XDRデバイスの洞察とセキュアなエンドポイントの統合のトラブルシューティング

内容

概要

このドキュメントでは、統合を設定し、Device InsightsとSecure Endpointの統合をトラブルシューティングする手順について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

XDR Device Insightsは、組織内のデバイスの統合ビューを提供し、セキュアエンドポイントなどの統合データソースからのインベントリを統合します。

XDR Device Insightsを使用すると、すべてのソースからの情報が統合され、XDR内のデバイスインサイトに表示されます。すべてのデバイス情報を全体的に表示し、データソースのポートフォリオ全体のデバイスをより効率的に調査する簡単な方法です。

有効化されると、デバイスインサイトは、XDRと統合したモジュールからインベントリとデバイ

スデータを自動的に取得する準備が整います。そのため、XDRと統合されたモジュールがすでに存在する場合、この機能を使用するためにモジュールを削除したり再度追加したりする必要はありません。

設定の詳細については、『Cisco XDRコンフィギュレーションモジュール』を参照してください。

トラブルシュート

このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。

セキュアエンドポイントモジュールの追加

- モジュールを有効にするユーザには、製品を統合するための管理者権限が必要です。

注：新しいソースを統合する場合は、手動で同期を行うか、自動同期が行われるのを待ってから、インベントリにレポートされるデバイスを確認する必要があります。

接続の確認

API接続を許可するには、使用している環境で次のFQDNが許可されていることを確認します。

- api.amp.cisco.com
- api.apjc.amp.cisco.com
- api.eu.am p.cisco.com

ユーザPostmanによる接続テスト

https://<AMP API地域FQDN>/v1/computers

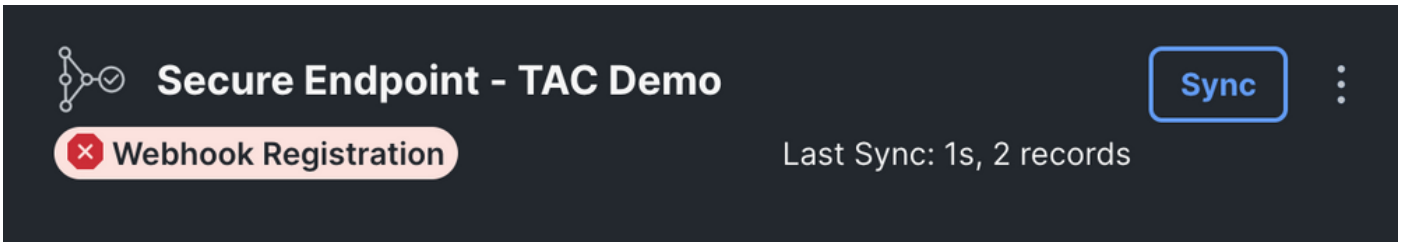
https://< AMP API地域FQDN>/v1/computers/<コネクタGUID>

