Cyber Vision Center 서버 문제 해결 및 관리

목차

소개

이 문서에서는 Cisco Cyber Vision Server의 유지 관리, 문제 해결 및 모니터링을 위해 수행할 수 있는 다양한 단계에 대해 설명합니다.

Cisco Cyber Vision에서는 OT(Operational Technology) 보안 상태를 심층적으로 볼 수 있습니다. Cyber Vision에서는 IT 보안 툴에 OT 자산 및 이벤트에 대한 정보를 제공하므로 네트워크 전체에서 더 쉽게 위험을 관리하고 보안 정책을 적용할 수 있습니다.

서버 업데이트

구축 시나리오를 기반으로 소프트웨어에 통합되는 취약성 수정, 버그 수정 및 새로운 기능을 위해 서버를 업데이트해야 합니다.

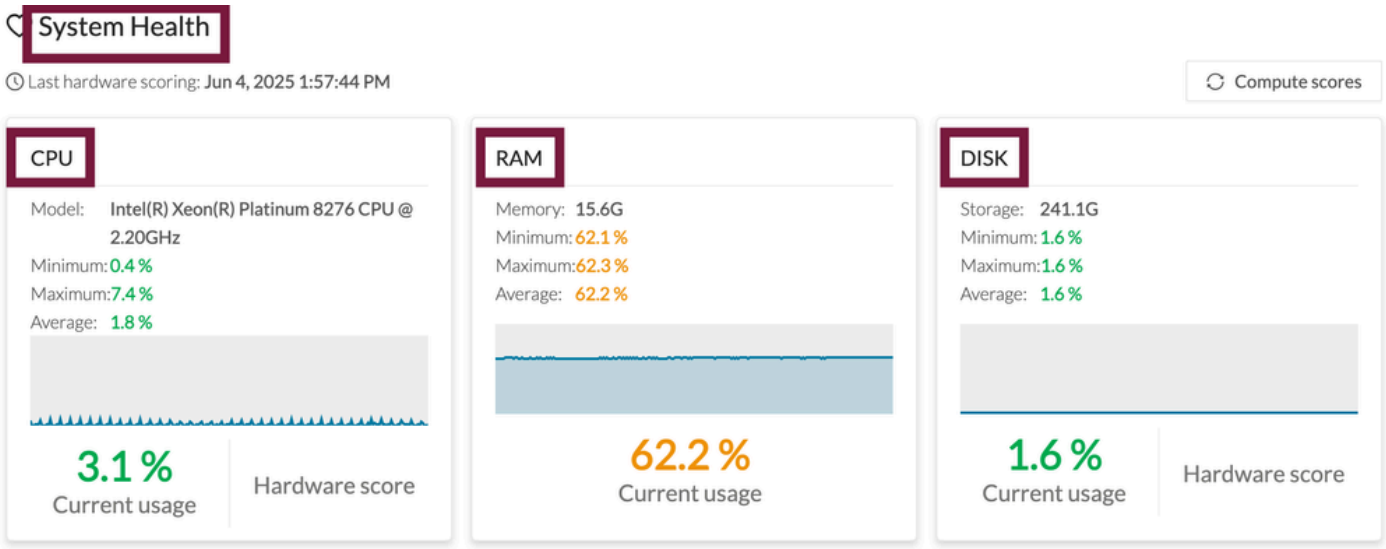
시스템 상태

- 시스템 상태 알림을 전송하도록 SNMPv3 트랩 구성

UI에서(기록 값 확인):

System Statistics (Center or Sensors)(시스템 통계(센터 또는 센서))로 이동하여 CPU 및 RAM 사용률을 확인합니다.

- 600% RAM 및 CPU 40% 주변 센서는 정상 상태가 될 것으로 예상됩니다.
- RAM 및 CPU 80% 정도의 중심부는 50%가 정상 상태일 것으로 예상됩니다.



