

# Habilitar Controle de Acesso na Política de Arquivo com Malware

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Impacto de desempenho](#)

[Troubleshooting](#)

[ASA](#)

[7000 e 8000 Series](#)

[FTD](#)

---

## Introdução

Este documento descreve como alocar para snort com o processo SFDataCorrelator para executar pesquisas SHA nos arquivos detectados.

## Pré-requisitos

- Licença de proteção e malware
- Política de arquivos usando malware

## Requisitos

- 5.3.0 e posterior
- ASA (todos os modelos)
- 7000 e 8000 Series (com exceção dos dispositivos "AMP")
- FTD em execução no ASA
- FTD em execução no chassi FXOS

## Componentes Utilizados

- Malware

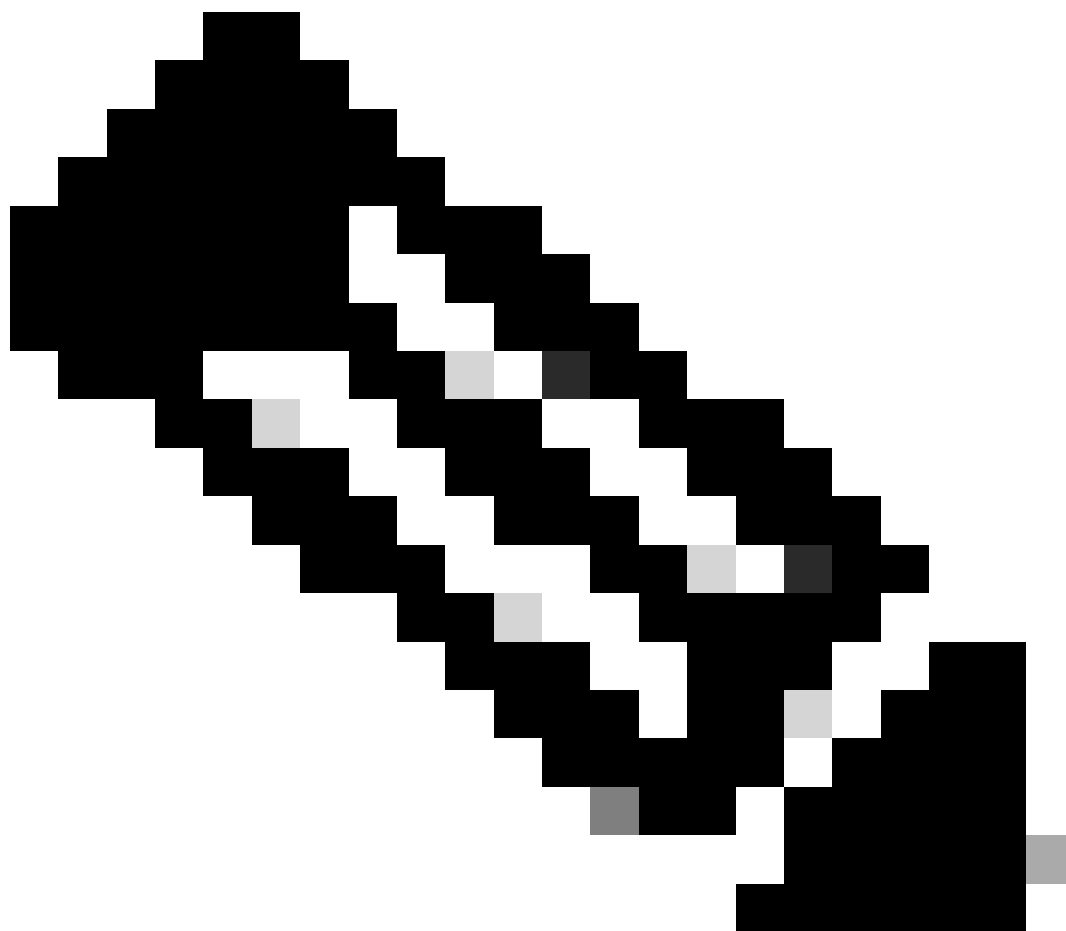
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

Ao habilitar uma política de Controle de Acesso com uma política de Arquivo que usa uma ação de Malware ou a opção "Armazenar Arquivos", uma CPU (ou duas em modelos maiores) pode ser tirada do snort.

## Impacto de desempenho

---



Observação: ao habilitar malware em dispositivos com menos recursos, o impacto no desempenho é maior.

- 
- Latência
  - Quedas
  - Alta utilização da CPU
  - Menor rendimento

# Troubleshooting

Remova a política de arquivo da Política de CA ou desabilite a Regra de CA usando a política de arquivo. Em seguida, reapply a política de CA para atribuir snort a todos os núcleos de CPU disponíveis.

