

Contenido

[Introducción](#)

[Genere el archivo del Troubleshooting](#)

[Datos adicionales del Troubleshooting](#)

Introducción

Un archivo del Troubleshooting contiene una colección de mensajes del registro, de datos de configuración, y de salidas de comando. Se utiliza para determinar el estatus de un sistema de Sourcefire. Si un ingeniero de soporte de Cisco le solicita enviar un archivo del Troubleshooting de su plataforma de las X-series de BlueCoat (también conocida como sensor de la viga transversal), siga las instrucciones en este documento. Este documento también proporciona una lista de los datos adicionales que pudieron ser necesarios analizar un problema.

Genere el archivo del Troubleshooting

1. Registro en su dispositivo de las X-series de BlueCoat como `Usuario administrador`.
2. Encuentre al grupo VAP para el software de Sourcefire.

```
show application vap-group
```

El producto siguiente es un ejemplo del comando antedicho. En este ejemplo, el grupo del vap es `sf53`.

```
show application vap-group
```

3. Después, necesitamos aumentar el privilegio de modo que poder shell remoto en el grupo sí mismo VAP:

```
unix su
```

4. Entonces, abra shell remoto una sesión:

```
rsh <VAP_group>_1
```

Por ejemplo,

```
rsh sf53_1
```

5. Ahora, cargue la aplicación específica de Sourcefire:

```
source /opt/sf/profile
```

6. Finalmente, genere un Troubleshooting:

```
sf_troubleshoot.pl -t <case_number>
```

Datos adicionales del Troubleshooting

1. Copias de todo el `/var/log/messages` * los archivos en el módulo del Control Processor

(CPM) son necesarios para el análisis y el propósito de Troubleshooting del registro. Un sensor de Sourcefire registra todos los mensajes de Syslog en el archivo de `/var/log/messages` de un CPM, bastante que en un módulo de procesador de la aplicación (APM) donde el software de Sourcefire se ejecuta.

Nota: Observe por favor * con `/var/log/messages` *. Utilice * para incluir todo el archivo de los mensajes del CPM.

2. Una configuración corriente de la plataforma de las X-series de BlueCoat permite que entendamos cómo un sensor está instalado y configurado en XOS. El siguiente comando copia una configuración corriente en un archivo de texto:

```
copy running-config /tmp/running_config.txt
```

3. Las salidas del siguiente comando son importantes determinar el estatus del módulo y del chasis:

```
show module statusshow chassis
```

4. Si un error o un síntoma es obvio en la interfaz del Web User, un tiro de pantalla de la interfaz Web es también útil identificar un problema.