FTD High CPU Core-waarschuwingen van Pruner.pl-proces

uitgeven

FMC genereert frequente meldingen van hoog CPU-gebruik voor meerdere beheerde FTD-apparaten en maakt zich zorgen over de prestaties en stabiliteit van de firewall. Met name de FMC-statusmonitor toont herhaalde CPU-kernpieken op specifieke kernen gedurende langere perioden, waarbij het interne Pruner.pl-achtergrondproces consequent te veel CPU verbruikt voor de opgegeven kernen. Ondanks deze kritieke CPU-waarschuwingen die in FMC verschijnen, wordt er geen door de gebruiker zichtbare impact op het verkeer waargenomen en blijft de algehele FTD-stabiliteit onaangetast.

milieu

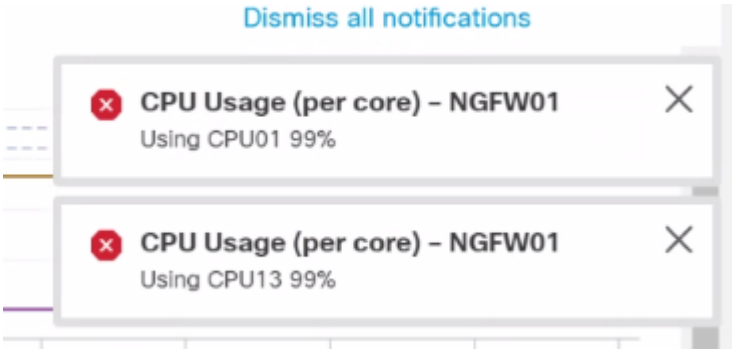
- FTD-softwareversie: 7.2.5 (geldt voor zowel virtuele als hardwaremodellen in alle versies lager dan 7.2.6)
- Apparaten beheerd door Firepower Management Center (FMC)

resolutie

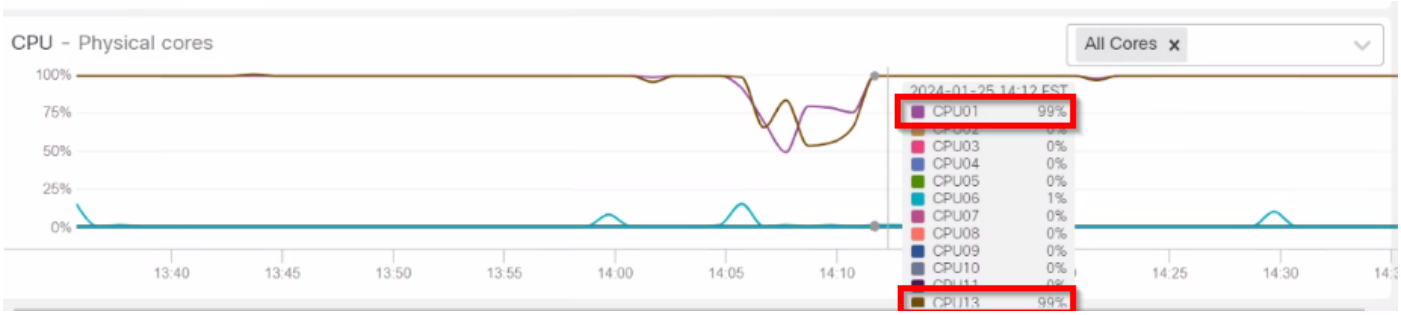
De oplossing omvat het upgraden van de getroffen FTD-apparaten naar een softwareversie die de oplossing voor het geïdentificeerde defect bevat.

Stappen voor probleemoplossing en analyse

1: Onderzoek de CPU-gebruikspatronen in de FTD Health Monitor-grafieken in de loop van de tijd om de omvang en timing van het probleem te identificeren. De analyse onthult herhaalde CPU-kernpieken op specifieke kernen die zich voordoen, terwijl het totale CPU- en geheugengebruik binnen het normale werkingsbereik bleef.



inline_image_0.png



inline_image_1.png

```
Health Monitor Alert | Time: Mon Jul 24 06:34:20 2023 UTC | Severity: critical | Module: CPU Usage (per
Health Monitor Alert | Time: Mon Jul 24 04:24:20 2023 UTC | Severity: critical | Module: CPU Usage (per
```

2: Analyseer FTD CLI en los problemen op uit de getroffen FTD om de hoofdoorzaak van een hoog CPU-gebruik te identificeren.

3: Controleer de verzamelde gegevens om te bepalen welke processen te veel CPU-bronnen verbruiken. De analyse van top.log-bestanden bevestigde dat het Pruner.pl-proces consequent hoge CPU's gebruikte op bepaalde kernen, waarbij het uitgiftepatroon rond een specifiek tijdsbestek begon.

```
root@FTDdevice:/home/admin# cd /ngfw/var/log/
root@FTDdevice:/ngfw/var/log# grep "Pruner.pl --persistent" top.log | grep -v "S   0.0"
 12341 root      20   0  458920 437816  10056 R 100.0   0.2   9452:10 /usr/bin/perl /ngfw/usr/local/sf/
 12341 root      20   0  437124 416148  10056 R 100.0   0.2   9453:13 /usr/bin/perl /ngfw/usr/local/sf/
 12341 root      20   0  437124 416148  10056 R 100.0   0.2   9454:13 /usr/bin/perl /ngfw/usr/local/sf/
 12341 root      20   0  437124 416148  10056 R  94.1   0.2   9455:15 /usr/bin/perl /ngfw/usr/local/sf/
 12341 root      20   0  437124 416148  10056 R 100.0   0.2   9456:18 /usr/bin/perl /ngfw/usr/local/sf/
```

De logs tonen ook een hoog aantal lege, 0-byte "*snort-unified.log" bestanden die de belangrijkste reden zijn voor het zo vaak draaien van Pruner.pl.

```
root@FTDdevice:/home/admin# cd /ngfw/var/sf/detection_engines/FTD-UUID/
root@FTDdevice:/ngfw/var/sf/detection_engines/FTD-UUID# ls -l instance-* | grep -ri "root       0.snor
-rw-r--r--  1 root    root        0 Nov 12 19:47 snort-unified.log.1699818430
-rw-r--r--  1 root    root        0 Nov 12 19:41 snort-unified.log.1699818093
-rw-r--r--  1 root    root        0 Nov 12 19:35 snort-unified.log.1699817758
-rw-r--r--  1 root    root        0 Nov 12 17:13 snort-unified.log.1699809226
-rw-r--r--  1 root    root        0 Nov 12 17:08 snort-unified.log.1699808890
-rw-r--r--  1 root    root        0 Nov 12 17:02 snort-unified.log.1699808554
```

Oplossing voor software-upgrade

1: Upgrade alle betrokken FTD-apparaten naar een softwareversie die de oplossing voor CSCwh79095 bevat. De minimaal aanbevolen versies zijn:

- FTD 7.2.7 (minimumversie van de vaste versie in 7.2.x-trein)
- FTD 7.4.1 of hoger (aanbevolen upgradepad)

2: Controleer na de upgrade de FMC-gezondheidswaarschuwingen om te bevestigen dat:

- CPU-gebruik per core blijft stabiel
- Er worden geen nieuwe kritieke alarmen opgewekt voor Pruner.pl of soortgelijke achtergrondprocessen
- Hoge CPU-waarschuwingen voor het Pruner.pl-proces komen niet meer voor

Preventie en best practices

Implementeer deze aanbevelingen om soortgelijke problemen te voorkomen:

- Vermijd het uitvoeren van oudere codetreinen op lange termijn en plan periodieke upgrades naar aanbevolen releases om te profiteren van bugfixes en beveiligingsupdates
- Voordat u belangrijke upgrades uitvoert, bekijkt u de release-notities van Cisco en zoekt u naar bekende fouten in huidige en doelversies
- Doorgaan met het bewaken van FMC-gezondheidswaarschuwingen na upgrades om de stabiliteit van het systeem te garanderen
- Bekijk alle speciale upgradeoverwegingen die in de opmerkingen bij de release zijn gedocumenteerd

Oorzaak

De hoge CPU-waarschuwingen worden veroorzaakt door een softwarefout in FTD 7.2.5 geïdentificeerd als Cisco Bug ID CSCwh79095. Dit defect is te wijten aan lege, 0-byte snort-unified.log-bestanden waardoor het interne Pruner.pl-achtergrondproces te veel CPU verbruikt op specifieke kernen. Dit veroorzaakt aanhoudende high-CPU-alarmen in FMC. Belangrijk is dat deze voorwaarde geen invloed heeft op het doorsturen van dataverkeer of de algehele stabiliteit van het apparaat; het genereert alleen kritieke CPU-waarschuwingen in de beheerinterface. Het probleem is gerelateerd aan dubbele bugs, waaronder CSCwe66384 (Pruner.pl en schijfbeheer met hoge CPU zonder duidelijke schijfproblemen) en CSCwf80946 (FTD: Pruner-proces met behulp van overmatige CPU-kernen van het systeem en het genereren van FMC HM-waarschuwingen).

Verwante inhoud

- Cisco Bug ID CSCwh79095 - Snort genereert een overmatig aantal snort-uniforme logbestanden met nul bytes (Fixed in: 7.2.7, 7.4.1, 7.6.0)
- Cisco Bug ID CSCwf77994 - Valse kritieke hoge CPU-waarschuwingen voor FTD-apparaatsysteemkernen die onmiddellijk veel gebruik maken (vastgelegd in: 7.2.9, 7.4.1, 7.6.0)
- Documentatie FTD/FMC-release en aanbevolen releases
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.