Problemen oplossen en een Cyber Vision Center-server beheren

Inhoud

Inleiding

In dit document worden de verschillende stappen beschreven die kunnen worden genomen om een Cisco Cyber Vision Server te onderhouden, problemen op te lossen en te bewaken.

Cisco Cyber Vision geeft u een diepgaand beeld van uw beveiligingspositie op het gebied van operationele technologie (OT). Cyber Vision voedt uw IT-beveiligingshulpmiddelen met informatie over OT-middelen en -gebeurtenissen, waardoor het gemakkelijker wordt om risico's te beheren en beveiligingsbeleid in uw hele netwerk af te dwingen.

Server-updates

Houd de server up-to-date voor kwetsbaarheidsoplossingen, bugfixes en nieuwe functies die in de software worden geïntegreerd op basis van implementatiescenario's.

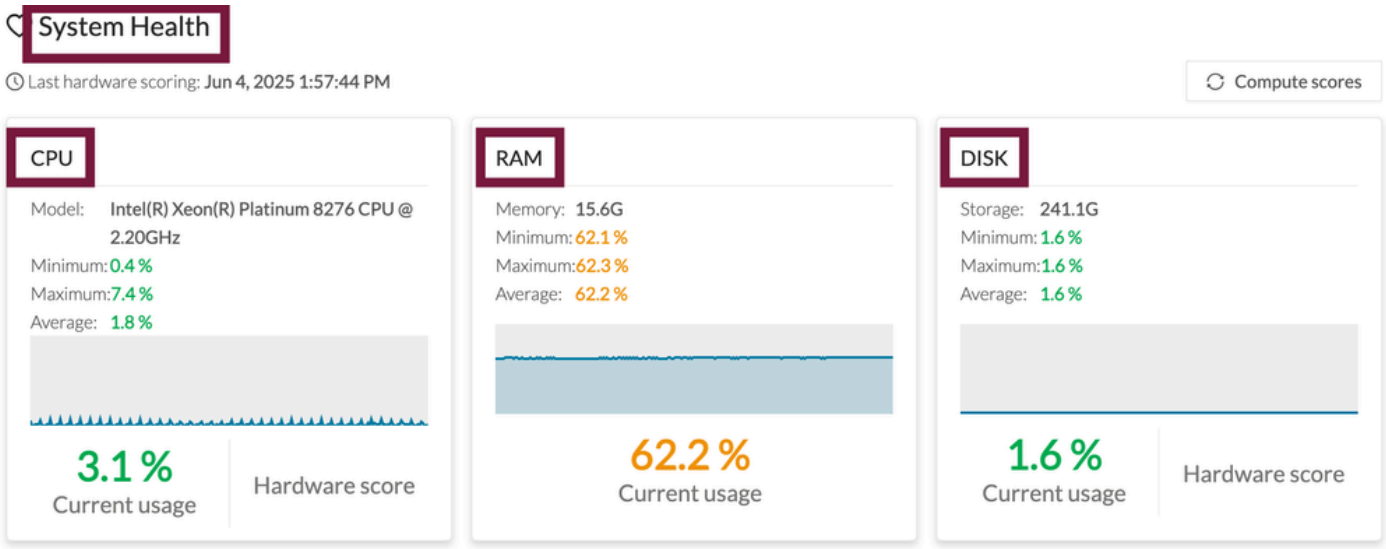
systeemgezondheid

- SNMPv3-traps configureren voor het verzenden van waarschuwingen over de systeemstatus

Vanaf de gebruikersinterface (om de historische waarde te controleren):

Navigeer naar System Statistics (Center of Sensors) en controleer het CPU- en RAM-gebruik.

- Sensoren rond 600% RAM en CPU 40% wordt verwacht dat ze in normale staat zijn.
- Centra ongeveer 80% RAM en CPU 50% wordt verwacht dat ze in normale staat zijn.



Deze waarden worden als referentie gebruikt. Deze middelen kunnen naar zeer hoge percentages gaan, maar zullen naar verwachting terugkomen na de voltooiing van een specifieke taak, maar zullen daar niet blijven.

Vanuit de CLI (real-time controle):

Gebruik de bovenste opdracht om het CPU- en RAM-gebruik te controleren om te begrijpen welke processen de bronnen verbruiken.

Het kan worden geverifieerd met behulp van het commando:

"TOP -N 1 -B" | HOOFD -N 5

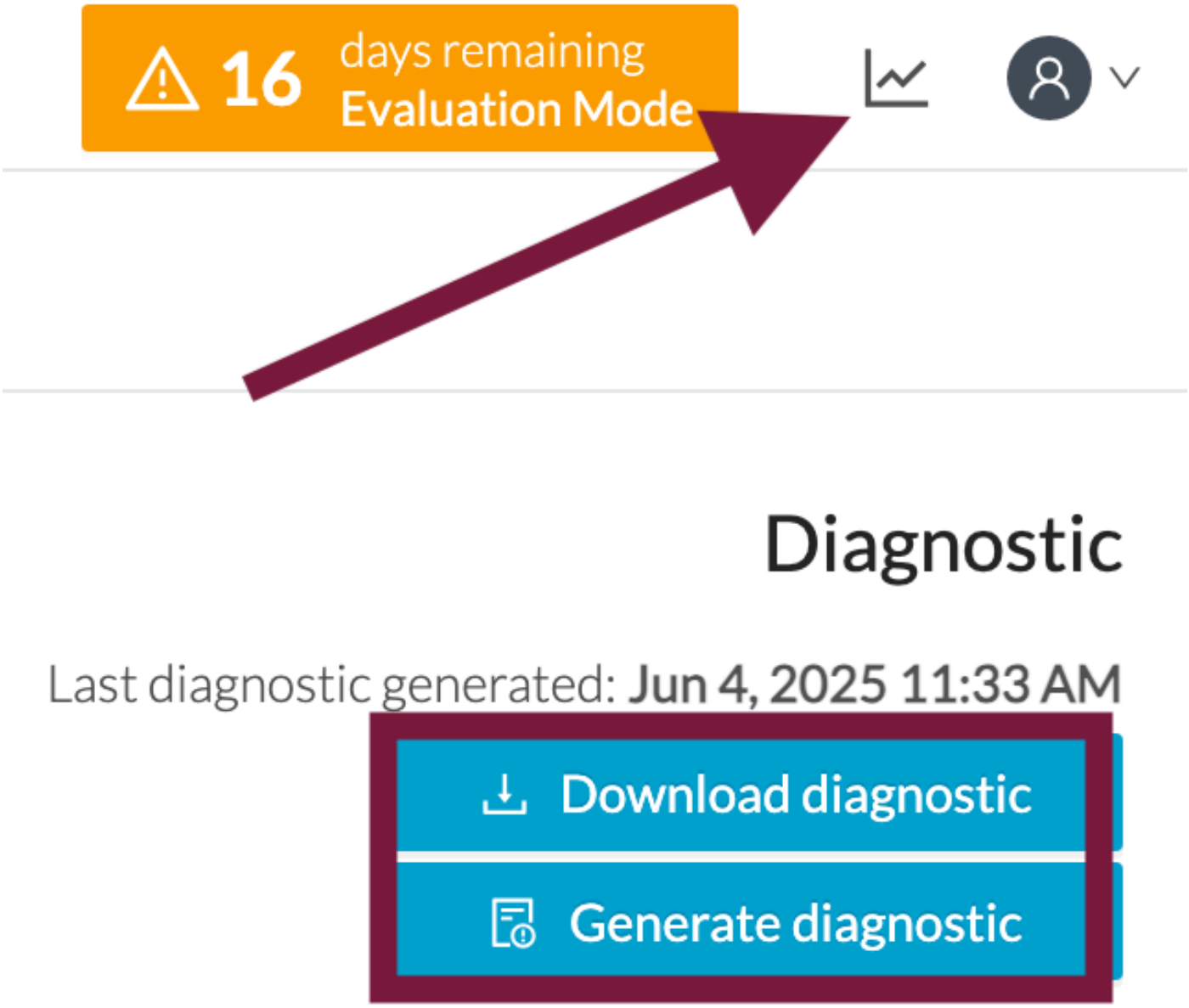
Verifieer systeemprocessen met de opdracht systemctl --failed. Deze opdracht wordt vaak gebruikt voor het oplossen van problemen om services of eenheden te identificeren die niet onverwacht zijn gestart of gestopt.

Systeemlogboeken

Er zijn verschillende logs beschikbaar op het platform:

Van de gebruikersinterface:

Genereer een diagnostisch bestand. Ga naar Systeemstatistieken (Centrum of Sensoren) en klik op Diagnostische gegevens genereren.



Vanuit de CLI:

Gebruik de opdracht sudo -i om toegang te krijgen tot de rootgebruikersmodus

Gebruik journalistieke opdrachten om systeemlogboeken bij te houden.

Journalctl -R (-R ✳ omgekeerd)

Journaal --sinds "2015-01-10" of --tot "2015-01-11 03:00"

Journalctl –u <naam proces>

Journaal -f (-f ✳ volgen)

Journalctl –PERR (fouten op systeem)

Ook kan de diagnosebundel worden gestart met behulp van de opdracht sbs-diag

Geavanceerde logs

Geavanceerde logboeken kunnen worden geactiveerd vanuit CLI voor deze services:

SBS-backend

SBS-Burrow

SBS-Marmotd

SBS-lsyncd-gather

SBS-LSYND-Communiceren

SBS-GSYNCD

SBS-NAD

SBS-ASPIC

parametrisch agens

Gebruik de opdracht sudo -i om toegang te krijgen tot de rootgebruikersmodus

Deze geavanceerde logboeken kunnen het systeem echt overspoelen met berichten, daarom moet het alleen worden gebruikt bij het werken met het TAC-team.

schijfruimte

- Alle gegevens die binnenkomen en geanalyseerd worden door Sensors opgeslagen in de database.
- Bewaak de beschikbare ruimte in de /data partitie met behulp van de opdracht df -h.
- Maak uw netwerkopnamen schoon onder /data/tmp/opnamen/. Gebruik de opdracht rm -rf /data/tmp/captures/* om alle opnamen te verwijderen als ze niet langer nodig zijn.
- Verwijder alle oudere diagnosebestanden.
- Verwijder oude en ongewenste gegevens in de database met de opdracht sbs-db purge-xxxxx.

verkeersvalidatie

Gebruik iptables en TCPdump om uw verkeersstroom te volgen.

Firewall bijhouden

De firewall van Iptables is ingeschakeld op de server. Gedropte pakketten worden geregistreerd als "DropInput en DropForward".

Verifieer iptables-tellers om gedropte pakketten erop te controleren (iptables –L –n –v | grep

Chain).

Zoek naar verloren pakketten in het logboek (journal | grep Drop).

TCPdump, gereedschap

Het kan worden gebruikt voor het observeren en oplossen van problemen op de netwerkinterface in de server.

Als het verkeer overstroomt, drukt u op ctrl+c om de opname te stoppen.

Voorbeelden

NTP-stromen bewaken (UDP/TCP 123): tcpdump –i [ethX] poort 123:

Om inkomend/uitgaand verkeer van een specifieke host te bewaken: tcpdump –i [ethX] host 1.2.3.4

U slaat de opname als volgt op in een pcap-bestand:

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.