

Содержание

[Введение](#)

[Шаги для сбора ключевых файлов](#)

Введение

Этот документ описывает, как проверить для и собрать ключевые файлы от устройства FirePOWER. Когда процесс на Устройстве FirePOWER встречается с критической проблемой, дампы рабочей памяти о процессе может быть сохранен как ключевой файл. Для определения основной причины сбоя техническая поддержка Cisco могла бы запросить ключевые файлы.

Шаги для сбора ключевых файлов

1. Соединитесь с CLI устройства с Secure Shell (SSH).
2. Станьте пользователем маршрута: `admin@FirePOWER~$ sudo su` -Если устройство является 7000 или устройством FirePOWER серии 8000, ASA, модуль SFR или Виртуальное устройство, вводит **эксперта**, чтобы перейти к CLI: `> expert`
`admin@FirePOWER~$`
3. Перейдите в `/var/common` папка, где расположены ключевые файлы. `root@FirePOWER:/var/home/admin~# cd /var/common`
4. Проверьте папку для файла. Данный пример показывает один ключевой файл. Однако вы могли бы найти несколько ключевых файлов. `root@FirePOWER:/var/common~# ls -ralsh | grep core`
`268K -rw----- 1 root admin 740K Sep 10 06:53 core.2179`
5. Сожмите файл. Ключевые файлы имеют потенциал, чтобы быть очень большими. Из-за внутренней структуры ключевых файлов, сжатие `gzip` может успешно сделать размер файла значительно меньшим. `root@FirePOWER:/var/common~# gzip core.2179` Если ключевые файлы заархивированы, прежде чем они будут сжаты, алгоритм `gzip` не в состоянии сжать файлы так же. Если файлы не сжаты, прежде чем они будут заархивированы, возможно, что пороги использования диска на устройстве могли бы быть превышены, и ключевые файлы удалены автоматически, чтобы препятствовать тому, чтобы было исчерпано дисковое пространство.
6. После того, как ключевые файлы являются `gzipped`, они могут быть сохранены вместе в `a .tar` архив для удобства в передачах файла. `root@FirePOWER:/var/common~# tar cvf core_file.gz.tar core.2179.gz` На этом этапе необходимо вызвать файл `core_file.gz.tar`. Если техническая поддержка Cisco запрашивает множественные ключевые файлы, можно тогда повторить предшествующие инструкции для каждого дополнительного файла. Удостоверьтесь, что дали эти уникальные имена файлов.
7. Для копирования этого файла безопасно с устройства FirePOWER с Протоколом SCP, введите эти команды: `root@FirePOWER:/var/common~# exit`
`admin@FirePOWER:/var/common~$ exit`
`>system file secure-copy hostname username destination_directory core_file.gz.tar` После нажатия **Enter** вам предлагают для пароля к удаленной системе. Файл скопирован по сети.

Примечание: В данном примере **имя хоста** обращается к названию или IP-адресу целевого удаленного хоста, **имя пользователя** задает имя пользователя на удаленном хосте, и **destination_directory** задает путь назначения на удаленном хосте.