排除故障和管理網路Vision Center伺服器

目錄

簡介

本檔案介紹維護、疑難排解和監控Cisco Cyber Vision伺服器可以採取的各種步驟。

Cisco Cyber Vision可讓您深入瞭解您的運營技術(OT)安全狀況。Cyber Vision向您的IT安全工具提供有關OT資產和事件的資訊，從而更輕鬆地在整個網路中管理風險和實施安全策略。

伺服器更新

根據部署方案保持伺服器更新，以查詢漏洞修復、漏洞修復以及整合到軟體的新功能。

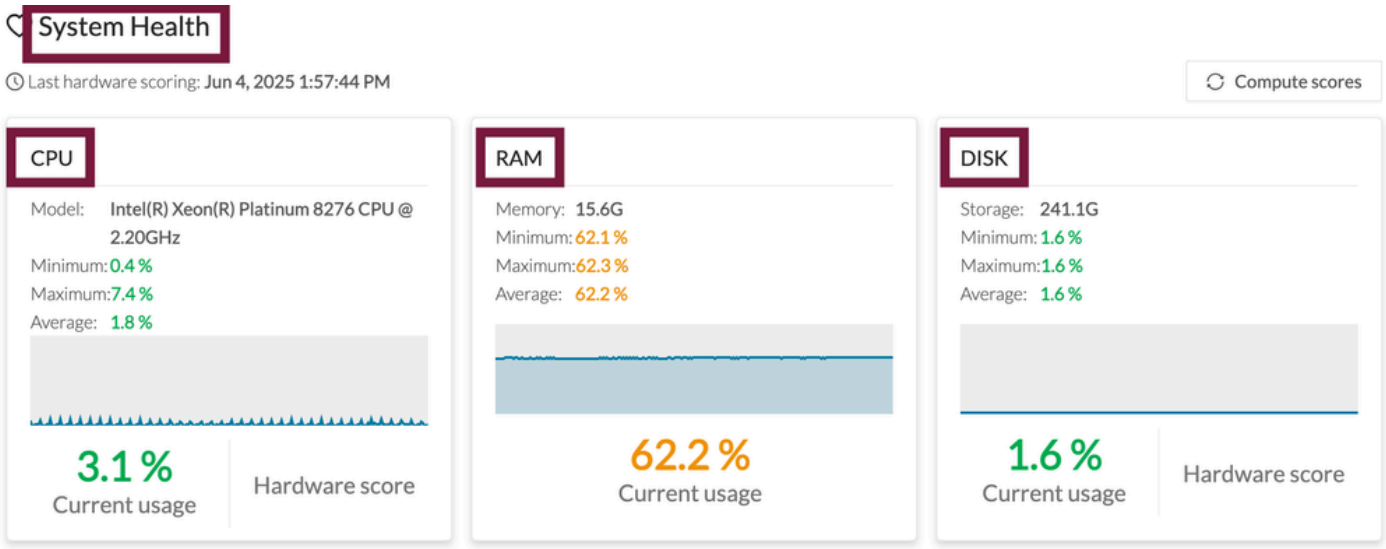
系統運行狀況

- 配置SNMPv3陷阱以傳送系統運行狀況警報

在UI中（檢查歷史值）：

導航到System Statistics（Center或Sensors）(系統統計資訊（中心或感測器）)並驗證CPU和RAM利用率。

- 600%RAM和40%CPU的感測器應處於正常狀態。
- 中心約80%的RAM和50%的CPU應處於正常狀態。



這些值用作參考。這些資源可以達到很高的百分比，但預計在完成特定任務後返回，但不會保留在那裡。

在CLI上（即時檢查）：

使用top命令檢查CPU和RAM利用率，以瞭解哪些進程正在佔用資源。

可以使用以下命令進行驗證：

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

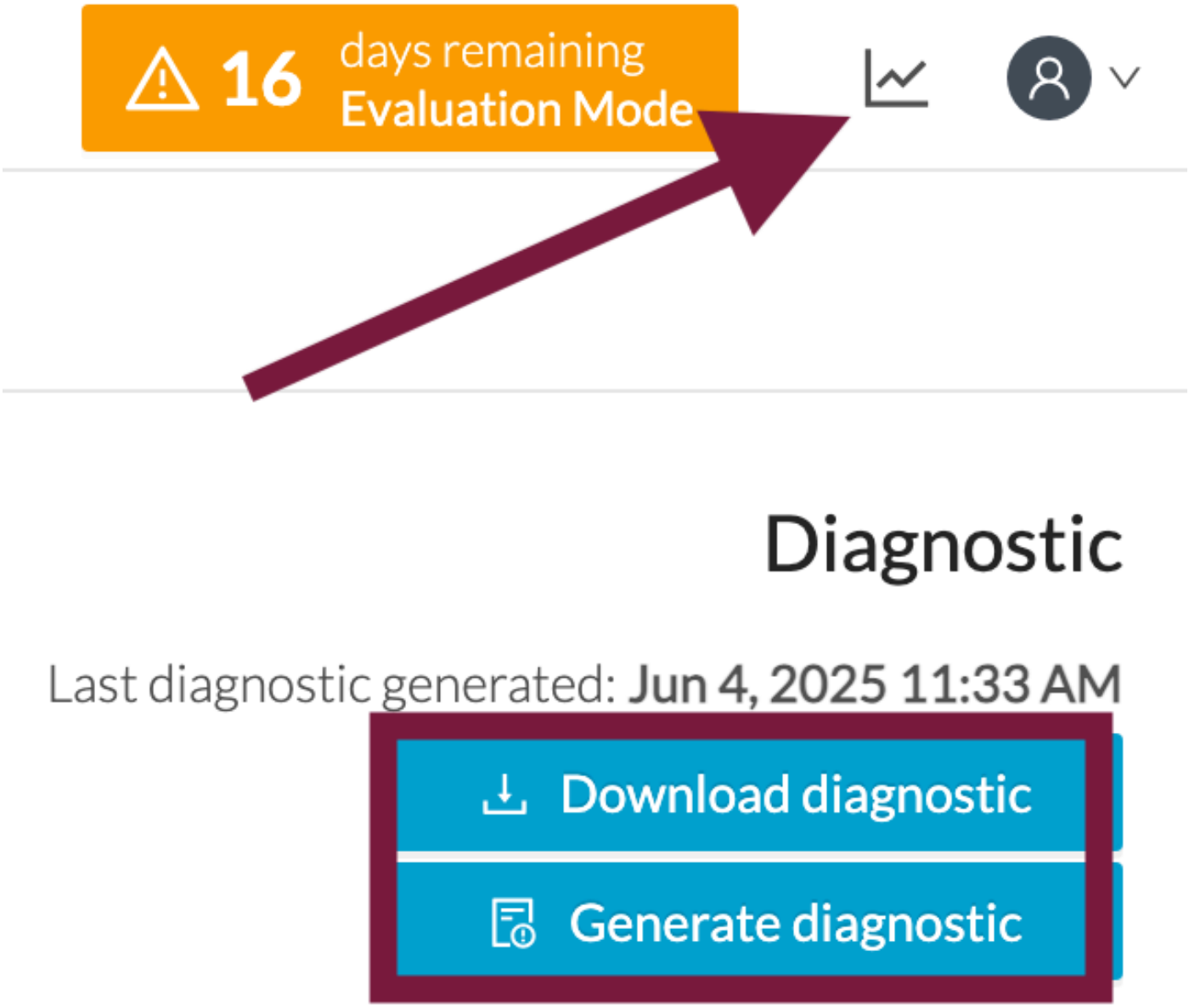
使用命令systemctl —failed命令驗證系統進程。此命令通常用於故障排除，以識別未意外啟動或停止的服務或裝置。

系統記錄

平台上有多個日誌：

在UI中：

生成診斷檔案。轉至System Statistics（Center或Sensors），然後點選Generate Diagnostic。



在CLI上：

使用sudo -i命令訪問根使用者模式

使用journaltcl命令跟蹤系統日誌。

journalctl -r(-r✳反向)

journalctl — 自「2015-01-10」或 — 至「2015-01-11 03:00」

