

Toegangsbeheer voor bestandsbeleid met Malware inschakelen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Effect op prestaties](#)

[Problemen oplossen](#)

[ASA](#)

[7000 en 8000 Series](#)

[FTD](#)

Inleiding

Dit document beschrijft hoe u de gegevens kunt toewijzen aan het snurken met het SFDataCorrelator-proces om SHA-lookups van de gedetecteerde bestanden uit te voeren.

Voorwaarden

- Licentie voor Protect and Malware
- Bestandsbeleid met malware

Vereisten

- 5.3.0 en hoger
- ASA (alle modellen)
- 7000 en 8000 reeks (met uitzondering van de AMP-apparaten)
- FTD uitgevoerd op ASA
- FTD actief op FXOS-chassis

Gebruikte componenten

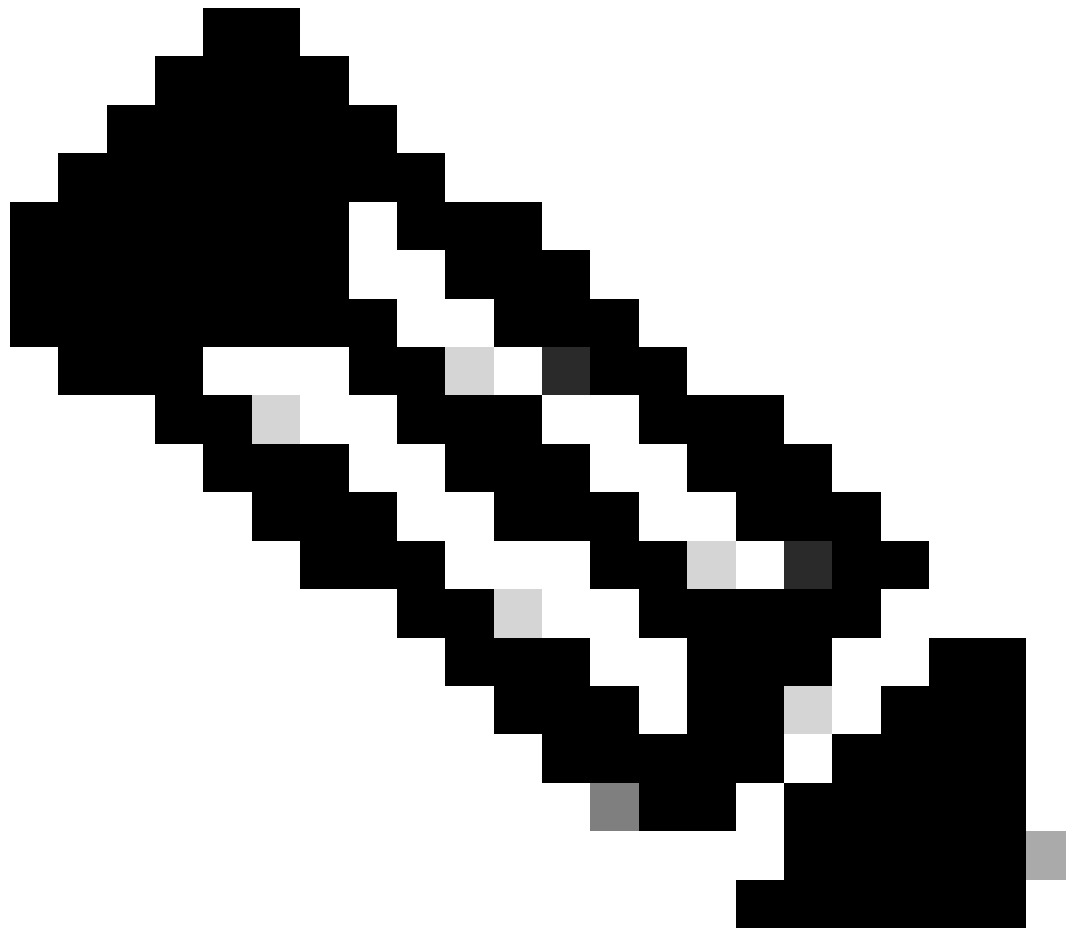
- Malware

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Wanneer u een Access Control-beleid inschakelt met een File-beleid dat gebruikmaakt van een Malware-actie of de optie "Store Files", kan een CPU (of twee op grotere modellen) worden verwijderd van de snelkoppeling.

Effect op prestaties



Opmerking: wanneer malware wordt ingeschakeld op apparaten met minder bronnen, is de impact op de prestaties groter.

