

Habilitar el control de acceso en la política de archivos con malware

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Impacto en el rendimiento](#)

[Troubleshoot](#)

[ASA](#)

[Series 7000 y 8000](#)

[FTD](#)

Introducción

Este documento describe cómo asignar a snort con el proceso SFDataCorrelator para realizar búsquedas SHA en los archivos detectados.

Prerequisites

- Licencia de protección y malware
- Política de archivos con malware

Requirements

- 5.3.0 y superior
- ASA (todos los modelos)
- series 7000 y 8000 (con la excepción de los appliances "AMP")
- FTD que se ejecuta en ASA
- FTD ejecutándose en chasis FXOS

Componentes Utilizados

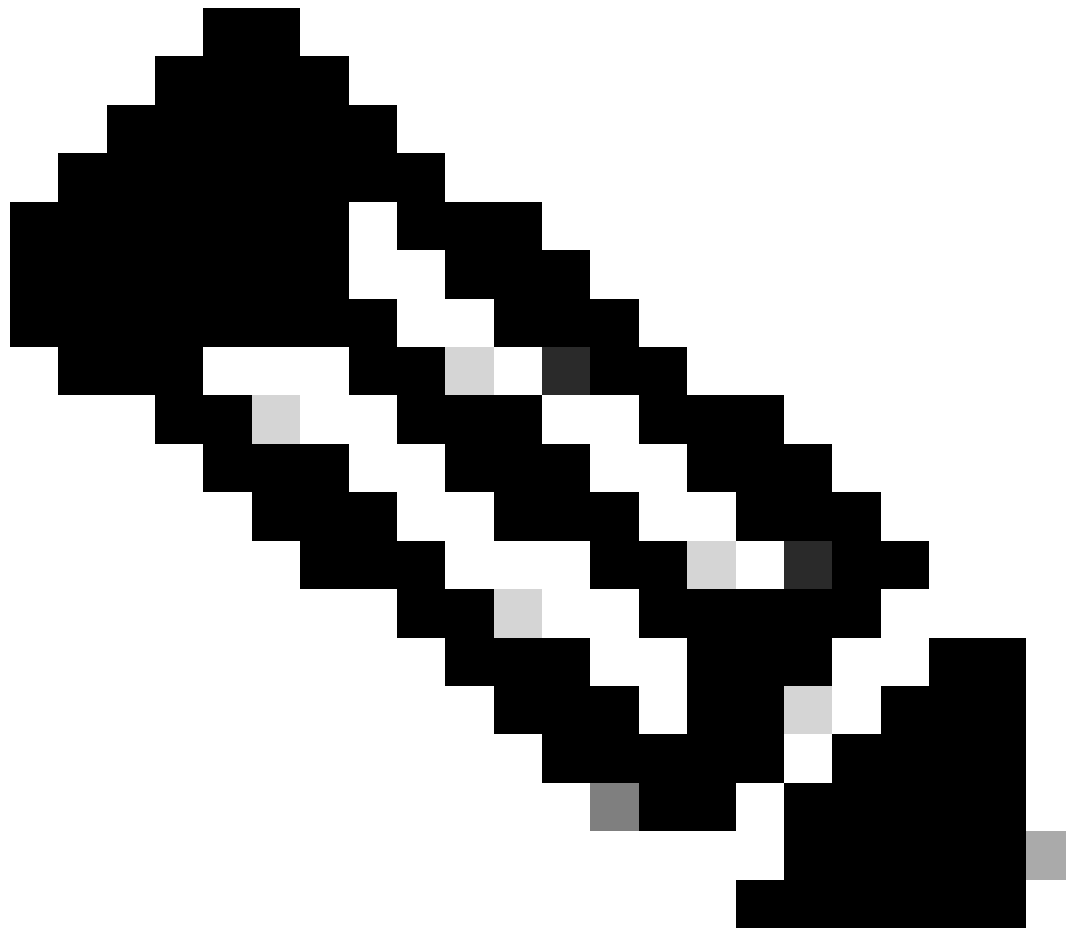
- Malware

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cuando se habilita una directiva de control de acceso con una directiva de archivo que utiliza una acción de Malware o una opción de "Almacenar archivos", se puede quitar una CPU (o dos en modelos más grandes) de la bujía.

Impacto en el rendimiento



Nota: al habilitar el malware en dispositivos con menos recursos, el impacto en el rendimiento es mayor.

-
- Latencia
 - Caídas
 - Uso elevado de la CPU
 - Menor rendimiento

Troubleshoot

Quite la política de archivos de la política de CA o inhabilite la regla de CA usando la política de archivos. A continuación, vuelva a aplicar la política de CA para asignar snort a todos los núcleos de CPU disponibles.

