TAC

ID de document : 118012

Mis à jour : Mai 20, 2015

Contribué par Nazmul Rajib, ingénieur TAC Cisco.

PDF de téléchargement
Copie
[+] Feedback

Produits connexes

- Centre 750 de Gestion de Cisco FireSIGHT
- Centre 3500 de Gestion de Cisco FireSIGHT
- Centre 1500 de Gestion de Cisco FireSIGHT
- Centre de Gestion de Cisco FireSIGHT
- Appliance virtuelle de centre de Gestion de Cisco FireSIGHT

Contenu

Introduction

Ce document décrit comment déterminer la cause principale et dépanner la question quand les événements de connexion disparaissent du centre de Gestion de FireSIGHT après que le système fonctionne pendant plusieurs jours. Il pourrait se produire en raison des paramètres de configuration du centre de Gestion.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance du centre de Gestion de FireSIGHT.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Centre de Gestion de FireSIGHT
- Version de logiciel 5.2 ou plus tard

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Dépannez

Étape 1 : Déterminez le nombre d'événements enregistrés

Afin de déterminer le nombre d'événements de connexion qui sont enregistrés sur un centre de Gestion de FireSIGHT,

1. Choisissez l'**analyse > les connexions > la vue de Tableau des événements de connexion**.
2. Développez la fenêtre de temps à un large éventail qui entoure tous les événements actuels, par exemple 12 mois.
3. Notez le nombre total de lignes au bas de page. Cliquez sur la dernière page et notez le groupe date/heure du dernier événement disponible de connexion.

Ces informations te donnent une idée de combien et de combien de temps vous pouvez retenir des événements de connexion avec votre configuration en cours.

Étape 2 : Déterminez l'option se connectante

Passez en revue que les connexions sont enregistré, et où dans l'écoulement que les connexions sont enregistré. Vous devriez se connecter des connexions selon les besoins de Sécurité et de conformité de votre organisation. Si votre but est de limiter le nombre d'événements que vous générez, seulement enable se connectant pour les règles essentielles à votre analyse. Cependant, si vous voulez une vue d'ensemble de votre trafic réseau, vous pouvez activer se connecter pour des règles supplémentaires de contrôle d'accès ou pour l'action par défaut. Vous pouvez désactiver la connexion se connectant pour le trafic non essentiel afin d'aider à retenir des événements de connexion pendant une plus longue période.

> **Conseil** : Afin d'optimiser la représentation, Cisco recommande que vous vous connectiez le début ou la fin de la connexion, mais pas chacun des deux.

Remarque: Pour une connexion unique, l'événement de fin-de-connexion contient toutes les informations dans l'événement de début-de-connexion aussi bien que les informations qui ont été recueillies au-dessus de la durée de la session. Pour la confiance et permettez les règles, Fin-de-connexion d'il est recommandé que est utilisé.

Ce tableau explique les différentes options se connectantes disponibles pour chaque action de règle :

Action de règle ou option de se connecter	Log au début	Log à l'extrémité
Confiance Action par défaut : Confiance	X	X
Laissez Action par défaut : Intrusion	X	X
Action par défaut : Détection Moniteur		X (requis)
Bloc Bloc avec la remise Action de Defaut : Bloc	X	
Bloc interactif Bloc interactif avec la remise	X	X (si sauté)
Renseignements de sécurité	X	

Étape 3 : Ajustez la taille de la base de données de connexion

Les événements de connexion dépendent taillé de les événements de nombre maximal de connexions plaçant dans la stratégie de système. Afin de changer la configuration :

1. Choisissez le **système > la stratégie de gens du pays > de système**.
2. Cliquez sur l'icône de *crayon* afin d'éditer la stratégie actuellement appliquée.
3. Choisissez les **événements de base de données > de base de données > de nombre maximal de connexions de connexion**.
4. Changez la valeur pour des **événements de nombre maximal de connexions**.
5. **La stratégie et la sortie de sauvegarde de** clic, et **s'appliquent** alors la stratégie à vos appliances.

La quantité maximale d'événements de connexion qui peuvent être enregistrés dépend du modèle de centre de Gestion :

Remarque: La limite maximum d'événement est partagée entre les événements de connexion et les événements de renseignements de sécurité ; la somme de maximum configurés pour les deux événements ne peut pas dépasser la limite maximum d'événement.

Modèle central de Gestion	Nombre maximal d'événements
FS750, DC750	50 millions
FS1500, DC1500	100 millions
FS2000	300 millions
FS3500, DC3500	500 millions
FS4000	1 milliard
Appliance virtuelle	10 millions

Attention : Une augmentation des limites de base de données peut avoir une incidence des performances défavorable sur le périphérique. Afin d'améliorer la représentation, vous devriez concevoir en fonction des limites d'événement le nombre d'événements que vous travaillez régulièrement avec.

Pour les widgets qui affichent des comptes d'opérations sur une plage de temps, le nombre total d'événements ne pourrait pas refléter le nombre d'événements pour lesquels les données détaillées sont en cas visualiseur disponible. Ceci se produit parce que le système taille parfois des détails de l'événement plus âgés pour gérer l'utilisation d'espace disque. Afin de réduire l'occurrence de l'élagage de détail de l'événement, vous pouvez régler avec précision l'événement se connectant pour se connecter seulement ces événements les plus importants pour votre déploiement.

Informations connexes

- Configurer des limites d'événement de base de données
- Support et documentation techniques - Cisco Systems

Cisco relatif prennent en charge des discussions de la Communauté

Cisco prennent en charge la Communauté est un forum pour que vous posiez et pour répondez à des questions, des suggestions de partage, et collabore avec vos pairs.

Référez-vous au Conventions relatives aux conseils techniques Cisco pour les informations sur des conventions utilisées dans ce document.

Mis à jour : Mai 20, 2015
ID de document : 118012