

Guía de Troubleshooting ASA: Registros que falta en el destino de syslog

Contenido

[Introducción](#)

[Antes de comenzar](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Información sobre la Función](#)

[Metodología de Troubleshooting](#)

[Análisis de datos](#)

[Revise la configuración del syslogging](#)

[Salida de la cola del registro de la demostración](#)

[Problemas Comunes](#)

[Información Relacionada](#)

[Introducción](#)

Este documento describe cómo resolver problemas el problema con la capacidad del dispositivo de seguridad adaptante (ASA) para enviar los Syslog a los diversos destinos, y, más concretamente, las cuestiones donde los síntomas tales como éstos se observan:

- Tiempo real lento que abre una sesión al Administrador de dispositivos de seguridad adaptante (ASDM).
- Syslog intermitentes que faltan en uno o más destinos de syslog.

[Antes de comenzar](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

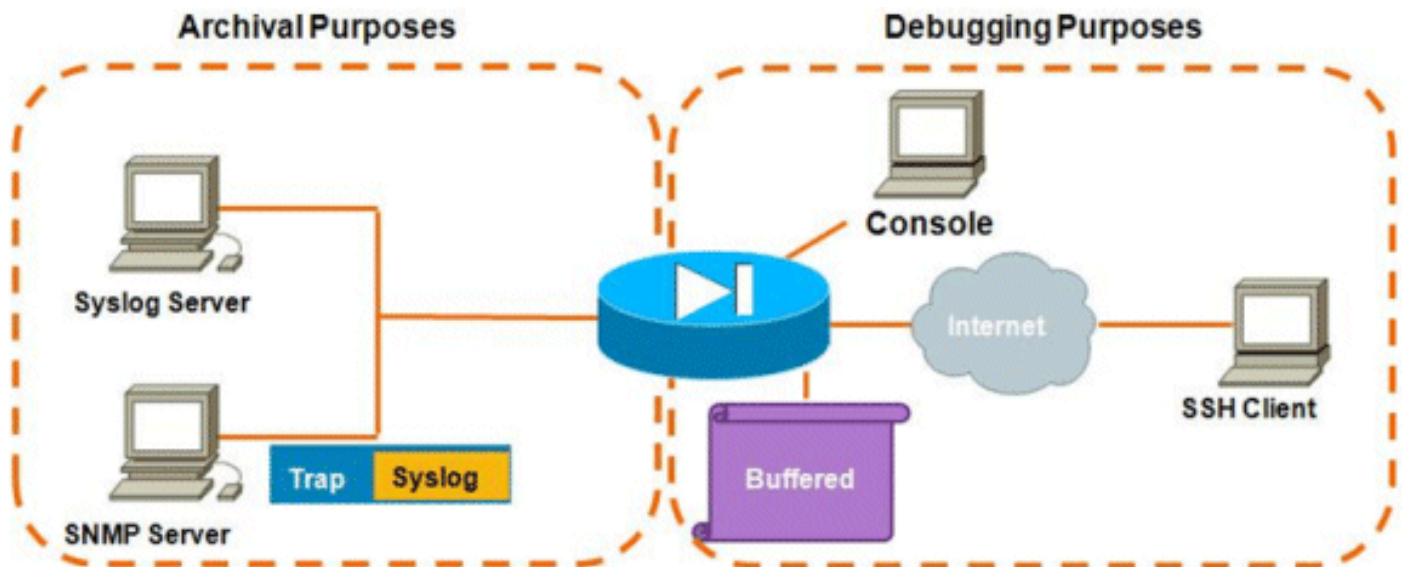
La información en este documento se basa en Cisco ASA y no se limita a una versión de software específica ASA.

[Convenciones](#)

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de Consejos Técnicos de Cisco](#).

