外部 Syslog サーバにアラートを送信するための FireSIGHT システムの設定

目次

概要

FireSIGHT システムでは、イベントのさまざまなビューが Web インターフェイスで提供されますが、重要なシステムの継続的なモニタリングを容易にするために外部イベント通知を設定することもできます。 次のいずれかが発生したときに、電子メール、SNMP トラップ、または syslog で通知するアラートを生成するように FireSIGHT システムを設定できます。 この記事では、外部の syslog サーバにアラートを送信するように FireSIGHT Management Center を設定する方法について説明します。

前提条件

要件

syslog および FireSIGHT Management Center に関する知識があることが推奨されます。 また、ファイアウォールで syslog ポート（デフォルトは 514）を許可する必要があります。

使用するコンポーネント

このドキュメントの情報は、ソフトウェア バージョン 5.2 以降に基づくものです。

> **注意**： このドキュメントの情報は、特定のラボ環境内のアプライアンスから作成され、初期（デフォルト）設定の状態から開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

侵入アラートの送信

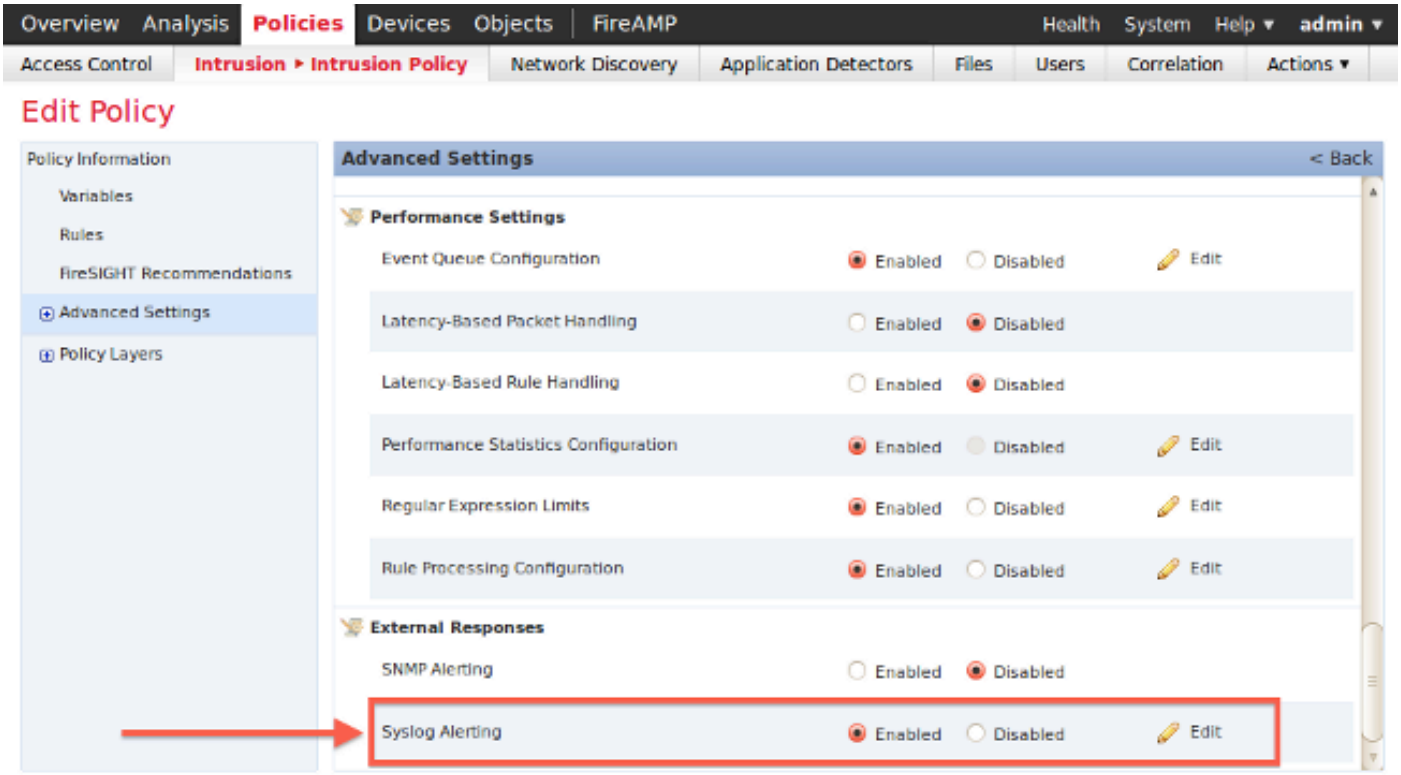
1. FireSIGHT Management Center の Web ユーザ インターフェイスにログインします。

