

Configurer un système FireSIGHT pour envoyer des alertes à un serveur Syslog externe

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Envoi d'alertes d'intrusion](#)

[Envoi d'alertes de santé](#)

[Partie 1 : Créer une alerte Syslog](#)

[Partie 2 : Créer des alertes Health Monitor](#)

[Envoi d'un indicateur d'impact, détection des événements et alertes de programmes malveillants](#)

Introduction

Bien qu'un système FireSIGHT offre plusieurs vues des événements dans son interface Web, vous pouvez configurer la notification d'événements externes pour faciliter la surveillance constante des systèmes critiques. Vous pouvez configurer un système FireSIGHT pour qu'il génère des alertes qui vous avertissent par e-mail, par déroutement SNMP ou par syslog lorsque l'un des éléments suivants est généré. Cet article décrit comment configurer FireSIGHT Management Center pour qu'il envoie des alertes sur un serveur Syslog externe.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez des connaissances sur Syslog et FireSIGHT Management Center. En outre, le port syslog (514 par défaut) doit être autorisé dans votre pare-feu.

Components Used

Les informations contenues dans ce document sont basées sur la version 5.2 ou ultérieure du logiciel.

Attention : Les informations de ce document sont créées à partir d'une appliance dans un environnement de travaux pratiques spécifique et ont démarré avec une configuration désactivée (par défaut). If your network is live, make sure that you understand the potential

impact of any command.

Envoi d'alertes d'intrusion

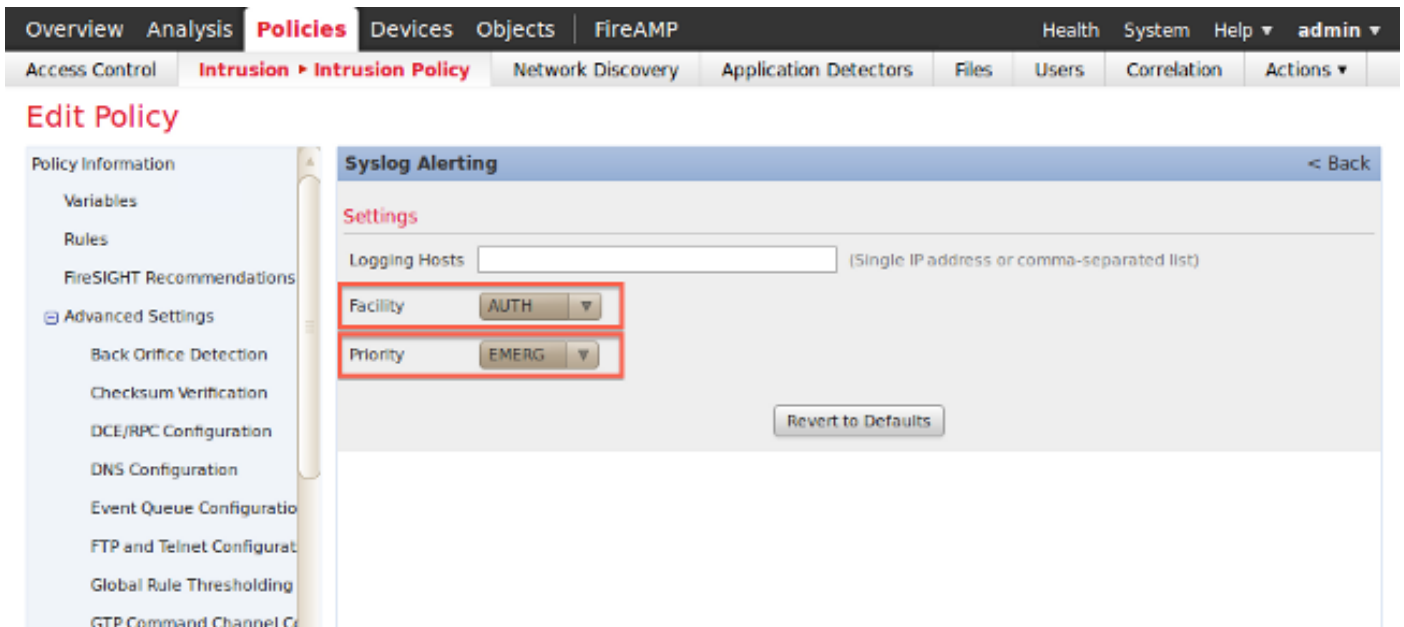
1. Connectez-vous à l'interface utilisateur Web de votre FireSIGHT Management Center.
2. Accédez à **Stratégies > Intrusion > Stratégie d'intrusion**.
3. Cliquez sur **Modifier** en regard de la stratégie que vous souhaitez appliquer.
4. Cliquez sur **Advanced Settings**.
5. Localisez **Syslog Alerting** dans la liste et définissez-le sur **Enabled**.

