Leitfaden zur ASA-Fehlerbehebung: Fehlende Protokolle bei Syslog-Ziel(en)

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie das Problem mit der Fähigkeit der Adaptive Security Appliance (ASA) behoben werden kann, Syslogs an verschiedene Ziele zu senden. Insbesondere werden Probleme bei Symptomen wie diesen beschrieben beschrieben behandelt:

- Langsame Echtzeit-Protokollierung im Adaptive Security Device Manager (ASDM).
- Gelegentliche Syslog-Einträge fehlen an einem oder mehreren Syslog-Zielen.

Bevor Sie beginnen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco ASA und sind nicht auf eine bestimmte ASA-Softwareversion beschränkt.

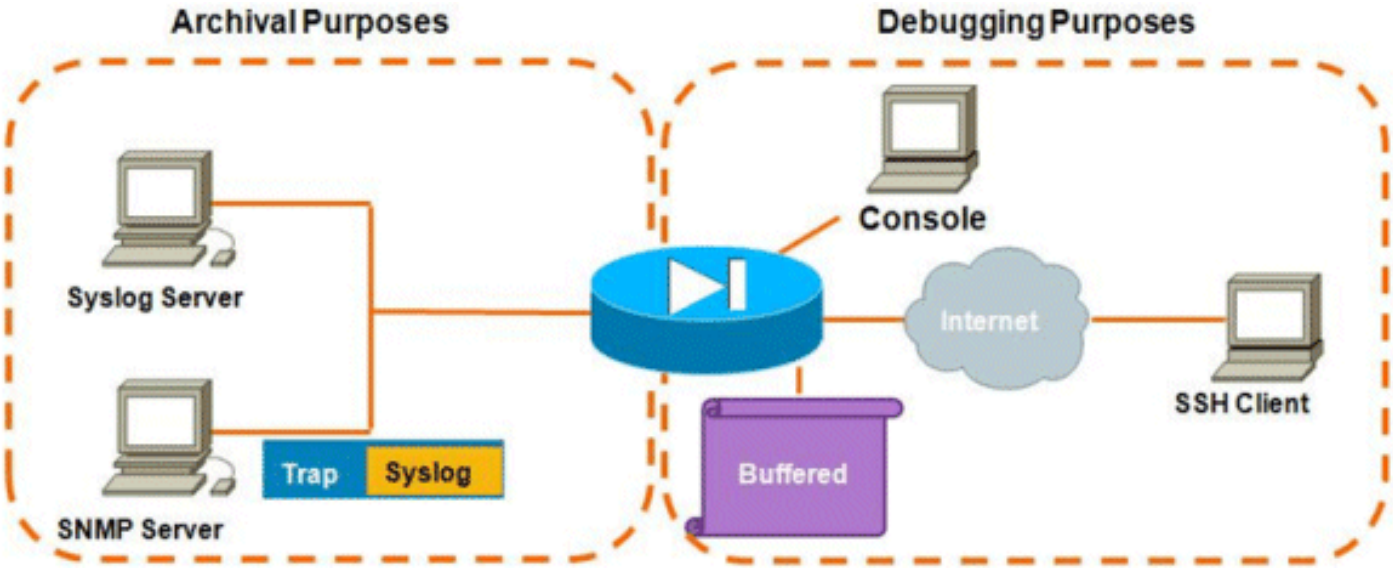
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips

Conventions.

Informationen zu Funktionen

ASAs sind wie die meisten anderen Cisco Geräte in der Lage, Syslogs an mehrere Syslog-Ziele zu senden. Einige der am häufigsten verwendeten Ziele sind hier aufgeführt:



Die Anzahl der möglichen Ziele ist ein echter Vorteil. Bei sorgfältiger Auswahl und entsprechend der hier gezeigten Darstellung lassen sich diese in zwei Hauptkategorien einteilen:

- Archivierung
- Debuggen/Problembehandlung in Echtzeit

In den meisten Netzwerken ist es ausreichend, nur die Archivierungsziele aktiviert zu haben, es sei denn, ein oder mehrere Debugziele sind erforderlich. Gleichzeitig und häufig entstehen Probleme, wenn mehrere Syslog-Ziele gleichzeitig auf hohen Protokollierungsebenen (z. B. Informationsstufe 6 oder höher) aktiviert werden.

