Alertes externes avec réponses aux alertes

Les rubriques suivantes décrivent comment envoyer des alertes d'événements externes à partir de Cisco Secure Firewall Management Center à l'aide des réponses aux alertes :

Réponses aux alertes Cisco Secure Firewall Management Center

Les notifications d'événements externes par SNMP, syslog ou par courriel peuvent faciliter la surveillance des systèmes essentiels. Cisco Secure Firewall Management Center utilise des *réponses aux alertes* configurables pour interagir avec les serveurs externes. Une *réponse à une alerte* est une configuration qui représente une connexion à un serveur de messagerie, SNMP ou syslog. On les appelle *des réponses,* car vous pouvez les utiliser pour envoyer des alertes en réponse à des événements détectés par Firepower. Vous pouvez configurer plusieurs réponses aux alertes pour envoyer différents types d'alertes à différents serveurs de surveillance ou personnes.

Remarque Selon votre périphérique et la version de Firepower, les réponses aux alertes peuvent ne pas être la meilleure façon d'envoyer des messages syslog. Consultez le chapitre *À propos de Syslog* dans les Guide de configuration Cisco Secure Firewall Management Center Device.

Remarque Les alertes qui utilisent des réponses aux alertes sont envoyées par Cisco Secure Firewall Management Center. Les alertes par courriel de prévention des intrusions, qui n'utilisent pas de réponses aux alertes, sont également envoyées par Cisco Secure Firewall Management Center. En revanche, les alertes SNMP et syslog basées sur le déclenchement de règles de prévention des intrusions individuelles sont envoyées directement par les périphériques gérés.

Dans la plupart des cas, les informations contenues dans une alerte externe sont les mêmes que celles de tout événement associé que vous avez enregistré à la base de données. Cependant, pour les alertes d'événement de corrélation où la règle de corrélation contient un suiveur de connexion, les informations que vous recevez sont les mêmes que pour une alerte de changement de profil de trafic, quel que soit le type d'événement de base.

Vous créez et gérez les réponses aux alertes sur la page des alertes (**Policies (politiques)** > **Actions** > **Alerts (alertes)**). Les nouvelles réponses aux alertes sont automatiquement activées. Pour arrêter temporairement la génération d'alertes, vous pouvez désactiver les réponses aux alertes plutôt que de les supprimer.

Les modifications apportées aux réponses aux alertes prennent effet immédiatement, sauf lors de l'envoi des journaux de connexion à une interruption SNMP ou à un serveur syslog.

Dans un déploiement multidomaine, lorsque vous créez une réponse à une alerte, elle appartient au domaine actuel. Cette réponse d'alerte peut également être utilisée par les domaines descendants.

Configurations prenant en charge les réponses aux alertes

Après avoir créé une réponse à une alerte, vous pouvez l'utiliser pour envoyer les alertes externes suivantes à partir de Cisco Secure Firewall Management Center.

Type d'alerte ou d'événement	Pour obtenir de plus amples renseignements
Événements d'intégrité, par module d'intégrité et niveau de gravité	Création des alertes de moniteur d'intégrité

Exigences et conditions préalables des réponses aux alertes

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin

Création d'une réponse à une alerte SNMP

Vous pouvez créer des réponses aux alertes SNMP à l'aide de SNMPv1, SNMPv2 ou SNMPv3 pour un type de périphérique sauf défense contre les menaces .

Remarque Lors de la sélection des versions de SNMP pour le protocole SNMP, notez que SNMPv2 prend en charge uniquement les communautés en lecture seule et SNMPv3 uniquement les utilisateurs en lecture seule. SNMPv3 prend également en charge le chiffrement avec AES128.

Si vous souhaitez surveiller les valeurs 64 bits avec SNMP, vous devez utiliser SNMPv2 ou SNMPv3. SNMPv1 ne prend pas en charge la surveillance 64 bits.

Avant de commencer

- Si votre système de gestion de réseau nécessite le fichier MIB (Management Information Base) de Cisco Secure Firewall Management Center, vous pouvez l'obtenir à l'emplacement `/etc/sf/DCEALERT.MIB`.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Alerts (alertes)**.

