# Abilita controllo di accesso su criteri file con malware

## Sommario



## Introduzione

In questo documento viene descritto come allocare l'ordinamento con il processo SFDataCorrelator per eseguire ricerche SHA sui file rilevati.

## Prerequisiti

- Licenza Protect and Malware
- Criterio file tramite malware

### Requisiti

- 5.3.0 e versioni successive
- ASA (tutti i modelli)
- serie 7000 e 8000 (ad eccezione degli accessori "AMP")
- FTD in esecuzione sull'appliance ASA
- FTD in esecuzione sullo chassis FXOS

### Componenti usati

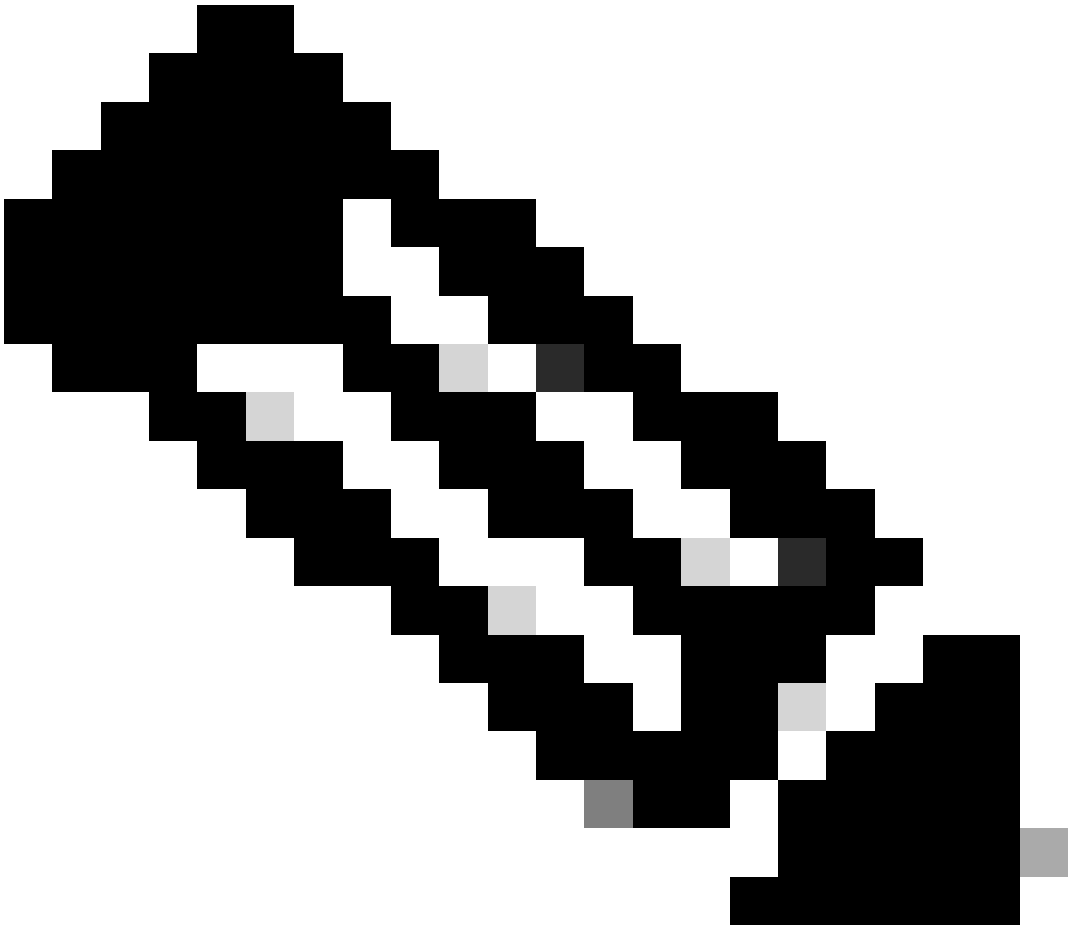
- Malware

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

Quando si attiva un criterio di controllo dell'accesso con un criterio File che utilizza un'azione Malware o un'opzione "Archivia file", è possibile sottrarre una CPU (o due su modelli più grandi) dall'ascolto.

## Conseguenze sulle prestazioni



Nota: quando si abilita il malware su appliance con risorse inferiori, l'impatto sulle prestazioni è maggiore.

- Latenza
- Cadute
- Elevato consumo della CPU
- Throughput inferiore

# Risoluzione dei problemi

Rimuovere il criterio file dal criterio CA o disattivare la regola CA utilizzando il criterio file. Quindi, riapplicare i criteri ACL per assegnare lo snort a tutti i core CPU disponibili.

