Diferencias entre los registros y los debugs en los dispositivos de seguridad adaptantes

Contenido

Introducción

Este documento proporciona una descripción simple para las funciones del debugging en los dispositivos de seguridad adaptantes (ASA) esa versión 8.4 y posterior del funcionamiento. Sin embargo, algunas de las características están disponibles solamente en la versión 9.5(2) y posterior.

Prerequisites

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ASA 5506-X con la versión de software ASA 9.5(2)
- Versión 7.5.2 del Cisco Adaptive Security Device Manager (ASDM)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Funciones básicas del registro

Mensajes del debug de la manija ASA diferentemente que los dispositivos del ® del Cisco IOS. Por abandono (a menos que se utiliza de “debug-traza registración”, que se describe más adelante,),

ella se visualiza en la pantalla cualquiera cuando usted está conectado a través del puerto de la consola o con el telnet/el Secure Shell (SSH), pero ella es totalmente independiente. Cuando usted utiliza la consola, ella aparece inmediatamente después que usted ingresa el comando debug. La misma acción también sucede con una sesión SSH.

La independencia significa que cuando usted habilita los debugs en el puerto de la consola y usted está conectado con SSH, los debugs no aparecen en SSH. Usted tiene que habilitarlos manualmente otra vez. También, si los debugs se habilitan en una sesión SSH no aparecerán en absoluto en la otra sesión. Usted puede referirle según el **debugging de la sesión.**

No hay tampoco necesidad de ingresar el **comando terminal monitor** en un ASA para mostrar los debugs, porque los debugs habilitados en el SSH o una sesión telnet aparecen sin importar este comando. El propósito de este comando es mucho diferente que en el ejemplo de los dispositivos Cisco IOS y de la configuración de syslog ASA describe esa característica profundizada.

Diferencia entre los mensajes del syslog y debug

Los debugs son mensajes especificados para un cierto protocolo o característica de los ASA. No hay nivel de debugs, en lugar son muy detallados y el nivel del detalle puede ser cambiado. También puede ser que no tengan un grupo fecha/hora, un código del mensaje, o un nivel de gravedad. Esto es dependiente en el debug determinado.

Este ejemplo muestra la diferencia entre los debugs y los mensajes de Syslog con respecto al mismo pedido de ping.

Éste es un ejemplo de la salida de los debugs después de que usted ingrese el **comando debug icmp trace**:

```
ICMP echo request from 10.229.24.48 to 10.48.67.75 ID=1 seq=29 len=32

ICMP echo reply from 10.48.67.75 to 10.229.24.48 ID=1 seq=29 len=32
```

Éste es un ejemplo de un **mensaje de Syslog** con respecto a la misma petición ICMP:

```
Jan 01 2016 13:29:22: %ASA-6-302020: Built inbound ICMP connection for faddr 10.229.24.48/1
 gaddr 10.48.67.75/0 laddr 10.48.67.75/0

Jan 01 2016 13:29:22: %ASA-6-302021: Teardown ICMP connection for faddr 10.229.24.48/1
 gaddr 10.48.67.75/0 laddr 10.48.67.75/0
```

Recoja los debugs

El tiempo de espera predeterminado para SSH o el telnet es cinco minutos y la sesión es disconnected después de esta época de la inactividad. El tiempo de espera predeterminado para la conexión de consola es 0, así que significa que abren una sesión al usuario hasta que el usuario termine la sesión manualmente.

Desafortunadamente la característica de registro es limitada por el descanso fijado en un método de Administración determinado, así que cuando la sesión SSH termina los debugs también paran.

Para continuar recogiendo los debugs por un tiempo extendido, usted tiene que utilizar la conexión de consola y entonces usted puede reorientarlos al servidor de Syslog con el comando

de la debug-**traza del registro**. Serán reorientados como mensaje de Syslog 711001 publicado en el nivel de gravedad 7. para parar el enviar esto de los mensajes a los registros, usted pueden utilizar el “no” del separador de millares antes del comando.

```
logging debug-trace
no logging debug-trace
```

De la versión 9.5.2, el ASA permite que usted continúe enviando los debugs como mensajes de Syslog después de un descanso o terminando la sesión en una conexión SSH/telnet/console. Si usted ingresa el **comando persistent de la debug-traza que** usted será selectivamente debugs claros capaces habilitados en una sesión de una diversa sesión y permanecerán activos en el fondo. Para inhabilitar esta característica, inserte el “no” antes del comando.

```
logging debug-trace persistent
no logging debug-trace persistent
```

Por abandono, todos los mensajes del debug tienen una gravedad del nivel 7. para filtrarlos de los mensajes no deseados que usted puede aumentar la gravedad de este mensaje a 3 así que usted recogerá solamente los mensajes de error al lado de los debugs. Inserte el “no” para inhabilitar este cambio de dirección.

```
logging message 711001 level 3
no logging message 711001 level 3
```

Configuración de muestra:

```
logging enable
logging host 10.0.0.1
logging trap errors
logging debug-trace persistent
logging message 711001 level errors
debug icmp trace
```

Estos comandos enable usted de enviar los mensajes de error y el Internet Control Message Protocol (ICMP) hace el debug de marcado también como errores al servidor de Syslog:

```
Jan 01 2016 13:30:22: %ASA-3-711001: ICMP echo request from 10.229.24.48 to 10.48.67.75 ID=1
 seq=29 len=32

Jan 01 2016 13:30:22: %ASA-3-711001: ICMP echo reply from 10.48.67.75 to 10.229.24.48 ID=1
 seq=29 len=32
```

Información Relacionada

- Ejemplo de la configuración de syslog ASA
- Soporte Técnico y Documentación - Cisco Systems