. 필드 및 해당 설정에 대한 도움말은 SNMP V3 사용자 구성 설정, 29 페이지의 내용을 참조하십시오.

팁 구성을 저장하기 전에 언제든지 모두 지우기 버튼을 클릭하여 창에 있는 모든 설정에 입력한 정보를 모두 삭제할 수 있습니다.

단계 **6** 액세스 권한 드롭다운에서 이 사용자에게 할당할 액세스 권한을 구성합니다.

단계 **7** 이 구성이 모든 클러스터 노드에 적용되도록 하려면 모든 노드에 적용 확인란을 선택합니다.

단계 **8** 저장을 클릭합니다.

단계 **9** 확인을 클릭하여 SNMP 마스터 에이전트를 다시 시작합니다.

참고 구성한 사용자를 사용하여 서버에 액세스하려면 해당 인증 및 프라이버시 설정을 사용하여 NMS에서이 사용자를 구성해야 합니다.

다음에 수행할 작업

원격 SNMP 엔진 ID 가져오기, 31 페이지

SNMP V3 사용자 구성 설정

다음 표에서는 SNMP V3 사용자 구성 설정에 대해 설명합니다.

표 ***13: SNMP V3*** 사용자 구성 설정

필드	설명
서버	이 설정은 알림 대상 찾기 절차를 수행할 때 서버를 지정했기 때문에 읽기 전용으로 표시됩니다. 액세스를 제공할 서버를 변경하려면 절차를 수행하여 SNMP 사용자를 찾습니다.
사용자 이름	필드에 액세스를 제공할 사용자의 이름을 입력합니다. 이 이름은 최대 32자로 구성되고 영문자, 하이픈(-) 및 밑줄(_) 조합이 포함될 수 있습니다. 팁 NMS(네트워크 관리 시스템)에 대해 이미 구성된 사용자를 입력합니다. 기존 SNMP 사용자의 경우 이 설정은 읽기 전용으로 표시됩니다.
인증 필요	인증을 요구하려면 확인란을 선택하고 암호 및 암호 다시 입력 필드에 암호를 입력한 다음 적절한 프로토콜을 선택합니다. 암호는 8자 이상을 포함해야 합니다. 참고 FIPS 모드 또는 고급 보안 모드가 활성화된 경우 프로토콜로 **SHA**를 선택합니다.
프라이버시 필요	인증 필요 확인란을 선택한 경우 프라이버시 정보를 지정할 수 있습니다. 프라이버시를 요구하려면 확인란을 선택하고 암호 및 암호 다시 입력 필드에 암호를 입력한 다음 프로토콜 확인란을 선택합니다. 암호는 8자 이상을 포함해야 합니다. 참고 FIPS 모드 또는 고급 보안 모드가 활성화된 경우, 프로토콜로 **AES128**를 선택합니다.
모든 호스트에서 SNMP 패킷 수락	모든 호스트에서 SNMP 패킷을 수락하려면 라디오 버튼을 클릭합니다.

필드	설명
다음 호스트의 SNMP 패킷만 수락	특정 호스트에서 SNMP 패킷을 수락하려면 라디오 버튼을 클릭합니다. 호스트 이름//IPv4/IPv6 주소 필드에 SNMP 패킷을 수락할 IPv4 또는 IPv6 주소를 입력하고 삽입을 클릭합니다. IPv4 주소는 점으로 구분된 십진수 형식입니다. 예를 들어 10.66.34.23. IPv6 주소는 콜론으로 구분된 16진수 형식입니다. 예를 들어 2001:0db8:85a3:0000:0000:8a2e:0370:7334 또는 2001:0db8:85a3::8a2e:0370:7334. SNMP 패킷을 수락할 각 주소에 대해 이 과정을 반복합니다. 주소를 삭제하려면 호스트 IPv4/IPv6 주소 목록 상자에서 해당 주소를 선택하고제거를 클릭합니다.
액세스 권한	드롭다운 목록 상자에서 액세스 수준에 대해 다음 옵션 중 하나를 선택합니다. 읽기 전용 MIB 개체의 값만 읽을 수 있습니다. **ReadWrite** MIB 개체의 값을 읽고 쓸 수 있습니다. **ReadWriteNotify** MIB 개체의 값을 읽고 쓰고 트랩에 대한 MIB 개체 값을 전송하고 메시지를 알릴 수 있습니다. **NotifyOnly** 트랩 및 알림 메시지에 대해서만 MIB 개체 값을 보낼 수 있습니다. **ReadNotifyOnly** MIB 개체의 값을 읽고 트랩 및 알림 메시지에 대한 값을 보낼 수 있습니다. 없음 트랩 정보는 읽거나 쓰거나 보낼 수 없습니다. 팁 트랩 구성 매개 변수를 변경하려면 NotifyOnly, ReadNotifyOnly 또는 ReadWriteNotify 권한을 사용하여 사용자를 구성합니다.
모든 노드에 적용	클러스터의 모든 노드에 사용자 구성을 적용하려면 이 확인란을 선택합니다. 이는 Unified Communications Manager 및 IM and Presence Service 클러스터에만 적용됩니다.