## 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)
```

## Serie 7000 e 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:
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

Su una delle piattaforme FTD, il comando precedente`pmtool show affnity` può essere eseguito dal prompt iniziale '>' dopo l'accesso SSH. Ad esempio:

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)

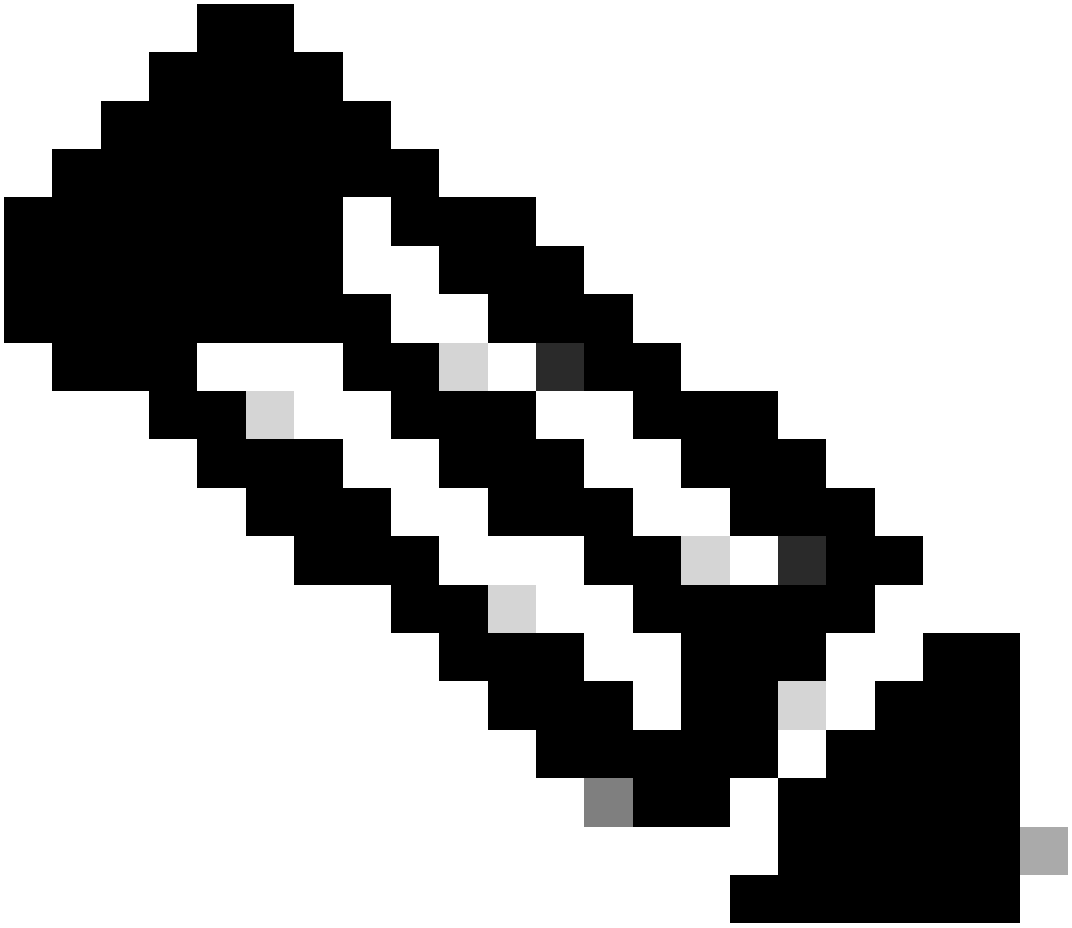
In risoluzione dei problemi relativi ai file, l'output delpmtool show affnity comando si trova nella directory command-outputs. Il nome del file è: **usr-local-sf-bin-pmtool show affinity.output**

L'output può essere piuttosto lungo se eseguito su un dispositivo di dimensioni maggiori per la risoluzione dei problemi. Di seguito sono riportati alcuni comandi grep per fornire una chiara indicazione del numero di CPU allocate ai processi snort e SFDataCorrelator.

[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

L'output precedente proviene dal dispositivo più grande corrente (FPR-9300 SM-44). Come si può vedere, ci sono 46 CPU allocate per lo snort e due allocate a SFDataCorrelator (poiché Malware Policy è abilitato).



**Nota**: in questi scenari l'analisi di Servizi terminal non è in grado di visualizzare correttamente tutti i grafici delle prestazioni di Servizi terminal

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).