為在BlueCoat X系列平台上運行的Sourcefire軟體生成故障排除資料

目錄

簡介

故障排除檔案包含日誌消息、配置資料和命令輸出的集合。它用於確定Sourcefire系統的狀態。如果思科支援工程師要求您從BlueCoat X系列平台（也稱為Crossbeam感測器）傳送故障排除檔案，請按照本文檔中的說明操作。本檔案也提供分析問題可能需要的額外資料的清單。

生成故障排除檔案

1.以管理員使用者身份登入BlueCoat X系列設備。

2.查詢Sourcefire軟體的VAP組。

```
show application vap-group
```

以下輸出是上述命令的示例。在本示例中，vap組是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.接下來，我們需要增加許可權，以便可以遠端外殼進入VAP組本身：

```
unix su
```

4.然後，開啟遠端外殼會話：

```
rsh
```

例如，

```
rsh sf53_1
```
5.現在，載入Sourcefire特定的應用程式：

```
source /opt/sf/profile
```
6.最後，生成故障排除：

```
sf_troubleshoot.pl -t
```

其他故障排除資料

1.控制處理器模組(CPM)上的所有/var/log/messages*檔案的副本對於日誌分析和故障排除是必需的。Sourcefire感測器將所有系統日誌消息記錄在CPM的/var/log/messages檔案中，而不是在運行Sourcefire軟體的應用程式處理器模組(APM)中。

附註：請記下*和/var/log/messages*。使用*包括CPM的所有消息檔案。

2. BlueCoat X系列平台的運行配置使我們能夠瞭解感測器在XOS上的安裝和配置方式。以下命令將運行配置複製到文本檔案中：

```
copy running-config /tmp/running_config.txt
```
3.以下命令輸出對於確定模組和機箱的狀態非常重要：

```
show module status

show chassis
```
4.如果Web使用者介面上出現明顯錯誤或症狀，則Web介面的截圖也有助於確定問題。