원격 SNMP 엔진 ID 가져오기

SNMP V3을 배포하는 경우 이 절차를 사용하여 알림 대상 구성에 필요한 원격 SNMP 엔진 ID를 가져옵니다.

참고 이 절차는 SNMP V3에 반드시 필요하지만, SNMP V1 또는 2C의 경우에는 선택 사항입니다.

프로시저

단계 **1** 명령줄 인터페이스에 로그인합니다.

단계 **2** `utils SNMP walk 1` CLI 명령을 실행합니다.

단계 **3** 구성된 커뮤니티 문자열(SNMP V1/V2) 또는 구성된 사용자(SNMP V3 사용)를 입력합니다.

단계 **4** 서버의 IP 주소를 입력합니다. 예를 들어, localhost의 경우 `127.0.0.1`을 입력합니다.

단계 **5** OID(개체 ID)로 `1.3.6.1.6.3.10.2.1.1.0`을 입력합니다.

단계 **6** 파일의 경우 `파일`을 입력합니다.

단계 **7** `y`를 입력합니다.
시스템 출력이 원격 SNMP 엔진 ID를 나타내는 HEX-STRING입니다.

단계 **8** SNMP가 실행 중인 각 노드에서 이 절차를 반복합니다.

다음에 수행할 작업

SNMP 알림 대상 구성, 31 페이지

SNMP 알림 대상 구성

이 절차를 사용하여 SNMP 트랩 및 알림에 대한 알림 대상을 구성합니다. 이 절차는 SNMP V1, V2c 또는 V3에 사용할 수 있습니다.

시작하기 전에

SNMP 커뮤니티 문자열 또는 SNMP 사용자를 아직 설정하지 않은 경우 다음 작업 중 하나를 완료합니다.

- SNMP V1/V2의 경우 다음을 참조하십시오. SNMP 커뮤니티 문자열 구성, 25 페이지
- SNMP V3의 경우 다음을 참조하십시오. SNMP 사용자 구성, 27 페이지

프로시저

단계 **1** Cisco Unifeid Serviceability에서 다음 중 하나를 선택합니다.

- SNMP V1/V2의 경우 **SNMP** > **V1/v2** > 알림 대상 을 선택합니다
- SNMP V3의 경우 [**SNMP** > **v3** > 알림 대상 을 선택합니다

단계 **2** 서버를 선택하고 찾기 를 클릭하여 기존 SNMP 알림 대상을 검색합니다. 선택적으로 검색 매개 변수를 입력하여 특정 대상을 찾을 수 있습니다.

단계 **3** 다음 중 하나를 수행합니다.

- 기존 SNMP 알림 대상을 편집하려면 알림 대상을 선택합니다.
- 새 SNMP 알림 대상을 추가하려면 새로 추가를 클릭합니다.

참고 기존 SNMP 알림 대상을 삭제하려면 대상을 선택하고 선택한 항목 삭제를 클릭합니다. 사용자를 삭제한 후에는 **Cisco SNMP Master Agent**를 다시 시작합니다.

단계 **4** 호스트 **IP** 주소 드롭다운에서 기존 주소를 선택하거나 새로 추가를 클릭하고 새 호스트 IP 주소를 입력합니다.

단계 **5** SNMP V1/V2에만 해당됩니다. **SNMP** 버전 필드에서 SNMP V1 또는 V2c를 구성하는지 여부에 따라 V1 또는 V2C 라디오 버튼을 선택합니다.

