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

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[侵入アラートの送信](#)
[ヘルス アラートの送信](#)
[パート 1： syslog アラートを作成する](#)
[パート 2： ヘルス モニタ アラートを作成する](#)
[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](#)

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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

侵入アラートの送信

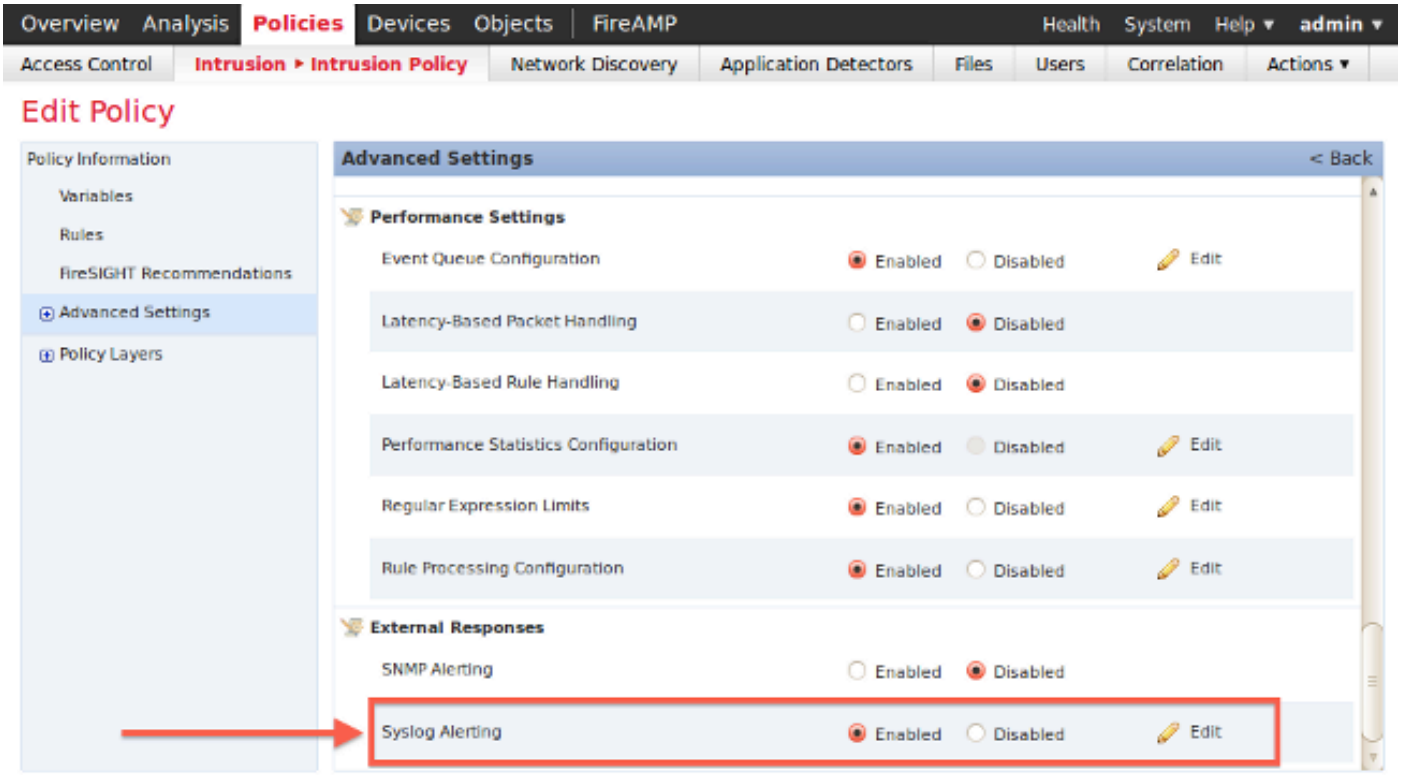
1. FireSIGHT Management CenterのWebユーザインターフェイスにログインします。

