マルウェアによるファイルポリシーのアクセス制御の有効化

内容

はじめに

このドキュメントでは、検出されたファイルでSHAルックアップを実行するために、SFDataCorrelator(SFDataCorrelator)プロセスを使用してSnortに割り当てる方法について説明します。

前提条件

- 保護およびマルウェアライセンス
- マルウェアを使用したファイルポリシー

要件

- 5.3.0 以降
- ASA（全モデル）
- 7000および8000シリーズ（「AMP」アプライアンスを除く）
- ASAで実行されるFTD
- FXOSシャーシ上で稼働するFTD

使用するコンポーネント

- マルウェア

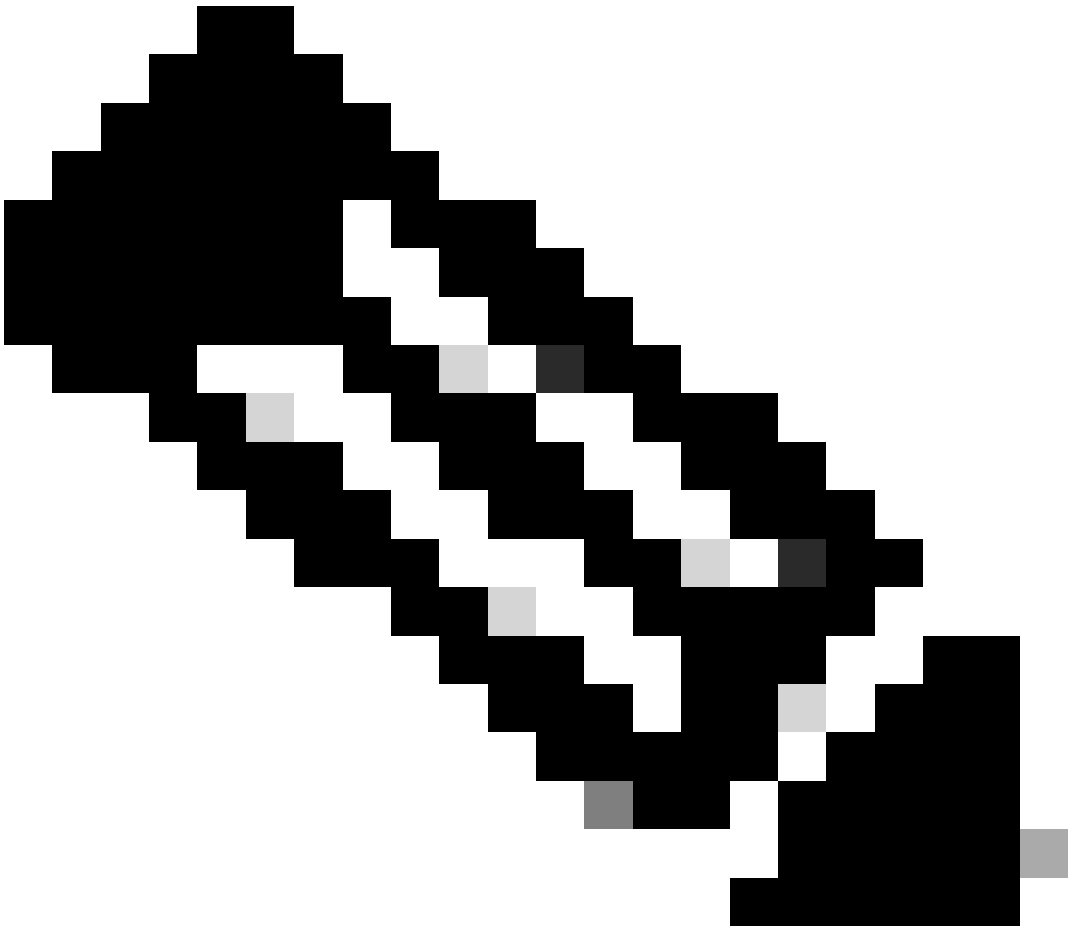
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して

ください。

背景説明

マルウェアのアクションまたは「ファイルの保存」オプションを使用するファイルポリシーでアクセスコントロールポリシーを有効にすると、CPU（またはより大規模なモデルでは2つ）をSnortから取り除くことができます。

パフォーマンスへの影響



注：低リソースアプライアンスでマルウェアを有効にすると、パフォーマンスへの影響が大きくなります。

- 遅延
- ドロップ
- CPU の使用率が高い

- 低スループット

トラブルシュート

ACポリシーからファイルポリシーを削除するか、ファイルポリシーを使用してACルールを無効にします。その後、ACポリシーを再適用して、使用可能なすべてのCPUコアにSnortを割り当てます。

