

# Содержание

[Введение](#)

[Генерируйте файл устранения неполадок](#)

[Дополнительные данные устранения неполадок](#)

## Введение

Файл устранения неполадок содержит набор сообщений журнала, данных о конфигурации и выходных данных команды. Это используется для определения статуса системы Sourcefire. Если специалист службы технической поддержки Cisco запрашивает вас передать файл устранения неполадок от своего BlueCoat Платформа Серии X (также известный как Датчик Поперечной балки), следуйте инструкциям на этом документе. Этот документ также предоставляет список дополнительных данных, которые могли бы быть необходимыми для анализа проблемы.

## Генерируйте файл устранения неполадок

1. Войдите в свой BlueCoat устройство Серии X как пользователь с правами администратора.

2. Найдите группу VAP для программного обеспечения Sourcefire.

```
show application vap-group
```

Следующий результат является примером вышеупомянутой команды. В данном примере var группа является sf53.

```
show application vap-group
```

3. Затем, мы должны увеличить привилегию так, чтобы мы могли удаленная оболочка в саму группу VAP:

```
unix su
```

4. Затем откройте сеанс удаленной оболочки:

```
rsh <VAP_group>_1
```

Пример,

```
rsh sf53_1
```

5. Теперь, загрузите Sourcefire определенное приложение:

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

6. Наконец, генерируйте устранение неполадок:

```
sf_troubleshoot.pl -t <case_number>
```

## Дополнительные данные устранения неполадок

1. Копии всех `/var/log/messages*` файлы на Модуле управляющего процессора (СРМ) необходимы для регистрационного анализа и цели устранения проблем. Датчик Sourcefire регистрирует все сообщения системного журнала на `/var/log/messages` файле СРМ, а не на Модуле прикладного процессора (АРМ), куда выполняется программное обеспечение Sourcefire.

**Примечание:** Обратите внимание `* c/var/log/messages*`. Используйте `*` для включения всего файла сообщений СРМ.

2. Рабочая конфигурация BlueCoat, который Платформа Серии X позволяет нам понимать, как датчик установлен и настроен на XOS. Следующая команда копирует рабочую конфигурацию в текстовый файл:

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

3. Выходные данные следующей команды важны для определения статуса модуля и шасси:

```
show module statusshow chassis
```

4. Если ошибка или признак очевидны на интерфейсе веба - пользователя, снимок экрана веб-интерфейса также полезен для определения проблемы.