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。

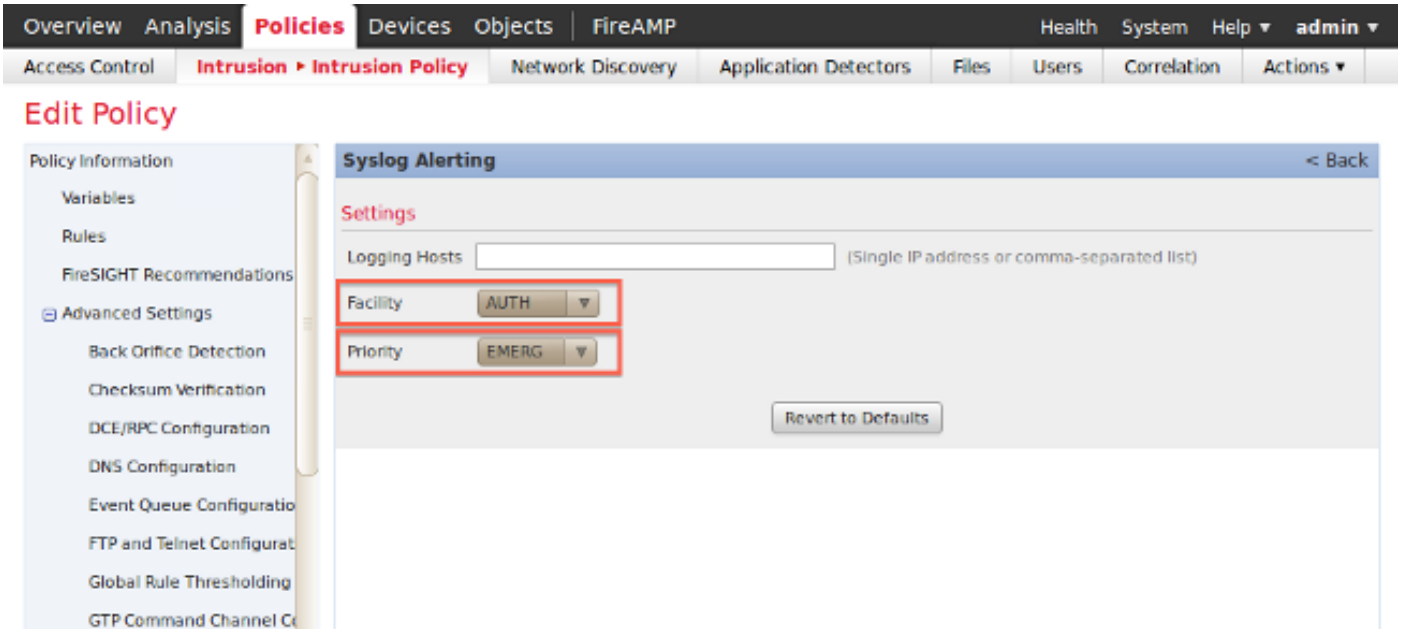
5.リストで[Syslog Alerting] を見つけて、[Enabled] に設定します。



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

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

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。

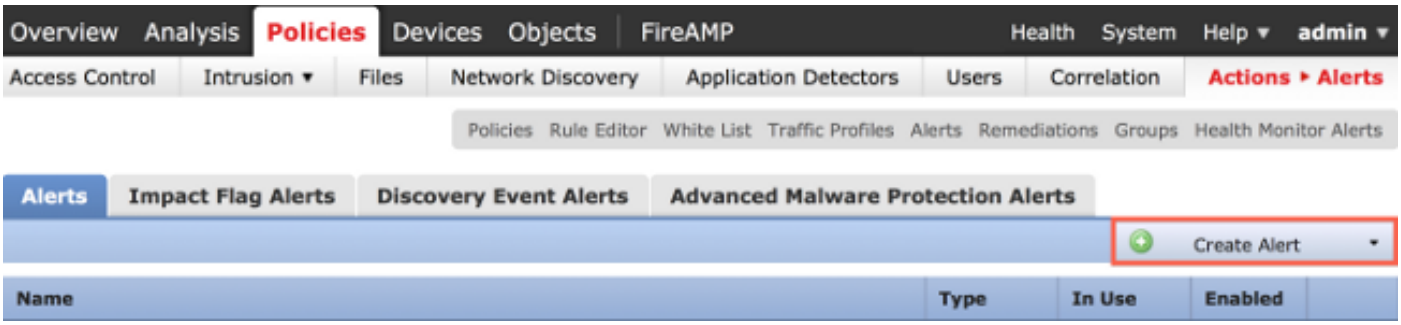
そのポリシーで侵入イベントがトリガーされると、侵入ポリシーに設定されている syslog サーバにもアラートが送信されます。

