Generieren von Fehlerbehebungsdaten für Sourcefire-Software, die auf der Plattform der BlueCoat X-Serie ausgeführt wird

Inhalt

[Einführung](#)
[Fehlerbehebungsdatei erstellen](#)
[Zusätzliche Fehlerbehebung für Daten](#)

Einführung

Eine Fehlerbehebungsdatei enthält eine Sammlung von Protokollmeldungen, Konfigurationsdaten und Befehlsausgaben. Sie wird verwendet, um den Status eines Sourcefire-Systems zu bestimmen. Wenn Sie von einem Cisco Support-Techniker aufgefordert werden, eine Fehlerbehebungsdatei von der BlueCoat X-Series-Plattform (auch Crossbeam Sensor genannt) zu senden, befolgen Sie die Anweisungen in diesem Dokument. Dieses Dokument enthält auch eine Liste der zusätzlichen Daten, die zur Analyse eines Problems erforderlich sein können.

Fehlerbehebungsdatei erstellen

1. Melden Sie sich als Administrator-Benutzer bei Ihrer Appliance der BlueCoat X-Serie an.

2. Suchen Sie die VAP-Gruppe für die Sourcefire-Software.

```
show application vap-group
```

Die folgende Ausgabe ist ein Beispiel für den oben angegebenen Befehl. In diesem Beispiel ist die vap-Gruppe 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. Als Nächstes müssen wir die Berechtigungen erhöhen, damit die Remote-Shell in die VAP-Gruppe selbst eingefügt werden kann:

```
unix su
```

4. Öffnen Sie anschließend eine Remote-Shell-Sitzung:

```
rsh
```

Beispiel:

```
rsh sf53_1
```

5. Laden Sie jetzt die Sourcefire-spezifische Anwendung:

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

6. Generieren Sie schließlich eine Fehlerbehebung:

```
sf_troubleshoot.pl -t
```

Zusätzliche Fehlerbehebung für Daten

1. Kopien aller /var/log/messages* Dateien im Control Processor Module (CPM) sind für die Protokollanalyse und Fehlerbehebung erforderlich. Ein Sourcefire-Sensor protokolliert alle Syslog-Meldungen in der /var/log/messages-Datei eines CPM, nicht in einem APM (Application Processor Module), in dem die Sourcefire-Software ausgeführt wird.

> Hinweis: Beachten Sie die * mit den /var/log/messages*. Verwenden Sie das *, um alle Nachrichten CPM-Dateien einzuschließen.

2. Eine laufende Konfiguration der BlueCoat X-Series-Plattform ermöglicht es uns zu verstehen, wie ein Sensor auf XOS installiert und konfiguriert wird. Mit dem folgenden Befehl wird eine aktuelle Konfiguration in eine Textdatei kopiert:

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

3. Die folgenden Befehlsausgaben sind wichtig, um den Status des Moduls und des Chassis zu bestimmen:

```
show module status
```

```
show chassis
```

4. Wenn auf der Webbenutzeroberfläche ein Fehler oder ein Symptom erkennbar ist, ist ein Screenshot der Webschnittstelle ebenfalls hilfreich, um ein Problem zu identifizieren.