启用带有恶意软件的文件策略访问控制

目录

简介

本文档介绍如何使用SFDataCorrelator进程分配到snort以对检测到的文件执行SHA查找。

先决条件

- 保护和恶意软件许可证
- 使用恶意软件的文件策略

要求

- 5.3.0及更高版本
- ASA（所有型号）
- 7000和8000系列（AMP设备除外）
- 在ASA上运行的FTD
- 在FXOS机箱上运行的FTD

使用的组件

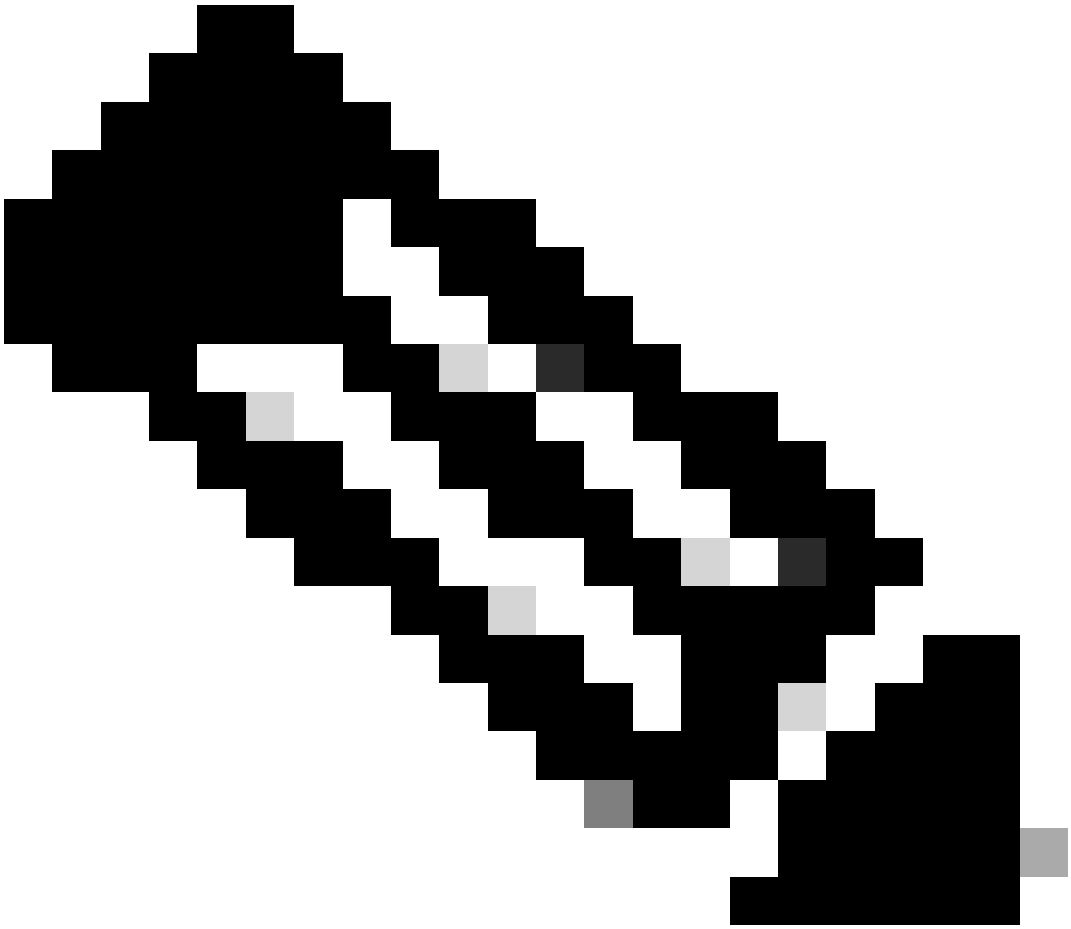
- 恶意软件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

