

Zugriffskontrolle in Dateirichtlinien mit Malware aktivieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Auswirkungen auf die Leistung](#)

[Fehlerbehebung](#)

[ASA](#)

[Serien 7000 und 8000](#)

[FTD](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie dem SFDataCorrelator-Prozess eine Sortierung zuweisen, um SHA-Suchvorgänge für die erkannten Dateien durchzuführen.

Voraussetzungen

- Schutz- und Malware-Lizenz
- Dateirichtlinie mit Malware

Anforderungen

- 5.3.0 und höher
- ASA (alle Modelle)
- Serie 7000 und 8000 (mit Ausnahme der "AMP"-Appliances)
- FTD auf ASA
- FTD wird auf FXOS-Chassis ausgeführt

Verwendete Komponenten

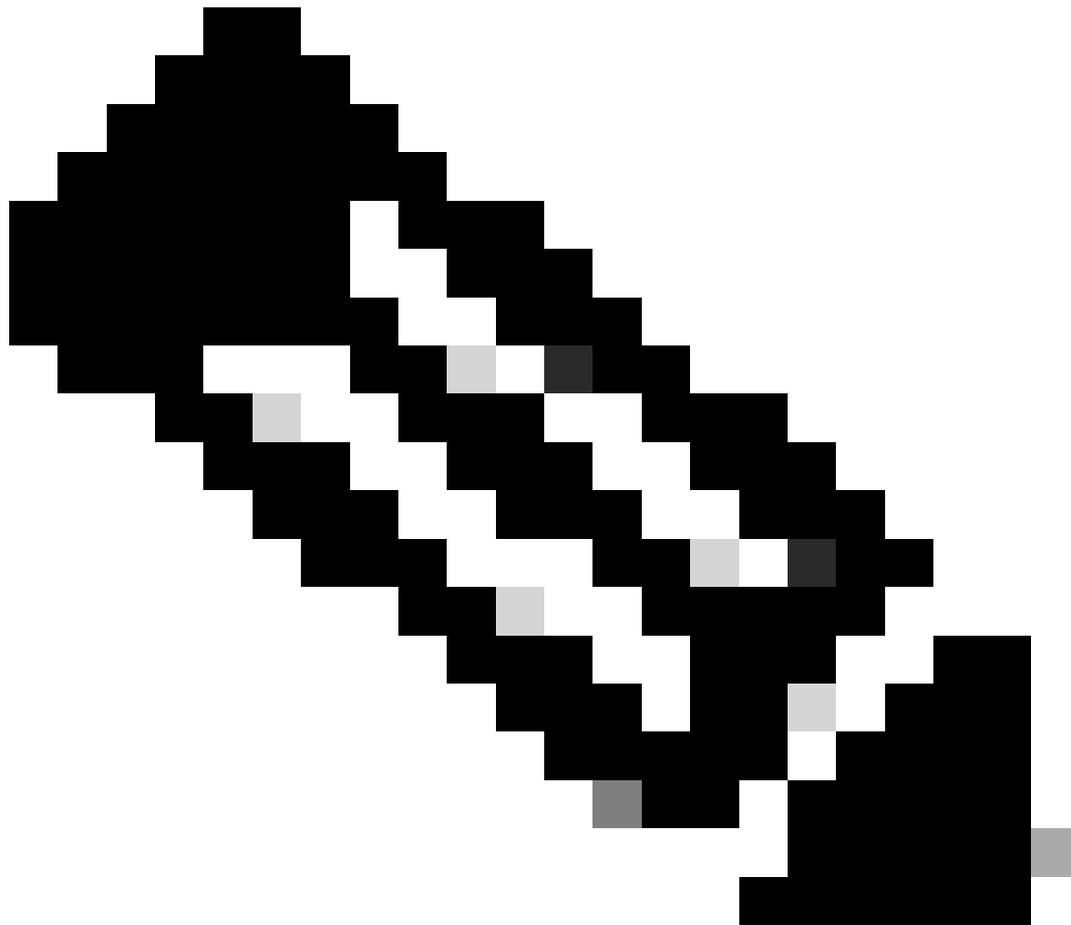
- Malware

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Wenn Sie eine Zugriffskontrollrichtlinie mit einer Dateirichtlinie aktivieren, die entweder eine Malware-Aktion oder die Option "Dateien speichern" verwendet, kann eine CPU (oder zwei auf größeren Modellen) vom Snort entfernt werden.

Auswirkungen auf die Leistung



Hinweis: Wenn Malware auf Appliances mit niedrigeren Ressourcen aktiviert wird, wirkt sich dies stärker auf die Leistung aus.