단계 **6** SNMP V1/V2의 경우 다음 단계를 완료하십시오.

a) SNMP V2에만 해당됩니다. 알림 유형 드롭다운에서 알림 또는 트랩을 선택합니다.
b) 구성한 커뮤니티 문자열을 선택합니다.

단계 **7** SNMP V3의 경우 다음 단계를 완료하십시오.

a) 알림 유형 드롭다운에서 알림 또는 트랩을 선택합니다.
b) 원격 **SNMP** 엔진 **ID** 드롭다운에서 기존 엔진 ID를 선택하거나 새로 추가를 선택하고 새 ID를 입력합니다.
c) 보안 수준 드롭다운에서 적절한 보안 수준을 할당합니다.

단계 **8** 이 구성이 모든 클러스터 노드에 적용되도록 하려면 모든 노드에 적용 확인란을 선택합니다.

단계 **9** 삽입을 클릭합니다.

단계 **10** 확인을 클릭하여 SNMP 마스터 에이전트를 다시 시작합니다.

예

참고 [알림 대상 구성 창에서 필드 설명 도움말은 다음 항목 중 하나를 참조하십시오.

- SNMP V1 및 V2c에 대한 알림 대상 설정, 33 페이지
- SNMP V3에 대한 알림 대상 설정, 34 페이지

다음에 수행할 작업

MIB2 시스템 그룹 구성, 36 페이지

SNMP V1 및 V2c에 대한 알림 대상 설정

다음 표에서는 SNMP V1/V2c에 대한 알림 대상 구성 설정에 대해 설명합니다.

표 ***14: SNMP V1/V2c***에 대한 알림 대상 구성 설정

필드	설명
서버	이 설정은 사용자가 알림 대상을 찾기 위해 절차를 수행할 때 서버를 지정했기 때문에 읽기 전용으로 표시됩니다. 알림 대상에 대한 서버를 변경하려면 절차를 수행하여 커뮤니티 문자열을 찾습니다.
호스트 IPv4/IPv6 주소	드롭다운 목록 상자에서 트랩 대상의 호스트 IPv4/IPv6 주소를 선택하거나 새로 추가를 클릭합니다. 새로 추가를 클릭하는 경우 호스트 IPv4/IPv6 주소 필드에 트랩 대상의 IPv4/IPv6 주소를 입력합니다. 기존 알림 대상의 경우 호스트 IP 주소 구성을 수정할 수 없습니다.
호스트 IPv4/IPv6 주소	필드에서 SNMP 패킷을 수락할 IPv4 또는 IPv6 주소를 입력합니다. IPv4 주소는 점으로 구분된 십진수 형식입니다. 예를 들어 10.66.34.23. IPv6 주소는 콜론으로 구분된 16진수 형식입니다. 예를 들어 2001:0db8:85a3:0000:0000:8a2e:0370:7334 또는 2001:0db8:85a3::8a2e:0370:7334.
포트 번호	필드에서 SNMP 패킷을 수신하는 대상 서버에 알림 수신 포트 번호를 입력합니다.
V1 또는 V2c	SNMP 버전 정보 창에서 해당 SNMP 버전 라디오 버튼(V1 또는 V2c)을 클릭합니다. 이 버튼은 사용 중인 SNMP 버전에 따라 달라집니다. • V1을 선택하는 경우 커뮤니티 문자열 설정을 구성합니다. • V2c를 선택하는 경우 알림 유형 설정을 구성한 다음 커뮤니티 문자열을 구성합니다.

필드	설명
커뮤니티 문자열	드롭다운 목록 상자에서 이 호스트가 생성하는 알림 메시지에 사용할 커뮤니티 문자열 이름을 선택합니다. 최소 알림 권한(ReadWriteNotify 또는 알림만)이 있는 커뮤니티 문자열만 표시됩니다. 이러한 권한을 사용하여 커뮤니티 문자열을 구성하지 않은 경우 드롭다운 목록 상자에 옵션이 표시되지 않습니다. 필요한 경우 새 uiCommunity 문자열 만들기를 클릭하여 커뮤니티 문자열을 만듭니다. IM and Presence만 해당: 최소 알림 권한이 있는 커뮤니티 문자열만 (ReadWriteNotify, ReadNotifyOnly 또는 알림만) 표시됩니다. 이러한 권한을 사용하여 커뮤니티 문자열을 구성하지 않은 경우 드롭다운 목록 상자에 옵션이 표시되지 않습니다. 필요한 경우 새 커뮤니티 문자열 만들기를 클릭하여 커뮤니티 문자열을 만듭니다.
알림 유형	드롭다운 목록 상자에서 적절한 알림 유형을 선택합니다.
모든 노드에 적용	클러스터의 모든 노드에 알림 대상 구성을 적용하려면 이 확인란을 선택합니다. 이는 Cisco Unified Communications Manager 및 IM and Presence Service 클러스터에만 적용됩니다.

SNMP V3에 대한 알림 대상 설정

다음 표에서는 SNMP V3에 대한 알림 대상 구성 설정에 대해 설명합니다.

표 *15: SNMP V3*에 대한 알림 대상 구성 설정

필드	설명
서버	이 설정은 사용자가 SNMP V3 알림 대상을 찾기 위해 절차를 수행할 때 서버를 지정했기 때문에 읽기 전용으로 표시됩니다. 알림 대상에 대한 서버를 변경하려면 절차를 수행하여 SNMP V3 알림 대상을 찾고 다른 서버를 선택합니다.
호스트 IPv4/IPv6 주소	드롭다운 목록 상자에서 트랩 대상의 호스트 IPv4/IPv6 주소를 선택하거나 새로 추가를 클릭합니다. 새로 추가를 클릭하는 경우 호스트 IPv4/IPv6 주소 필드에 트랩 대상의 IPv4/IPv6 주소를 입력합니다. 기존 알림 대상의 경우 호스트 IP 주소 구성을 수정할 수 없습니다.
호스트 IPv4/IPv6 주소	필드에서 SNMP 패킷을 수락할 IPv4 또는 IPv6 주소를 입력합니다. IPv4 주소는 점으로 구분된 십진수 형식입니다. 예를 들어 10.66.34.23. IPv6 주소는 콜론으로 구분된 16진수 형식입니다. 예를 들어 2001:0db8:85a3:0000:0000:8a2e:0370:7334 또는 2001:0db8:85a3::8a2e:0370:7334.

필드	설명
포트 번호	필드에 대상 서버에 대한 알림 수신 포트 번호를 입력합니다.
알림 유형	드롭다운 목록 상자에서 알림 또는 트랩을 선택합니다. 팁 알림 옵션을 선택하는 것이 좋습니다. 알림 기능은 응답될 때까지 메시지를 재전송하므로 트랩보다 더 안정적으로 수행할 수 있습니다.
원격 SNMP 엔진 ID	이 설정은 알림 유형 드롭다운 목록 상자에서 알림을 선택한 경우 표시됩니다. 드롭다운 목록 상자에서 엔진 ID를 선택하거나 새로 추가를 선택합니다. 새로 추가를 선택한 경우에는 16진수 값이 필요한 원격 SNMP 엔진 ID 필드에 ID를 입력합니다.
보안 레벨	드롭다운 목록 상자에서 사용자에 대한 적절한 보안 수준을 선택합니다. **noAuthNoPriv** 인증 또는 프라이버시가 구성되지 않았습니다. **authNoPriv** 인증을 구성했지만 프라이버시를 구성하지 않았습니다. **authPriv** 인증 및 프라이버시가 구성되었습니다.
사용자 정보 창	창에서 다음 작업 중 하나를 수행하여 사용자와 알림 대상을 연결하거나 연결을 해제합니다. 1. 새 사용자를 만들려면 새 사용자 만들기를 클릭합니다. 2. 기존 사용자를 수정하려면 사용자의 라디오 버튼을 클릭한 다음 선택한 사용자 업데이트를 클릭합니다. 3. 사용자를 삭제하려면 사용자의 라디오 버튼을 클릭한 다음 선택한 사용자 삭제를 클릭합니다. 표시되는 사용자는 알림 대상에 대해 구성한 보안 레벨에 따라 달라 집니다.
모든 노드에 적용	클러스터의 모든 노드에 알림 대상 구성을 적용하려면 이 확인란을 선택합니다. 이는 Cisco Unified Communications Manager 및 IM and Presence Service 클러스터에만 적용됩니다.

MIB2 시스템 그룹 구성

이 절차를 사용하여 MIB-II 시스템 그룹에 대한 시스템 연결 및 시스템 위치를 구성합니다. 예를 들어 시스템 연락처로 관리자 555-121-6633, 시스템 위치로 SanJose, Bldg 23, 2nd floor를 입력할 수 있습니다. 이 절차는 SNMP V1, V2 및 V3에 사용할 수 있습니다.

