

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[不正侵入アラートの送信](#)

[健全性アラートの送信](#)

[パート 1: Syslog アラートを作成して下さい](#)

[パート 2: ヘルス モニタ アラートを作成して下さい](#)

[影響フラグを送信して、イベントおよび Malware アラートを検出して下さい](#)

概要

FireSIGHT システムがその中のイベントのさまざまな概観を提供する間、Webインターフェイスは、重要なシステムの一定したモニタリングを促進するために外部イベント通知を設定したいと思う場合もあります。次のいずれかが生成されるとき電子メール、SNMPトラップ、または syslog によって知らせるアラートを生成するために FireSIGHT システムを設定できます。この技術情報は送信するために FireSIGHT Management Center を設定する方法を警告します 外部の syslog サーバの記述します。

前提条件

要件

Cisco は Syslog および FireSIGHT Management Center のナレッジがあることを推奨します。また、syslogポート (デフォルトはファイアウォールで 514) 必要があります許すあります。

使用するコンポーネント

この文書に記載されている情報はソフトウェア バージョン 5.2 またはそれ以降に基づいています。

注意： この資料の情報は特定のラボ 環境のアプリケーションから作成され、初期 (デフォルト) 設定と開始します。 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。

不正侵入アラートの送信

1. FireSIGHT Management Center の Web ユーザ ユーザー・ インターフェースにログイン して 下さい。
2. ポリシー > 不正侵入 > 不正侵入 ポリシーへのナビゲート。
3. 適用したいと思うポリシーの隣で『Edit』 をクリック して 下さい。
4. 設定を『Advanced』 をクリック して 下さい。
5. 警告 する Syslog をリストで見つけ、イネーブルになったに設定 して 下さい。

The screenshot shows the 'Edit Policy' interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'FireAMP', 'Health', 'System', 'Help', and 'admin'. Below this, a secondary navigation bar shows 'Access Control', 'Intrusion > Intrusion Policy', 'Network Discovery', 'Application Detectors', 'Files', 'Users', 'Correlation', and 'Actions'. The main content area is titled 'Edit Policy' and has a left sidebar with 'Policy Information', 'Variables', 'Rules', 'FireSIGHT Recommendations', 'Advanced Settings', and 'Policy Layers'. The 'Advanced Settings' section is expanded, showing 'Performance Settings' and 'External Responses'. Under 'External Responses', 'Syslog Alerting' is checked and highlighted with a red box. A red arrow points from the 'Advanced Settings' link in the sidebar to this box.

6. Syslog 警告の権限の隣で『Edit』 をクリック して 下さい。
7. ログイン Hosts フィールドの syslog サーバの IP アドレスをタイプ して 下さい。
8. ドロップダウン メニューから適切なファシリティおよび重大度を選択 して 下さい。 これらは デフォルト値である特定のファシリティまたは重大度のためのアラートを受け入れるために syslog サーバが設定されなければ残すことができます。

The screenshot shows the 'Syslog Alerting' configuration page. The top navigation bar is the same as in the previous image. The left sidebar is expanded to show 'Advanced Settings' > 'Syslog Alerting'. The main content area is titled 'Syslog Alerting' and has a '< Back' link. Under the 'Settings' section, there is a 'Logging Hosts' text input field with a placeholder '(Single IP address or comma-separated list)'. Below this are two dropdown menus: 'Facility' (set to 'AUTH') and 'Priority' (set to 'EMERG'). Both dropdown menus are highlighted with red boxes. A 'Revert to Defaults' button is located below the dropdowns.