Étape 2 Dans le menu déroulant **Create Alert** (créer une alerte), choisissez **Create SNMP Alert** (créer une alerte SNMP).

Étape 3 Modifiez les champs de configuration de l'alerte SNMP :

a) **Name** (Nom) : saisissez un nom pour identifier la réponse SNMP.

b) **Trap Server** (serveur de déroutement) : saisissez le nom d'hôte ou l'adresse IP du serveur de déroutement SNMP.

Remarque Le système ne vous avertit **pas** si vous saisissez une adresse IPv4 non valide (comme 192.169.1.456) dans ce champ. Au lieu de cela, l'adresse non valide est traitée comme un nom d'hôte.

c) **Version** : choisissez la version SNMP que vous souhaitez utiliser dans la liste déroulante. SNMPv3 est la valeur par défaut.

Choisissez parmi :

- **SNMPv1** ou **SNMPv2** : saisissez un nom de communauté SNMP en lecture seule dans le champ **Community String** (Chaîne de communauté), puis passez à la fin de la procédure.

  Remarque Ne pas inclure de caractères spéciaux (< > / % # & ? , etc.) dans le nom de l'identifiant de communauté SNMP.

- Pour **SNMPv3** : saisissez le nom de l'utilisateur que vous souhaitez authentifier auprès du serveur SNMP dans le champ **User Name** (nom d'utilisateur) et passez à l'étape suivante.

d) **Authentication Protocol** (protocole d'authentification) : choisissez le protocole que vous souhaitez utiliser pour chiffrer l'authentification dans la liste déroulante.

Choisissez parmi :

- **MD5** : fonction de hachage Message Digest 5 (MD5).
- **SHA** : Fonction de hachage Secure Hash Algorithm (SHA).

e) **Authentication Password**(mot de passe d'authentification) : saisissez le mot de passe pour activer l'authentification.

f) :**Privacy Protocol** (Protocole de confidentialité) : choisissez le protocole que vous souhaitez utiliser pour chiffrer un mot de passe privé dans la liste déroulante.

Choisissez parmi :

- **DES** : norme de chiffrement des données (DES) utilisant des clés de 56 bits dans un algorithme de bloc de clés secrètes symétriques.
- **AES** : norme de chiffrement avancée (AES) utilisant des clés de 56 bits dans un algorithme de chiffrement symétrique.
- **AES128** : AES utilisant des clés de 128 bits dans un algorithme de chiffrement symétrique. Une clé plus longue offre une sécurité plus élevée, mais une réduction des performances.

g) **Privacy Password**(mot de passe de confidentialité) : saisissez le mot de passe de confidentialité requis par le serveur SNMP. Si vous spécifiez un mot de passe privé, la confidentialité est activée et vous devez également spécifier un mot de passe d'authentification.

h) **Engine ID** (ID de moteur) : saisissez un identifiant pour le moteur SNMP, en notation hexadécimale, en utilisant un nombre pair de chiffres.

Lorsque vous utilisez SNMPv3, le système utilise une valeur d'ID de moteur pour coder le message. Votre serveur SNMP a besoin de cette valeur pour décoder le message.

Cisco vous recommande d'utiliser la version hexadécimale de l'adresse IP de Cisco Secure Firewall Management Center. Par exemple, si le Cisco Secure Firewall Management Center a pour adresse IP 10.1.1.77, utilisez 0a01014D0.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

Les modifications seront appliquées immédiatement, SAUF :

Si vous utilisez des réponses aux alertes pour envoyer des journaux de connexion, vous devez déployer les modifications de configuration après avoir modifié ces réponses aux alertes.

Création d'une réponse à une alerte Syslog

Lors de la configuration d'une réponse à une alerte syslog, vous pouvez préciser la gravité et la facilité associées aux messages du journal système pour vous assurer qu'ils sont traités correctement par le serveur de journal système. La fonction indique le sous-système qui crée le message, et la gravité définit la gravité du message. Les installations et les gravités ne sont pas affichées dans le message qui s'affiche dans le journal système, mais sont plutôt utilisées pour indiquer au système qui reçoit le message du journal comment le classer.

