次のステップ

次のステップ

セキュリティ分析とロギング（オンプレミス） の一部として syslog イベントデータを Secure Network Analytics アプライアンスに渡すようにファイアウォール展開を設定したら、次の手順を実行できます。

- Management Center オンラインヘルプを確認します。
- Secure Network Analytics の詳細については、マネージャ Web アプリケーションのオンラインヘルプを参照してください。

Secure Network Analytics アプライアンスに保存されている接続イベントを使用した Management Center での作業

デバイスがセキュリティ分析とロギング（オンプレミス） を使用して Secure Network Analytics アプライアンスに接続イベントを送信している場合、management center のイベントビューアとコンテキストエクスプローラでリモートに保存されたイベントを表示および操作し、レポートの生成時にそれらのイベントを含めることができます。management center のイベントから相互起動して、Secure Network Analytics アプライアンスの関連データを表示することもできます。

デフォルトでは、指定した時間範囲に基づいて適切なデータソースが自動的に選択されます。データソースをオーバーライドする場合は、次の手順を使用します。

重要 データソースを変更すると、選択した内容は、サインアウト後でも、変更するまでは、イベントデータソース（レポートを含む）に依存するすべての関連する分析機能で維持されます。選択した内容は他の management center ユーザーには適用されません。

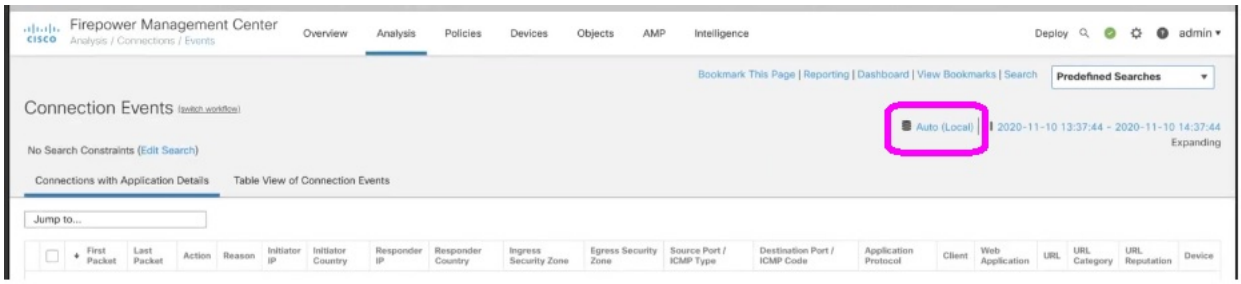
選択したデータソースは、優先順位の低い接続イベントにのみ使用されます。他のすべてのイベントタイプ（侵入、ファイル、マルウェアイベント、それらのイベントに関連付けられた接続イベント、およびセキュリティ インテリジェンス イベント）は、データソースに関係なく表示されます。

始める前に

ウィザードを使用して接続イベントを セキュリティ分析とロギング（オンプレミス） に送信しました。

ステップ 1 management center Web インターフェイスで、接続イベントデータを表示するページ（[Analysis] > [Connections] > [Events] など）に移動します。

ステップ 2 ページに表示されるデータソースをクリックし、オプションを選択します。



注意 [Local] を選択すると、ローカルデータが選択した時間範囲全体で使用できない場合でも、management center で使用可能なデータのみ表示されます。この状況が発生していることは通知されません。

ステップ 3 （任意）Secure Network Analytics アプライアンスで関連データを直接表示するには、IP アドレスやドメインなどの値を右クリック（統合イベントビューアでクリック）し、相互起動オプションを選択します。

相互起動を使用したイベントの調査

Management Center でイベントを表示しているときに、特定のイベントデータ（たとえば、IP アドレス）を右クリックして、マネージャ で関連するデータを表示できます。

ステップ 1 Management Center でイベントが表示される次のページのいずれかに移動します。

- ダッシュ ボード（[概要（Overview）] > [ダッシュボード（Dashboards）]）、または

- イベントビューアページ（イベントのテーブルが含まれている [分析（Analysis）] メニューにあるオプション）

ステップ 2 対象のイベントフィールドを右クリックして、セキュリティ分析とロギング（オンプレミス）相互起動リソースを選択します。別のブラウザウィンドウに マネージャ が開きます。まだログインしていない場合は、ユーザー名とパスワードの入力を求められることがあります。クエリを実行するデータの量、マネージャ の速度と需要によってはクエリが処理されるまでに時間がかかる場合があります。

ステップ 3 マネージャ にサインインします。