注：セキュアエンドポイントは、認可方式として基本認証を使用します。

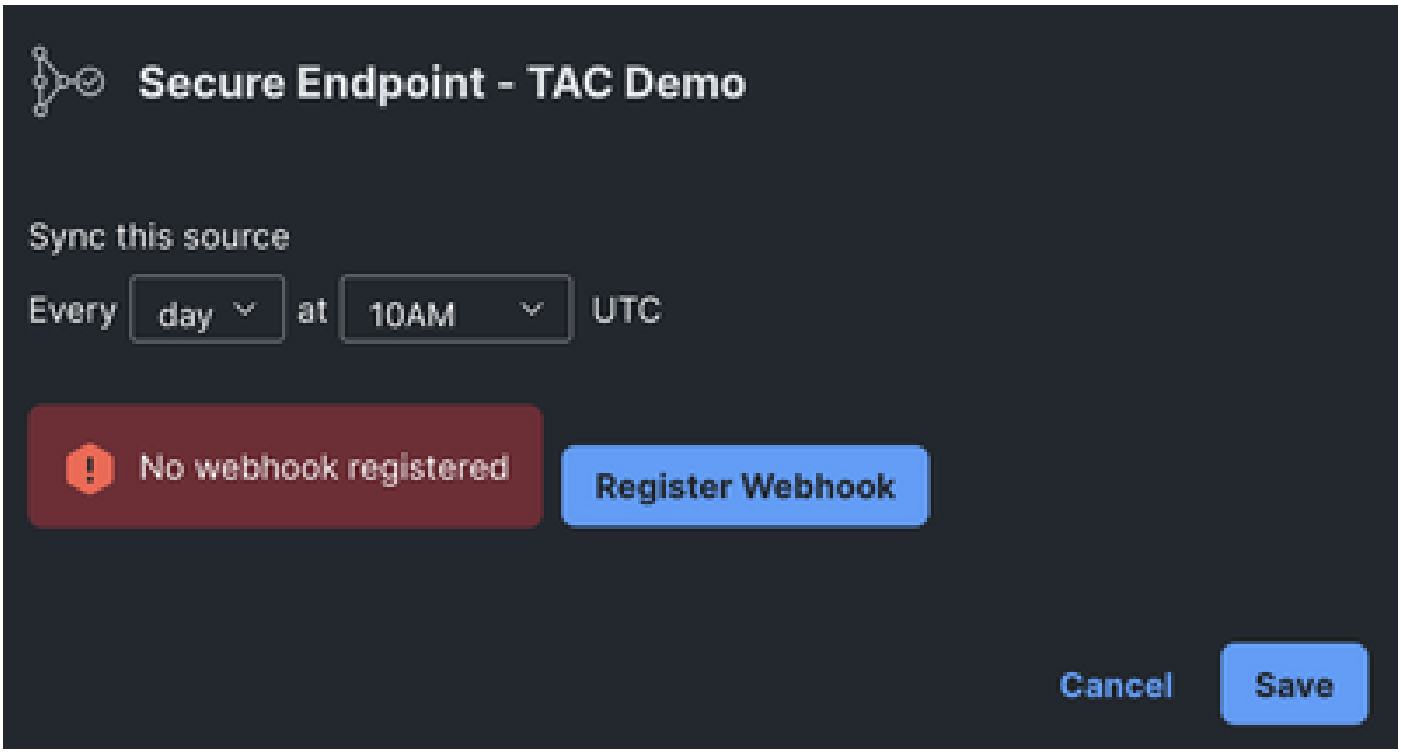
デバイス番号の不一致

- Device Insightsは過去90日間の情報を保存しますが、Secure Endpointは30日間の情報を保存します。デバイスの数が一致しない場合は、関係するコンピュータの最後の画面が90日を超えていないことを確認します。
- セキュアエンドポイントコンソールに、両方のコンソールで不一致を引き起こす重複したコネクタがないことを確認します。

