排除故障并管理Cyber Vision Center服务器

目录

简介

本文档介绍维护、故障排除和监控Cisco Cyber Vision Server可以采取的各种步骤。

Cisco Cyber Vision可让您深入了解运营技术(OT)的安全状态。Cyber Vision向IT安全工具提供有关OT资产和事件的信息，从而更轻松地在整个网络中管理风险和实施安全策略。

服务器更新

根据部署场景不断更新服务器，以查找漏洞修复、漏洞修复以及集成到软件的新功能。

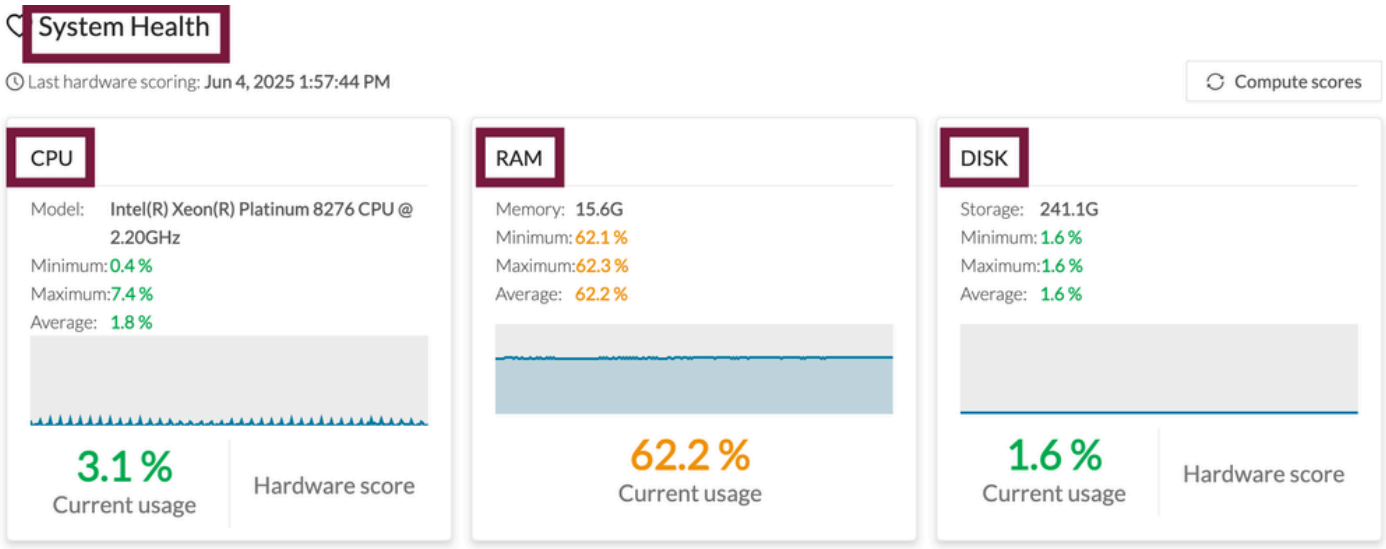
系统运行状况

- 配置SNMPv3陷阱以发送系统运行状况警报

从UI（检查历史值）：

导航到System Statistics(Center or Sensors)(系统统计信息（中心或传感器）并验证CPU和RAM利用率。

- RAM为600%、CPU为40%的传感器预计为正常状态。
- 中心约80%的RAM和50%的CPU应处于正常状态。



这些值用作参考。这些资源所占百分比可能非常高，但预计会在特定任务完成之后返回，但不会继续保留。

从CLI（实时检查）：

使用top命令检查CPU和RAM利用率，以了解哪些进程正在消耗资源。

可以使用以下命令进行验证：

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

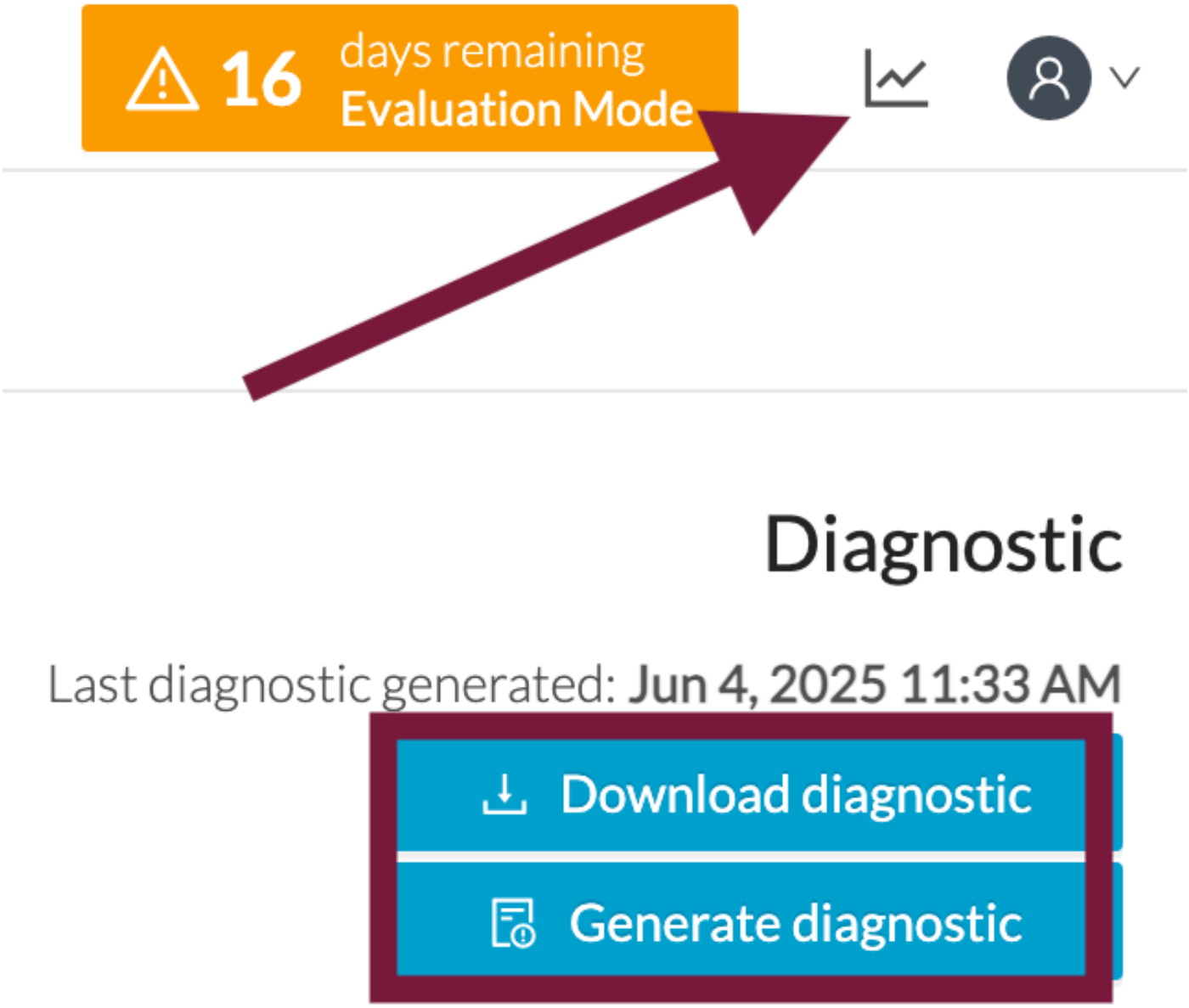
使用命令systemctl —failed验证系统进程。此命令通常用于故障排除目的，以识别未意外启动或停止的服务或设备。

系统日志

平台上有多个日志：

在UI中：

生成诊断文件。转至System Statistics(Center or Sensors)，然后点击Generate Diagnostic。



从 CLI：

使用sudo -i命令访问根用户模式

使用journaltcl命令跟踪系统日志。

journalctl -r(-r✳反向)

journalctl — 自“2015-01-10”或 — 直到“2015-01-11 03:00”

journalctl -u <进程名称>

journalctl -f(-f✳跟随)

journalctl -p err（系统上的错误）

此外，可以使用命令sbs-diag启动诊断捆绑包

高级日志

可以从CLI为这些服务激活高级日志：

sbs-backend

sbs-burrow

sbs-marmotd

sbs-lsyncd-gather

sbs-lsynd-communicate

sbs-gsyncd

sbs-nad

sbs-aspic

pxgrid-agent

使用sudo -i命令访问根用户模式

这些高级日志确实会向系统发送大量消息，因此只有在与TAC团队合作时才能使用。

磁盘空间

- 传感器传入和分析的所有数据都存储在数据库中。
- 使用命令df -h监控/data分区中的可用空间。
- 在/data/tmp/captures/下清除网络捕获。如果不再需要所有捕获，请使用命令rm -rf /data/tmp/captures/*将其删除。
- 删除所有旧的诊断文件。
- 使用命令sbs-db purge-xxxxx清除数据库中的旧数据和不需要的数据。

流量验证

使用iptables和TCPdump跟踪流量。

防火墙跟踪

Iptables防火墙在服务器上启用。丢弃的数据包记录为“DropInput and DropForward”。

验证iptables计数器以检查其上丢弃的数据包(iptables -L -n -v | grep Chain)。

在日志中查找丢弃的数据包(journalctl) | grep Drop)。

TCPdump工具

它可用于观察和排除服务器中网络接口上的流量。

如果流量泛洪，请按ctrl+c停止捕获。

Examples

要监控NTP流量(UDP/TCP 123)，请执行以下操作：tcpdump -i [ethX]端口123 :

要监控来自特定主机的传入/传出流量，请执行以下操作：tcpdump -i [ethX] host 1.2.3.4

要将捕获保存到pcap文件，请执行以下操作：

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。