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)
```

Series 7000 y 8000

```
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

En cualquiera de las plataformas FTD, el `pmtool show affinity` comando anterior se puede ejecutar desde el prompt `>` inicial

después del acceso SSH. Por ejemplo:

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)
```

En los archivos de solución de problemas, el `pmtool show affinity` resultado del comando se encuentra en el directorio `command-output`. El

nombre del archivo es: **`usr-local-sf-bin-pmtool show affinity.output`**

El resultado puede ser bastante largo si se ejecuta en una solución de problemas desde un dispositivo más grande. Estos son algunos comandos `grep` para darle una indicación clara de cuántas CPU están asignadas a los procesos `snort` y `SFDataCorrelator`.

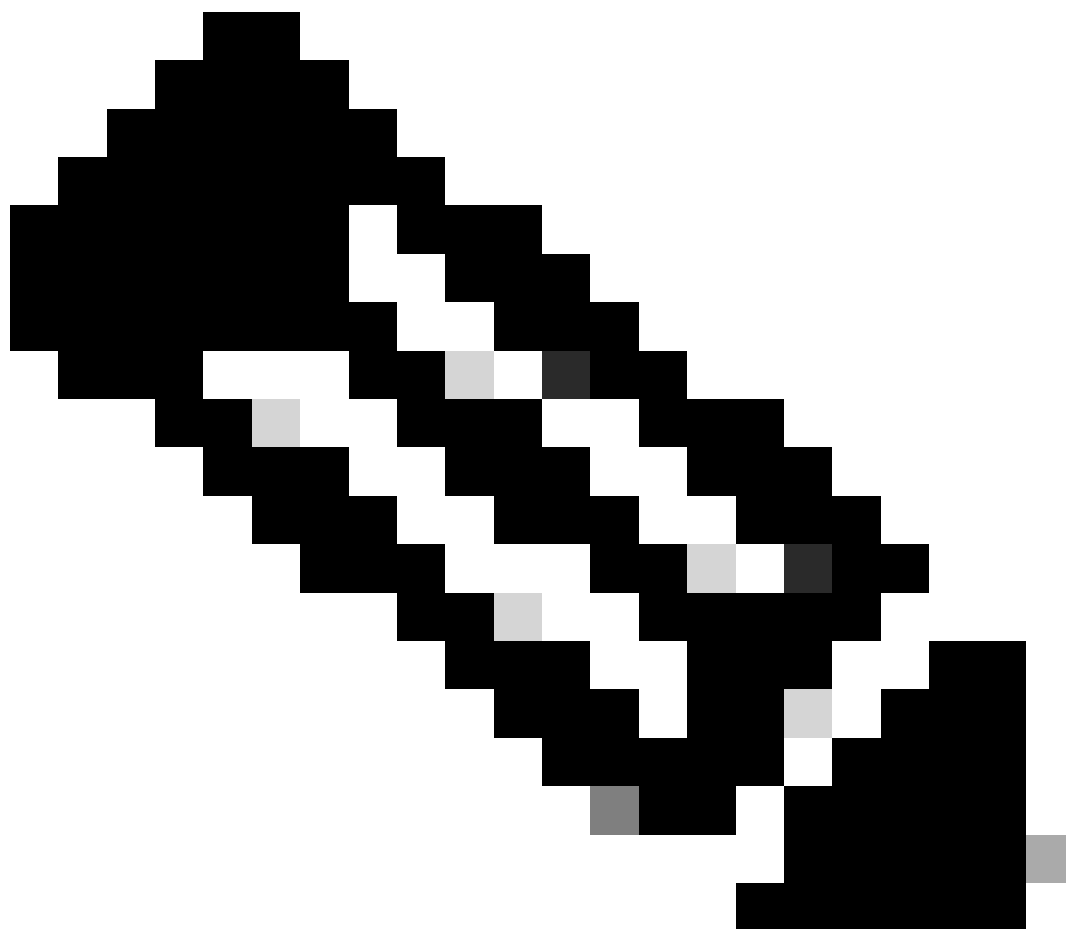
```
[user@tex command-outputs]$ grep snort usr-local-sf-bin-pmtool\ show\ affinity.output |wc -l
```

```
46
```

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

```
2
```

La salida anterior es del dispositivo más grande actual (FPR-9300 SM-44). Como puede ver, hay 46 CPU asignadas a snort y dos asignadas a SFDataCorrelator (desde que se habilita la política de malware).



Nota: El análisis de TS no puede mostrar correctamente todos los gráficos de rendimiento de DE en estos escenarios

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).