2. [Policies] > [Intrusion] > [Intrusion Policy] に移動します。

3. 適用するポリシーの横にある [Edit] をクリックします。

4. [Advanced Settings] をクリックします。

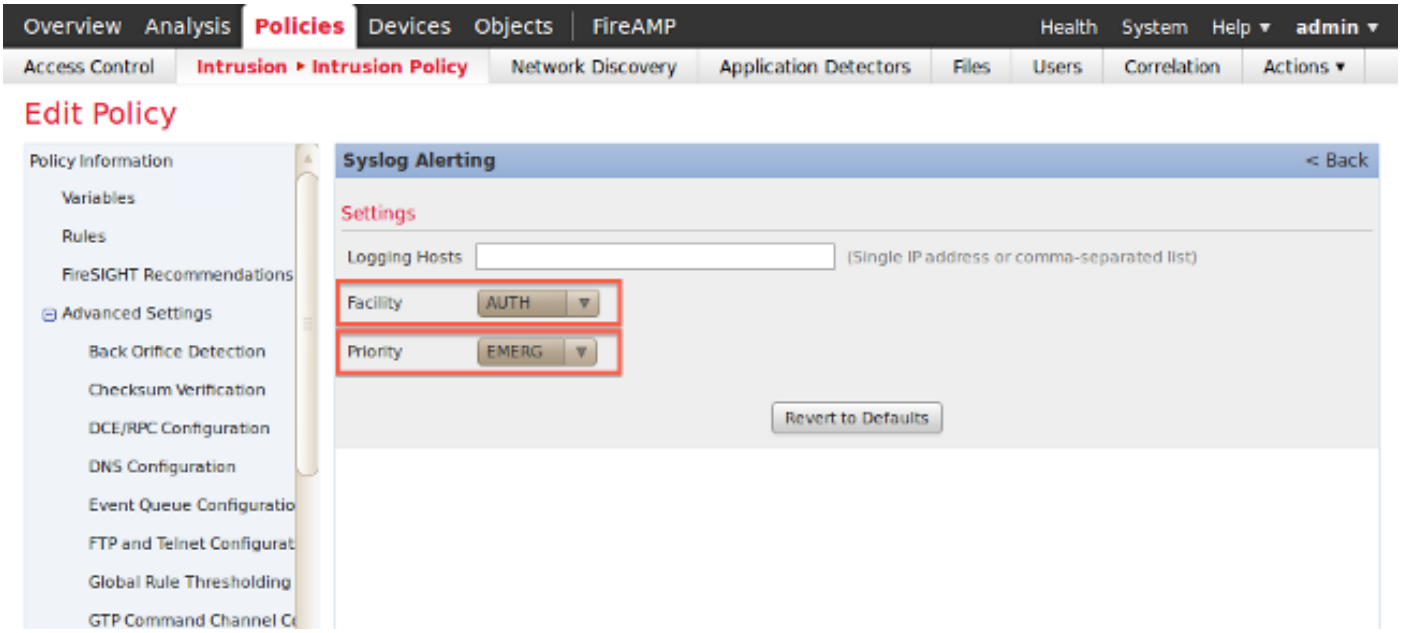
5. リスト内の [Syslog Alerting] を見つけ、これを [Enabled] に設定します。



6. [Syslog Alerting] の右横にある [Edit] をクリックします。

7. [Logging Hosts] フィールドに syslog サーバの IP アドレスを入力します。

8. ドロップダウン メニューから適切な [Facility] と [Severity] を選択します。 特定のファシリティまたは重大度のアラートを受け入れるように syslog サーバを設定するのではないかぎり、これらはデフォルト値のままにしておくことができます。



9. この画面の左上部にある [Policy Information] をクリックします。

10. [Commit Changes] ボタンをクリックします。

11. 侵入ポリシーを再適用します。

> **注:** アラートを生成するには、アクセス制御ルールでこの侵入ポリシーを使用します。 設定されているアクセス制御ルールがない場合は、この侵入ポリシーをアクセス制御ポリシーのデフォルト アクションとして使用するように設定し、アクセス制御ポリシーを再適用します。

