Guía de solución de problemas de ASA: Registros faltantes en los Destinos de Syslog

Contenido

Introducción
Antes de comenzar
Requirements
Componentes Utilizados
Convenciones
Información sobre la Función
Metodología de solución de problemas
Análisis de datos
Revisar la configuración de Syslogging
Salida de show logging queue
Problemas Comunes
Información Relacionada

Introducción

Este documento describe cómo resolver el problema con la capacidad del dispositivo de seguridad adaptable (ASA) para enviar registros del sistema a varios destinos y, más específicamente, problemas donde se observan síntomas como estos:

- Registro lento en tiempo real en Adaptive Security Device Manager (ASDM).
- Faltan syslogs intermitentes en uno o más destinos syslog.

Antes de comenzar

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

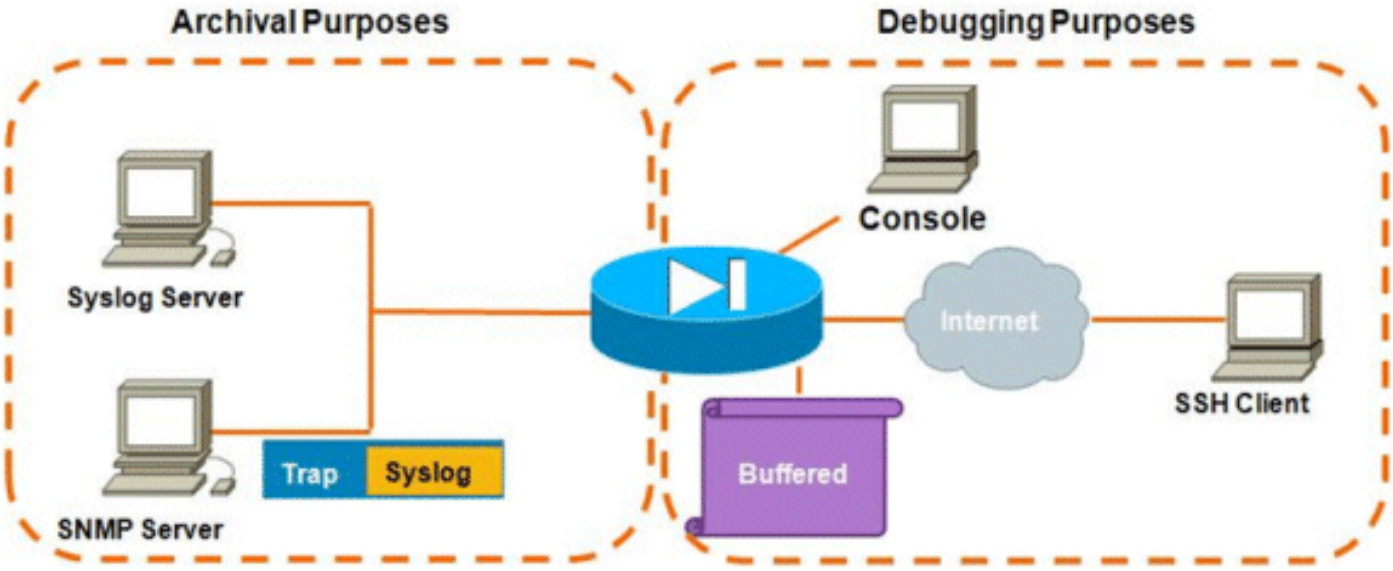
Convenciones

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 los otros dispositivos de Cisco, pueden enviar registros del sistema a varios destinos de syslog. Aquí se ilustran algunos de los destinos más utilizados:



El número de destinos posibles es una ventaja real. Si se eligen cuidadosamente, y como se ilustra aquí, pueden clasificarse ampliamente en dos categorías principales según el propósito al que sirven:

- Archival
- Depuración/resolución de problemas en tiempo real

En la mayoría de las redes, es suficiente tener solamente los destinos de archivado habilitados a menos que uno o más de los destinos de depuración sean necesarios. Al mismo tiempo, y con mucha frecuencia, los problemas se deben a la habilitación simultánea de varios destinos syslog a niveles de registro altos, como información (nivel 6) o superior.

Metodología de solución de problemas

Siempre que se producen problemas cuando se produce una pérdida de información de syslog en uno o más destinos, hay dos cosas que debe verificar:

- Revise la configuración de syslogging (salida de **show run logging**).
- Observe el resultado de **show logging queue**.

Análisis de datos

Revisar la configuración de Syslogging

Complete estos pasos:

1. Asegúrese de que el mensaje syslog que está buscando no esté desactivado por el

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

2. Una vez confirmado, observe el número de destinos syslog habilitados y el nivel en el que se envía cada registro a cada uno. Este es un ejemplo de tal configuración:

```
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 está enviando registros del sistema a 4 destinos diferentes a nivel informativo (Nivel 6).

Salida de show logging queue

Con una configuración como la anterior, donde varios destinos reciben grandes cantidades de mensajes de registro, puede encontrarse con una situación en la que ASA descarta mensajes de syslog debido a un desbordamiento de la cola de registro. En tales casos, el resultado será similar a este:

```
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
```

De forma predeterminada, la cola de registro contiene 512 mensajes.

Problemas Comunes

Cuando encuentre problemas en los que no se están grabando los mensajes de syslog, tenga en cuenta estas opciones:

- Desactive el registro de la consola. El inicio de sesión en la consola **no debe** estar habilitado para el funcionamiento normal. El registro de la consola se debe utilizar solamente para la resolución de problemas en tiempo real, con bajo nivel de registro o bajo tráfico. Al iniciar sesión en la consola a una velocidad alta, el proceso de registro limitará la velocidad de los mensajes de forma drástica. La consola sólo es capaz de registrar mensajes a 9600 bps, y no requiere un montón de registros antes de comenzar a volcar más a la consola de lo que la consola puede enviar a la pantalla. En esta situación, los registros empezarán a almacenarse en la cola de registro. Una vez que se complete la cola de registro, los mensajes serán descartados.
- Aumente el tamaño de la cola de registro más allá de 512. La cola de registro máxima es 1024 en ASA-5505, 2048 en ASA-5510 y 8192 en todas las demás plataformas. Nota: La cola de registro se utiliza para "ráfagas" de syslogs. Si la velocidad sostenida de syslogs es más rápida de lo que ASA puede transmitirlos a los diversos destinos, ningún límite de cola de registro será lo suficientemente grande.
- Inhabilite los mensajes de syslog individuales que no le interese archivar. Ejecute el comando no logging message *<syslog_id>* para inhabilitar los syslogs individuales.

- Tenga cuidado de registrar mensajes en el disco (flash) del ASA. Escribir en el flash es una operación muy lenta. El registro excesivo en la memoria flash hará que el ASA almacene los archivos syslog en la memoria, agotando finalmente toda la memoria disponible (RAM). Además, el registro de grandes cantidades de mensajes syslog en flash puede elevar la CPU. Se recomienda registrar solamente los mensajes de nivel 1 en flash (que cubren los eventos críticos del sistema).

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems