Guide de dépannage ASA : Manquer des logs aux destinations de Syslog

Contenu

Introduction

Ce document décrit comment dépanner le problème avec la capacité de l'appliance de sécurité adaptable (ASA) pour envoyer des Syslog à de diverses destinations, et, plus spécifiquement, des questions où on observe des symptômes de ce type :

- Adaptive Security Device Manager logging on en temps réel lent (ASDM).
- Syslog intermittents manquant à un ou plusieurs destinations de Syslog.

Avant de commencer

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur Cisco ASA et elles ne sont pas limitées à une version de logiciel de la particularité ASA.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux

Conventions relatives aux conseils techniques Cisco.

Les informations de caractéristique

Les ASA, comme la plupart des autres périphériques de Cisco, sont capables d'envoyer des Syslog à de plusieurs destinations de Syslog. Certaines des destinations généralement utilisées sont illustrées ici :

Le nombre de destinations possibles est un avantage réel. Si choisis soigneusement, et comme illustré ici, ils peuvent être largement classifiés dans deux catégories principales basées sur l'objectif qu'ils atteignent :

- Archivistique
- Élimination des imperfections/dépannage en temps réel

Dans la plupart des réseaux, il est suffisant pour faire activer juste les destinations archivistiques à moins qu'un ou plusieurs des destinations d'élimination des imperfections soient nécessaires. En même temps, et tout à fait souvent, les problèmes résultent d'activer de plusieurs destinations de Syslog simultanément à la haute se connectant des niveaux tels qu'informationnel (niveau 6) ou en haut.

Dépannage de la méthodologie

Toutes les fois que les questions se produisent où il y a une perte des informations de Syslog à un ou plusieurs destinations, il y a deux choses que vous devriez vérifier :

- Passez en revue la configuration syslogging (sortie de **se connecter exécuté par exposition**).
- Regardez la sortie de la **file d'attente de show logging**.

Analyse de données

Passez en revue la configuration de Syslogging

Procédez comme suit :

1. Assurez-vous que le message de Syslog que vous recherchez n'est pas désactivé par l'**aucune** commande du **message de journalisation** *<ID>*.
2. Une fois que confirmé, regardez le nombre de destinations de Syslog activées et du niveau auxquels chaque log est envoyé à chacun. C'est un exemple d'une telle configuration :

```
logging enable
logging timestamp
logging standby
logging console informational
logging buffered informational
logging trap informational
logging asdm informational
logging device-id hostname
logging host inside 172.16.110.32
```

Dans cet exemple, l'ASA envoie des Syslog à 4 destinations différentes au niveau informationnel (niveau 6).

Sortie de file d'attente de show logging

Avec une configuration telle que ce qui précède, où les plusieurs destinations reçoivent un grand nombre de messages de log, vous pouvez s'exécuter dans une situation où l'ASA relâche des messages de Syslog dus à un dépassement du logging queue. En pareil cas, la sortie ressemblera à ceci :

```
ciscoasa# show logging queue Logging Queue length limit : 512 msg(s) 2352325 msg(s) discarded
due to queue overflow 0 msg(s) discarded due to memory allocation failure Current 512 msg on
queue, 512 msgs most on queue
```

Par défaut, le logging queue tient 512 messages.

Problèmes courants

En s'exécutant dans des questions où des messages de Syslog ne sont pas enregistrés, considérez ces options :

- Journalisation console de débronchement. Ouvrir une session à la console **ne devrait pas** être activé pour le fonctionnement normal. La journalisation console devrait être utilisée seulement pour le dépannage en temps réel, avec le niveau se connectant bas ou le faible trafic. Ouvrir une session à la console à un haut débit entraînera au processus se connectant sévèrement au rate-limit les messages. La console est seulement capable des messages de journalisation à 9600 bps, et elle ne prend pas a des logs avant qu'elle commence essayer pour vider plus à la console que la console peut sortir à l'écran. Dans cette situation, les logs commenceront à être mis en mémoire tampon dans le logging queue. Une fois que le logging queue se remplit, des messages queue-seront relâchés.
- Augmentez la taille du logging queue au delà de 512. Le logging queue maximum est 1024 sur l'ASA 5505, 2048 sur l'ASA 5510, et 8192 sur toutes autres Plateformes. Remarque: Le logging queue est utilisé pour des « rafales » des Syslog. Si le débit soutenu de Syslog est plus rapide que l'ASA peut les transmettre aux diverses destinations, aucune limite de logging queue ne sera assez grande.
- Désactivez les différents messages de Syslog que vous n'êtes pas intéressé à archiver. N'émettez l'aucune commande de *<syslog_id> de* message de journalisation afin de désactiver différents Syslog.
- Faites attention des messages de journalisation au disque (éclair) de l'ASA. L'inscription à l'éclair est une exécution très lente. Se connecter excessif à flasher fera mettre en mémoire tampon l'ASA les fichiers de Syslog dans la mémoire, épuisant par la suite toute la mémoire disponible (RAM). Supplémentaire, se connecter un grand nombre de messages de Syslog pour flasher peut élever la CPU. Il est recommandé pour se connecter seulement les messages du niveau 1 pour flasher (qui couvrent des événements de système essentiels).

Informations connexes

- Support et documentation techniques - Cisco Systems