Cyber Vision Center Serverのトラブルシューティングと管理

内容

はじめに

このドキュメントでは、Cisco Cyber Vision Serverのメンテナンス、トラブルシューティング、および監視に使用できるさまざまな手順について説明します。

Cisco Cyber Visionでは、運用テクノロジー(OT)のセキュリティポスチャを詳細に把握できます。 Cyber Visionは、OT資産やイベントに関する情報をITセキュリティツールに提供し、ネットワーク全体のリスク管理とセキュリティポリシーの適用を容易にします。

サーバの更新

導入シナリオに基づいてソフトウェアに統合される脆弱性修正、バグ修正、および新機能について、サーバを常に最新の状態に保ちます。

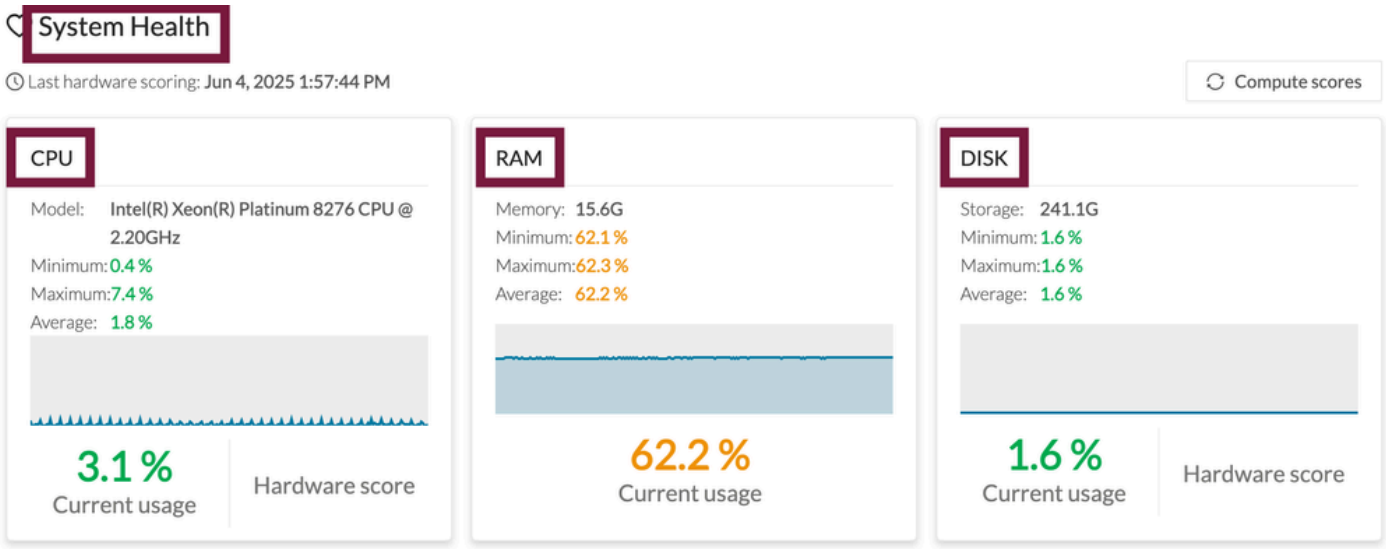
システムヘルス

- システムのヘルスアラートを送信するためのSNMPv3トラップの設定

UIから（履歴値を確認するため）:

System Statistics（CenterまたはSensors）に移動し、CPUとRAMの使用率を確認します。

- 600%のRAMと40%のCPUの周りのセンサーは正常な状態にあると予想されます。
- センターの約80 %のRAMと50 %のCPUは正常な状態であると予想されます。



これらは参照として使用される値です。これらのリソースは非常に高い割合で使用される可能性がありますが、特定のタスクが完了した後に戻ってくることが予想されますが、残りません。

CLIから（リアルタイムチェック）:

