

BlueCoat X シリーズ プラットフォームで動作する Sourcefire ソフトウェア用のトラブルシューティング データの生成

内容

[概要](#)

[トラブルシューティング ファイルの生成](#)

[その他のトラブルシューティングデータ](#)

概要

トラブルシューティング ファイルには、一連のログ メッセージ、構成データ、およびコマンド出力が含まれています。これは、Sourcefire システムのステータスを判別するために使用されます。BlueCoat X シリーズ プラットフォーム (クロスビーム センサーとも呼ばれる) からトラブルシューティング ファイルを送信するようにシスコ サポート エンジニアから要求された場合は、このドキュメントの指示に従ってください。このドキュメントでは、問題の分析に必要な可能性がある追加データのリストも示します。

トラブルシューティング ファイルの生成

1. 管理者ユーザーとして BlueCoat X シリーズ アプライアンスにログインします。
2. Sourcefire ソフトウェアの VAP グループを検索します。

```
show application vap-group
```

次に、上記のコマンドの出力例を示します。この例では、vap グループは sf53 です。

```
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. 次に、VAP グループ自体にリモートシェルを実行できるように、特権を増やす必要があります。

```
unix su
```

4.次に、リモートシェルセッションを開きます。

```
rsh
```

たとえば、

```
rsh sf53_1
```

5.ここで、Sourcefire固有のアプリケーションをロードします。

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

6.最後に、トラブルシューティングを生成します。

```
sf_troubleshoot.pl -t
```

その他のトラブルシューティングデータ

1.ログ分析とトラブルシューティングを行う際には、Control Processor Module(CPM)上のすべての/var/log/messages*ファイルのコピーが必要です。Sourcefireセンサーは、Sourcefireソフトウェアが稼働するアプリケーションプロセッサモジュール(APM)ではなく、CPMの/var/log/messagesファイルにすべてのsyslogメッセージを記録します。

注： /var/log/messages*とともに*を書き留めてください。*を使用して、CPMのすべてのメッセージファイルを含めます。

2. BlueCoat Xシリーズプラットフォームの実行コンフィギュレーションを使用すると、センサーをXOSにインストールして設定する方法を理解できます。次のコマンドは、実行コンフィギュレーションをテキストファイルにコピーします。

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

3.次のコマンド出力は、モジュールとシャーシのステータスを確認するために重要です。

```
show module status
```

```
show chassis
```

4. Webユーザインターフェイスでエラーや症状が明らかであれば、Webインターフェイスのスクリーンショットも問題を特定するのに役立ちます。