프로시저

단계 **1** Cisco 통합 서비스 가용성에서 **SNMP** > **SystemGroup** > **MIB2** 시스템 그룹을 선택합니다.
단계 **2** 서버 드롭다운에서 노드를 선택하고 이동을 클릭합니다.
단계 **3** 시스템 연결 및 시스템 위치 필드를 완료합니다.
단계 **4** 이러한 설정이 모든 클러스터 노드에 적용되도록 하려면 모든 노드에 적용 확인란을 선택합니다.
단계 **5** 저장을 클릭합니다.
단계 **6** 확인을 클릭하여 SNMP 마스터 에이전트 서비스를 다시 시작합니다.

예

참고 필드 설명 도움말은 다음을 참조하십시오. MIB2 시스템 그룹 설정, 36 페이지

참고 모두 지우기를 클릭하여 필드를 지울 수 있습니다. 모두 지우기를 클릭한후 저장을 클릭하면 레코드가 삭제됩니다.

MIB2 시스템 그룹 설정

다음 표에서는 MIB2 시스템 그룹 구성 설정을 설명합니다.

표 ***16: MIB2*** 시스템 그룹 구성 설정

필드	설명
서버	드롭다운 목록 상자에서 연락처를 구성할 서버를 선택한 다음 이동을 클릭합니다.
시스템 연락처	문제가 발생했을 때 알릴 사람을 입력합니다.
시스템 위치	시스템 연락처로 식별되는 사람의 위치를 입력합니다.

필드	설명
모든 노드에 적용	클러스터의 모든 노드에 시스템 구성을 적용하려면 선택합니다. 이는 Unified Communications Manager 및 IM and Presence Service 클러스터에만 적용됩니다.

CISCO-SYSLOG-MIB 트랩 매개 변수

다음 지침을 사용하여 시스템에서 CISCO-SYSLOG-MIB 트랩 설정을 구성합니다.

- SNMP Set 작업을 사용하여 clogsNotificationEnabled (1.3.6.1.4.1.9.9.41.1.1.2)를 True로 설정합니다. 예를 들어, net-SNMP set 유틸리티를 사용하여 linux 명령줄에서 다음을 사용하여 이 OID를 True로 설정합니다.

  ```
  SNMPset -c <커뮤니티 문자열>-v2c <송신기 ip 주소> 1.3.6.1.4.1.9.9.41.1.1.2.0 i 1
  ```

  SNMP Set 작업에 다른 SNMP 관리 애플리케이션을 사용할 수도 있습니다.

- SNMP Set 작업을 사용하여 clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3) 값을 설정합니다. 예를 들어, net-SNMP set 유틸리티를 사용하여 linux 명령줄에서 다음을 사용하여 이 OID 값을 설정합니다.

  ```
  SNMPset-c public-v2c <송신기 ip 주소> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <값>
  ```

  <값> 설정에 대한 심각도 번호를 입력합니다. 심각도 값은 심각도가 감소하면 증가합니다. 값 1(긴급)은 가장 높은 심각도를 나타내고 값 8(디버그)은 최저 심각도를 나타냅니다. Syslog 에이전트는 사용자가 지정한 값보다 큰 메시지는 무시합니다. 예를 들어, 모든 syslog 메시지를 트래핑 하려면 값 8을 사용합니다.

  심각도 값은 다음과 같습니다.

  - 1: 긴급
  - 2: 알림
  - 3: 위험
  - 4: 오류
  - 5: 경고
  - 6: 공지
  - 7: 정보
  - 8: 디버그)

  SNMP Set 작업에 다른 SNMP 관리 애플리케이션을 사용할 수도 있습니다.

참고 기록하기 전에 Syslog는 지정된 Syslog 버퍼 크기보다 큰 모든 트랩 메시지 데이터를 자릅니다. Syslog 트랩 메시지 길이 제한은 255바이트입니다.

CISCO-CCM-MIB 트랩 매개 변수

- SNMP Set 작업을 사용하여 ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2)을 30-3600 범위의 값으로 설정합니다. 예를 들어, net-SNMP set 유틸리티를 사용하여 linux 명령줄에서 다음을 사용하여 이 OID 값을 설정합니다.

```
SNMPset -c <커뮤니티 문자열> -v2c <송신기 ip 주소> 1.3.6.1.4.1.9.9.156.1.9.2 .0
i <값>
```

SNMP Set 작업에 다른 SNMP 관리 애플리케이션을 사용할 수도 있습니다.

