Cisco Cyber Vision의 센서 업데이트 방법 이해

목차

소개

이 문서에서는 구축 및 문제 해결 지침과 함께 셀프 업데이트 및 확장 업데이트 방법을 사용하여 Cisco Cyber Vision 센서를 업데이트하는 방법에 대해 설명합니다.

배경 정보

Cisco Cyber Vision은 센서 업데이트를 위한 두 가지 기본 메커니즘을 제공합니다. 자체 업데이트 및 내선 번호 업데이트 릴리스 4.4.0에서 향상된 기능을 통해 이제 셀프 업데이트 기능을 폭넓게 사용할 수 있으므로 배포 방법과 상관없이 모든 센서를 업데이트할 수 있습니다.

셀프 업데이트

- 업데이트 메커니즘:

포트 5671(센서 센터 통신에 사용되는 것과 동일한 포트)을 사용하여 RMQ(RabbitMQ) 터널을 통해 업데이트가 수행됩니다.

- 지원되는 구축:
    - 모든 센서 구축 방법(확장, 웹 또는 CLI)
    - 릴리스 4.4.0부터는 설치 방식과 상관없이 모든 센서에 대해 자동 업데이트 기반을 사용할 수 있습니다
    - 릴리스 4.4.1 이상: 모든 센서는 자동 업데이트 기능을 통해 자동으로 업데이트할 수 있습니다.

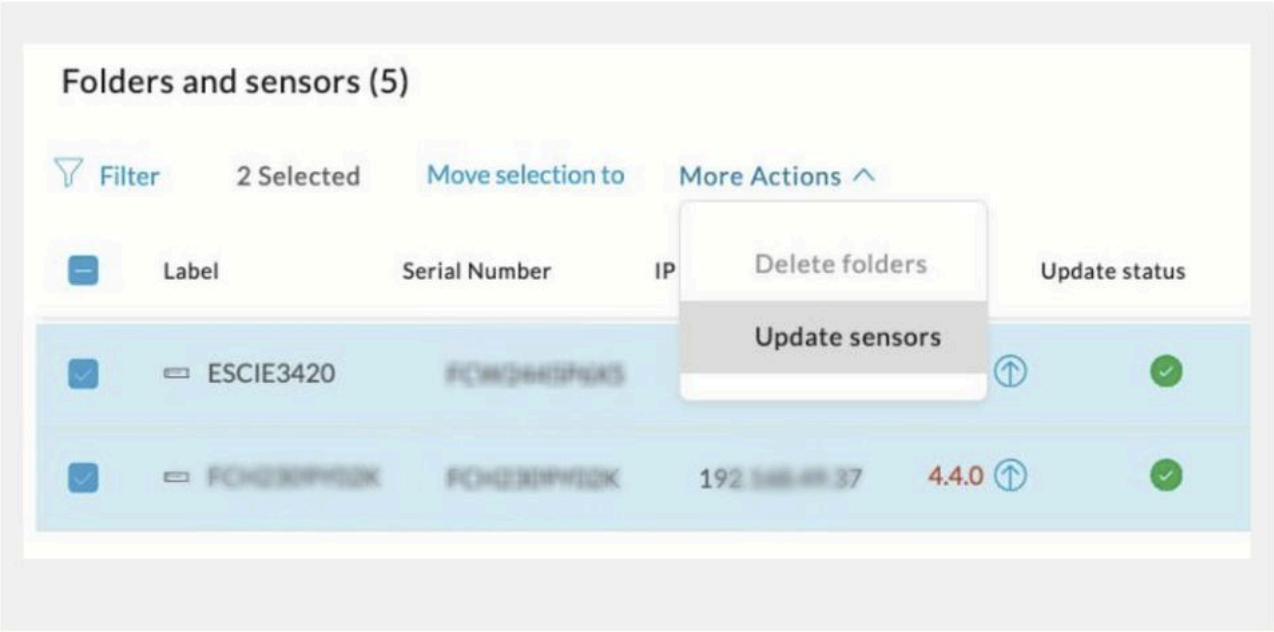
- 업데이트 범위:

센서 컨테이너 내의 특정 이진 파일만 업데이트됩니다. 전체 컨테이너가 교체되지 않습니다.