Astuces Pour des informations plus détaillées sur le fonctionnement et la configuration de syslog, consultez la documentation de votre système. Sur les systèmes UNIX, les pages de `manuel` pour `syslog` et `syslog.conf` fournissent des informations conceptuelles et des instructions de configuration.

Bien que vous puissiez choisir n'importe quel type de fonctionnalité lors de la création d'une réponse à une alerte de journal système, vous devez en choisir une qui a du sens en fonction de votre serveur de journal système. Tous les serveurs syslog ne prennent pas en charge toutes les installations. Pour les serveurs Syslog UNIX, le fichier `syslog.conf` doit indiquer quelles installations sont enregistrées dans quels fichiers journaux sur le serveur.

Avant de commencer

- Cette procédure n'est pas la méthode recommandée pour envoyer des messages syslog dans de nombreux cas.
- Confirmez que le serveur syslog peut accepter les messages distants.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Alerts (alertes)**.

Étape 2 Dans le menu déroulant **Create Alert** (créer une alerte), choisissez **Create Syslog Alert**(créer une alerte Syslog).

Étape 3 Saisissez un **nom** pour l'alerte.

Étape 4 Dans le champ **Host** (hôte), saisissez le nom d'hôte ou l'adresse IP de votre serveur Syslog.

Remarque Le système ne vous avertit **pas** si vous saisissez une adresse IPv4 non valide (comme 192.168.1.456) dans ce champ. Au lieu de cela, l'adresse non valide est traitée comme un nom d'hôte.

Étape 5 Dans le champ **Port**, saisissez le port utilisé par le serveur pour les messages du journal système. Par défaut, cette valeur est 514.

Étape 6 Dans la liste des **Facility** (installations), choisissez une installation décrite dans Fonctions d'alertes Syslog, à la page 5.

Étape 7 Dans la liste **Severity** (gravité), choisissez un niveau de gravité décrit dans Niveaux de gravité Syslog, à la page 6.

Étape 8 Dans le champ **Tag** (Balise), saisissez le nom de la balise que vous souhaitez voir apparaître dans le message du journal système.

Par exemple, si vous souhaitez que tous les messages envoyés au journal système soient précédés de `FromMC`, saisissez `FromMC` dans le champ.

Étape 9 Cliquez sur **Save** (enregistrer).

Prochaine étape

Les modifications seront appliquées immédiatement, SAUF :

Si vous utilisez des réponses aux alertes pour envoyer les journaux de connexion à un serveur syslog, vous devez déployer les modifications de configuration après avoir modifié ces réponses aux alertes.

Fonctions d'alertes Syslog

Le tableau suivant répertorie les fonctionnalités de Syslog que vous pouvez sélectionner.

Tableau 1 : Fonctions Syslog disponibles

Facility (ressource)	Description
AUTH	Un message associé à la sécurité et à l'autorisation.
AUTHPRIV	Un message d'accès restreint associé à la sécurité et à l'autorisation. Sur de nombreux systèmes, ces messages sont transférés vers un fichier sécurisé.
CONSOLE	Un message d'alerte.
CRON	Un message généré par le daemon clock. Notez que les serveurs Syslog exécutant un système d'exploitation Linux utiliseront la `fonction CRON`.
DÉMON	Un message généré par un daemon du système.
FTP	Un message généré par le daemon FTP.
KERN	Un message généré par le noyau. Sur de nombreux systèmes, ces messages sont imprimés sur la console lorsqu'ils s'affichent.
LOCAL0-LOCAL7	Un message généré par un processus interne.
LPR	Un message généré par le sous-système d'impression.
MESSAGERIE	Message généré par un système de messagerie.
ACTUALITÉS	Un message généré par le sous-système de nouvelles du réseau.
NTP;	Un message généré par le daemon NTP.
SÉCURITÉ	Un message généré par le sous-système d'audit.
JOURNAL SYSTÈME	Un message généré par le daemon syslog.
SOLARIS-CRON	Un message généré par le daemon clock. Notez que les serveurs syslog exécutant un système d'exploitation Windows utiliseront la fonction `CLOCK`.
Webex	Un message généré par un processus au niveau utilisateur.
UUCP	Un message généré par le sous-système UUCP.