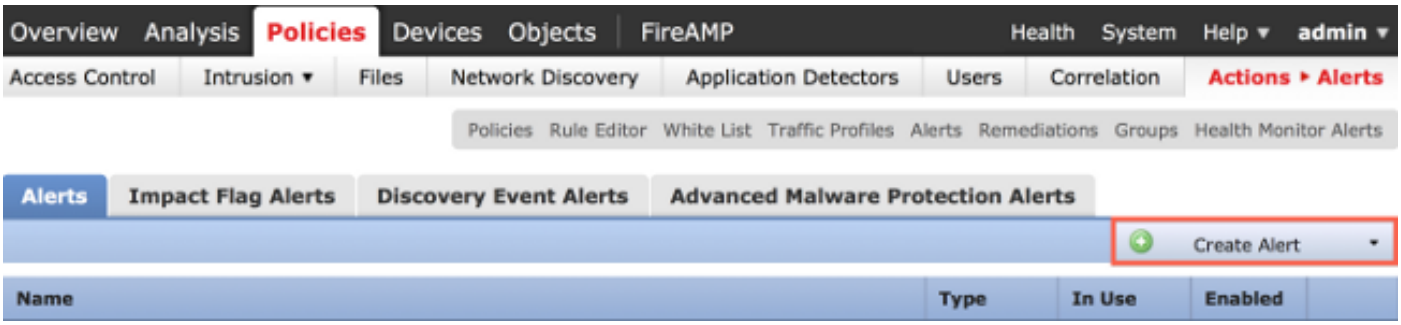
そのポリシーで侵入イベントがトリガーされると、侵入ポリシーに設定されている syslog サーバにもアラートが送信されます。

ヘルス アラートの送信

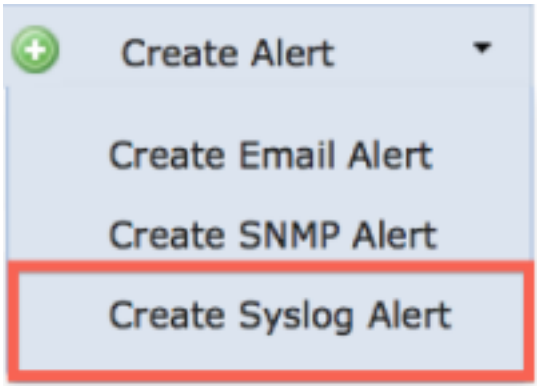
パート 1： syslog アラートを作成する

1. FireSIGHT Management Center の Web ユーザ インターフェイスにログインします。

2. [Policies] > [Actions] > [Alerts] の順に移動します。



3. Web インターフェイスの右側にある [Create Alert] を選択します。



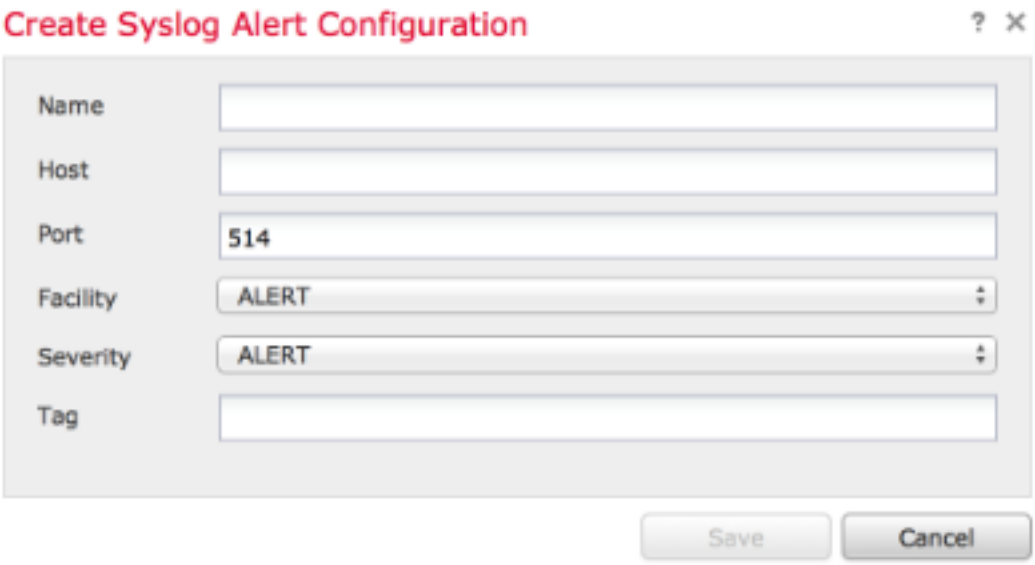
4. [Create Syslog Alert] をクリックします。 設定ポップアップ ウィンドウが表示されます。