topコマンドを使用してCPUとRAMの使用率をチェックし、どのプロセスがリソースを消費しているかを把握します。

これは、次のコマンドを使用して確認できます。

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

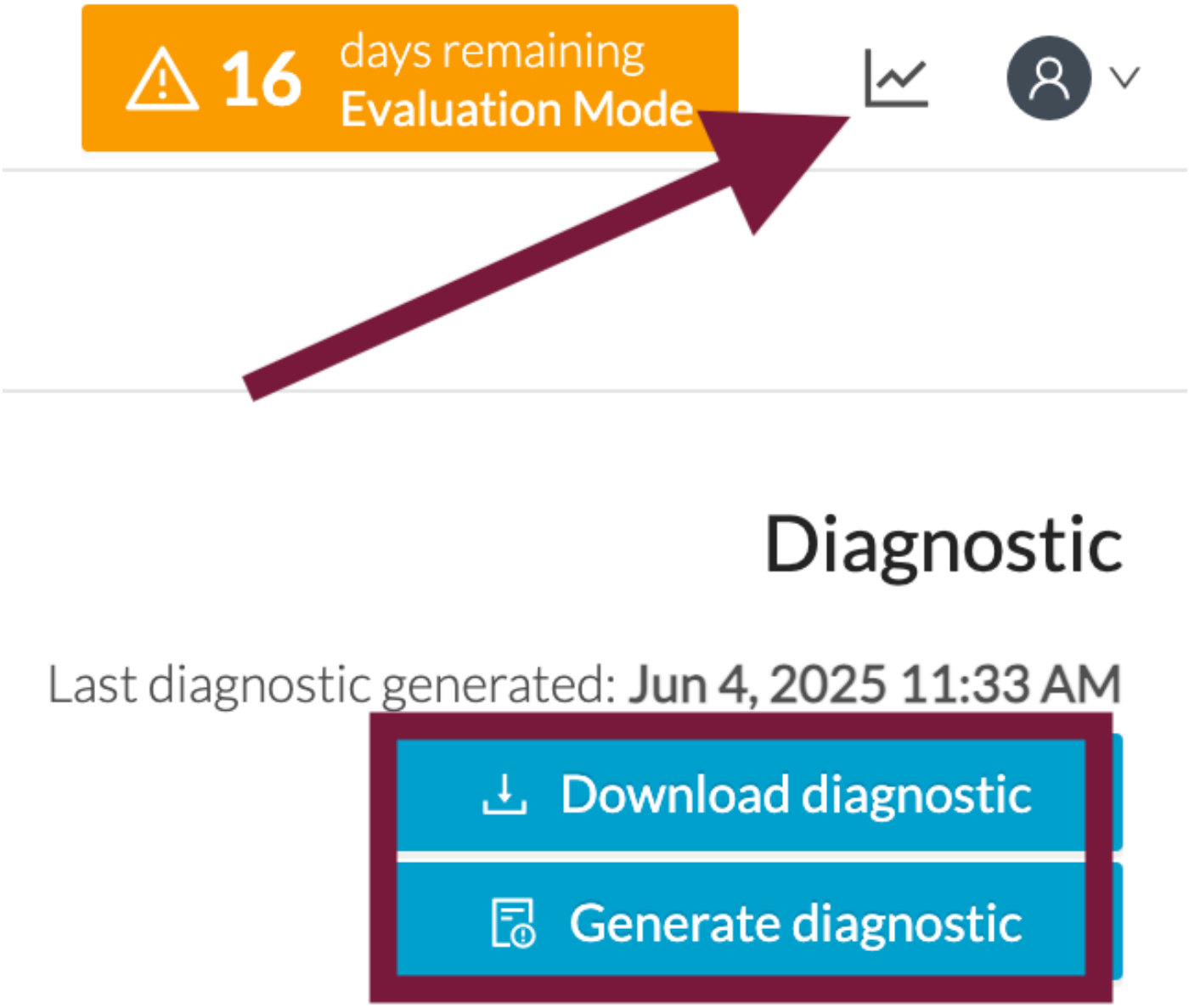
コマンドsystemctl —failedを使用して、システムプロセスを確認します。このコマンドは、通常、予期せず開始または停止しなかったサービスまたはユニットを特定するために、トラブルシューティングの目的で使用されます。

システム ログ

プラットフォームでは、次のログを使用できます。

UIから：

診断ファイルを生成します。System Statistics (Center or Sensors)に移動し、Generate Diagnosticをクリックします。



CLI から、

sudo -iコマンドを使用して、rootユーザモードにアクセスします

journaltclコマンドを使用して、システムログを追跡します。

journalctl -r (-r ✳　reverse)

journalctl —since "2015-01-10"または – until "2015-01-11 03:00"

journalctl -u <プロセス名>

journalctl -f (-f✳続く)

journalctl -p err (システム上のエラー)

また、診断バンドルは、sbs-diagコマンドを使用して起動することもできます

詳細ログ

詳細なログは、CLIから次のサービスに対してアクティブ化できます。

sbsバックエンド

SBSバロウ

sbs-marmotd

sbs-lsyncd-gather（収集）

sbs-lsynd-communicate（非同期コミュニケーション）

SBS-GSYNCD

sbs-nad

SBSアスピック

PXGRIDエージェント

sudo -iコマンドを使用して、rootユーザモードにアクセスします

これらの高度なログは、実際にシステムにメッセージをフラッディングさせる可能性があるため、TACチームと連携する場合にのみ使用する必要があります。

ディスク領域

- センサーが受信して分析したすべてのデータは、データベースに保存されます。
- df -hコマンドを使用して、/dataパーティション内の使用可能な領域を監視します。
- /data/tmp/captures/でネットワークキャプチャをクリーンアップします。不要になったキャプチャをすべて削除するには、rm -rf /data/tmp/captures/*コマンドを使用します。
- 古い診断ファイルをすべて削除します。
- sbs-db purge-xxxxxコマンドを使用して、データベース内の古いデータと不要なデータを消去します。

トラフィックの検証

iptablesとTCPdumpを使用してトラフィックフローを追跡します。

ファイアウォール追跡

Iptablesファイアウォールがサーバーで有効になっています。ドロップされたパケットは「DropInput and DropForward」として記録されます。

iptablesカウンタを確認し、そのカウンタでドロップされたパケットを確認します(iptables -L -n -v | grep Chain)。

ログでドロップされたパケットを探します(journalctl | grep Drop)。

TCPdumpツール

サーバのネットワークインターフェイス上のトラフィックの監視とトラブルシューティングに使用できます。

トラフィックがフラッディングされた場合は、Ctrl+Cを押してキャプチャを停止します。

例

NTPフロー(UDP/TCP 123)を監視するには、tcpdump -i [ethX] port 123 :

特定のホストからの着信/発信トラフィックを監視するには、tcpdump -i [ethX] host 1.2.3.4

キャプチャをpcapファイルに保存するには、次の手順を実行します。

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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。