Fehlerbehebung und Verwaltung eines Cyber Vision Center-Servers

Inhalt

Einleitung

Dieses Dokument beschreibt die verschiedenen Schritte, die zur Wartung, Fehlerbehebung und Überwachung eines Cisco Cyber Vision Servers unternommen werden können.

Mit Cisco Cyber Vision erhalten Sie einen detaillierten Einblick in den Sicherheitsstatus Ihrer Betriebstechnologie (OT). Cyber Vision versorgt Ihre IT-Sicherheitstools mit Informationen zu OT-Ressourcen und -Ereignissen, was das Risikomanagement und die Durchsetzung von Sicherheitsrichtlinien im gesamten Netzwerk vereinfacht.

Server-Updates

Behalten Sie den Server auf dem neuesten Stand, um Schwachstellen- und Bugfixes zu beheben und neue Funktionen zu nutzen, die je nach Bereitstellungsszenario in die Software integriert werden.

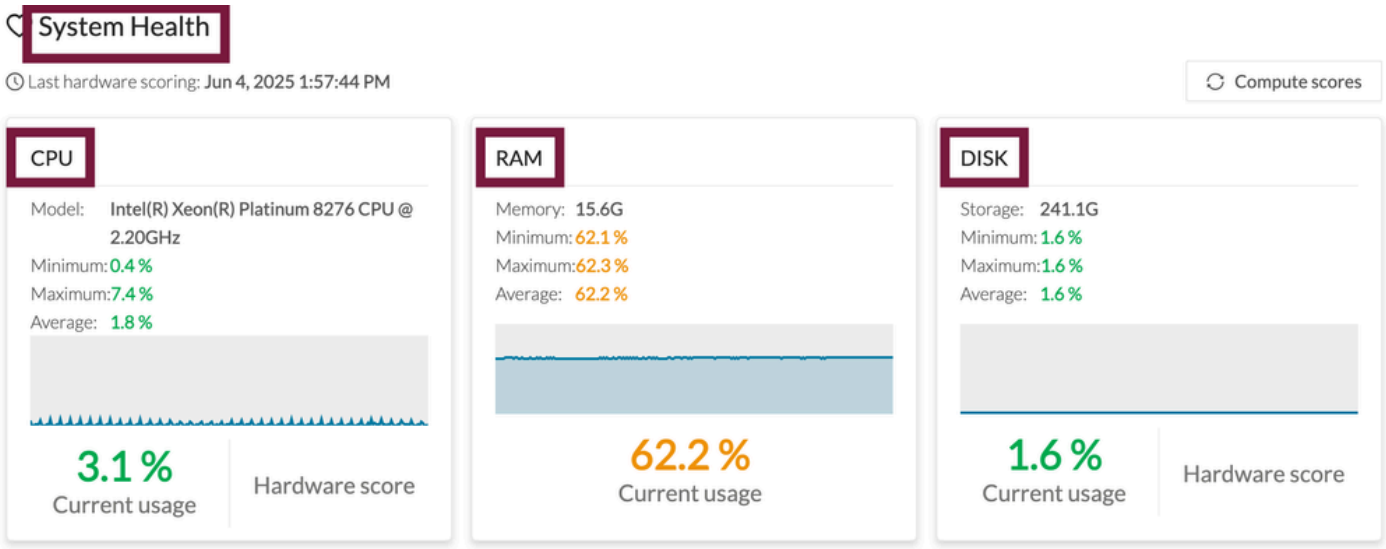
Systemstatus

- Konfigurieren von SNMPv3-Traps zum Senden von Systemzustandswarnungen

Über die Benutzeroberfläche (zur Prüfung des historischen Werts):

Navigieren Sie zu Systemstatistiken (Mitte oder Sensoren), und überprüfen Sie die CPU- und RAM-Auslastung.

- Sensoren mit rund 600 % RAM und 40 % CPU dürften sich im Normalzustand befinden.
- Etwa 80 % RAM und CPU 50 % des Speichers dürften sich im Normalzustand befinden.



