Troubleshoot and Manage a Cyber Vision Center Server

Contents

Introduction

This document describes the various steps that can be taken to maintain, troubleshoot, and monitor a Cisco Cyber Vision Server.

Cisco Cyber Vision gives you an in-depth view of your operational technology (OT) security posture. Cyber Vision feeds your IT security tools with information on OT assets and events, making it easier to manage risks and enforce security policies throughout your network.

Server Updates

Keep the server updated for vulnerability fixes, bug fixes and new features that get integrated to the software based on deployment scenarios.

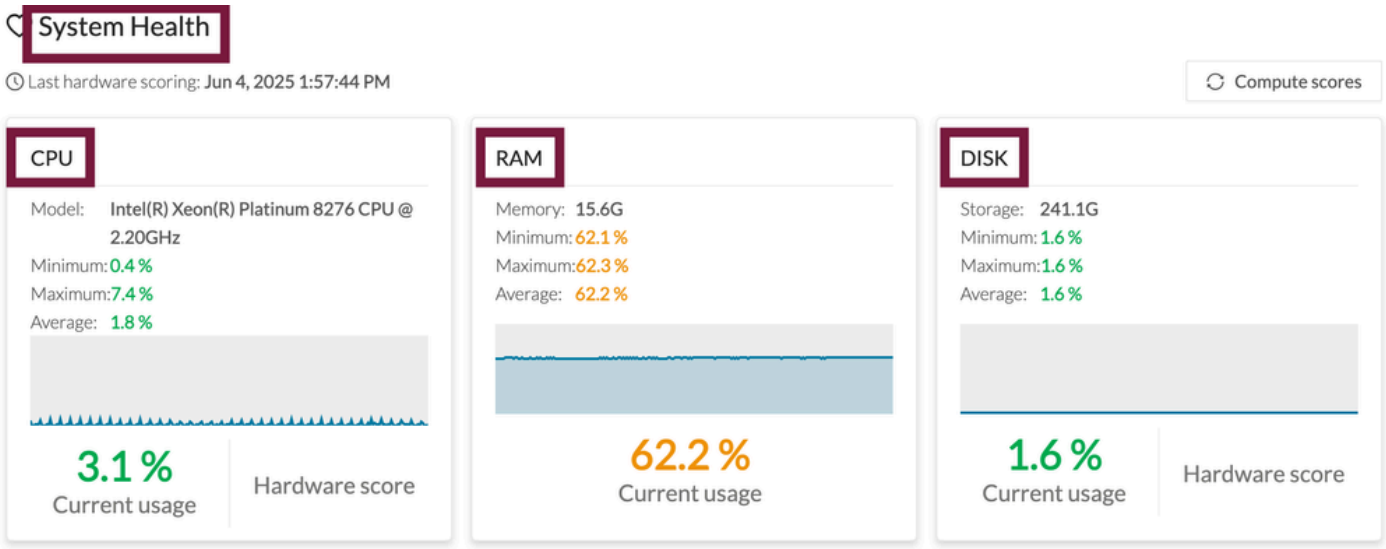
System Health

- Configure SNMPv3 traps to send system health alerts

From the UI (to check historic value):

Navigate to System Statistics (Center or Sensors) and to verify the CPU and RAM utilization.

- Sensors around 600% RAM and CPU 40% are expected to be in normal condition.
- Centers around 80% RAM and CPU 50% are expected to be in normal condition.



These are values used as a reference. These resources can go to very high percentages but are expected to come back after the completion of specific task but not remain there.

From the CLI (real-time check):

Use the top command to check CPU and RAM utilization to understand which processes are consuming the resources.

It could be verified using the command:

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

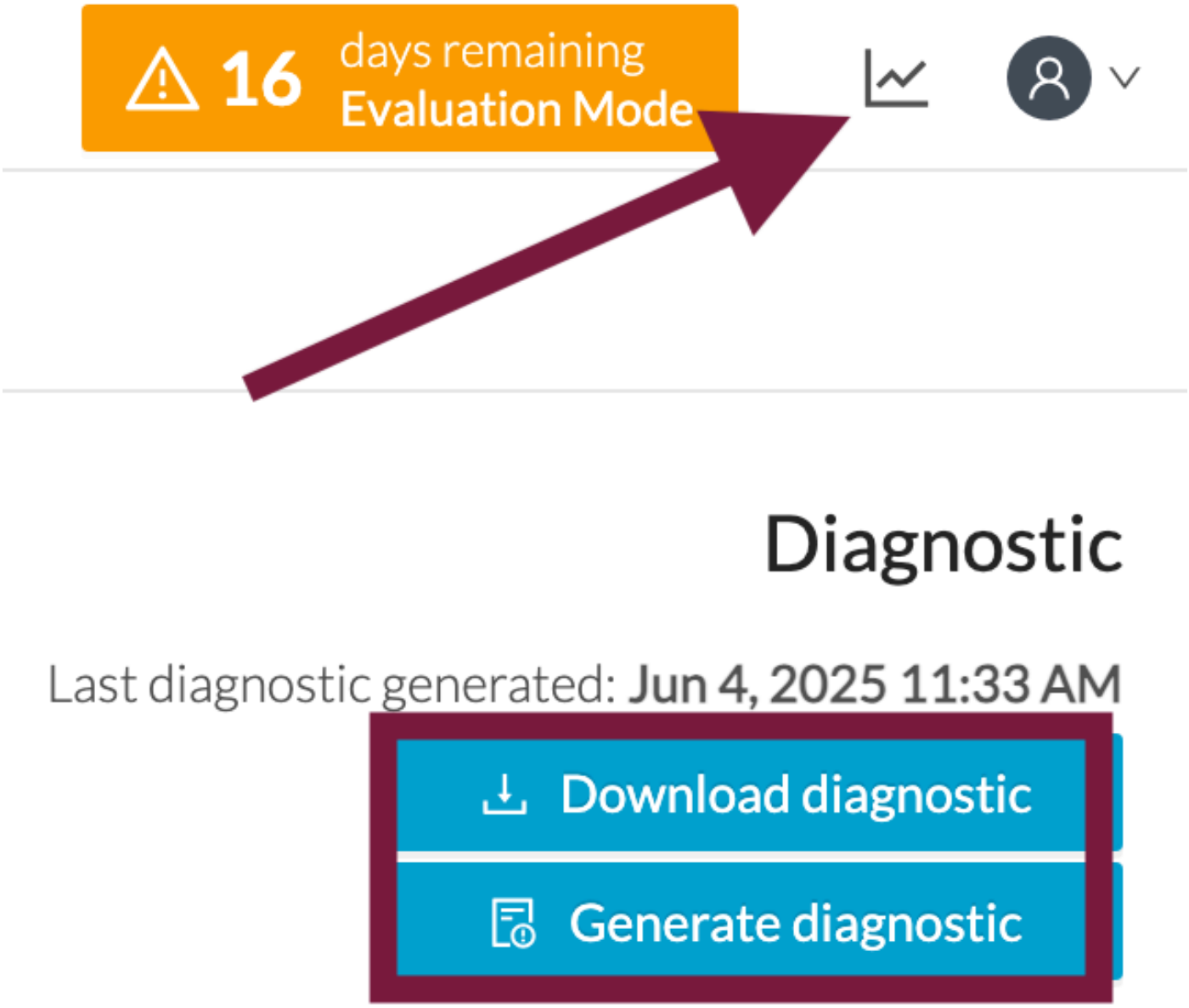
Verify system processes using the command systemctl --failed command. This command is commonly used for troubleshooting purposes to identify services or units that did not start or stopped unexpectedly.

System logs

Several logs are available on the platform:

From the UI:

Generate a diagnostic file. Go to System Statistics (Center or Sensors) and click on Generate Diagnostic.



From the CLI:

Use sudo -i command to access root user mode

Use journaltcl commands to track system logs.

journalctl -r (-r ✳ reverse)

journalctl --since "2015-01-10“ or --until "2015-01-11 03:00"

journalctl –u <process name>

journalctl -f (-f ✳▪ follow)

journalctl –p err (errors on system)

Also, the diagnostics bundle can be launched using the command sbs-diag

Advanced logs

Advanced logs can be activated from CLI for these services:

sbs-backend

sbs-burrow

sbs-marmotd

sbs-lsyncd-gather

sbs-lsynd-communicate

sbs-gsyncd

sbs-nad

sbs-aspic

pxgrid-agent

Use sudo -i command to access root user mode

These advanced logs can really flood the system with messages, hence, must only be used when working with the TAC team.

Disk Space

- All the data coming in and analyzed by Sensors are stored into the database.
- Monitor the available space in the /data partition using the command df -h.
- Clean up your network captures under /data/tmp/captures/. Use the command rm -rf /data/tmp/captures/* to delete all captures if they are no longer needed.
- Delete all older diagnostic files.
- Purge old & undesired data in the database using the command sbs-db purge-xxxxx.

Traffic Validation

Using iptables and TCPdump to follow your traffic flow.

Firewall Tracking

Iptables firewall is enabled on the server. Dropped packets are logged as “DropInput and DropForward”.

Verify iptables counters to check dropped packets on it (iptables –L –n –v | grep Chain).

Look for dropped packets in the log (journalctl | grep Drop).

TCPdump tool

It can be used for observing & troubleshooting traffic on the network interface in the server.

If the traffic gets flooded, press ctrl+c to stop the capture.

Examples

To monitor NTP flows (UDP/TCP 123): tcpdump –i [ethX] port 123 :

To monitor incoming/outgoing traffic from a specific host: tcpdump –i [ethX] host 1.2.3.4

To save the capture into a pcap file:

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