## ASA

```
root@Sourcefire3D:~# grep "SW\|MODEL" /etc/sf/ims.conf
SWVERSION=5.3.1
SWBUILD=152
MODEL_CLASS="3D Sensor"
MODELNUMBER=72
MODEL="ASA5545"
MODEL_TYPE=Sensor
MODELID=H
```

```
root@Sourcefire3D:~# pmtool show affinity
```

```
Received status (0):
```

```
Affinity Status
```

```
System CPU Affinity: 08 (desired: 08)
```

```
Process CPU Affinity:
```

```
Node 0:
```

```
CPU 0:
```

```
CPU 1:
```

```
SFDataCorrelator (/usr/local/sf/bin/SFDataCorrelator) (2, desired: 2)
```

```
CPU 2:
```

```
d54fff2a-37f7-11e4-a1bd-d47ac274f5bf-d01 (/var/sf/detection_engines/d54fff2a-37f7-11e4-a1bd-d47ac274f5b
```

```
CPU 3:
```

```
CPU 4:
```

```
d54fff2a-37f7-11e4-a1bd-d47ac274f5bf-d02 (/var/sf/detection_engines/d54fff2a-37f7-11e4-a1bd-d47ac274f5b
```

```
CPU 5:
```

```
d54fff2a-37f7-11e4-a1bd-d47ac274f5bf-d03 (/var/sf/detection_engines/d54fff2a-37f7-11e4-a1bd-d47ac274f5b
```

```
Device Affinity (0 PENDING):
```

```
kvm_ivshmem (desired: 01):
```

```
10: kvm_ivshmem (01)
```

```
Process Affinity:
```

```
SFDataCorrelator (desired: 02, actual: 02)
```

## 7000 e 8000 Series

```
root@8250a-sftac:~# grep "SW\|MODEL" /etc/sf/ims.conf
```

```
SWVERSION=5.3.0
```

```
SWBUILD=571
```

```
MODEL_CLASS="3D Sensor"
```

```
MODELNUMBER=63
```

```
MODEL="3D8250"
```

```
MODEL_TYPE=Sensor
```

```
MODELID=C
```

```
root@8250a-sftac:~# pmtool show affinity
```

```
Received status (0):
```

```
Affinity Status
```

```
System CPU Affinity: fffff0 (desired: fffff0)
Process CPU Affinity:
Node 0:
CPU 0:
CPU 2:
SFDDataCorrelator (/usr/local/sf/bin/SFDDataCorrelator) (c, desired: c)
CPU 4:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d01 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d2068538813)
CPU 6:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d03 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d2068538813)
CPU 8:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d05 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d2068538813)
CPU 10:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d07 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d2068538813)
CPU 12:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d09 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d2068538813)
CPU 14:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d10 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d2068538813)
CPU 16:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d02 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d2068538813)
CPU 18:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d04 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d2068538813)
CPU 20:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d06 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d2068538813)
CPU 22:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d08 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d2068538813)
Node 1:
CPU 1:
CPU 3:
SFDDataCorrelator (/usr/local/sf/bin/SFDDataCorrelator) (c, desired: c)
CPU 5:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d11 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d2068538813)
CPU 7:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d12 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d2068538813)
CPU 9:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d13 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d2068538813)
CPU 11:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d14 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d2068538813)
CPU 13:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d15 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d2068538813)
CPU 15:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d16 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d2068538813)
CPU 17:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d17 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d2068538813)
CPU 19:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d18 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d2068538813)
CPU 21:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d19 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d2068538813)
CPU 23:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d20 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d2068538813)
Endpoint CPUs:
c0e1: 0 (desired: -1)
c1e1: 1 (desired: -1)
Process Affinity:
SFDDataCorrelator (desired: 0c, actual: 0c)
```

## FTD

Em qualquer uma das plataformas FTD, o comando anterior `pmtool show affinity` pode ser executado a partir do

prompt '>' inicial após o acesso SSH. Por exemplo:

Copyright 2004-2017, Cisco and/or its affiliates. All rights reserved.

Cisco is a registered trademark of Cisco Systems, Inc.

All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.2.1 (build 6)

Cisco Firepower 2110 Threat Defense v6.2.1 (build 327)

```
> pmtool show affinity
```

```
Received status (0):
```

```
Affinity Status
```

```
System CPU Affinity: 0 (desired: 0)
```

```
Process CPU Affinity:
```

```
CPU 0:
```

```
CPU 1:
```

```
65a99306-360b-11e7-a8f4-5671cccf5a71-d01 (/ngfw/var/sf/detection_engines/65a99306-360b-11e7-a8f4-5671cccf5a71/snort) (?, desired: 1,5)
```

```
CPU 2:
```

```
65a99306-360b-11e7-a8f4-5671cccf5a71-d02 (/ngfw/var/sf/detection_engines/65a99306-360b-11e7-a8f4-5671cccf5a71/snort) (?, desired: 2,6)
```

```
CPU 3:
```

```
65a99306-360b-11e7-a8f4-5671cccf5a71-d03 (/ngfw/var/sf/detection_engines/65a99306-360b-11e7-a8f4-5671cccf5a71/snort) (?, desired: 3,7)
```

```
CPU 4:
```

```
CPU 5:
```

```
65a99306-360b-11e7-a8f4-5671cccf5a71-d01 (/ngfw/var/sf/detection_engines/65a99306-360b-11e7-a8f4-5671cccf5a71/snort) (?, desired: 1,5)
```

```
CPU 6:
```

```
65a99306-360b-11e7-a8f4-5671cccf5a71-d02 (/ngfw/var/sf/detection_engines/65a99306-360b-11e7-a8f4-5671cccf5a71/snort) (?, desired: 2,6)
```

```
CPU 7:
```

```
65a99306-360b-11e7-a8f4-5671cccf5a71-d03 (/ngfw/var/sf/detection_engines/65a99306-360b-11e7-a8f4-5671cccf5a71/snort) (?, desired: 3,7)
```