Diese Werte werden als Referenz verwendet. Diese Ressourcen können sehr hoch angesetzt werden, werden aber voraussichtlich nach Abschluss einer bestimmten Aufgabe wieder verfügbar sein, aber nicht beibehalten.

Über die CLI (Echtzeitprüfung):

Verwenden Sie den obersten Befehl, um die CPU- und RAM-Auslastung zu überprüfen, um zu ermitteln, welche Prozesse die Ressourcen belegen.

Sie konnte mithilfe des folgenden Befehls überprüft werden:

'top -n 1 -b' | Kopf -n 5

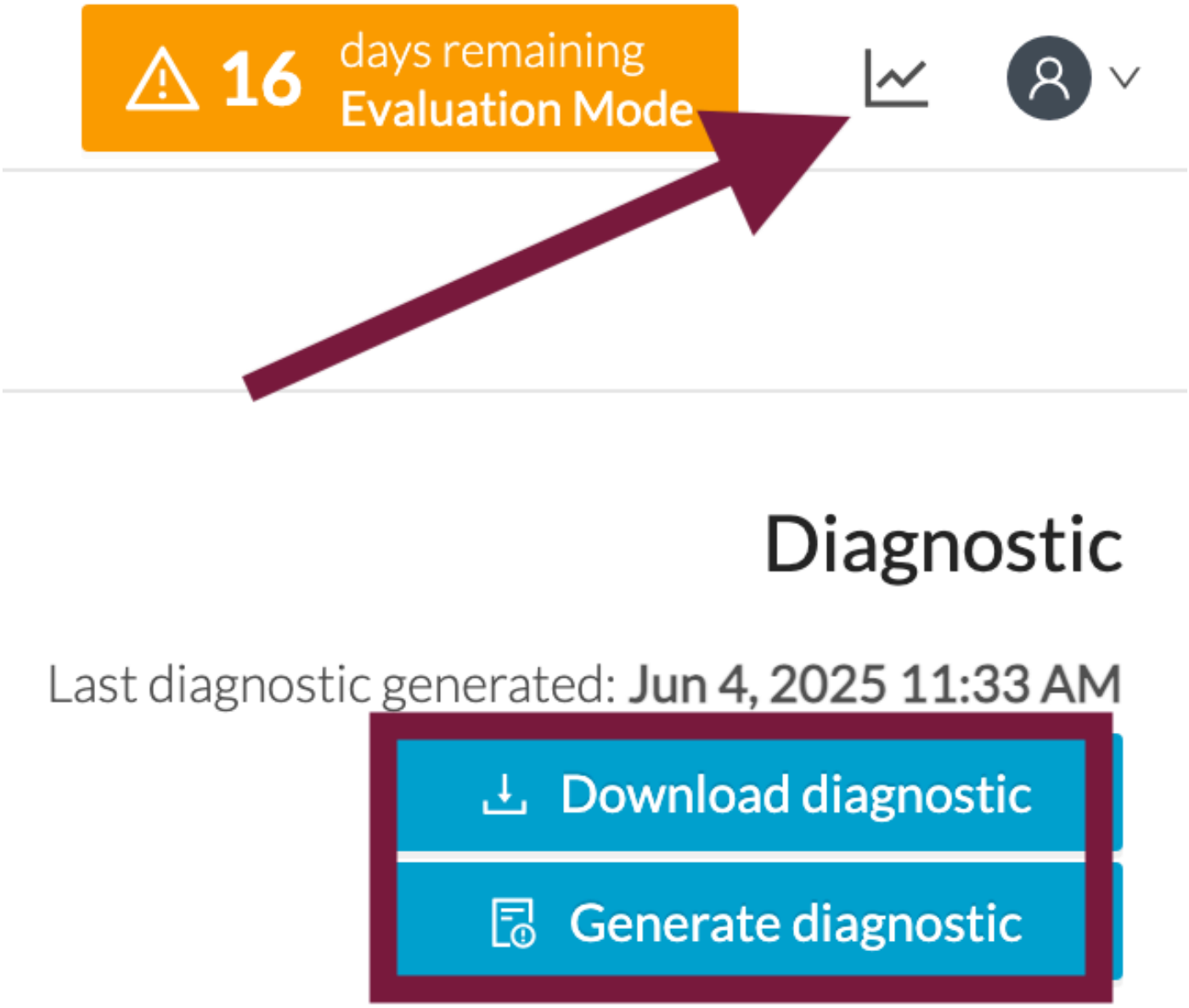
Überprüfen Sie die Systemprozesse mit dem Befehl systemctl —failed. Dieser Befehl wird häufig zur Fehlerbehebung verwendet, um Dienste oder Einheiten zu identifizieren, die nicht unerwartet gestartet oder beendet wurden.

