

# Índice

[Introdução](#)

[Etapas para recolher arquivos principais](#)

## Introdução

Este documento descreve como verificar e recolher arquivos principais de um dispositivo da potência de fogo. Quando um processo em um dispositivo da potência de fogo encontra um problema crítico, uma descarga da memória running do processo pode ser salva como um arquivo principal. A fim determinar a causa de raiz da falha, o Suporte técnico de Cisco pôde pedir os arquivos principais.

## Etapas para recolher arquivos principais

1. Conecte ao CLI do dispositivo com o Shell Seguro (ssh).
2. Torna-se um usuário de raiz: `admin@FirePOWER~$ sudo su` -Se o dispositivo é um dispositivo da potência de fogo do 7000 ou 8000 Series, módulo ASA SFR, ou dispositivo virtual, inscreva o **perito** a fim ir ao CLI: `> expert`  
`admin@FirePOWER~$`
3. Vá ao dobrador de `/var/common`, onde os arquivos principais são encontrados. `root@FirePOWER:/var/home/admin~# cd /var/common`
4. Verifique o dobrador para ver se há o arquivo. Este exemplo mostra um arquivo principal. Contudo, você pôde encontrar mais de um arquivo principal. `root@FirePOWER:/var/common~# ls -ralsh | grep core`  
`268K -rw----- 1 root admin 740K Sep 10 06:53 core.2179`
5. Comprima o arquivo. Os arquivos principais têm o potencial ser muito grandes. Devido à estrutura interna dos arquivos principais, a compressão do gzip pode com sucesso fazer o tamanho do arquivo significativamente menor. `root@FirePOWER:/var/common~# gzip core.2179` Se os arquivos principais são arquivados antes que estejam comprimidos, o algoritmo do gzip não pode comprimir tanto quanto os arquivos. Se os arquivos não são comprimidos antes que estejam arquivados, é possível que os limites de utilização do disco no dispositivo puderam ser excedidos e os arquivos principais suprimiram automaticamente a fim impedir o espaço de disco da exaustão.
6. Depois que os arquivos principais gzipped, podem ser armazenados junto em um arquivo de `.tar` para a conveniência em transferências de arquivo. `root@FirePOWER:/var/common~# tar cvf core_file.gz.tar core.2179.gz` Neste momento, você deve ter um arquivo chamado `core_file.gz.tar`. Se o Suporte técnico de Cisco pede arquivos principais múltiplos, você pode então repetir as instruções prévias para cada arquivo adicional. Certifique-se dar estes nomes exclusivos dos arquivos.
7. A fim copiar com segurança este arquivo do dispositivo da potência de fogo com Secure Copy (SCP), incorpore estes comandos: `root@FirePOWER:/var/common~# exit`  
`admin@FirePOWER:/var/common~$ exit`  
`>system file secure-copy hostname username destination_directory core_file.gz.tar` Depois que você pressiona **entre**, você estão alertados para a senha ao sistema remoto. O arquivo é copiado através da rede.

Nota: Neste exemplo, o **hostname** refere o nome ou o endereço IP de Um ou Mais Servidores Cisco ICM NT do host remoto do alvo, o **username** especifica o nome do usuário no host remoto, e o **destination\_directory** especifica o caminho de destino no host remoto.