啟用對含有惡意軟體的檔案策略的訪問控制

目錄

簡介

本文檔介紹如何使用SFDataCorrelator進程分配到snort以對檢測到的檔案執行SHA查詢。

必要條件

- 保護和惡意軟體許可證
- 使用惡意軟體的檔案策略

需求

- 5.3.0及更高版本
- ASA（所有型號）
- 7000和8000系列（AMP裝置除外）
- 在ASA上運行的FTD
- 在FXOS機箱上執行的FTD

採用元件

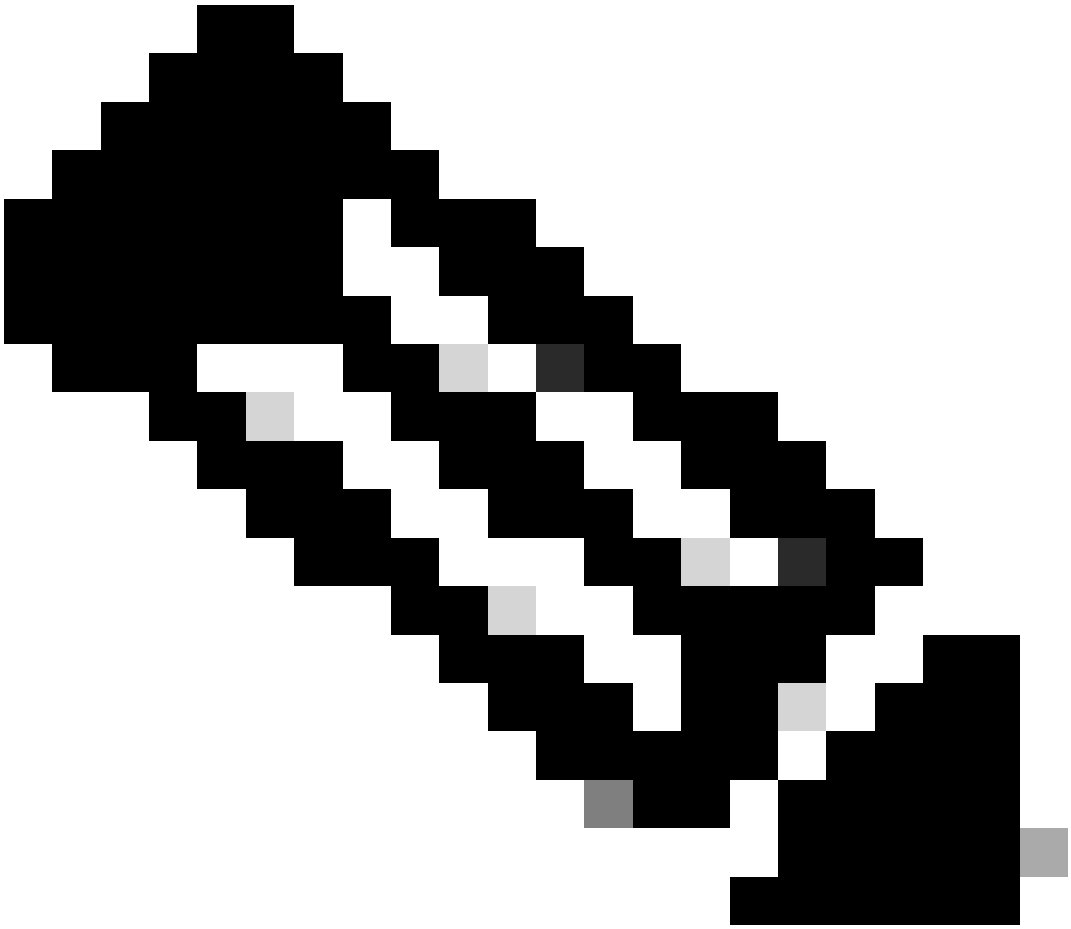
- 惡意軟體

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

啟用具有使用惡意軟體操作或「儲存檔案」選項的檔案策略的訪問控制策略時，可以使CPU（或較大型號的兩個）從snort中消失。

效能影響



註：在較低資源裝置上啟用惡意軟體時，對效能的影響更大。

- 延遲
- 丟棄
- 高CPU
- 低吞吐量

疑難排解

從AC策略中刪除檔案策略或使用檔案策略停用AC規則。然後重新應用AC策略，將snort分配給所有可用的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8000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