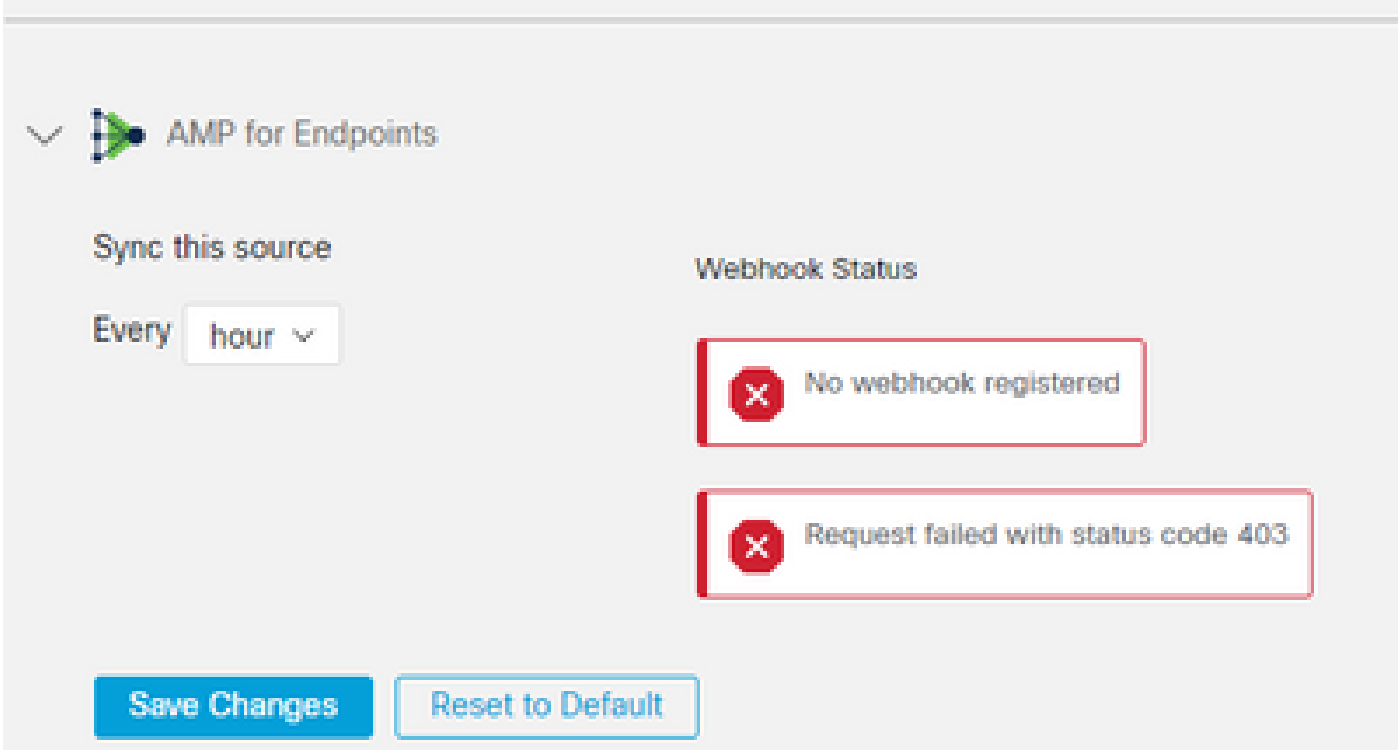
シナリオ 1.Webhook登録なし



Source Settingに移動し、Register Webhookボタンをクリックします。要求が実行されると、図に示すようにWebhookのステータスが表示されます。



シナリオ 2.HTTPエラー。



400 – 正しくない要求

401 – 許可されていません

403 – 禁止

404 – メソッドは許可されていません

HTTPエラーの場合は、設定されているAPIクレデンシャルを確認し、収集した情報がXDRのモジュール設定に貼り付けられた情報と一致することを確認します。

ブラウザの問題

Device Insightsに誤ったデータが表示された場合は、別のブラウザまたはプライベートウィンドウでテストを行い、誤ったブラウザキャッシュまたは古いブラウザキャッシュを破棄します。

複数組織の問題

Secure Endpoint統合モジュールは、Enableボタンを使用します。そのため、現在、セキュアエンドポイントは1つのセキュアエンドポイントコンソールにのみリンクできますが、ユーザがこれらの組織の管理者である場合は、1つのXDRで複数のセキュアエンドポイントモジュールをリンクできます。つまり、複数のセキュアエンドポイント組織の管理者は、1つのXDRダッシュボードのAPIモジュールを介してこれらすべてをリンクできます。セキュアエンドポイントコンソールが別のXDR組織にまだ統合されていないことを確認します。

XDRポータルは複数のSecure Endpointインスタンスを統合できますが、Secure Endpointは1つのXDRインスタンスにのみ統合できます。

HARログ

Device Insightsとセキュアエンドポイントの統合で問題が解決しない場合は、「XDRコンソールからのHAR口グの収集」でブラウザからHAR口グを収集する方法を確認し、TACサポートに連絡して、より詳細な分析を実行してください。

関連情報

- XDR口グイン（ドキュメント）
- テクニカル サポートとドキュメント - Cisco Systems

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。