이는 참조로 사용되는 값입니다. 이러한 리소스는 매우 높은 비율로 이동할 수 있지만 특정 작업을 완료한 후 다시 돌아올 것으로 예상되지만 그대로 남아 있지는 않습니다.

CLI에서(실시간 확인):

top 명령을 사용하여 리소스를 소비하는 프로세스를 파악하기 위해 CPU 및 RAM 사용률을 확인합니다.

다음 명령을 사용하여 확인할 수 있습니다.

'상위 -n 1 -b' | 머리 -n 5

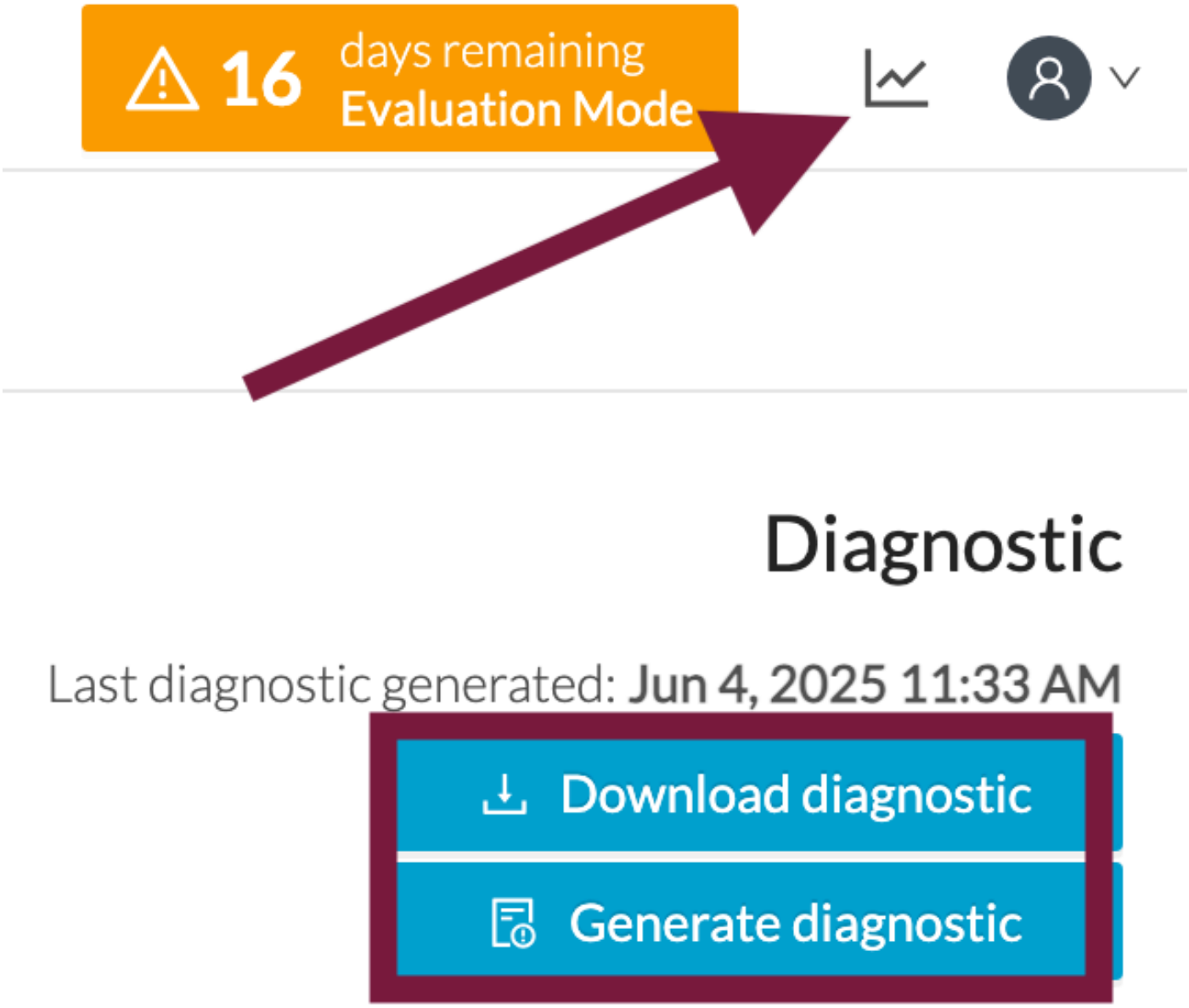
systemctl —failed 명령을 사용하여 시스템 프로세스를 확인합니다. 이 명령은 일반적으로 문제 해결을 위해 예기치 않게 시작되거나 중지된 서비스 또는 유닛을 식별하는 데 사용됩니다.