- SNMP Set 작업을 사용하여 ccmPhoneStatusUpdateAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.4)을 30-3600 범위의 값으로 설정합니다. 예를 들어, net-SNMP set 유틸리티를 사용하여 linux 명령줄에서 다음을 사용하여 이 OID 값을 설정합니다.

```
SNMPset -c <커뮤니티 문자열> -v2c <송신기 ip 주소> 1.3.6.1.4.1.9.9.156.1.9.4.0 i
 <값>
```

SNMP Set 작업에 다른 SNMP 관리 애플리케이션을 사용할 수도 있습니다.

CISCO-UNITY-MIB 트랩 매개 변수

Cisco Unity Connection에만 해당: Cisco Unity Connection SNMP 에이전트는 트랩 알림을 활성화하지 않지만 Cisco Unity Connection 알람에서 트랩이 트리거될 수 있습니다. Cisco Unity Connection 서비스 가용성의 Cisco Unity Connection 알람 정의는 알람 > 정의 화면에서 볼 수 있습니다.

CISCO-SYSLOG-MIB를 사용하여 트랩 매개 변수를 구성할 수 있습니다.

관련 항목

CISCO-SYSLOG-MIB 트랩 매개 변수, 37 페이지

SNMP 마스터 에이전트 다시 시작

모든 SNMP 구성을 완료한 후에는 SNMP 마스터 에이전트 서비스를 다시 시작합니다.

프로시저

단계 **1** Cisco 통합 서비스 가용성에서 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.

단계 **2** 서버를 선택하고 이동을 클릭합니다.

단계 3 **SNMP** 마스터 에이전트를 선택합니다.

단계 4 재시작을 클릭합니다.

SNMP 트랩 설정

CLI 명령을 사용하여 구성 가능한 SNMP 트랩 설정을 설정합니다. SNMP 트랩 구성 매개 변수 및 권장 구성 팁은 CISCO-SYSLOG-MIB, CISCO-CCM-MIB 및 CISCO-UNITY-MIB용으로 제공됩니다.

SNMP 트랩 구성

이 절차를 사용하여 SNMP 트랩을 구성합니다.

시작하기 전에

시스템에서 SNMP를 구성합니다. 자세한 내용은 SNMP 구성 작업 흐름, 23 페이지를 참조하십시오.

SNMP 커뮤니티 문자열(SNMP V1/V2의 경우) 또는 SNMP 사용자(SNMP V3의 경우)에 대한 액세스 권한이 **ReadWriteNotify**, **ReadNotify**, **NotifyOnly** 설정 중 하나로 설정되어 있는지 확인합니다.

프로시저

단계 1 CLI에 로그인하고 `utils SNMP test` CLI 명령을 실행하여 SNMP가 실행되고 있는지 확인합니다.

단계 2 특정 SNMP 트랩(예: CcmPhoneFailed 또는 MediaResourceListExhausted 트랩)을 생성하려면 SNMP 트랩 생성, 39 페이지을 수행합니다.

단계 3 트랩이 생성되지 않으면 다음 단계를 수행하십시오.

- Cisco 통합 서비스 가용성에서 알람 > 구성을 선택하고 **CM** 서비스 및 **Cisco CallManager**를 선택합니다.
- 모든 노드에 적용 확인란을 선택합니다.
- 로컬 Syslogs 아래의 알람 이벤트 수준 드롭다운 목록 상자를 정보로 설정합니다.

단계 4 트랩을 재현하고 해당 알람이 CiscoSyslog 파일에 기록되는지 확인합니다.

SNMP 트랩 생성

이 섹션에서는 특정 유형의 SNMP 트랩을 생성하는 프로세스를 설명합니다. 개별 트랩을 생성하기 위해서는 SNMP를 서버에서 설정하고 실행해야 합니다. SNMP 트랩을 생성하도록 시스템을 설정하는 방법에 대한 지침은 SNMP 트랩 구성, 39 페이지의 내용을 참조하십시오.

참고 개별 SNMP 트랩에 대한 처리 시간은 생성하려고 하는 트랩에 따라 달라집니다. 일부 SNMP 트랩은 생성하는 데 몇 분 정도 걸릴 수 있습니다.