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および8000シリーズ

```
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:
SFDataCorrelator (/usr/local/sf/bin/SFDataCorrelator) (c, desired: c)
CPU 4:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d01 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d206853881
CPU 6:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d03 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d206853881
CPU 8:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d05 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d206853881
CPU 10:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d07 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d206853881
CPU 12:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d09 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d206853881
CPU 14:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d10 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d206853881
CPU 16:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d02 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d206853881
CPU 18:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d04 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d206853881
CPU 20:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d06 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d206853881
CPU 22:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d08 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d206853881
Node 1:
CPU 1:
CPU 3:
SFDataCorrelator (/usr/local/sf/bin/SFDataCorrelator) (c, desired: c)
CPU 5:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d11 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d206853881
CPU 7:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d12 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d206853881
CPU 9:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d13 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d206853881
CPU 11:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d14 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d206853881
CPU 13:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d15 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d206853881
CPU 15:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d16 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d206853881
CPU 17:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d17 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d206853881
CPU 19:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d18 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d206853881
CPU 21:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d19 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d206853881
CPU 23:
3a3b8424-c8d3-11e4-98f5-1d2068538813-d20 (/var/sf/detection_engines/3a3b8424-c8d3-11e4-98f5-1d206853881
Endpoint CPUs:
c0e1: 0 (desired: -1)
c1e1: 1 (desired: -1)
Process Affinity:
SFDataCorrelator (desired: 0c, actual: 0c)
```

FTD

どのFTDプラットフォームでも、SSHアクセス後に最初の「>」プロンプトから前のpmtool show affnityコマンドを実行できます。例：

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)
```

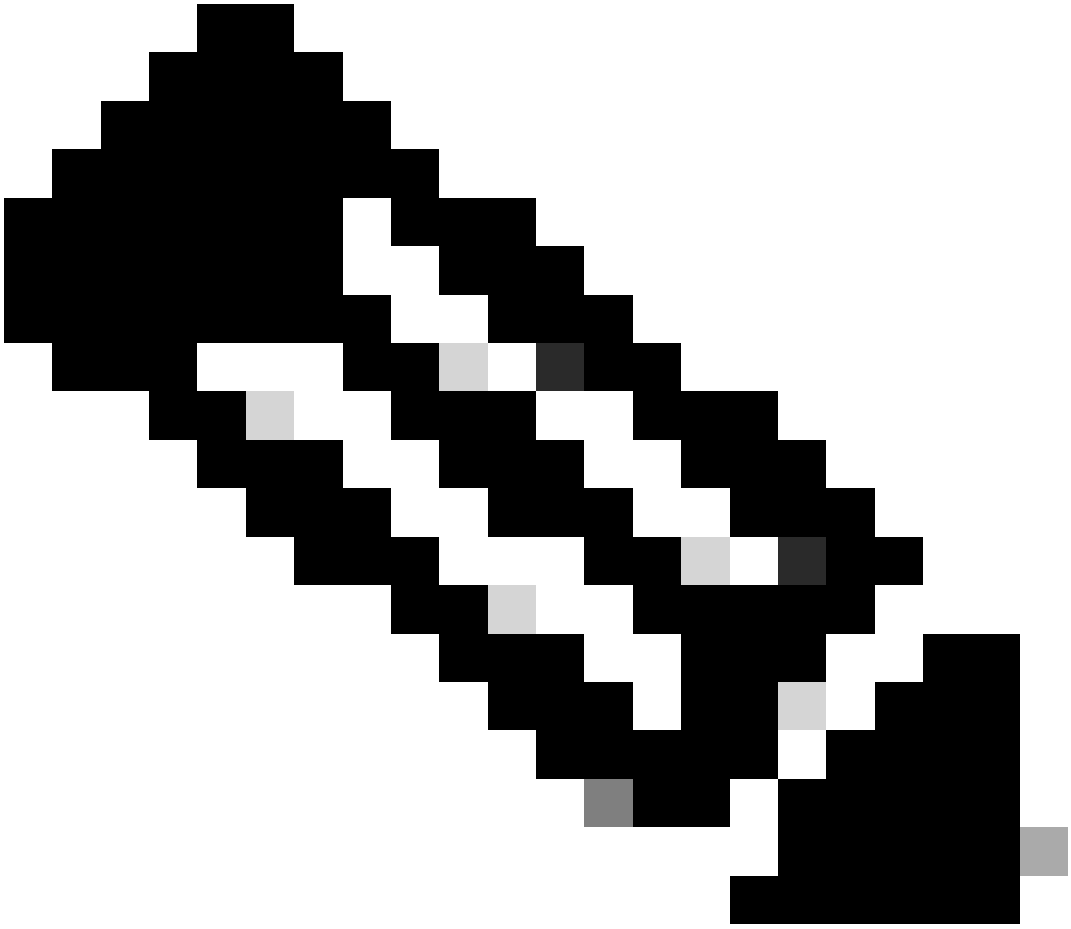
トラブルシューティングファイルでは、pmtool show affnityコマンドの出力はcommand-outputsディレクトリにあります。ファイル名は**usr-local-sf-bin-pmtool show affinity.output**です。

より大規模なアプライアンスからトラブルシューティングを行う場合、出力は非常に長くなる可能性があります。grepコマンドを使用すると、SnortおよびSFDataCorrelatorのプロセスに割り当てられているCPUの数がわかりやすくなります。

```
[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
```

上記の出力は、現在最大のデバイス(FPR-9300 SM-44)から得られたものです。Snortには46のCPUが割り当てられ、SFDataCorrelatorには2つのCPUが割り当てられています（マルウェアポリシーが有効になっているため）。



注:TS分析では、これらのシナリオのDEパフォーマンスグラフ全体を正しく表示することはできません

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。