9. この画面の左上の近くで**ポリシー情報**をクリックして下さい。

10. **託変更**ボタンをクリックして下さい。

11. 不正侵入 ポリシーを再適用して下さい。

注 生成されるべきアラートのためにアクセスコントロール ルールでこの不正侵入 ポリシーを使用して下さい。 設定される、アクセスコントロール ポリシーのデフォルト アクションとして使用されるべきこの不正侵入 ポリシー 設定される アクセスコントロール ルールがないしアクセスコントロール ポリシーを再適用すれば。

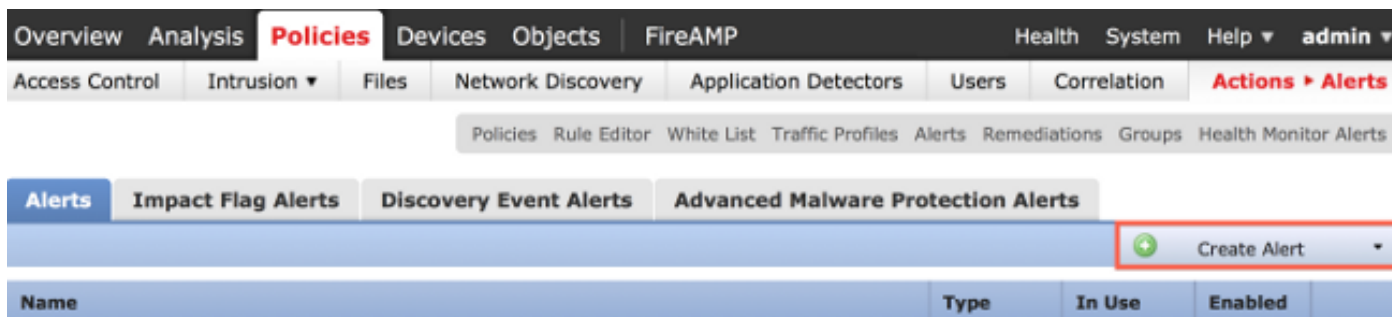
この場合不正侵入 イベントがそのポリシーで引き起こされれば、アラートはまた不正侵入 ポリシーで設定される syslog サーバに発信されます。

健全性アラートの送信

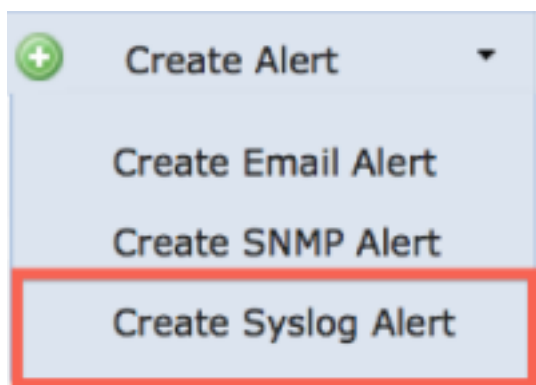
パート 1: Syslog アラートを作成して下さい

1. FireSIGHT Management Center の Web ユーザ ユーザー・ インターフェイスにログインして下さい。

2. **ポリシー > 操作 > アラート**へのナビゲート。



3. アラートを『Create』を選択して下さい、Webインターフェイスの右側にある。



4. Syslog アラートを『Create』をクリックして下さい。設定 ポップアップウィンドウは現われます。

5. アラートに名前をつけて下さい。

- [Host] フィールドの syslog サーバの IP アドレスを記入して下さい。
- syslog サーバによってポートをもし必要なら変更して下さい (デフォルトポートは 514) あります。
- 適切なファシリティおよび重大度を選択して下さい。

Create Syslog Alert Configuration



? X

Name	<input type="text"/>
Host	<input type="text"/>
Port	514
Facility	ALERT
Severity	ALERT
Tag	<input type="text"/>

Save Cancel

- [Save] ボタンをクリックします。ポリシー > アクションに > Alerts ページ戻ります。
- Syslog 設定を有効に して下さい。

Create Alert

Type	In Use	Enabled	
Syslog	In Use	<input checked="" type="checkbox"/>	 

パート 2: ヘルス モニタ アラートを作成して下さい

ちょうど作成した syslog アラートを使用する次の手順はヘルス モニタ アラートを設定するためにステップを記述します (前のセクションで):

