Configurez un système de FireSIGHT pour envoyer des alertes à un serveur externe de Syslog

Contenu

Introduction

Tandis qu'un système de FireSIGHT fournit de diverses vues des événements dans lui est l'interface web, vous peut vouloir configurer la notification d'événement externe pour faciliter la surveillance constante des systèmes essentiels. Vous pouvez configurer un système de FireSIGHT pour générer les alertes qui vous informent par l'intermédiaire de l'email, du déroutement SNMP, ou du Syslog quand un du suivant est généré. Cet article décrit comment configurer un centre de Gestion de FireSIGHT pour envoyer des alertes sur un serveur externe de Syslog.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance sur le Syslog et le centre de Gestion de FireSIGHT. En outre, on doit permettre le port de Syslog (le par défaut est 514) dans votre Pare-feu.

Composants utilisés

Les informations dans ce document sont basées sur la version de logiciel 5.2 ou plus tard.

Attention : Les informations sur ce document sont créées d'une appliance dans un environnement de travaux pratiques spécifique, et commencées par une configuration (par défaut) effacée. Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Envoi des alertes d'intrusion

1. Connectez-vous dans l'interface utilisateur d'utilisateur web de votre centre de Gestion de FireSIGHT.

2. Naviguez vers des **stratégies** > l'**intrusion** > la **stratégie d'intrusion**.

3. Cliquez sur Edit à côté de la stratégie que vous voulez s'appliquer.

4. Cliquez sur en fonction les **paramètres avancés**.

5. Localisez le **Syslog alertant** dans la liste et placez-le à **activer**.

6. Cliquez sur Edit à côté de la droite de l'**alerte de Syslog**.

7. Tapez l'adresse IP de votre serveur de Syslog sur le gisement d'**hôtes de journalisation**.

8. Choisissez une **installation** et une **sévérité** appropriées du menu déroulant. Ceux-ci peuvent être laissés aux valeurs par défaut à moins qu'un serveur de Syslog soit configuré pour recevoir des alertes pour une certaine installation ou sévérité.

9. Cliquez sur en fonction les **informations de stratégie** près du en haut à gauche de cet écran.

10. Cliquez sur le bouton de **modifications de validation**.

11. Réappliquez votre stratégie d'intrusion.

Note: Pour que les alertes soient générées, utilisez cette stratégie d'intrusion dans la règle de contrôle d'accès. S'il n'y a aucune règle de contrôle d'accès configurée, alors placez cette stratégie d'intrusion à utiliser comme action par défaut de la stratégie de contrôle d'accès, et réappliquez la stratégie de contrôle d'accès.

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

Envoi des alertes de santés

Partie : Créez une alerte de Syslog

1. Connectez-vous dans l'interface utilisateur d'utilisateur web de votre centre de Gestion de FireSIGHT.

2. Naviguez vers des **stratégies > des actions > des alertes**.

3. Choisi **créez l'alerte**, qui est du côté droit de l'interface web.

4. Le clic **créent l'alerte de Syslog**. Une fenêtre contextuelle de configuration apparaît.

5. Fournissez un nom pour l'alerte.

6. Complétez l'adresse IP de votre serveur de Syslog dans le **champ Host**.

7. Changez le port si nécessaire par votre serveur de Syslog (le port par défaut est 514).

8. Sélectionnez une **installation** et une **sévérité** appropriées.

9. Cliquez sur le bouton de sauvegarde. Vous reviendrez à la page de **stratégies > d'actions > d'alertes**.

10. Activez la configuration de Syslog.

Partie : Créez les alertes de moniteur de santés

L'instruction suivante décrit les étapes pour configurer des **alertes de moniteur de santés** qui utilise l'alerte de Syslog que vous avez juste créée (dans la section précédente) :

1. Allez à la page de **stratégies > d'actions > d'alertes**, et choisissez les **alertes de moniteur de santés**, qui est près du dessus de la page.

2. Donnez à l'alerte de santés un nom.

3. Choisissez une **sévérité** (maintenant la touche Ctrl tandis que cliquer sur peut être utilisé pour sélectionner plus d'un type de sévérité).

4. Du columnm de **module** choisissez les modules de santés pour lesquels vous voudriez envoyer des alertes au serveur de Syslog (par exemple, utilisation du disque).

5. Sélectionnez l'alerte précédemment créée de Syslog de la colonne d'**alertes**.

6. Cliquez sur le bouton de sauvegarde.

En envoyant l'indicateur d'incidence, découvrez l'événement et les alertes de malware

Vous pouvez également configurer un centre de Gestion de FireSIGHT pour envoyer des alertes de Syslog pour des événements avec un indicateur spécifique d'incidence, type spécifique des événements de détection et d'événements de malware. Afin de faire cela, vous devez la partie : Créez une alerte de Syslog et puis configurez le type d'événements que vous voulez envoyer à votre serveur de Syslog. Vous pouvez faire cela en naviguant vers la page de **stratégies >**

d'actions > d'alertes, et puis en sélectionnant un onglet pour le type vigilant désiré.