5. アラートの名前を指定します。

6. [Host] フィールドに syslog サーバの IP アドレスを入力します。

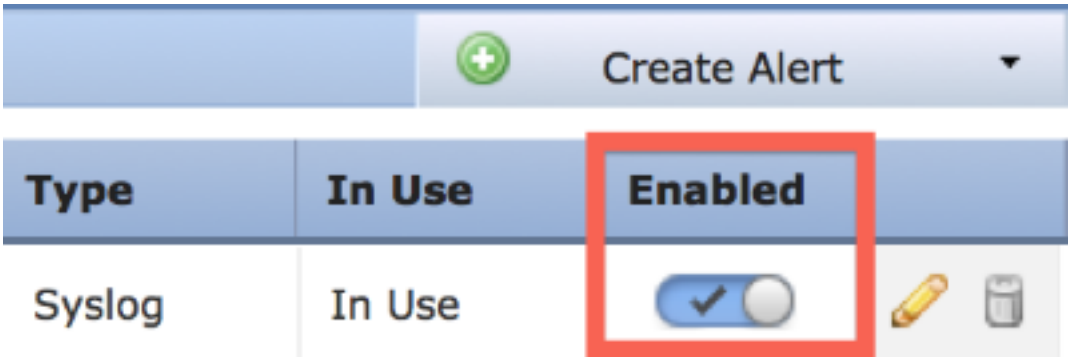
7. 必要な場合は、syslog サーバのポートを変更します（デフォルト ポートは 514 です）。

8. 適切な [Facility] と [Severity] を選択します。



9. [Save] ボタンをクリックします。 [Policies] > [Actions] > [Alerts] ページに戻ります。

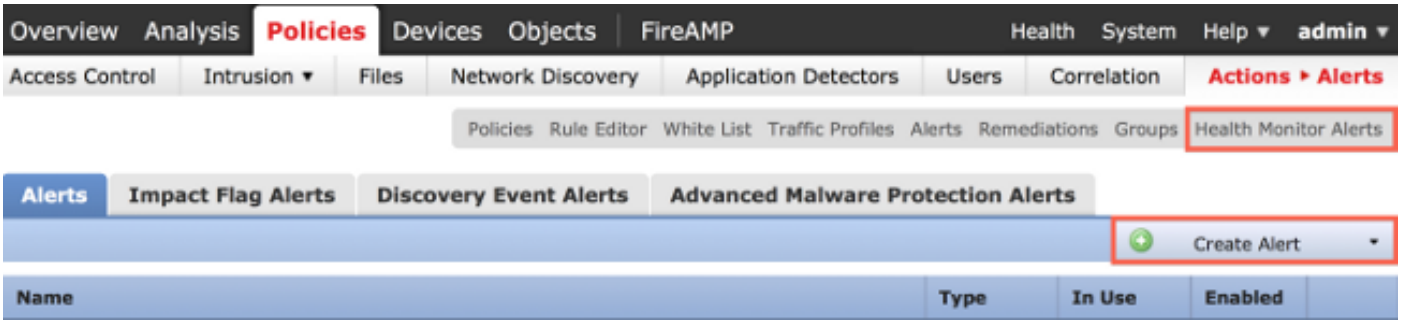
10. syslog 設定を有効にします。



パート 2： ヘルス モニタ アラートを作成する

次の手順では、（前の項で）作成した syslog アラートを使用するヘルス モニタ アラートの設定手順について説明します。

1. [Policies] > [Actions] > [Alerts] ページに移動し、ページ上部の [Health Monitor Alerts] を選択します。



2. ヘルス アラートに名前を付けます。

3. [Severity] を選択します（複数の重大度タイプを選択するには、Ctrl キーを押しながらクリックします）。

4. [Module] 列から、syslog サーバにアラートを送信するヘルス モジュール（たとえば、[Disk Usage]）を選択します。

5. [Alerts] 列から、以前に作成した syslog アラートを選択します。

6. [Save] ボタンをクリックします。

影響フラグ アラート、検出イベント アラート、マルウェア アラートの送信

特定の影響フラグを含むイベント、特定タイプの検出イベント、特定タイプのマルウェア イベントの syslog アラートを送信するように FireSIGHT Management Center を設定することもできます。 これを行うには、「パート 1： syslog アラートを作成する」を実行してから、syslog サーバに送信するイベントのタイプを設定する必要があります。 そのためには、[Policies] > [Actions] > [Alerts] に移動し、目的のアラート タイプのタブを選択します。