

# 为运行在BlueCoat X系列平台上的Sourcefire软件生成故障排除数据

## 目录

### [简介](#)

### [生成故障排除文件](#)

### [其他故障排除数据](#)

## 简介

故障排除文件包含日志消息、配置数据和命令输出的集合。它用于确定Sourcefire系统的状态。如果思科支持工程师要求您从BlueCoat X系列平台（也称为Crossbeam传感器）发送故障排除文件，请按照本文档中的说明进行操作。本文档还提供分析问题可能需要的其他数据的列表。

## 生成故障排除文件

- 1.以管理员用户身份登录BlueCoat X系列设备。
- 2.查找Sourcefire软件的VAP组。

```
show application vap-group
```

以下输出是上述命令的示例。在本例中，vap组为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.接下来，我们需要增加权限，以便我们能够远程外壳到VAP组本身：

```
unix su
```

- 4.然后，打开远程外壳会话：

```
rsh
```

例如，

```
rsh sf53_1
```

5.现在，加载Sourcefire特定应用：

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

6.最后，生成故障排除：

```
sf_troubleshoot.pl -t
```

## 其他故障排除数据

1.控制处理器模块(CPM)上所有/var/log/messages\*文件的副本对于日志分析和故障排除的目的是必需的。Sourcefire传感器将所有系统日志消息记录在CPM的/var/log/messages文件中，而不是在运行Sourcefire软件的应用处理器模块(APM)上。

**注意：**请记下带/var/log/messages\*的\*。使用\*包含CPM的所有消息文件。

2. BlueCoat X系列平台的运行配置使我们能够了解如何在XOS上安装和配置传感器。以下命令将运行配置复制到文本文件中：

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

3.以下命令输出对于确定模块和机箱的状态非常重要：

```
show module status
```

```
show chassis
```

4.如果Web用户界面上出现明显错误或症状，Web界面的屏幕截图也有助于识别问题。