Guide de dépannage ASA : Journaux manquants sur les destinations Syslog

Contenu

Introduction

Ce document décrit comment résoudre le problème lié à la capacité de l'ASA (Adaptive Security Appliance) à envoyer des Syslog vers différentes destinations, et plus précisément, les problèmes où des symptômes tels que ceux-ci sont observés :

- Lenteur de la journalisation en temps réel sur Adaptive Security Device Manager (ASDM).
- Syslogs intermittent manquant sur une ou plusieurs destinations Syslog.

Avant de commencer

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur Cisco ASA et ne se limitent pas à une version spécifique du logiciel ASA.

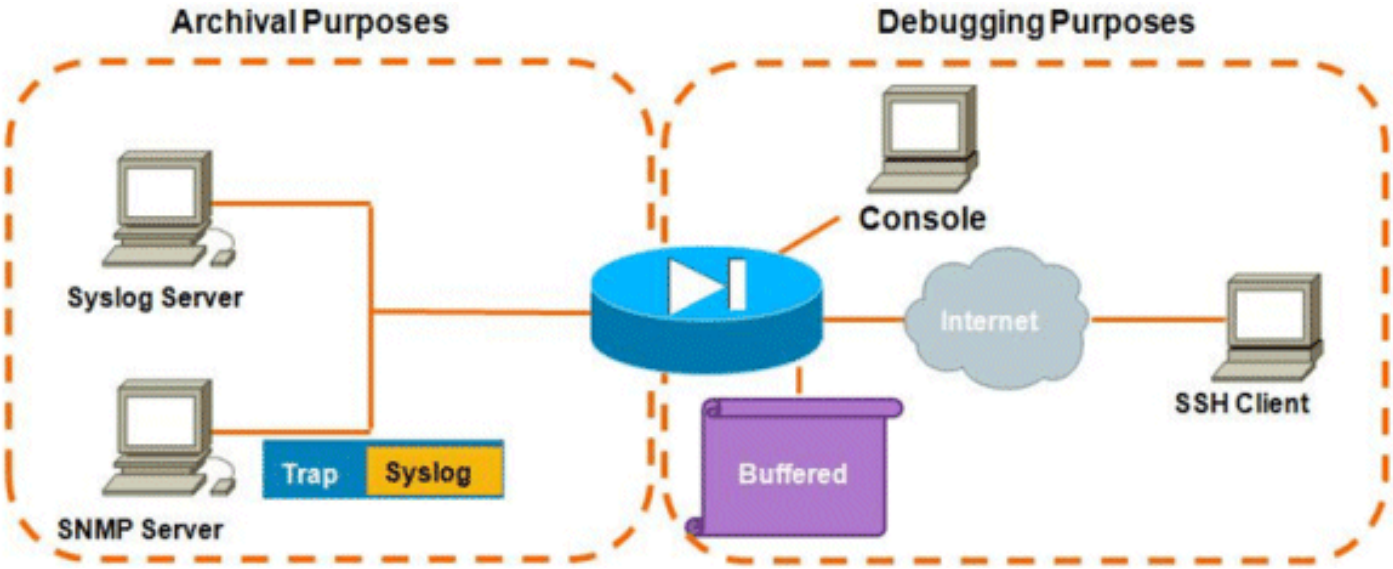
Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions

utilisées pour les conseils techniques de Cisco.

Informations sur les fonctionnalités

Les ASA, comme la plupart des autres périphériques Cisco, sont capables d'envoyer des Syslog vers plusieurs destinations Syslog. Voici quelques-unes des destinations les plus utilisées :



Le nombre de destinations possibles est un réel avantage. Si elles sont choisies avec soin, et comme l'illustre le présent document, elles peuvent être classées en deux grandes catégories en fonction de l'objet qu'elles servent :

- Archivé
- Débogage/dépannage en temps réel

Dans la plupart des réseaux, il suffit d'activer uniquement les destinations d'archivage, sauf si une ou plusieurs des destinations de débogage sont nécessaires. En même temps, et très souvent, les problèmes résultent de l'activation simultanée de plusieurs destinations syslog à des niveaux de journalisation élevés tels que les informations (niveau 6) ou supérieures.

Méthodologie de dépannage

Lorsque des problèmes surviennent lorsqu'il y a perte d'informations Syslog sur une ou plusieurs destinations, vous devez vérifier deux choses :

- Examinez la configuration syslogging (sortie de **show run logging**).
- Regardez la sortie de **show logging queue**.

Analyse des données

Vérifier la configuration Syslogging

Procédez comme suit :

1. Assurez-vous que le message syslog que vous recherchez n'est pas désactivé par la

commande **no logging message** *<ID>.*

2. Une fois la confirmation effectuée, examinez le nombre de destinations syslog activées et le niveau d'envoi de chaque journal à chacune d'elles. Voici 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 syslogs à 4 destinations différentes au niveau des informations (niveau 6).

Sortie de la commande show logging queue

Avec une configuration comme celle ci-dessus, où plusieurs destinations reçoivent de grands volumes de messages de journal, vous pouvez vous retrouver dans une situation où l'ASA abandonne les messages syslog en raison d'un débordement de la file d'attente de journalisation. Dans ce cas, le résultat sera similaire à celui-ci :

```
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, la file d'attente de journalisation contient 512 messages.

Problèmes courants

Lorsque vous rencontrez des problèmes où les messages Syslog ne sont pas enregistrés, tenez compte des options suivantes :

- Désactivez la journalisation de console. La connexion à la console **ne doit pas** être activée pour un fonctionnement normal. La journalisation de console doit être utilisée uniquement pour le dépannage en temps réel, avec un niveau de journalisation faible ou un trafic faible. Si vous vous connectez à la console à un débit élevé, le processus de journalisation limitera considérablement le débit des messages. La console ne peut consigner les messages qu'à 9 600 bps, et il ne faut pas de journaux avant de commencer à essayer de vider plus de messages sur la console que la console ne peut afficher à l'écran. Dans ce cas, les journaux commenceront à être mis en mémoire tampon dans la file d'attente de journalisation. Une fois que la file d'attente de journalisation est remplie, les messages sont abandonnés.
- Augmentez la taille de la file d'attente de journalisation au-delà de 512. La file d'attente de journalisation maximale est 1024 sur les modèles ASA-5505, 2048 sur les modèles ASA-5510 et 8192 sur toutes les autres plates-formes. Note: La file d'attente de journalisation est utilisée pour les « rafales » de syslogs. Si le taux soutenu de syslogs est plus rapide que celui que l'ASA peut transmettre aux différentes destinations, aucune limite de file d'attente de journalisation ne sera suffisante.

- Désactivez les messages syslog individuels que vous ne souhaitez pas archiver. Émettez la commande no logging message *<syslog_id>* afin de désactiver des syslogs individuels.
- Veillez à consigner les messages sur le disque (flash) de l'ASA. L'écriture sur la mémoire flash est une opération très lente. Une journalisation excessive vers la mémoire flash entraîne la mise en mémoire tampon des fichiers syslog par l'ASA, ce qui finit par épuiser toute la mémoire disponible (RAM). En outre, la consignation de grandes quantités de messages syslog dans la mémoire flash peut élever le processeur. Il est recommandé de consigner uniquement les messages de niveau 1 dans la mémoire Flash (qui couvrent les événements système critiques).

Informations connexes

- Support et documentation techniques - Cisco Systems