-
- Latentie
 - Drops
 - Hoge CPU
 - Lagere doorvoersnelheid

Problemen oplossen

Verwijder het bestandsbeleid uit het AC-beleid of schakel de AC-regel uit met behulp van het bestandsbeleid. Vervolgens past u het AC-beleid opnieuw toe om snurken toe te wijzen aan alle beschikbare CPU-cores.

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 en 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

Op elk FTD-platform kan de vorige `pmtool show affinity` opdracht vanaf de eerste `>`-prompt na SSH-toegang worden

uitgevoerd. Voorbeeld:

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)
```

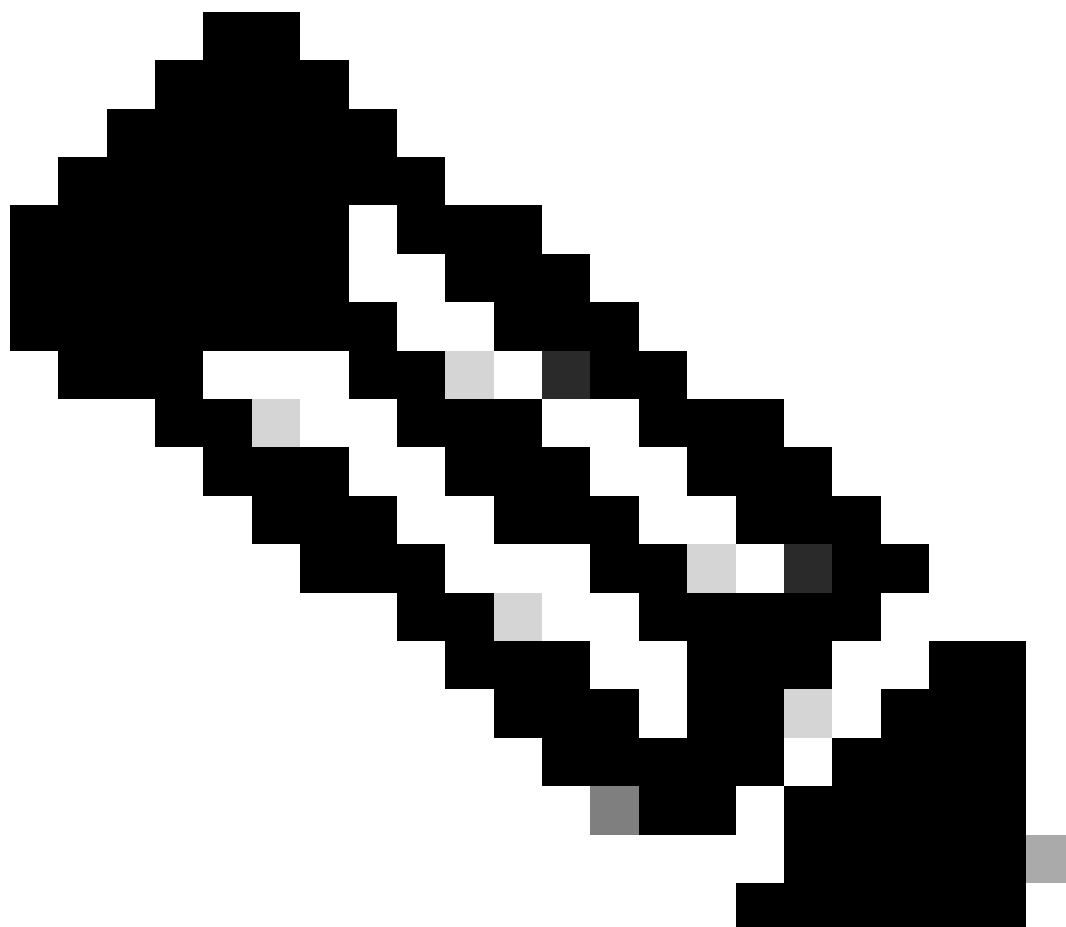
In bestanden voor probleemoplossing bevindt de pmtool show affinity opdrachtoutput zich in de map voor opdrachtoutput. De naam van het bestand is: **usr-local-sf-bin-pmtool toon affinity.output**

De uitvoer kan vrij lang zijn als deze via een probleemoplossing wordt uitgevoerd vanaf een groter apparaat. Hier zijn een aantal grep commando's om u een duidelijke indicatie te geven van hoeveel CPU's zijn toegewezen aan de snort- en SFDataCorrelator-processen.

```
[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
```

De vorige uitgang is van het huidige grootste apparaat (FPR-9300 SM-44). Zoals u kunt zien, zijn er 46 CPU's toegewezen aan snurken en twee toegewezen aan SFDataCorrelator (sinds Malware Policy is ingeschakeld).



Opmerking: TS Analysis kan niet correct de volledige DE-prestatiegrafieken in deze scenario's weergeven

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.