Niveaux de gravité Syslog

Le tableau suivant répertorie les niveaux de gravité standard de journal système que vous pouvez sélectionner.

Tableau 2 : Niveaux de gravité Syslog

Niveau	Description
ALERTE	Une condition qui doit être corrigée immédiatement.

Niveau	Description
CRIT	Une condition critique.
DÉBOGAGE	Les messages contenant des informations de débogage.
EMERG	Un état d'urgence diffusé à tous les utilisateurs.
ERR	Une condition d'erreur.
INFO	Des messages informatifs.
AVIS	Conditions qui ne sont pas des conditions d'erreur, mais qui nécessitent votre attention.
AVERTISSEMENT	Message d'avertissement.

Création d'une réponse à une alerte par courriel

Avant de commencer

- Confirmez que le Cisco Secure Firewall Management Center peut résoudre-restaurer sa propre adresse IP.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Alerts (alertes)**.

Étape 2 Dans le menu déroulant **Create Alert** (créer une alerte), choisissez **Create Email Alert**(créer une alerte par courriel).

Étape 3 Saisissez un **nom** pour la réponse à l'alerte.

Étape 4 Dans le champ **À**, saisissez les adresses courriel auxquelles vous souhaitez envoyer des alertes, séparées par des virgules.

Étape 5 Dans le champ **De**, saisissez l'adresse courriel que vous souhaitez voir apparaître comme l'expéditeur de l'alerte.

Étape 6 En regard de **Hôte du relais**, vérifiez que le serveur de messagerie répertorié est celui que vous souhaitez utiliser pour envoyer l'alerte.

Astuces Pour changer de serveur de messagerie, cliquez sur **Edit** ( ).

Étape 7 Cliquez sur **Save** (enregistrer).

Configuration des alertes Défense contre les programmes malveillants

Vous pouvez configurer le système pour qu'il vous avertisse chaque fois qu'un événement lié à un programme malveillant, y compris un événement rétrospectif, est généré par défense contre les programmes malveillants (c'est-à-dire qu'un « événement lié au réseau malveillant » est généré.) Vous ne pouvez pas envoyer d'alertes concernant les événements malveillants générés par AMP pour les points terminaux (« événements liés aux programmes malveillants basés sur les points terminaux »).

Avant de commencer

- Configurez une politique de fichiers pour effectuer des recherches dans le nuage de programmes malveillants et associez cette politique à une règle de contrôle d'accès,. Consultez la section *Présentation du contrôle d'accès* dans Guide de configuration Cisco Secure Firewall Management Center Device pour en savoir plus.
- Vous devez avoir la licence Défense contre les programmes malveillants pour configurer ces alertes.

Procédure

Étape 1 Choisissez **Policies (politiques)** > **Actions** > **Alerts (alertes)**.

Étape 2 Cliquez sur **Alertes avancées de protection contre les programmes malveillants**.

Étape 3 Dans la section **Alertes**, choisissez la réponse à l'alerte que vous souhaitez utiliser pour chaque type d'alerte.

Astuces Pour créer une réponse à une alerte, choisissez **New** (nouveau) dans une liste déroulante.

Étape 4 Dans la section **Event Configuration** (configuration de l'événement), cochez les cases correspondant aux alertes que vous souhaitez recevoir pour chaque type d'événement lié à un programme malveillant.

Il faut garder à l'esprit que **tous les événements de programmes malveillants de réseau comprennent les événementsrétrospectifs**.

(Par définition, les événements de programmes malveillants basés sur le réseau n'incluent pas les événements générés par AMP pour les points terminaux.)

Étape 5 Cliquez sur **Save** (enregistrer).

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.