Fehlerbehebungsmethode

Wenn Probleme auftreten, bei denen Syslog-Informationen an einem oder mehreren Zielen verloren gehen, sollten Sie zwei Punkte überprüfen:

- Überprüfen Sie die Syslogging-Konfiguration (Ausgabe von **show run logging**).
- Schauen Sie sich die Ausgabe der **Warteschlange für die Anzeigeprotokollierung an.**

Datenanalyse

Überprüfen der Syslogging-Konfiguration

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass die gesuchte Syslog-Meldung nicht durch den Befehl **no logging** ***<ID>*** deaktiviert ist.

2. Überprüfen Sie nach der Bestätigung die Anzahl der aktivierten Syslog-Ziele und die Ebene, auf der die einzelnen Protokolle an die einzelnen Protokolle gesendet werden. Dies ist ein Beispiel für eine solche Konfiguration:

```
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
```

In diesem Beispiel sendet die ASA Syslogs an 4 verschiedene Ziele auf Informationsebene (Stufe 6).

Ausgabe der Show Logging Queue

Bei einer Konfiguration wie der oben beschriebenen, bei der mehrere Ziele große Mengen an Protokollmeldungen empfangen, kann es vorkommen, dass die ASA Syslog-Meldungen aufgrund eines Überlaufs der Protokollierungswarteschlange verwirft. In solchen Fällen sieht die Ausgabe ähnlich aus wie folgt:

```
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
```

Standardmäßig enthält die Protokollierungswarteschlange 512 Meldungen.

Häufige Probleme

Wenn Probleme auftreten, bei denen Syslog-Meldungen nicht aufgezeichnet werden, sollten Sie folgende Optionen in Betracht ziehen:

- Deaktivieren Sie die Konsolenprotokollierung. Die Anmeldung bei der Konsole **sollte nicht** für den normalen Betrieb aktiviert werden. Konsolenprotokollierung sollte nur für die Fehlerbehebung in Echtzeit verwendet werden, entweder bei niedriger Protokollierung oder bei geringem Datenverkehr. Wenn Sie sich bei hoher Geschwindigkeit bei der Konsole anmelden, werden die Meldungen beim Protokollierungsprozess stark eingeschränkt. Die Konsole kann Nachrichten nur mit einer Geschwindigkeit von 9.600 Bit/s protokollieren, und es werden keine Protokolle benötigt, bevor versucht wird, mehr auf die Konsole zu übertragen, als die Konsole auf den Bildschirm ausgeben kann. In dieser Situation werden die Protokolle in der Protokollierungswarteschlange gepuffert. Sobald die Protokollierungswarteschlange gefüllt ist, werden Nachrichten zum Tail-Drop verworfen.
- Erhöhen Sie die Größe der Protokollierungswarteschlange auf mehr als 512. Die maximale Protokollierungswarteschlange für ASA-5505, 2048 für ASA-5510 und 8192 für alle anderen Plattformen beträgt 1024. Hinweis: Die Protokollierungswarteschlange wird für "Bursts" von Syslogs verwendet. Wenn die anhaltende Anzahl von Syslogs schneller ist, als die ASA sie an die verschiedenen Ziele übertragen kann, ist die Beschränkung für die Protokollierungswarteschlange nicht groß genug.

- Deaktivieren Sie einzelne Syslog-Meldungen, die Sie nicht archivieren möchten. Geben Sie den Befehl no logging message *<syslog_id>* ein, um einzelne Syslogs zu deaktivieren.
- Achten Sie darauf, Nachrichten auf der Festplatte (Flash) der ASA zu protokollieren. Das Schreiben in den Blitz ist eine sehr langsame Operation. Eine übermäßige Protokollierung des Flash-Speichers führt dazu, dass die ASA die Syslog-Dateien im Speicher puffert und schließlich alle verfügbaren Speichermodule (RAM) ausschaltet. Darüber hinaus kann die Protokollierung großer Mengen von Syslog-Meldungen in Flash die CPU erhöhen. Es wird empfohlen, nur Meldungen der Stufe 1 zu protokollieren, die als Flash-Speicher angezeigt werden (in denen kritische Systemereignisse behandelt werden).

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems