

# Informazioni sulla profilatura delle regole Snort 3 e sulla profilatura della CPU sull'interfaccia utente di FMC

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Panoramica delle funzionalità](#)

[Creazione profilo](#)

[Profiler regole](#)

[Creazione profilo regole operative](#)

[Menu Profiling Snort 3](#)

[Creazione profilo regola di avvio](#)

[Risultati profiler regole](#)

[Scarica i risultati](#)

[Profilatura CPU](#)

[Panoramica del profiler CPU Snort 3](#)

[Scheda Profiling CPU](#)

[Spiegazione dei risultati del profiler CPU](#)

[Risultato profiler CPU - Scarica snapshot](#)

[Filtraggio dei risultati del profiling CPU](#)

---

## Introduzione

In questo documento viene descritta la regola Snort 3 e la funzionalità di profiling della CPU aggiunta in FMC 7.6.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza di Snort 3
- Secure Firepower Management Center (FMC)
- Secure Firepower Threat Defense (FTD)

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Questo documento è valido per tutte le piattaforme Firepower
- Secure Firewall Threat Defense Virtual (FTD) con software versione 7.6.0
- Secure Firewall Management Center Virtual (FMC) con software versione 7.6.0

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.

## Panoramica delle funzionalità

- La profilatura di regole e CPU esisteva già in Snort ma era accessibile solo tramite la CLI FTD. L'obiettivo di questa funzionalità è estendere le funzionalità di profilatura e renderle più semplici.
- Abilitare i problemi di prestazioni relativi alle regole per le intrusioni di debug e modificare le configurazioni delle regole singolarmente prima di contattare TAC per assistenza nella risoluzione dei problemi.
- Comprendere quali moduli hanno prestazioni insoddisfacenti quando lo Snort 3 utilizza una CPU elevata.
- Creare un modo semplice per eseguire il debug e ottimizzare i criteri di analisi delle intrusioni e della rete per migliorare le prestazioni.

## Creazione profilo

- Sia la profilatura delle regole che la profilatura della CPU vengono eseguite sull'FTD e i relativi risultati vengono memorizzati sul dispositivo e recuperati dal FMC.
- È possibile eseguire più sessioni di profiling contemporaneamente su dispositivi diversi.
- È possibile eseguire contemporaneamente il profiling delle regole e quello della CPU.
- In caso di Alta disponibilità, la profilatura può essere avviata solo sul dispositivo attivo all'inizio della sessione.  
Per le impostazioni cluster, è possibile eseguire la profilatura in ogni nodo del cluster.
- Se viene attivata una distribuzione mentre è in corso una sessione di profilatura, viene visualizzato un avviso per l'utente.

Se l'utente sceglie di ignorare l'avviso e la distribuzione, la sessione di profilatura corrente verrà annullata e il risultato del profiler mostrerà un messaggio relativo a questa operazione.

È necessario avviare una nuova sessione di profilatura senza essere interrotta da una distribuzione per ottenere i risultati effettivi della profilatura.

## Profiler regole

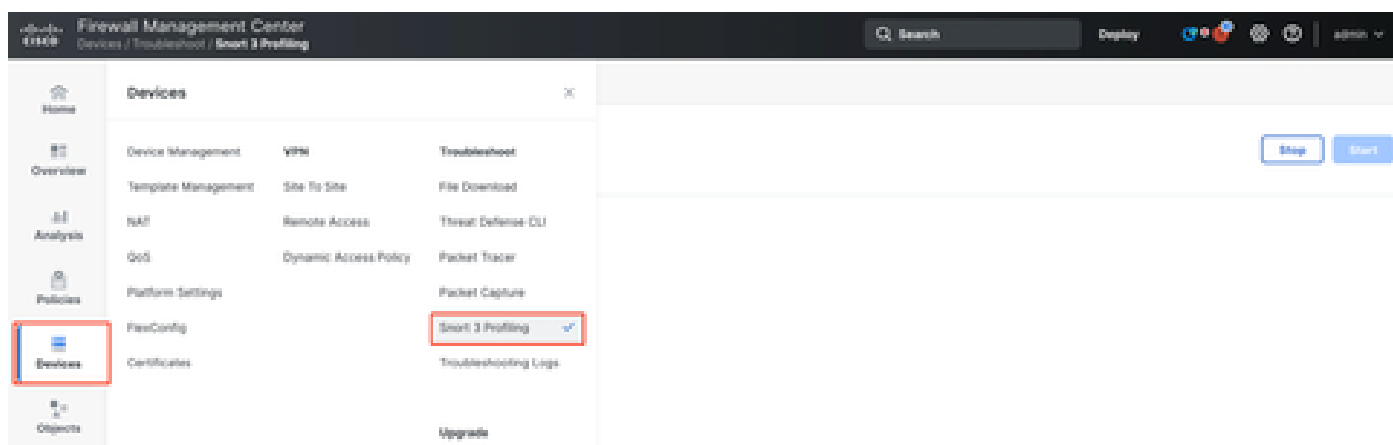
- Il profiler delle regole Snort 3 raccoglie dati sulla quantità di tempo impiegata per elaborare un insieme di regole di intrusione Snort 3, evidenziando in tal modo i potenziali problemi, mostrando le regole con prestazioni insoddisfacenti.
- Profiler regole visualizza le 100 regole IPS il cui controllo ha richiesto più tempo.
- L'attivazione di Profiler regole non richiede il ricaricamento o il riavvio di Snort 3.
- I risultati del profiling delle regole vengono salvati in formato JSON nella directory `/ngfw/var/sf/sync/snort_profiling/` e sincronizzati nel FMC.
- Il profiler delle regole giace all'interno dello Snort 3 e controlla il traffico con il meccanismo di rilevamento intrusioni dello Snort 3; l'abilitazione della profilatura delle regole non ha alcun impatto significativo sulle prestazioni.

## Creazione profilo regole operative

- Il traffico deve passare attraverso il dispositivo
- Avviare il profiling delle regole selezionando un dispositivo, quindi facendo clic sul pulsante Start
  - L'avvio di una sessione di profilatura determina la creazione di un'attività che può essere monitorata in Notifiche in Attività
- La durata predefinita di una sessione di profilatura delle regole è di 120 minuti
  - La sessione di profilatura delle regole può essere interrotta prima, prima del completamento, premendo il pulsante Arresta
- I risultati possono essere visualizzati nella GUI e scaricati
- La Cronologia profilatura visualizza i risultati delle sessioni di profilatura precedenti. L'utente può esaminare uno specifico risultato di profilatura facendo clic su una scheda nel pannello laterale sinistro Cronologia profilatura.

## Menu Profiling Snort 3

È possibile accedere alla pagina Profiling dal menu Devices > Snort 3 Profiling. La pagina contiene la profilatura di regole e CPU, suddivisa in due schede.



Dispositivi

## Creazione profilo regola di avvio

Per avviare una sessione di profilatura delle regole, fare clic su Avvia. La sessione viene interrotta automaticamente dopo 120 minuti.

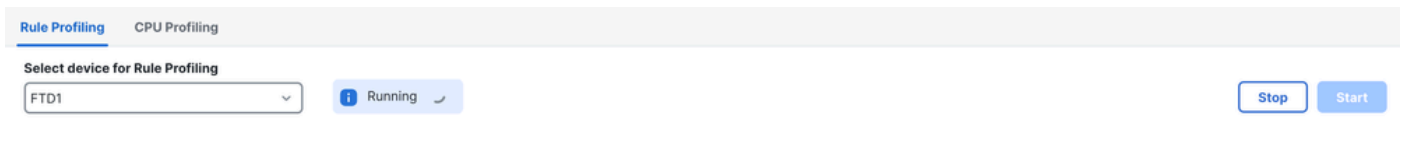
Un utente non può configurare la durata della sessione di profilatura, ma può arrestarla prima che siano trascorse le due ore.



The screenshot shows the 'Rule Profiling' section of a management console. At the top, there are two tabs: 'Rule Profiling' (selected) and 'CPU Profiling'. Below the tabs, there is a dropdown menu labeled 'Select device for Rule Profiling' with 'FTD1' selected. To the right of the dropdown are two buttons: 'Stop' and 'Start', both highlighted with a red box. Below this is a section titled 'Rule Profiling Results - FTD1 - 22 minutes ago'. It contains a table with the following data:

Start: 2025-01-16 10:35:40 IST	Access Control Policy: test	VDB: 392	Snort Version: 3.1791-121
Finish: 2025-01-16 10:37:10 IST	Access Control Policy revision time: 2025-01-15 13:15:26 IST	LSP: lsp-rel-20250114-1341	Device Version: 7.6.0-113

### Creazione profilo regola



The screenshot shows the 'Rule Profiling' section of a management console. At the top, there are two tabs: 'Rule Profiling' (selected) and 'CPU Profiling'. Below the tabs, there is a dropdown menu labeled 'Select device for Rule Profiling' with 'FTD1' selected. To the right of the dropdown is a status indicator that says 'Running' with a blue information icon and a dropdown arrow. To the right of the status indicator are two buttons: 'Stop' and 'Start'.



Rule Profiling started 8 seconds ago

Profiling takes around 120 minutes. The task manager will send notification when the profiling task is complete.

In esecuzione

Dopo l'avvio della sessione di profilatura delle regole, viene creata un'attività. È possibile selezionare Notifiche > Attività.

20+ total
0 waiting
3 running
0 retrying
20+ success
🔍 Filter

1 failure

🌀 Rule profiler
2m 6s

Generate Rule Profiling File  
 Generate rule profiling file for FTD1  
 Remote status: Generating rule profiling file

Attività

Per interrompere una sessione di profilatura delle regole in corso, nel caso sia necessario interromperla prima dell'arresto automatico, fare clic su Arresta e confermare.

Interrompi profilatura

Dopo aver selezionato un dispositivo, nella sezione Risultati profilatura regole viene visualizzato automaticamente il risultato più recente.

La tabella contiene le statistiche relative alle regole che hanno impiegato più tempo per l'elaborazione in ordine decrescente in base al tempo totale (in microsecondi (µs) impiegato.consumato.

Filter by % of Snort time  Search Total 40

GuidSid	Rule Description	% of Snort Time	Rev	Checks	Matches	Alerts	Time (µs)	Avg/Check	Avg/Match	Avg/Non-Match	Timeouts	Suspends
1:23224	EXPLOIT-KIT Redkit exploit kit landing page Requested - 8Digit.html	0.00003%	13	17	0	0	143	8	0	8	0	0
1:28585	FILE-PDF Adobe Acrobat Reader OTF font head table size overflow atte...	0.00001%	8	16	0	0	49	3	0	3	0	0
1:47030	MALWARE-CNC Win.Malware.Innaput variant outbound connection	0.00001%	1	37	0	0	44	1	0	1	0	0
1:37651	MALWARE-TOOLS Win.Trojan.Downloader outbound connection attempt	0.00001%	3	6	0	0	42	7	0	7	0	0

## Risultati profiler regole

L'output del profiler delle regole per una regola IPS include i campi seguenti:

- % di tempo di snort - Tempo impiegato per l'elaborazione della regola, in relazione al tempo dell'operazione Snort 3
- Controlli: numero di esecuzioni della regola IPS.
- Corrispondenze: numero di volte in cui la regola IPS ha trovato una corrispondenza completa
- Avvisi - Numero di volte in cui la regola IPS ha attivato un avviso IPS
- Tempo (µs) - Tempo in microsecondi impiegato da Snort per il controllo della regola IPS
- Media/Controllo - Tempo medio impiegato da Snort per un controllo della regola
- Media/Corrispondenza - Tempo medio impiegato da Snort per un controllo che ha restituito una corrispondenza
- Media/Non corrispondenza - Tempo medio impiegato da Snort per un controllo che non ha restituito una corrispondenza
- Timeout - Numero di volte in cui la regola ha superato il valore di Gestione regola - Soglia configurata nelle impostazioni delle prestazioni basate sulla latenza del criterio AC
- Sospensioni: numero di volte in cui la regola è stata sospesa a causa di violazioni di soglia consecutive

## Scarica i risultati

- L'utente può scaricare il risultato del profiling ("istantanea") facendo clic sul pulsante "Scarica istantanea". Il file scaricato è in formato .csv e contiene tutti i campi della pagina dei risultati del profiling.
- Estrarre dal file .csv della copia istantanea:

Device,Start Time,End Time,GID:SID,Rule Description,% of Snort Time,Rev,Checks,Matches,Alerts,Time (µs)

Visualizzazione file .csv snapshot:

Rule\_Profiling\_172.16.0.102\_2024-03-13 11\_08\_41

Device	Start Time	End Time	GID:SID	Rule Description	% of Snort Time	Rev	Checks	Matches	Alerts	Time (µs)	Avg/Check	Avg/Match	Avg/Non-Match	Timeouts	Suspends
172.16.0.102	2024-03-13 11:05:41	2024-03-13 11:07:21	2000:1000001	TEST 1	0.00014	1	4	4	1	284	71	71	0	0	0
172.16.0.102	2024-03-13 11:05:41	2024-03-13 11:07:21	1:28585	FILE-PDF Adobe Acrobat Reader OTF font head table size overflow attempt	0.00006	8	4	0	0	113	28	0	28	0	0
172.16.0.102	2024-03-13 11:05:41	2024-03-13 11:07:21	1:23224	EXPLOIT-KIT Redkit exploit kit landing page Requested - 8Digit.html	0.00003	13	4	0	0	64	16	0	16	0	0
172.16.0.102	2024-03-13 11:05:41	2024-03-13 11:07:21	1:55993	PROTOCOL-ICMP Microsoft Windows IPv6 DNSSEC option record denial of service attempt	0.00002	1	4	0	0	32	8	0	8	0	0

Snapshot

## Profilatura CPU

### Panoramica del profiler CPU Snort 3

- Il profiler della CPU definisce il profilo del tempo CPU impiegato dai moduli/ispettori dello Strumento 3 per elaborare i pacchetti in un determinato intervallo di tempo. Fornisce un'analisi della quantità di CPU utilizzata da ogni modulo rispetto alla CPU totale utilizzata dal processo Snort 3.
- L'utilizzo di CPU Profiler non richiede il ricaricamento della configurazione o il riavvio dell'Snort 3, evitando così tempi di inattività.
- Il risultato del profiler CPU visualizza il tempo di elaborazione impiegato da tutti i moduli durante l'ultima sessione di profilatura.
- I risultati del profiling della CPU vengono salvati in formato JSON nella directory `/ngfw/var/sf/sync/cpu_profiling/` e sincronizzati nella directory `/var/sf/peers/<UUID dispositivo>/sync/cpu_profiling` della console centrale di configurazione.
- È stata aggiunta una nuova pagina di profiling dello script 3 nell'interfaccia utente di FMC
- È possibile accedere a questa pagina dalla scheda Dispositivi > Snort 3 Profiling > Profiling CPU
- Utilizzare Scarica snapshot nella scheda Profilo CPU per scaricare uno snapshot dei risultati del profiling in formato CSV.

## Scheda Profiling CPU

È possibile accedere alla pagina Profiling CPU dalla scheda Dispositivi > Snort 3 Profiling menu > Profiling CPU.

Contiene un selettore di dispositivo, i pulsanti Start/Stop, il pulsante Scarica istantanea, una sezione dei risultati di profilatura e una sezione Cronologia profilatura sul lato sinistro che è espansa quando si fa clic su di essa.

The screenshot shows the Cisco Firewall Management Center (FMC) interface. The main content area displays the CPU Profiling results for device FTD1. The results are as follows:

Module	% Total of CPU time	Time (µs)	Avg/Check	% Caller
daq	100	6674110782	893694	100
perf_monitor	0	39946	5	0
firewall	0	16360	2	0
mpse	0	2181	0	0

### Profilatura Cpu

Per avviare una sessione di profiling della CPU, fare clic su Avvia. Questa pagina viene visualizzata all'avvio della sessione.

Rule Profiling **CPU Profiling**

Select device for CPU Profiling

FTD1

Stop Start

**CPU Profiling Results - FTD1** (30 seconds ago) [Download Snapshot](#)

Start: 2025-01-16 10:18:25 IST    Access Control Policy: test    VDB: 392    Snort Version: 3.1.79.1-121  
 Finish: 2025-01-16 11:14:01 IST    Access Control Policy revision time: 2025-01-15 13:15:26 IST    LSP: lsp-rel-20250114-1341    Device Version: 7.6.0-113

Filter by % of Snort time  Search  Total **4**

Module	% Total of CPU time	Time (µs)	Avg/Check	% Caller
daq	100	6674110782	893694	100
perf_monitor	0	39946	5	0
firewall	0	16360	2	0
mpse	0	2181	0	0

Inizio

Rule Profiling **CPU Profiling** [Dismiss all notifications](#)

Select device for CPU Profiling

FTD1 Running

**CPU profiler**  
 Generate CPU Profiling File  
**Generate CPU profiling file for FTD1**  
 Remote status: Generating CPU profiling file

CPU Profiling started 8 seconds ago  
 Profiling takes around 120 minutes. The task manager will send notification when the profiling task is complete.

In esecuzione

Dopo l'avvio della sessione di profiling della CPU, viene creata un'attività. È possibile selezionare Notifiche > Attività.



20+ total

0 waiting

2 running

0 retrying

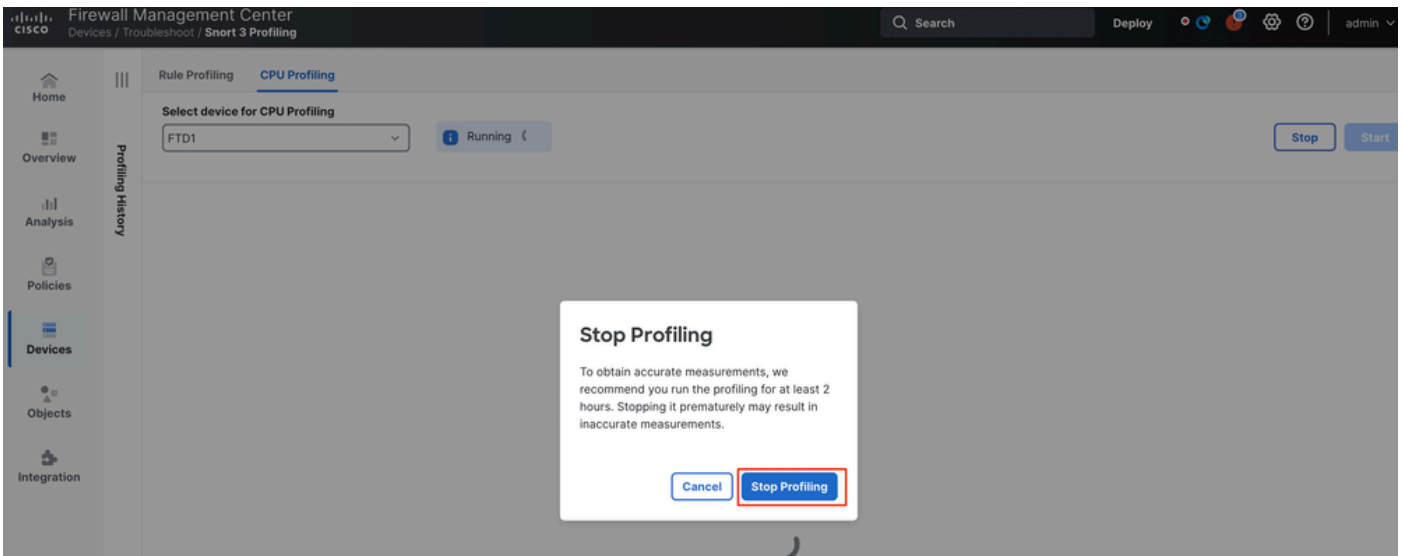
20+ success

1 failure

 CPU profiler  
 Generate CPU Profiling File  
 Generate CPU profiling file for FTD1  
 Remote status: Generating CPU profiling file

Attività

- Per interrompere una sessione di profiling della CPU in corso, fare clic su Arresta.
- Viene visualizzata una finestra di dialogo di conferma. fare clic su Interrompi profilatura.



Interrompi esecuzione

L'ultimo risultato del profiling viene visualizzato nella sezione Risultati profiling CPU.

CPU Profiling Results - FTD1 (29 seconds ago) [Download Snapshot](#)

Start: 2025-05-16 11:20:38 EDT    Access Control Policy: local    VDB: 203  
 Finish: 2025-05-16 11:23:04 EDT    Access Control Policy revision time: 2025-01-15 13:10:38 EDT    LBP: lbp-101-20050114-10341    Report Version: 3.1.79.6-1021    Device Version: FTD-0-112

Filter by % of Short time   Total 4

Module	% Total of CPU time	Time (µs)	Avg/Check	% Caller
diag	100	1048448000	900060	100
perf_monitor	0	1660	4	0
firewall	0	923	3	0
mgmt	0	101	0	0

## Spiegazione dei risultati del profiler CPU

- La colonna "Modulo" indica il nome del modulo/del controllo.
- La colonna "% del tempo totale CPU" indica la percentuale di tempo impiegato dal modulo rispetto al tempo totale impiegato dall'Snort 3 nell'elaborazione del traffico. Se questo valore è notevolmente superiore a quello di altri moduli, il modulo contribuisce maggiormente a prestazioni insoddisfacenti dello Snort 3.
- "Tempo ( $\mu$ s)" rappresenta il tempo totale in microsecondi impiegato da ciascun modulo.
- "Media/Verifica" rappresenta il tempo medio impiegato dal modulo per ogni richiamo del modulo.
- "% Caller" indica il tempo impiegato dal sottomodulo (se configurato) rispetto al modulo principale. Viene utilizzato principalmente per il debug degli sviluppatori.

## Risultato profiler CPU - Scarica snapshot

- L'utente può scaricare lo snapshot dei risultati del profiling facendo clic su Scarica snapshot. Il file scaricato è in formato .csv e contiene tutti i campi della pagina dei risultati del profiling, come mostrato in questo esempio.
- Estrarre dal file .csv della copia istantanea:

CPU\_Profiling\_FTD1\_2025-01-16 00\_55\_45

Device	Start Time	End Time	Module	% Total of CPU time	Time ( $\mu$ s )	Avg/Check	%/Caller
FTD1	2025-01-16 00:50:30	2025-01-16 00:53:34	daq	100	366446909	900360	100
FTD1	2025-01-16 00:50:30	2025-01-16 00:53:34	perf_monitor	0	1662	4	0
FTD1	2025-01-16 00:50:30	2025-01-16 00:53:34	firewall	0	923	2	0
FTD1	2025-01-16 00:50:30	2025-01-16 00:53:34	mpse	0	101	0	0

Snapshot

## Filtraggio dei risultati del profiling CPU

I risultati della profilatura possono essere filtrati utilizzando:

- "Filtra in base alla percentuale di tempo di snort": consente di filtrare i moduli la cui esecuzione ha richiesto più dell'n% del tempo di profilatura.
- Ricerca: consente di eseguire una ricerca di testo in qualsiasi campo presente nella tabella dei risultati.

È possibile ordinare qualsiasi colonna ad eccezione di "Modulo" facendo clic sulla relativa intestazione.

Module	% Total of CPU time	Time ( $\mu$ s)	Avg/Check	% Caller
rule_eval	20.89	26138283	3	20.89
mpse	14.11	17661177	0	14.11



## 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).