ヘルス アラートの送信

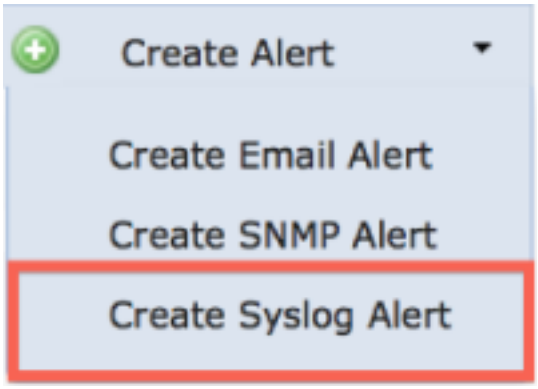
パート 1： syslog アラートを作成する

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] 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。



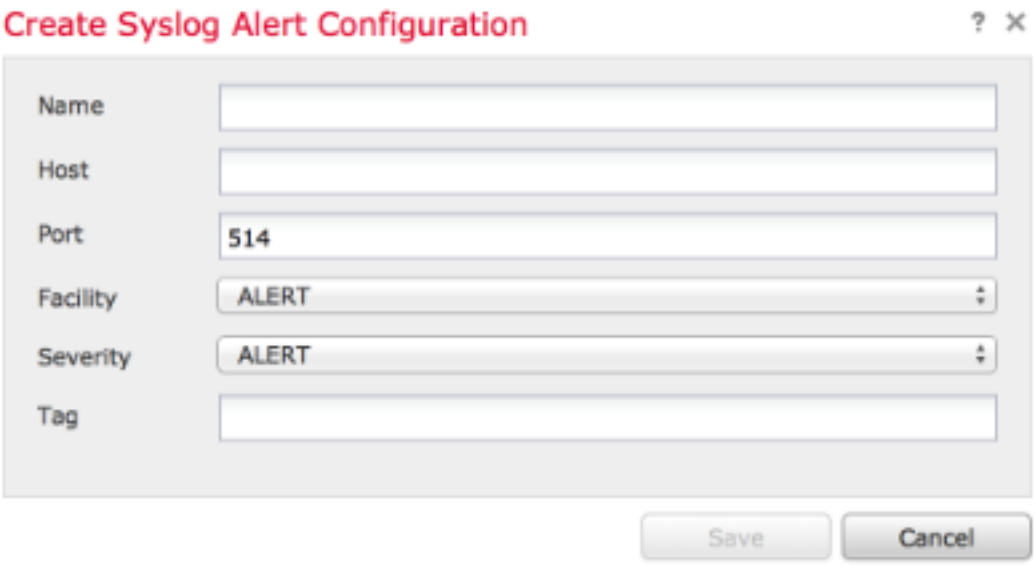
4. [Create Syslog Alert] をクリックします。設定ポップアップ ウィンドウが表示されます。

5.アラートの名前を指定します。

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

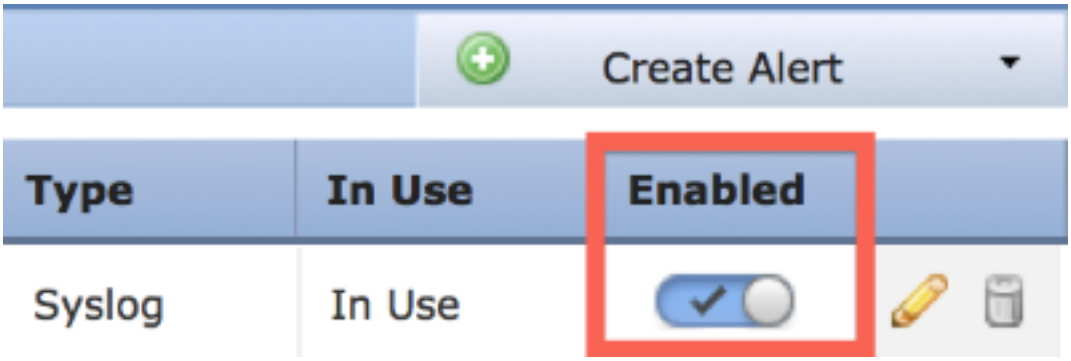
7. syslogサーバで必要に応じてポートを変更します（デフォルトのポートは514です）。