- ポリシー > アクションに > Alerts ページ行き、ヘルス モニタ アラートを選択して下さい、ページの上の近くにある。

Overview Analysis **Policies** Devices Objects FireAMP Health System Help admin

Access Control Intrusion Files Network Discovery Application Detectors Users Correlation **Actions > Alerts**

Policies Rule Editor White List Traffic Profiles Alerts Remediations Groups **Health Monitor Alerts**

Alerts Impact Flag Alerts Discovery Event Alerts Advanced Malware Protection Alerts

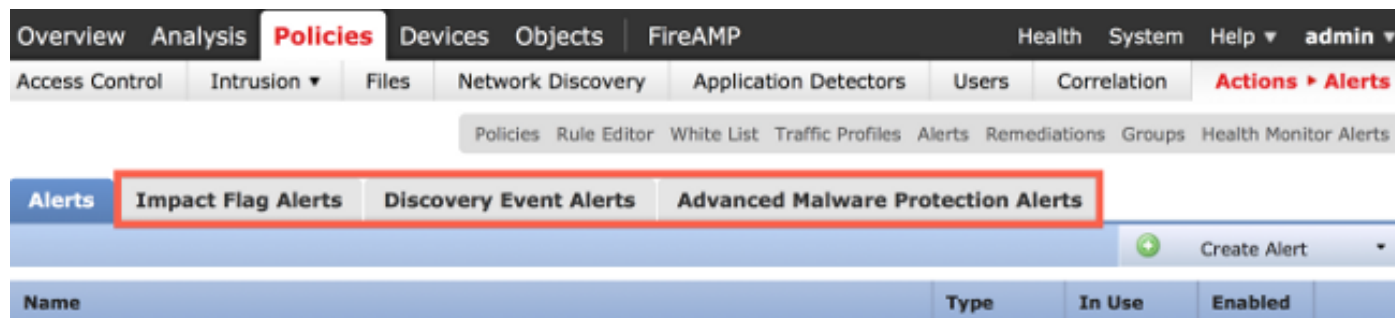
Create Alert

Name	Type	In Use	Enabled
------	------	--------	---------

8. 脆弱性スキャンの結果を syslog に選択して、ヘルス モニタ アラートを使用することを望む健康性間ジ、重大度を選択して下さい (脆弱性スキャンの結果を維持する方法)。影響アラートを送信して、イベントおよび Malware アラートを検

出して下さい

またディスカバリ イベントおよび malware イベントの特定の種類特定の影響フラグのイベントのための syslog アラートを発信するために FireSIGHT Management Center を設定できます。それをするために、[Part 1](#) となります:[Syslog アラートを作成し](#)、次に syslog サーバに送ってほしいイベントの種類を設定して下さい。> Alerts ページ ポリシー > アクションへのナビゲートし、望ましいアラート タイプにタブを選択することによってそれを行うことができます。



The screenshot shows the FireSIGHT Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'FireAMP'. Below this, there are sub-navigation tabs for 'Access Control', 'Intrusion', 'Files', 'Network Discovery', 'Application Detectors', 'Users', 'Correlation', and 'Actions > Alerts'. A secondary bar contains 'Policies', 'Rule Editor', 'White List', 'Traffic Profiles', 'Alerts', 'Remediations', 'Groups', and 'Health Monitor Alerts'. The main content area has three tabs: 'Alerts', 'Impact Flag Alerts', 'Discovery Event Alerts', and 'Advanced Malware Protection Alerts'. The 'Advanced Malware Protection Alerts' tab is highlighted with a red box. To the right of the tabs is a 'Create Alert' button with a green plus icon. Below the tabs is a table with columns for 'Name', 'Type', 'In Use', and 'Enabled'.

Name	Type	In Use	Enabled
------	------	--------	---------