표 ***17: SNMP*** 트랩 생성

SNMP 트랩	프로세스
ccmPhoneStatusUpdate	CcmPhoneStatusUpdate 트랩을 트리거하려면 다음과 같이 하십시오. **1.** CcmAlarmConfig Info MIB 테이블에서 ccmPhoneStatusUpdateAlarmInterv (1.3.6.1.4.1.9.9.156.1.9.4) = 30 이상으로 설정합니다. **2.** Cisco Unified Communications Manager 관리에 로그인합니다. **3.** 서비스 중이고 Unified Communications Manager에 등록된 전화기의 경우 전화기를 재설정합니다. 전화기를 등록 해제한 다음 재등록하면 ccmPhoneStatusUpdate 트랩을 생성합니다.
ccmPhoneFailed	CcmPhoneFailed 트랩을 트리거하려면 다음과 같이 하십시오. **1.** CcmAlarmConfigInfo MIB 테이블에서 ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2) = 30 이상으로 설정합니다. **2.** Cisco Unified Communications Manager 관리에서 전화기의 MAC 주소를 잘못된 값으로 변경합니다. **3.** Cisco Unified Communications Manager 관리에서 전화기를 재등록합니다. **4.** 전화기가 TFTP 서버 A를 가리키도록 설정하고 전화기를 다른 서버에 연결합니다.
ccmGatewayFailed	CcmGatewayFailed SNMP 트랩을 트리거하려면 다음과 같이 하십시오. **1.** CcmGatewayAlarmEnable (1.3.6.1.4.1.9.9.156.1.9.6)이 true로 설정되어 있는지 확인합니다. **2.** Cisco Unified Communications Manager 관리에서 게이트웨이의 MAC 주소를 잘못된 값으로 변경합니다. **3.** 게이트웨이를 재부팅합니다.

SNMP 트랩	프로세스
ccmGatewayLayer2Change	레이어 2가 모니터링되는(예: MGCP 백홀 로드) 작동하는 게이트웨이에서 ccmGatewayLayer2Change 트랩을 트리거하려면 다음을 수행합니다. **1.** CcmAlarmConfig Info MIB 테이블에서 ccmGatewayAlarmEnable (1.3.6.1.4.1.9.9.156.1.9.6.0) = true로 설정합니다. **2.** Cisco Unified Communications Manager 관리에서 게이트웨이의 MAC 주소를 잘못된 값으로 변경합니다. **3.** 게이트웨이를 재설정합니다.
MediaResourceListExhausted	MediaResourceListExhausted 트랩을 트리거하려면 다음과 같이 하십시오. **1.** Cisco Unified Communications Manager 관리에서 표준 전화회의 브리지 리소스 (CFB-2) 중 하나를 포함하는 미디어 리소스 그룹을 만듭니다. **2.** 사용자가 만든 미디어 리소스 그룹을 포함하는 미디어 리소스 그룹 목록을 만듭니다. **3.** 전화기 구성 창에서 미디어 리소스 그룹 목록 필드를 사용자가 만든 미디어 리소스 그룹 목록으로 설정합니다. **4.** IP Voice Media Streaming 서비스를 중지합니다. 이 작업으로 인해 ConferenceBridge 리소스(CFB-2)가 작동하지 않습니다. **5.** 미디어 리소스 그룹 목록을 사용하는 전화기로 전화회의 통화를합니다. "전화회의 브리지를 사용할 수 없음" 메시지가 전화기 화면에 표시됩니다.
RouteListExhausted	RouteListExhausted 트랩을 트리거하려면 다음과 같이 하십시오. **1.** 하나의 게이트웨이를 포함하는 경로 그룹을 만듭니다. **2.** 방금 만든 경로 그룹을 포함하는 경로 그룹 목록을 만듭니다. **3.** 경로 그룹 목록을 통해 통화를 라우팅하는 고유한 경로 패턴을 생성합니다. **4.** 게이트웨이를 등록 해제합니다. **5.** 전화기 중 하나에서 경로 패턴과 일치하는 번호로 전화를 겁니다.

SNMP 트랩	프로세스
MaliciousCallFailed	MaliciousCallFailed 트랩을 트리거하려면 다음과 같이 하십시오. **1.** 사용 가능한 모든 "MaliciousCall" 소프트 키를 포함하는 소프트 키 템플릿을 생성합니다. **2.** 새 소프트 키 템플릿을 네트워크의 전화기에 할당하고 전화기를 재설정합니다. **3.** 전화기 사이에 전화를 겁니다. **4.** 통화 중에 "MaliciousCall" 소프트 키를 선택합니다.
ccmCallManagerFailed	**1.** `show process list` CLI 명령을 실행하여 CallManager 애플리케이션 ccm의 PID(프로세스 식별자)를 가져옵니다. 이 명령은 여러 프로세스 및 PID를 반환합니다. 알람을 생성하기 위해 중지해야 하는 PID이기 때문에, 특히 ccm에 대한 PID를 구해야 합니다. **2.** `delete process <pid>` 충돌 CLI 명령을 실행합니다. **3.** CLI 명령을 실행합니다. CallManager 실패 알람은 내부 오류가 생성될 때 생성됩니다. 이러한 내부 오류에는 CPU 부족으로 인한 내부 스레드 종료, CallManager 서버를 16초 이상 일시 중지, 타이머 문제를 포함할 수 있습니다. 이 알람을 수동으로 생성할 수는 없습니다. 참고 ccmCallManagerFailed 알람 또는 트랩을 생성하면 CallManager 서비스를 종료하고 코어 파일을 생성합니다. 혼동을 피하려면 코어 파일을 즉시 삭제하는 것이 좋습니다.
syslog 메시지를 트랩으로	특정 심각도 보다 높은 syslog 메시지를 트랩으로 받으려면 clogBasic 테이블에서 다음 두 개의 MIB 개체를 설정합니다. **1.** ClogNotificationsEnabled (1.3.6.1.4.1.9.9.41.1.1.2)를 true(1)로 설정합니다. 기본값은 false(2)입니다. 예를 들어 SNMPset -c <커뮤니티 문자열> -v 2c <송신기 ip 주소> 1.3.6.1.4.1.9.9.41.1.1.2.0 I 1 **2.** ClogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3)를 트랩이 생성될 수준보다 큰 수준으로 설정합니다. 기본값은 경고(5)입니다. 알람 심각도가 구성된 심각도 수준보다 작거나 같은 모든 syslog 메시지는 트랩으로 전송됩니다. 예를 들어, SNMPset -c <커뮤니티 문자열> -v 2c <송신기 ip 주소> 1.3.6.1.4.1.9.9.41.1.1.3.0 I <값>

SNMP 추적 구성

Unified Communications Manager의 경우 성능 및 모니터링 서비스 그룹에서 Cisco CallManager SNMP 서비스를 선택하여 Cisco 통합 서비스 가용성의 추적 구성 창에서 Cisco CallManager SNMP 에이전트에 대한 추적을 구성할 수 있습니다. 모든 에이전트에 대한 기본 설정이 존재합니다. Cisco CDP 에이전트 및 Cisco Syslog 에이전트의 경우, *Cisco* 통합 솔루션에 대한 명령줄 인터페이스 참조 설명서에 설명된 대로 CLI를 사용하여 추적 설정을 변경합니다.

Cisco Unity Connection의 경우 연결 SNMP 에이전트 구성 요소를 선택하여Cisco Unity Connection 서비스 가용성의 추적 구성 창에서 Cisco Unity Connection SNMP 에이전트에 대한 추적을 구성할 수 있습니다.

SNMP 문제 해결

문제 해결 팁은 이 섹션을 참조하십시오. 모든 기능 및 네트워크 서비스가 실행되고 있는지 확인합니다.

문제

시스템에서 MIB를 폴링할 수 없습니다.

이 조건은 커뮤니티 문자열 또는 SNMP 사용자가 시스템에 구성되어 있지 않거나 시스템에 구성된 것과 일치하지 않음을 의미합니다. 기본적으로 시스템에는 커뮤니티 문자열이나 사용자가 구성되어 있지 않습니다.

해결 방법

SNMP 구성 창을 사용하여 커뮤니티 문자열 또는 SNMP 사용자가 시스템에 올바르게 구성되어 있는지 확인합니다.

문제

시스템에서 알림을 수신할 수 없습니다.

이 조건은 시스템에 알림 대상이 올바르게 구성되지 않았음을 의미합니다.

해결 방법

알림 대상(V1/V2c 또는 V3) 구성 창에서 알림 대상을 적절하게 구성했는지 확인하십시오.