Les événements de connexion semblent disparaître de FireSIGHT Management Center

Table des matières

Introduction

Ce document décrit comment déterminer la cause première et résoudre le problème lorsque des événements de connexion disparaissent de FireSIGHT Management Center après plusieurs jours d'exécution du système. Cela peut se produire en raison des paramètres de configuration du centre de gestion.

Conditions préalables

Exigences

Cisco vous recommande de connaître FireSIGHT Management Center.

Composants utilisés

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

- Centre de gestion FireSIGHT
- Version de logiciel 5.0 ou ultérieure

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Dépannage

Étape 1 : Déterminer le nombre d'événements stockés

Afin de déterminer le nombre d'événements de connexion qui sont stockés dans FireSIGHT Management Center,

1. Choisissez **Analysis > Connections > Table View of Connection Events**.
2. Étendez la fenêtre de temps à une plage étendue qui englobe tous les événements actuels, par exemple 12 mois.
3. Notez le nombre total de lignes au bas de la page. Cliquez sur la dernière page et notez l'horodatage du dernier événement Connection disponible.

Ces informations vous donnent une idée du nombre et de la durée de conservation des événements de connexion avec votre configuration actuelle.

Étape 2 : Déterminer l'option de journalisation

Vérifiez quelles connexions sont consignées et à quel endroit dans le flux elles sont consignées. Vous devez consigner les connexions en fonction des besoins de votre entreprise en matière de sécurité et de conformité. Si votre objectif est de limiter le nombre d'événements que vous générez, n'activez la journalisation que pour les règles essentielles à votre analyse. Toutefois, si vous souhaitez une vue globale du trafic réseau, vous pouvez activer la journalisation pour des règles de contrôle d'accès supplémentaires ou pour l'action par défaut. Vous pouvez désactiver la consignation des connexions pour le trafic non essentiel afin de conserver les événements de connexion pendant une période plus longue.

> **Conseil** : Afin d'optimiser les performances, Cisco recommande de consigner le début ou la fin de la connexion, mais pas les deux.

> **Note**: Pour une connexion unique, l'événement de fin de connexion contient toutes les informations de l'événement de début de connexion ainsi que les informations collectées pendant la durée de la session. Pour les règles Trust et Allow, il est recommandé d'utiliser End-of-Connection.

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

Action de règle ou option de journalisation	Se connecter au début	Se connecter à la fin
Trust Action par défaut : Trust	X	X
Allow Action par défaut : Intrusion Action par défaut : Découverte	X	X
Monitor		X (obligatoire)
Block Block with reset Action par défaut : Block	X	

Interactive Block Interactive Block with reset	X	X (si contourné)
Renseignements De Sécurité	X	

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

Les événements de connexion sont élagués en fonction du paramètre Maximum Connection Events de la stratégie système. Pour modifier le paramètre :

1. Choisissez **System > Local > System Policy**.
2. Cliquez sur l'icône *crayon* afin de modifier la stratégie actuellement appliquée.
3. Choisissez **Database > Connection Database > Maximum Connection Events**.
4. Modifiez la valeur de **Maximum Connection Events**.
5. Cliquez sur **Save Policy and Exit**, puis sur **Apply** the policy to your appliances.

La quantité maximale d'événements de connexion pouvant être stockée dépend du modèle Management Center :

> **Note**: La limite d'événements maximale est partagée entre les événements de connexion et les événements de sécurité adaptative ; la somme des maximums configurés pour les deux événements ne peut pas dépasser la limite maximale d'événements.

Modèle Management Center	Nombre maximal d'événements
FS750, DC750	50 millions
FS1500, DC1500	100 millions
FS2000	300 millions
FS3500, DC3500	500 millions
FS4000	1 milliard
Appareil virtuel	10 millions

> **Mise en garde** : Une augmentation des limites de base de données peut avoir un impact négatif sur les performances du périphérique. Afin d'améliorer les performances, vous devez adapter les limites d'événements au nombre d'événements avec lesquels vous travaillez régulièrement.

Pour les widgets qui affichent le nombre d'événements sur une plage de temps, le nombre total d'événements peut ne pas refléter le nombre d'événements pour lesquels des données détaillées sont disponibles dans l'observateur d'événements. Cela se produit parce que le système élague parfois des détails d'événements plus anciens pour gérer l'utilisation de l'espace disque. Afin de minimiser l'occurrence de l'élagage des détails des événements, vous pouvez affiner la journalisation des événements pour n'enregistrer que les événements les plus importants pour votre déploiement.

Informations connexes

- Configuration des limites des événements de base de données
- Technical Support & Documentation - Cisco Systems

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.