Systemprotokolle

Mehrere Protokolle sind auf der Plattform verfügbar:

Über die Benutzeroberfläche:

Erstellen Sie eine Diagnosedatei. Gehen Sie zu Systemstatistik (Mitte oder Sensoren) und klicken Sie auf Diagnose generieren.



Über die CLI:

Verwenden des Befehls sudo -i für den Zugriff auf den Root-Benutzermodus

Verwenden Sie journaltcl-Befehle, um Systemprotokolle zu verfolgen.

journalctl -r (-r ✳ rückwärts)

journalctl - seit "2015-01-10" oder - bis "2015-01-11 03:00"

journalctl -u <Prozessname>

journalctl -f (-f ✳ folgen)

journalctl -p err (Fehler im System)

Außerdem kann das Diagnosepaket mit dem Befehl sbs-diag gestartet werden.

Fortschrittliche Protokolle

Über die CLI können erweiterte Protokolle für die folgenden Services aktiviert werden:

SBS-Backend

sbs-burrow

sbs-marmotd

sbs-lsyncd-gather

sbs-lsynd-Communicate

sbs-gsyncd

sbs-and

sbs-aspisch

pxgrid-agent

Verwenden des Befehls sudo -i für den Zugriff auf den Root-Benutzermodus

Diese erweiterten Protokolle können das System mit Meldungen überfluten und dürfen daher nur bei der Arbeit mit dem TAC-Team verwendet werden.

Festplattenspeicher

- Sämtliche Daten, die von Sensoren eingehen und analysiert werden, werden in der Datenbank gespeichert.
- Überwachen Sie den verfügbaren Speicherplatz in der Partition /data mit dem Befehl df -h.
- Bereinigen Sie Ihre Netzwerkaufzeichnungen unter /data/tmp/captures/. Verwenden Sie den Befehl rm -rf /data/tmp/captures/*, um alle Captures zu löschen, wenn sie nicht mehr benötigt werden.
- Löschen Sie alle älteren Diagnosedateien.
- Löschen Sie alte und unerwünschte Daten in der Datenbank mit dem Befehl sbs-db purge-xxxxx.

Datenverkehrsvalidierung

Verwenden Sie iptables und TCPdump, um Ihren Datenverkehrsfluss zu verfolgen.

Firewall-Nachverfolgung

Iptables-Firewall ist auf dem Server aktiviert. Verworfene Pakete werden als "DropInput und DropForward" protokolliert.

Überprüfen Sie die iptables-Zähler, um verworfene Pakete darauf zu überprüfen (iptables -L -n -v) | grep Chain).

Suche nach verworfenen Paketen im Protokoll (journalctl | grep Drop).

TCP-Dump-Tool

Es kann zur Überwachung und Fehlerbehebung von Datenverkehr an der Netzwerkschnittstelle im Server verwendet werden.

Wenn der Datenverkehr überflutet wird, drücken Sie Strg+C, um die Erfassung zu stoppen.

Beispiele

So überwachen Sie NTP-Datenflüsse (UDP/TCP 123): tcpdump -i [ethX] Port 123 :

So überwachen Sie eingehenden/ausgehenden Datenverkehr von einem bestimmten Host: tcpdump -i [ethX] host 1.2.3.4

So speichern Sie die Aufzeichnung in einer pcap-Datei:

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.