The screenshot shows the 'Edit Policy' interface for an 'Intrusion Policy'. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'FireAMP'. The 'Policies' section is active, showing 'Intrusion > Intrusion Policy'. The 'Advanced Settings' section is expanded, displaying a list of configuration options:

Setting	Enabled	Disabled	Action
Event Queue Configuration	<input checked="" type="radio"/>	<input type="radio"/>	Edit
Latency-Based Packet Handling	<input type="radio"/>	<input checked="" type="radio"/>	
Latency-Based Rule Handling	<input type="radio"/>	<input checked="" type="radio"/>	
Performance Statistics Configuration	<input checked="" type="radio"/>	<input type="radio"/>	Edit
Regular Expression Limits	<input checked="" type="radio"/>	<input type="radio"/>	Edit
Rule Processing Configuration	<input checked="" type="radio"/>	<input type="radio"/>	Edit
SNMP Alerting	<input type="radio"/>	<input checked="" type="radio"/>	
Syslog Alerting	<input checked="" type="radio"/>	<input type="radio"/>	Edit

A red arrow points from the 'Advanced Settings' link in the left sidebar to the 'Syslog Alerting' row, which is highlighted with a red box.

6. Cliquez sur **Modifier** en regard de l'option **Alertes Syslog**.
7. Tapez l'adresse IP de votre serveur Syslog dans le champ **Logging Hosts**.
8. Choisissez un **domaine** et une **gravité** appropriés dans le menu déroulant. Ces valeurs peuvent être conservées aux valeurs par défaut, sauf si un serveur Syslog est configuré pour accepter des alertes pour une fonctionnalité ou un niveau de gravité spécifique.



9. Cliquez sur **Policy Information** dans la partie supérieure gauche de cet écran.

10. Cliquez sur le bouton **Valider les modifications**.

11. Réappliquez votre stratégie d'intrusion.

Note: Afin que les alertes soient générées, utilisez cette stratégie d'intrusion dans la règle de contrôle d'accès. Si aucune règle de contrôle d'accès n'est configurée, définissez cette stratégie d'intrusion comme action par défaut de la stratégie de contrôle d'accès, puis réappliquez la stratégie de contrôle d'accès.

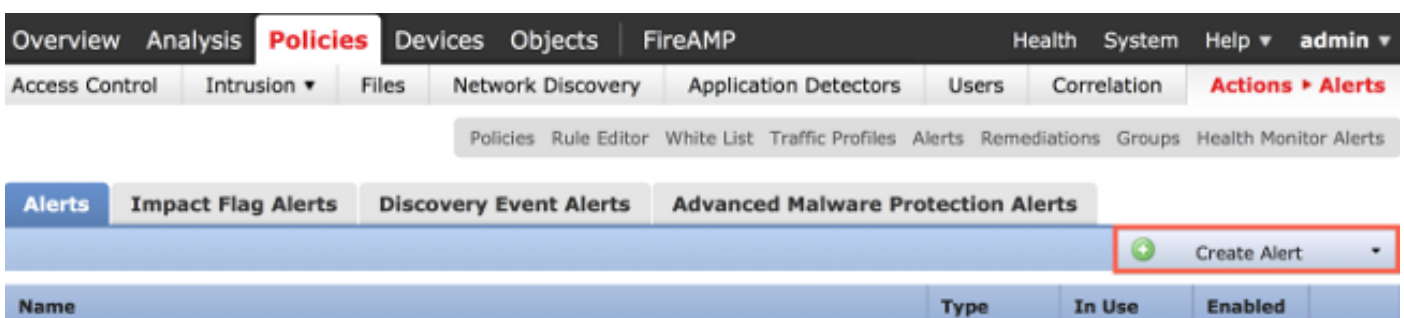
Désormais, si un événement d'intrusion est déclenché sur cette stratégie, une alerte est également envoyée au serveur Syslog configuré sur la stratégie d'intrusion.

Envoi d'alertes de santé

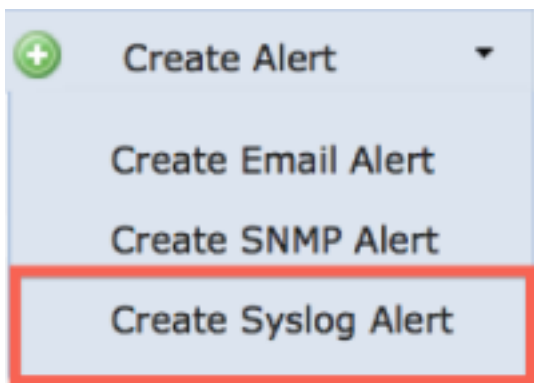
Partie 1 : Créer une alerte Syslog

1. Connectez-vous à l'interface utilisateur Web de votre FireSIGHT Management Center.

2. Accédez à **Politiques > Actions > Alertes**.



3. Sélectionnez **Create Alert**, qui se trouve sur le côté droit de l'interface Web.



4. Cliquez sur **Create Syslog Alert**. Une fenêtre contextuelle de configuration apparaît.
5. Entrez un nom pour l'alerte.
6. Complétez l'adresse IP de votre serveur Syslog dans le champ **Host**.
7. Modifiez le port si votre serveur Syslog le requiert (le port par défaut est 514).
8. Sélectionnez une **installation** et une **gravité** appropriées.

