Diferencias entre registros y depuraciones en dispositivos de seguridad adaptables

Contenido

Introducción

Este documento proporciona una descripción sencilla de la funcionalidad de depuración en Adaptive Security Appliances (ASA) que ejecutan la versión 8.4 y posteriores. Sin embargo, algunas de las funciones solo están disponibles en la versión 9.5(2) y posteriores.

Prerequisites

Requirements

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 software ASA versión 9.5(2)
- Versión 7.5.2 de Cisco Adaptive Security Device Manager (ASDM)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Funcionalidad Básica de Registro

Los ASA manejan los mensajes de depuración de manera diferente que los dispositivos Cisco IOS®. De forma predeterminada (a menos que se utilice "logging debug-trace", que se describe más adelante), se muestran en la pantalla cuando se conecta a través del puerto de la consola o a través de Telnet/Secure Shell (SSH), pero son completamente independientes. Cuando utiliza la

consola, aparecen inmediatamente después de ingresar el comando debug. La misma acción también sucede con una sesión SSH.

La independencia significa que cuando habilita los debugs en el puerto de la consola y está conectado a través de SSH, los debugs no aparecen en SSH. Debe volver a habilitarlos manualmente. Además, si las depuraciones están habilitadas en una sesión SSH, no aparecerán en absoluto en la otra sesión. Puede referirse a él como **depuración por sesión.**

Tampoco es necesario ingresar el comando **terminal monitor** en un ASA para mostrar las depuraciones, porque las depuraciones habilitadas en SSH o una sesión telnet aparecen independientemente de este comando. El propósito de este comando es muy diferente que en los dispositivos Cisco IOS y el Ejemplo de Configuración de Syslog ASA describe esa función en profundidad.

Diferencia entre Mensajes de Syslog y Debug

Los debugs son mensajes especificados para un protocolo o función determinados de ASA. No hay nivel de depuraciones, en su lugar son muy detalladas y se puede cambiar el nivel de detalle. También es posible que no tengan una marca de tiempo, un código de mensaje o un nivel de gravedad. Esto depende de la depuración específica.

Este ejemplo muestra la diferencia entre los mensajes de depuración y syslog en relación con la misma solicitud de ping.

Este es un ejemplo de resultado de debug después de ingresar 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
```

Este es un ejemplo de un mensaje **syslog** con respecto a la misma solicitud 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
```

Recopilar depuraciones

El tiempo de espera predeterminado para SSH o telnet es de cinco minutos y la sesión se desconecta después de este tiempo de inactividad. El tiempo de espera predeterminado para la conexión de consola es 0, lo que significa que el usuario ha iniciado sesión hasta que el usuario se desconecte manualmente.

Desafortunadamente, la función de registro está limitada por el tiempo de espera establecido en un método de administración determinado, por lo que cuando la sesión SSH finaliza, las depuraciones también se detienen.

Para continuar recolectando los debugs durante un tiempo prolongado, debe utilizar la conexión de consola y luego redirigirlos al servidor syslog con el comando **logging debug-trace**. Se redirigirán como mensaje de syslog 711001 emitido en el nivel de gravedad 7. Para detener el

envío de estos mensajes a los registros, puede utilizar insertar "no" antes del comando.

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

Desde la versión 9.5.2, el ASA le permite continuar enviando depuraciones como mensajes syslog después de un tiempo de espera o desconectarse en una conexión SSH/telnet/console. Si ingresa el comando **debug-trace persistent** podrá borrar selectivamente las depuraciones habilitadas en una sesión de una sesión diferente y permanecerán activas en segundo plano. Para inhabilitar esta función, inserte "no" antes del comando.

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

De forma predeterminada, todos los mensajes de depuración tienen una gravedad del nivel 7. Para filtrarlos de mensajes no deseados, puede elevar la gravedad de este mensaje a 3 para que recopile solamente los mensajes de error junto a las depuraciones. Inserte "no" para inhabilitar este redireccionamiento.

```
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 le permiten enviar mensajes de error y depuraciones de protocolo de mensajes de control de Internet (ICMP) marcadas también como errores al servidor 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 configuración de Syslog de ASA
- Soporte Técnico y Documentación - Cisco Systems