Na solução de problemas de arquivos, a saída `pmtool show affinity` do comando está no diretório `command-outputs`. O nome do arquivo é: **usr-**

**local-sf-bin-pmtool show affinity.output**

A saída pode ser muito longa se executada em uma solução de problemas de um dispositivo maior. Aqui estão alguns comandos `grep` para fornecer uma indicação clara de quantas CPUs estão alocadas para os processos `snort` e `SFDataCorrelator`.

```
[user@tex command-outputs]$ grep snort usr-local-sf-bin-pmtool\ show\ affinity.output |wc -l
```

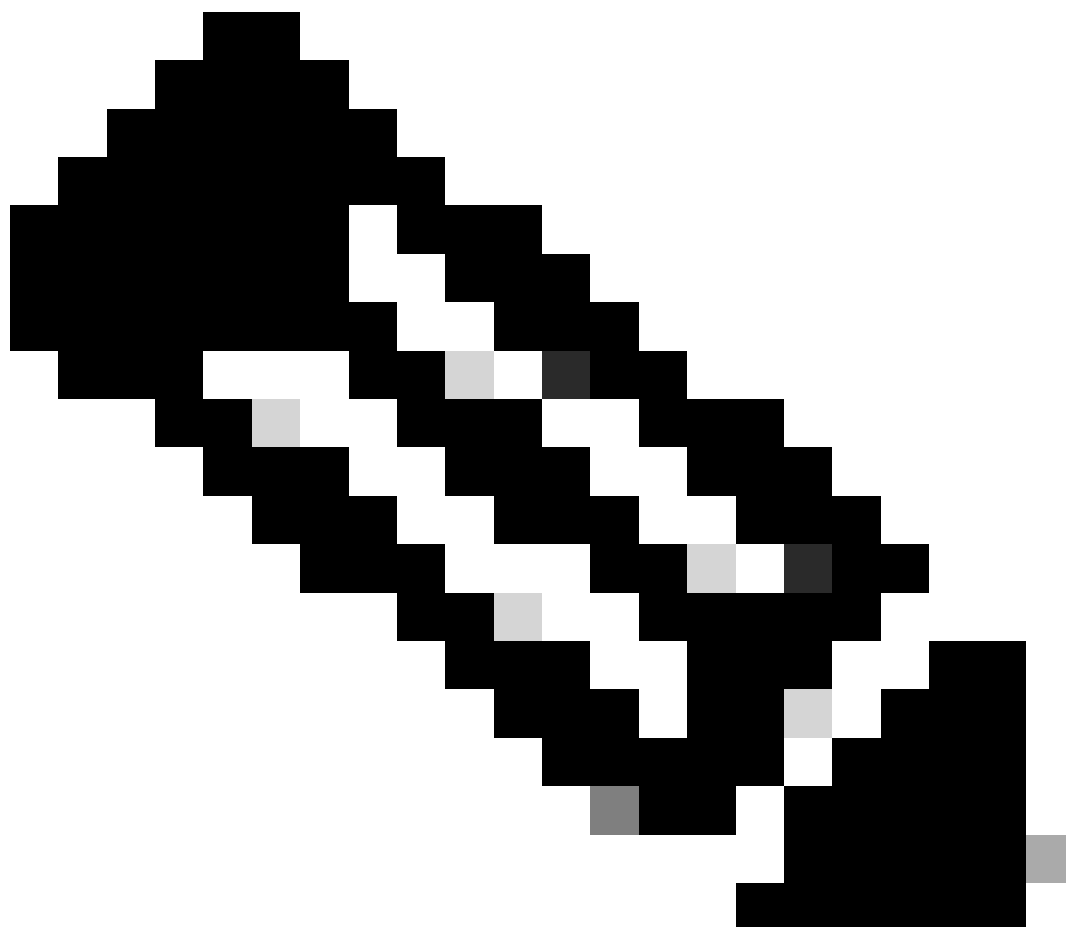
```
46
```

```
[user@tex command-outputs]$ grep "/SFDataC" usr-local-sf-bin-pmtool\ show\ affinity.output |wc -l
```

```
2
```

A saída anterior é do maior dispositivo atual (FPR-9300 SM-44). Como você pode ver, há 46 CPUs alocadas para snort e duas alocadas para SFDataCorrelator (já que a Política de Malware está habilitada).

---



**Observação:** o TS Analysis não pode exibir corretamente todos os gráficos de desempenho do DE nesses cenários

---

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.