Genere la solución de problemas de datos para el software Sourcefire que se ejecuta en la plataforma BlueCoat serie X

Contenido

Introducción

Un archivo de resolución de problemas contiene una colección de mensajes de registro, datos de configuración y resultados de comandos. Se utiliza para determinar el estado de un sistema Sourcefire. Si un ingeniero de soporte de Cisco le solicita que envíe un archivo de solución de problemas desde su plataforma BlueCoat serie X (también conocida como sensor Crossbeam), siga las instrucciones de este documento. Este documento también proporciona una lista de los datos adicionales que podrían ser necesarios para analizar un problema.

Generar archivo de resolución de problemas

1. Inicie sesión en su dispositivo BlueCoat serie X como usuario administrador.

2. Busque el grupo VAP para el software Sourcefire.

show application vap-group

El siguiente resultado es un ejemplo del comando anterior. En este ejemplo, el grupo vap es sf53.

```
VAP Group                    : sf53
App ID : SfSensor
Name : SF Sensor
Version : 5.3.0.1
Release : 55
Start on Boot : yes
App Monitor : on
App State (sf530_1) : Up
```

3. A continuación, necesitamos aumentar los privilegios para que podamos acceder de forma remota al propio grupo VAP:

unix su

4. A continuación, abra una sesión de shell remoto:

```
rsh
```

Por ejemplo,

```
rsh sf53_1
```

5. Ahora, cargue la aplicación específica de Sourcefire:

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

6. Por último, genere una solución de problemas:

```
sf_troubleshoot.pl -t
```

Datos adicionales para la resolución de problemas

1. Se necesitan copias de todos los archivos /var/log/messages* en el Módulo de procesador de control (CPM) para el análisis de registros y la resolución de problemas. Un sensor de Sourcefire registra todos los mensajes syslog en el archivo /var/log/messages de un CPM, en lugar de en un Módulo de procesador de aplicaciones (APM) donde se ejecuta el software Sourcefire.

> **Nota:** Tenga en cuenta el * con el /var/log/messages*. Use el * para incluir todos los mensajes del archivo CPM.

2. Una configuración en ejecución de la plataforma BlueCoat serie X nos permite comprender cómo se instala y configura un sensor en XOS. El siguiente comando copia una configuración en ejecución en un archivo de texto:

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

3. Los siguientes resultados del comando son importantes para determinar el estado del módulo y el chasis:

```
show module status
```

```
show chassis
```

4. Si un error o síntoma es obvio en la interfaz de usuario web, una captura de pantalla de la interfaz web también es útil para identificar un problema.