- 자동 업데이트 프로세스(4.4.1):
    - Center 인터페이스에서 업데이트할 센서를 선택합니다
    - 센터에서 센서의 작업 큐에 새 업데이트 작업을 추가합니다
    - 센서가 업데이트 파일을 자동으로 수집하고 검증합니다

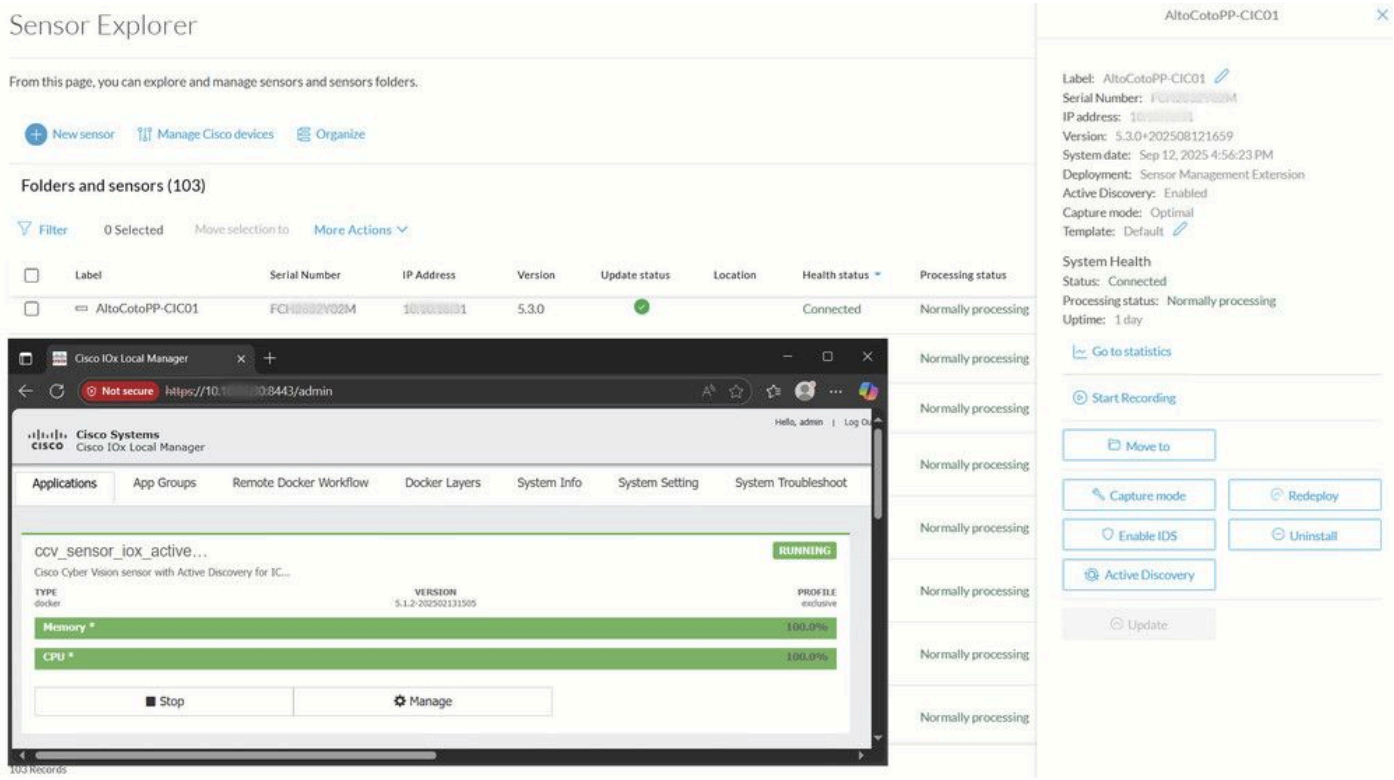
- 새 버전이 적용되면 센서 서비스가 다시 시작됩니다

센서를 업데이트하려면 Center Sensor Explorer GUI에서 More Actions(추가 작업) > Update Sensors(센서 업데이트)로 이동합니다.



참고: 자동 업데이트 후 Center GUI(Sensor Explorer)에 표시되는 센서 버전은 업데이트된 새 릴리스를 반영하고 IOx Local Manager는 이전 버전을 계속 표시합니다(다음 이미지 참조).

이는 자체 업데이트 방식이 전체 IOx 컨테이너를 업그레이드하지 않고 표준 센서-센터 연결을 통해 패키지를 다운로드하는 방식으로 내부 센서 서비스만 업데이트하기 때문에 발생합니다.



- 작업 처리:
  - 업데이트는 센터에서 일괄 관리합니다.
  - 한 센서에서 업데이트가 실패하면 다른 센서에 대한 작업이 계속됩니다
- 문제 해결 제한 사항:

진단 파일 및 센서 로그가 장애 후 너무 늦게 수집되면 관련 정보가 누락되는 경우가 많습니다.

내선 번호 업데이트

- 업데이트 메커니즘:

업데이트는 플랫폼과 센터 간의 포트 443에서 HTTPS 연결을 사용하여 수행됩니다.

- 지원되는 구축:

확장 방법을 통해 구축된 센서에만 사용할 수 있습니다.

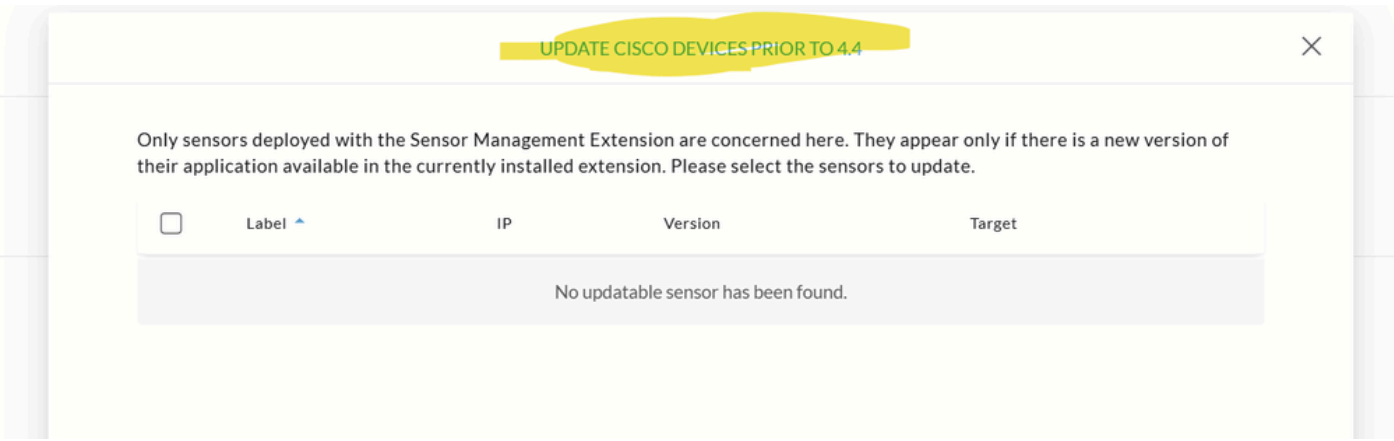
- 업데이트 범위:

업데이트 중에 전체 센서 컨테이너가 교체됩니다.

확장자로 모든 센서를 업데이트하려면 Admin(관리) > Sensors(센서) > Sensor Explorer(센서 탐색기) > Manage Cisco Devices(Cisco 디바이스 관리) > Update Cisco Devices(Cisco 디바이스 업데이트)로 이동하거나 센서의 오른쪽 패널에 있는 재구축 버튼을 사용합니다.

전체 절차는 버전 4.2.0 이상의 센서 설치 설명서를 참조하십시오.

참고: 릴리스 5.2.1부터는 Cisco Cyber Vision에서 4.4 이상 버전을 실행하는 센서에 대해 확장 방법을 통한 디바이스 업데이트를 더 이상 지원하지 않습니다.



- 문제 해결 지침:
  - 센서 IP가 아닌 플랫폼 IP에서 패킷 캡처 필터링 사용
  - 로그를 위한 센터 진단 파일 검토

문제 해결 정보

- 자동 업데이트의 경우, 효과적인 트러블슈팅을 위해 장애 발생 직후 진단 파일 및 센서 로그를 수집합니다.
- 익스텐션 업데이트의 경우 플랫폼과 센터 간의 HTTPS 트래픽을 분석하고 센터 진단 로그를 사용합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.