-
- Latenz
 - Herunterfallen
 - Hohe CPU-Auslastung
 - Geringerer Durchsatz

Fehlerbehebung

Entfernen Sie die Dateirichtlinie aus der AC-Richtlinie, oder deaktivieren Sie die AC-Regel mithilfe der Dateirichtlinie. Wenden Sie dann die Wechselstromrichtlinie erneut an, um allen verfügbaren CPU-Kernen Snort zuzuweisen.

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)
```

Serien 7000 und 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

Auf allen FTD-Plattformen kann der vorherige `pmtool show affinity` Befehl von der ursprünglichen Eingabeaufforderung `>`

nach dem SSH-Zugriff ausgeführt werden. Beispiele:

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)
```

Bei Dateien zur Fehlerbehebung befindet sich die `pmtool show affinity` Befehlsausgabe im Verzeichnis Befehlsausgaben. Der Name der Datei ist:

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

Die Ausgabe kann sehr lang sein, wenn sie auf einer Fehlerbehebung von einer größeren Appliance ausgeführt wird. Hier sind einige `grep`-

Befehle, die Ihnen einen klaren Hinweis darauf geben, wie viele CPUs dem `snort`- und `SFDataCorrelator`-Prozess zugewiesen sind.

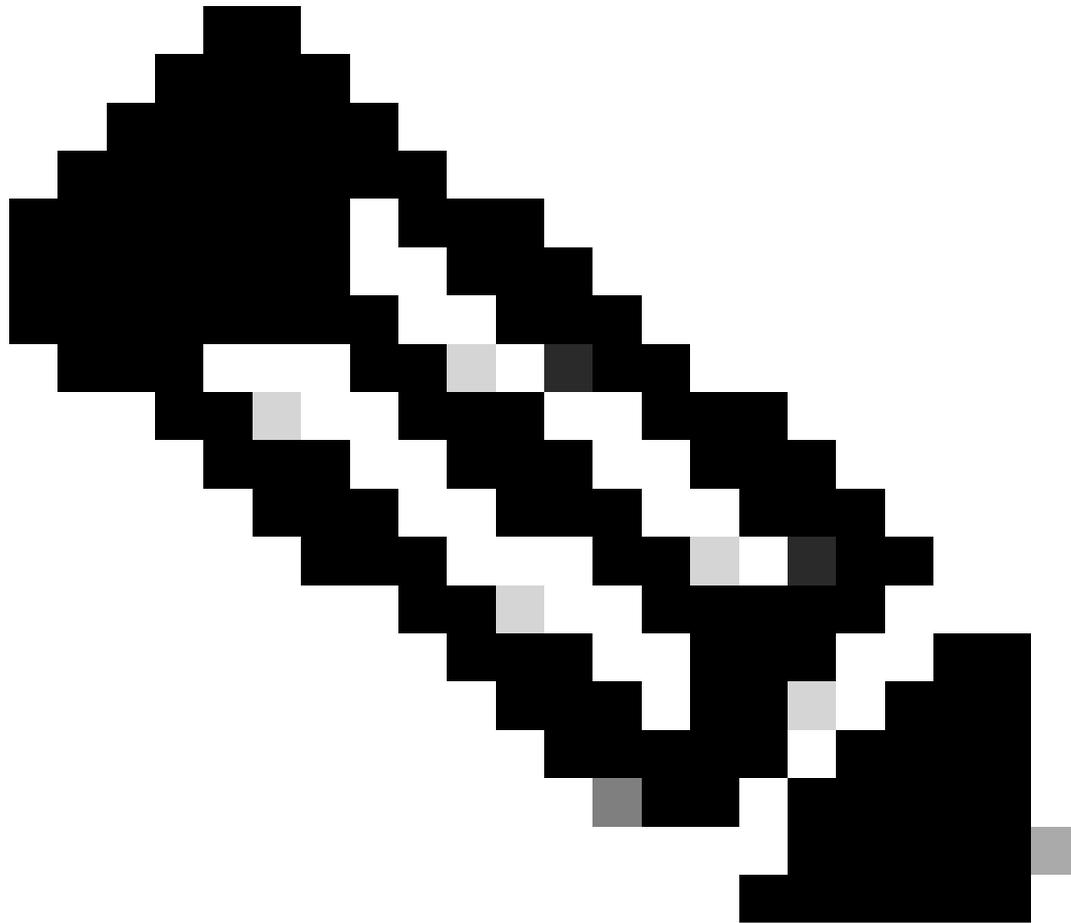
```
[user@tex command-outputs]$ grep snort usr-local-sf-bin-pmtool\ show\ affinity.output |wc -l
```

```
46
```

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

```
2
```

Die vorherige Ausgabe stammt vom derzeit größten Gerät (FPR-9300 SM-44). Wie Sie sehen, sind 46 CPUs für snort und zwei für SFDataCorrelator zugewiesen (da Malware Policy aktiviert ist).



Hinweis: TS Analysis kann in diesen Szenarien nicht die gesamten DE-Leistungsdigramme korrekt anzeigen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.