在使用恶意软件操作或“存储文件”选项的文件策略中启用访问控制策略时，可以取消snort的CPU（或较大型号的两个）。

性能影响



注意：在资源较少的设备上启用恶意软件时，对性能的影响更大。

- 延迟
- 丢弃
- 高 CPU 利用率
- 更低的吞吐量

故障排除

从AC策略中删除文件策略或使用文件策略禁用AC规则。然后重新应用AC策略，将snort分配给所有可用的CPU核心。

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和800系列

```
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

在所有FTD平台上，前面的pmtool show affnity命令都可以在访问SSH后从最初的“>”提示符下运行。例如：

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)

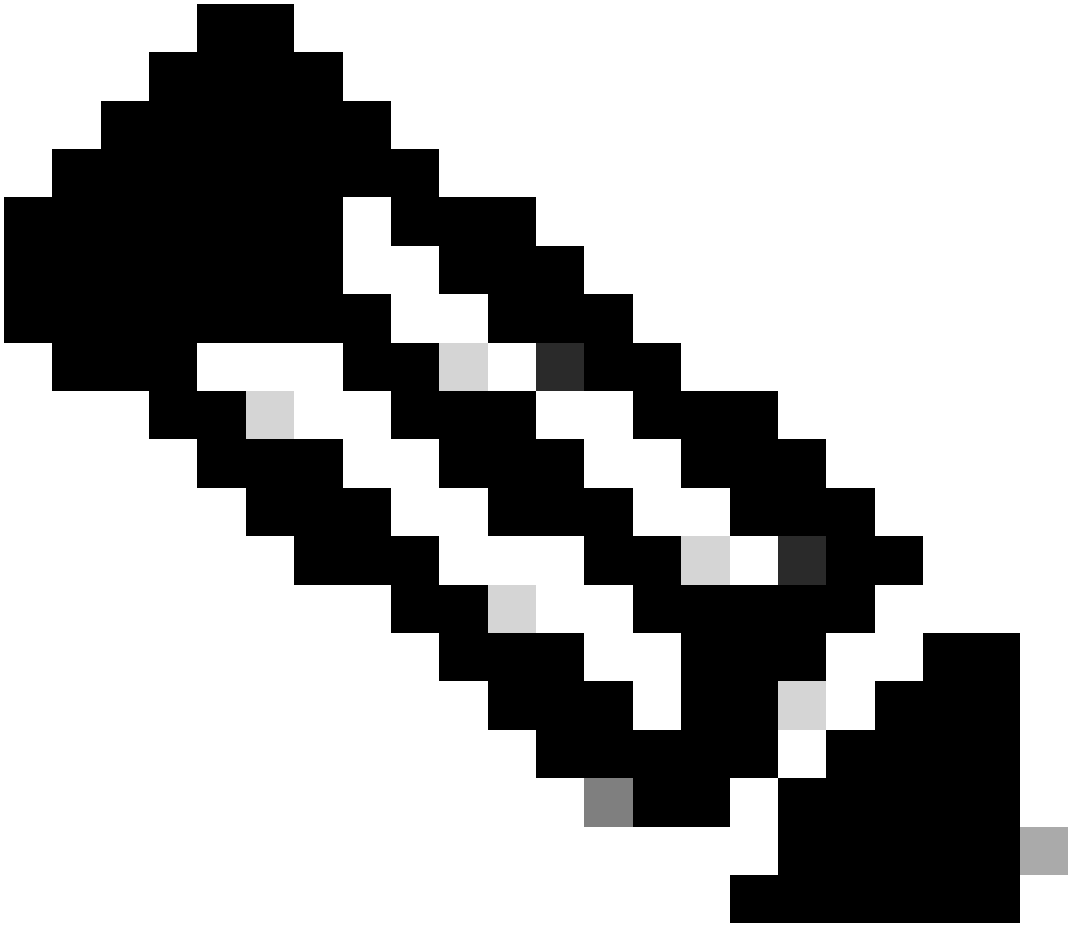
在故障排除文件中，pmtool show affnity命令输出在command-outputs目录中。文件的名称是：**usr-local-sf-bin-pmtool show affinity.output**

如果在较大设备的故障排除上运行，则输出可能相当长。下面是一些grep命令，用于明确指示分配给snort和SFDataCorrelator进程的CPU数量。

[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

上一个输出来自当前最大设备(FPR-9300 SM-44)。如您所见，有46个CPU分配给snort，2个CPU分配给SFDataCorrelator（因为已启用恶意软件策略）。



注意：在这些情况下，TS分析无法正确显示整个DE性能图表

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。