journalctl -u <進程名稱>

journalctl -f(-f✳關注)

journalctl -p err（系統上的錯誤）

此外，還可以使用命令sbs-diag啟動診斷捆綁包

高級日誌

可以從CLI為這些服務啟用高級日誌：

sbs-backend

sbs-burrow

sbs-marmotd

sbs-lsyncd-gather

sbs-lsynd-communicate

sbs-gsyncd

sbs-nad

sbs-aspic

pxgrid-agent

使用sudo -i命令訪問根使用者模式

這些高級日誌確實會向系統傳送大量消息，因此，僅當與TAC團隊合作時才必須使用。

磁碟空間

- Sensors（感測器）傳入和分析的所有資料都儲存在資料庫中。
- 使用命令df -h監控/data分割槽中的可用空間。
- 在/data/tmp/captures/下清除網路捕獲。如果不再需要所有捕獲，請使用命令rm -rf /data/tmp/captures/*將其刪除。
- 刪除所有較舊的診斷檔案。
- 使用sbs-db purge-xxxxx命令清除資料庫中的舊資料和不需要的資料。

流量驗證

使用iptables和TCPdump跟蹤您的流量。

防火牆追蹤

伺服器上啟用了Iptables防火牆。丟棄的資料包將記錄為「DropInput and DropForward」。

驗證iptables計數器以檢查其上丟棄的資料包(iptables -L -n -v) | grep Chain)。

在日誌中查詢丟棄的資料包(journalctl) | grep Drop)。

TCPdump工具

它可用於觀察和排除伺服器中網路介面上的流量。

如果流量泛洪，請按ctrl+c停止捕獲。

範例

要監控NTP流(UDP/TCP 123):tcpdump -i [ethX]埠123 :

要監控來自特定主機的傳入/傳出流量，請執行以下操作：tcpdump -i [ethX]主機1.2.3.4

要將捕獲儲存到pcap檔案，請執行以下操作：

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。