在任何FTD平台上，先前的pmtool show affnity命令均可從SSH訪問後的初始「>」提示符運行。舉例來說：

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)

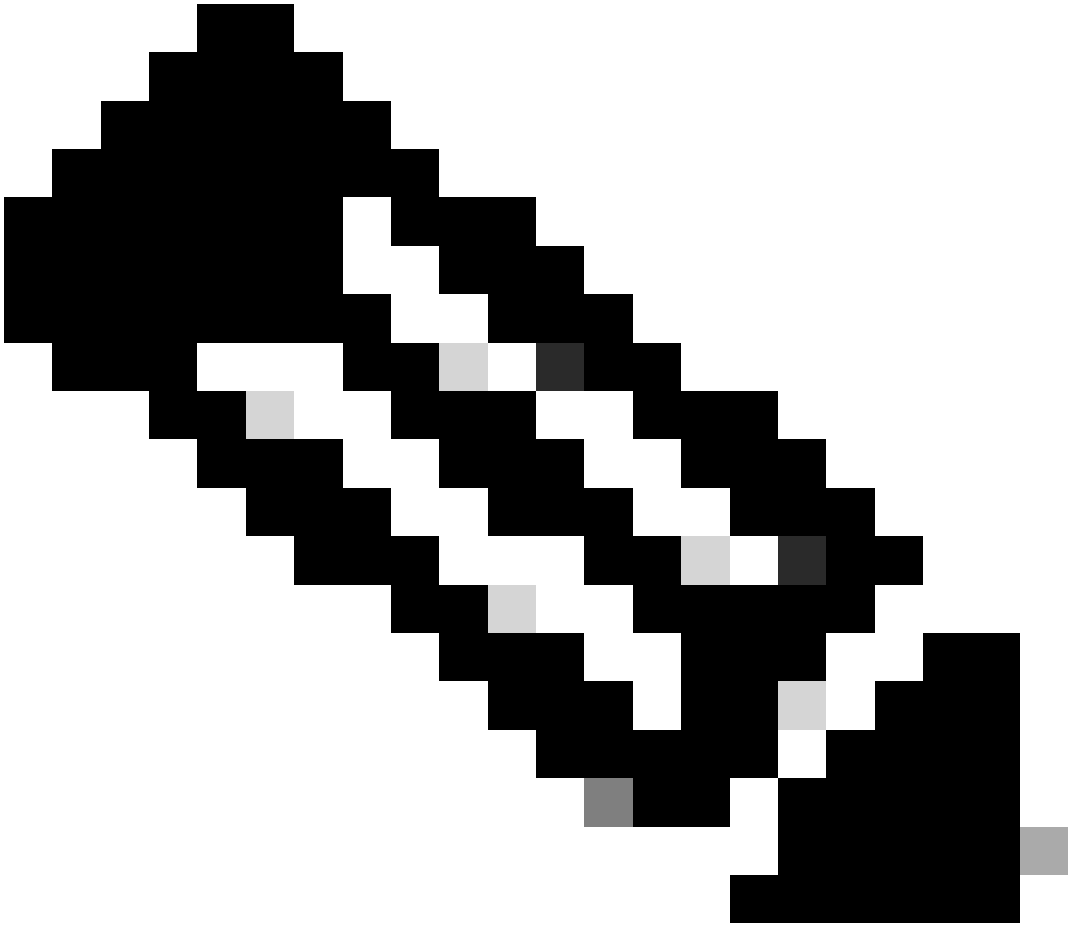
在故障排除檔案中，pmtool show affnity命令輸出位於命令輸出目錄中。檔案的名稱為：**usr-local-sf-bin-pmtool show affinity.output**

如果在較大型裝置的故障排除上運行，輸出可能會非常長。以下是一些grep命令，用於清楚地指示分配給snort和SFDataCorrelator進程的CPU數量。

[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

先前的輸出來自目前最大的裝置(FPR-9300 SM-44)。如您所見，有46個CPU分配給snort，2個CPU分配給SFDataCorrelator（因為已啟用惡意軟體策略）。



注意：TS分析無法在這些情況下正確顯示整個DE效能圖表

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。