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。**

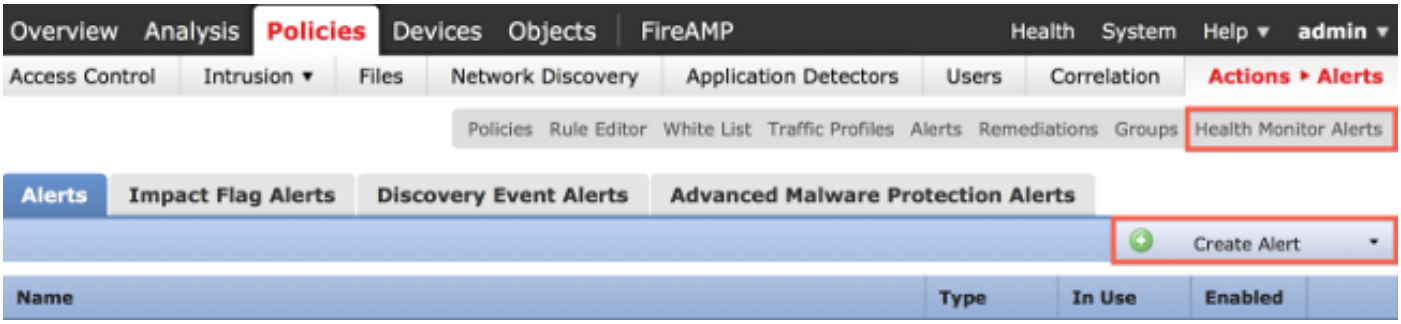
10. Syslog設定を有効にします。



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、ページの上部近くにある[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（Ctrlキーを押しながらクリックすると、複数の重大度タイプを選択できます）。

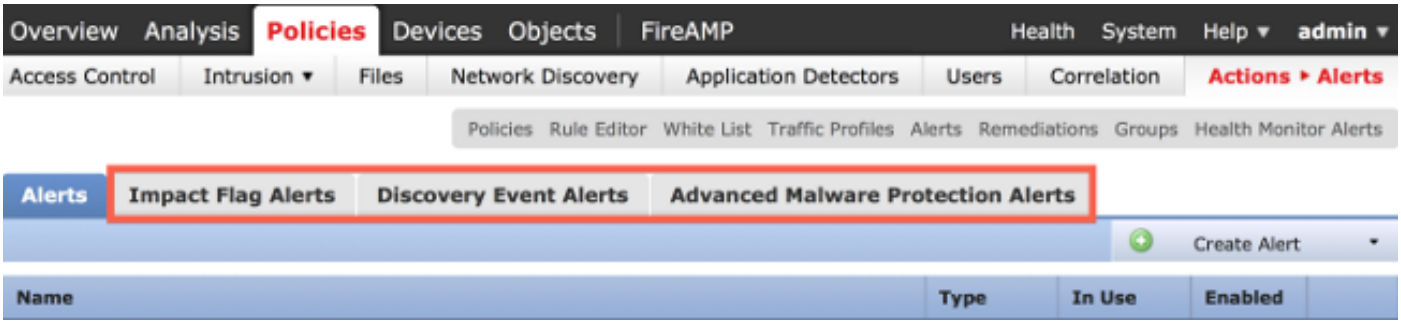
4. [Module] 列から、syslogサーバにアラートを送信するヘルスモジュールを選択します（たとえば、[Disk Usage]）。

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。**



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。