Información sobre la Función

Los ASA, como la mayoría de otros dispositivos de Cisco, son capaces de enviar los Syslog a los destinos de syslog múltiples. Algunos de los destinos generalmente usados se ilustran aquí:



El número de destinos posibles es una ventaja real. Si están elegidos cuidadosamente, y según lo ilustrado aquí, pueden ser clasificados ampliamente en dos categorías principales basadas en el propósito que sirven:

- Archival
- Debugging en tiempo real/troubleshooting

En la mayoría de las redes, es suficiente hacer apenas los destinos archivales habilitar a menos que uno o más de los destinos del debugging sean necesarios. Al mismo tiempo, y muy a menudo, los problemas resultan de habilitar los destinos de syslog múltiples simultáneamente en los altos niveles de registro tales como informativo (el nivel 6) o arriba.

Metodología de Troubleshooting

Siempre que ocurran los problemas donde hay una pérdida de Información de syslog en uno o más destinos, hay dos cosas que usted debe marcar:

- [Revise la configuración del syslogging \(salida del registro del funcionamiento de la demostración\).](#)
- [Mire la salida de la cola del registro de la demostración.](#)

Análisis de datos

Revise la configuración del syslogging

Complete estos pasos:

1. Asegurese que el mensaje de Syslog que usted está buscando no es inhabilitado por el **ningún** comando del **mensaje de registraci3n** <ID>.
2. Una vez que est3 confirmado, mire el n3mero de destinos de syslog habilitados y del nivel en los cuales cada registro se env3e a cada uno. 3ste es un ejemplo de tal

```
configuraci3n: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
```

En este ejemplo, el ASA est3 enviando los Syslog a 4 diversos destinos en el nivel informativo (nivel 6).

Salida de la cola del registro de la demostraci3n

Con una configuraci3n tal como el antedicho, donde los destinos m3ltiples est3n recibiendo una gran cantidad de mensajes del registro, usted puede ejecutarse en una situaci3n donde el ASA cae los mensajes de Syslog debido a un desbordamiento de la cola del registro. En estos casos, la salida aparecer3 similar a esto:

```
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
```

Por abandono, la cola del registro lleva a cabo 512 mensajes.

Problemas Comunes

Al ejecutarse en los problemas donde los mensajes de Syslog no se est3n registrando, considere estas opciones:

- Inhabilite el registro de la consola. La apertura de sesi3n a la consola **no se debe** habilitar para el funcionamiento normal. El registro de la consola se debe utilizar solamente para el Troubleshooting en tiempo real, con el nivel de registro bajo o el poco tr3fico. La apertura de sesi3n a la consola a una alta velocidad causar3 a tarifa-l3mite del proceso del registro seriamente los mensajes. La consola es solamente capaz de los mensajes de registraci3n en 9600 BPS, y no toma a de los registros antes de que comience a intentar vaciar m3s a la consola que la consola puede hacer salir a la pantalla. En esta situaci3n, los registros comenzar3n a ser mitigados en la cola del registro. Una vez que la cola del registro se llena, los mensajes Tail-ser3n ca3dos.
- Aumente el tama3o de la [cola del registro](#) m3s all3 de 512. La cola m3xima del registro es 1024 en el ASA-5505, 2048 en el ASA-5510, y 8192 en el resto de las Plataformas. Nota: La cola del registro se utiliza para las "explosiones" de los Syslog. Si la velocidad sostenida de los Syslog es m3s r3pida que el ASA puede transmitirlos a los diversos destinos, no hay l3mite de cola del registro bastante grande.
- Inhabilite los mensajes de Syslog individuales que usted no est3 interesado en archivar. Publique el [comando no logging message <syslog_id>](#) para inhabilitar los Syslog individuales.
- Tenga cuidado de los mensajes de registraci3n al disco (flash) del ASA. La escritura al flash es una operaci3n muy lenta. El registro excesivo a contellear har3 el ASA mitigar los archivos

del Syslog para arriba en la memoria, agotando eventual toda la memoria disponible (RAM). Además, la registración de una gran cantidad de mensajes de Syslog para contellear puede elevar el CPU. Se recomienda para registrar solamente los mensajes del nivel 1 para contellear (que cubren los eventos de sistema crítico).

[Información Relacionada](#)

- [Soporte Técnico y Documentación - Cisco Systems](#)