시스템 로그

여러 로그를 플랫폼에서 사용할 수 있습니다.

UI에서:

진단 파일을 생성합니다. System Statistics (Center or Sensors)(시스템 통계(센터 또는 센서)로 이동하여 Generate Diagnostic(진단 생성)을 클릭합니다.



CLI에서:

sudo -i 명령을 사용하여 루트 사용자 모드에 액세스합니다

시스템 로그를 추적하려면 journaltcl 명령을 사용합니다.

journalctl -r (-r ✳ 역방향)

journalctl - "2015-01-10" 이후 또는 - "2015-01-11 03:00"까지

journalctl -u <프로세스 이름>

journalctl -f (-f ✳ 후속)

journalctl -p 오류(시스템의 오류)

또한 sbs-diag 명령을 사용하여 진단 번들을 시작할 수 있습니다

고급 로그

다음 서비스에 대해 CLI에서 고급 로그를 활성화할 수 있습니다.

sbs 백엔드

sbs 버로우

sbs-marmotd

sbs-lsyncd-gather

sbs-lsynd-communicate

sbs-gsyncd

sbs-nad

sbs-aspic

pxgrid 에이전트

sudo -i 명령을 사용하여 루트 사용자 모드에 액세스합니다

이러한 고급 로그는 실제로 시스템에서 메시지를 플러딩할 수 있으므로 TAC 팀과 작업할 때만 사용해야 합니다.

디스크 공간

- 센서가 분석하고 들어오는 모든 데이터는 데이터베이스에 저장됩니다.
- df -h 명령을 사용하여 /data 파티션의 사용 가능한 공간을 모니터링합니다.
- /data/tmp/captures/ 아래에서 네트워크 캡처를 정리합니다. 더 이상 필요하지 않은 모든 캡처를 삭제하려면 rm -rf /data/tmp/captures/* 명령을 사용합니다.
- 이전 진단 파일을 모두 삭제합니다.
- sbs-db purge-xxxxx 명령을 사용하여 데이터베이스에서 원하지 않는 이전 데이터를 삭제합니다.

트래픽 검증

TCPdump 및 iptables를 사용하여 트래픽 흐름을 따릅니다.

방화벽 추적

Iptables 방화벽이 서버에서 활성화되어 있습니다. 삭제된 패킷은 "DropInput and DropForward"로 기록됩니다.

Iptables 카운터를 확인하여 삭제된 패킷을 확인합니다(iptables -L -n -v | grep 체인).

로그에서 삭제된 패킷 찾기(journalctl) | grep Drop)을 클릭합니다.

TCPdump 툴

서버의 네트워크 인터페이스에서 트래픽을 관찰하고 문제를 해결하는 데 사용할 수 있습니다.

트래픽이 플러딩되면 ctrl+c를 눌러 캡처를 중지합니다.

예

NTP 플로우(UDP/TCP 123)를 모니터링하려면 tcpdump -i [ethX] 포트 123 :

특정 호스트의 수신/발신 트래픽을 모니터링하려면 tcpdump -i [ethX] host 1.2.3.4

캡처를 pcap 파일에 저장하려면

tcpdump -i [ethX] host 1.2.3.4 -r /data/tmp/your_file.pcap

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.