Create Syslog Alert Configuration ? X

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

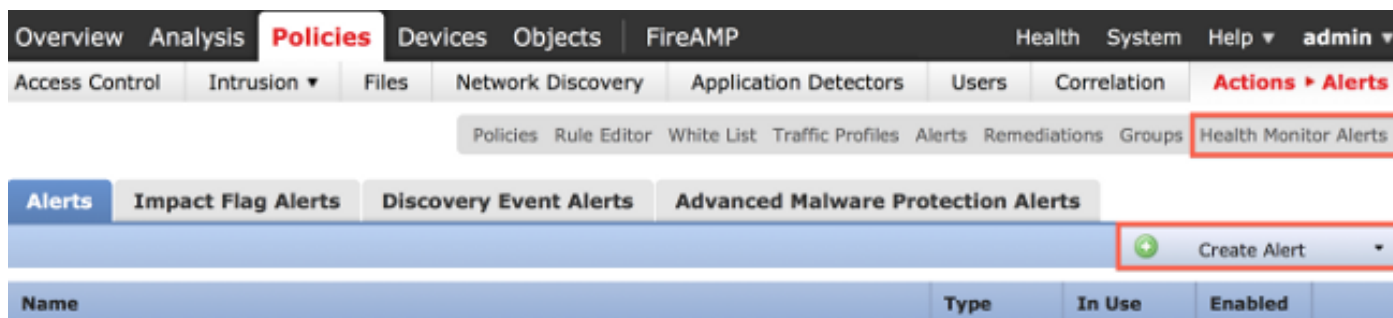
9. Cliquez sur le bouton **Enregistrer**. Vous revenez à la page **Politiques > Actions > Alertes**.
10. Activez la configuration Syslog.

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

Partie 2 : Créer des alertes Health Monitor

L'instruction suivante décrit les étapes de configuration des **alertes du Moniteur d'intégrité** qui utilisent l'alerte syslog que vous venez de créer (dans la section précédente) :

1. Accédez à la page **Stratégies > Actions > Alertes** et choisissez **Alertes du moniteur d'état**, qui se trouve en haut de la page.



2. Donnez un nom à l'alerte d'intégrité.

3. Choisissez un **niveau de gravité** (maintenez la touche CTRL enfoncée et cliquez sur peut être utilisé pour sélectionner plusieurs types de gravité).

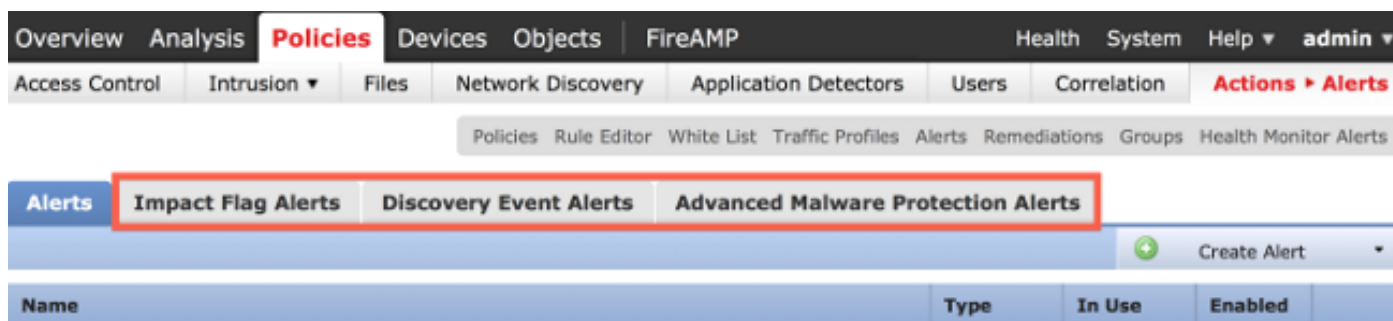
4. Dans la colonne **Module**, sélectionnez les modules d'intégrité pour lesquels vous souhaitez envoyer des alertes au serveur Syslog (par exemple, Utilisation du disque).

5. Sélectionnez l'alerte Syslog précédemment créée dans la colonne **Alertes**.

6. Cliquez sur le bouton **Enregistrer**.

Envoi d'un indicateur d'impact, détection des événements et alertes de programmes malveillants

Vous pouvez également configurer un FireSIGHT Management Center pour qu'il envoie des alertes Syslog pour les événements avec un indicateur d'impact spécifique, un type spécifique d'événements de détection et des événements de programmes malveillants. Pour ce faire, vous devez passer à la [Partie 1 : Créez une alerte Syslog](#), puis configurez le type d'événements que vous souhaitez envoyer à votre serveur Syslog. Pour ce faire, accédez à la page **Politiques > Actions > Alertes**, puis sélectionnez un onglet pour le type d'alerte souhaité.



À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.