

BlueCoat X-Series 플랫폼에서 실행되는 Sourcefire 소프트웨어의 문제 해결 데이터 생성

목차

[소개](#)

[문제 해결 파일 생성](#)

[추가 문제 해결 데이터](#)

소개

문제 해결 파일에는 로그 메시지, 컨피그레이션 데이터 및 명령 출력의 컬렉션이 포함됩니다. Sourcefire 시스템의 상태를 확인하는 데 사용됩니다. Cisco Support Engineer가 BlueCoat X-Series 플랫폼(Crossbeam Sensor라고도 함)에서 문제 해결 파일을 보내도록 요청하는 경우 이 문서의 지침을 따르십시오. 또한 이 문서에서는 문제 분석에 필요한 추가 데이터 목록을 제공합니다.

문제 해결 파일 생성

1. BlueCoat X-Series 어플라이언스에 관리자 사용자로 로그인합니다.
2. Sourcefire 소프트웨어의 VAP 그룹을 찾습니다.

```
show application vap-group
```

다음 출력은 위 명령의 예입니다. 이 예에서 vap 그룹은 sf53입니다.

```
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. 다음으로, 원격 셸을 VAP 그룹 자체에 추가할 수 있는 권한을 늘려야 합니다.

```
unix su
```

4. 원격 셸 세션을 엽니다.

```
rsh
```

예를 들어

```
rsh sf53_1
```

5. 이제 Sourcefire 관련 애플리케이션을 로드합니다.

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

6. 마지막으로, 문제를 생성합니다.

```
sf_troubleshoot.pl -t
```

추가 문제 해결 데이터

1. 로그 분석 및 문제 해결 목적을 위하여 CPM(컨트롤 프로세서 모듈)에 있는 모든 파일 `/var/log/messages*` 파일의 복사본이 필요합니다. Sourcefire 센서는 Sourcefire 소프트웨어가 실행되는 APM(Application Processor Module)이 아닌 CPM의 `/var/log/messages` 파일에 모든 syslog 메시지를 기록합니다.

참고: `/var/log/messages*`와 함께 `*`를 기록해 두십시오. CPM의 모든 메시지 파일을 포함하려면 `*`를 사용합니다.

2. BlueCoat X-Series 플랫폼의 실행 중인 컨피그레이션을 통해 센서가 XOS에 설치 및 구성된 방식을 이해할 수 있습니다. 다음 명령은 실행 중인 컨피그레이션을 텍스트 파일로 복사합니다.

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

3. 모듈 및 새시의 상태를 확인하려면 다음 명령 출력이 중요합니다.

```
show module status
```

```
show chassis
```

4. 웹 사용자 인터페이스에서 오류 또는 증상이 분명한 경우 웹 인터페이스의 스크린샷을 통해 문제를 식별할 수 있습니다.