Alertas de núcleo de CPU alto FTD del proceso Pruner.pl

Problema

FMC genera frecuentes alertas de uso elevado de la CPU para varios dispositivos FTD gestionados, y genera preocupaciones sobre el rendimiento y la estabilidad del firewall. Específicamente, el monitor de estado de FMC muestra picos repetidos del núcleo de la CPU en núcleos específicos durante períodos prolongados, con el proceso de fondo interno Pruner.pl consumiendo constantemente una CPU excesiva para los núcleos especificados. A pesar de que estas alertas críticas de la CPU aparecen en FMC, no se observa ningún impacto en el tráfico visible para el usuario y la estabilidad del FTD general no se ve afectada.

Entorno

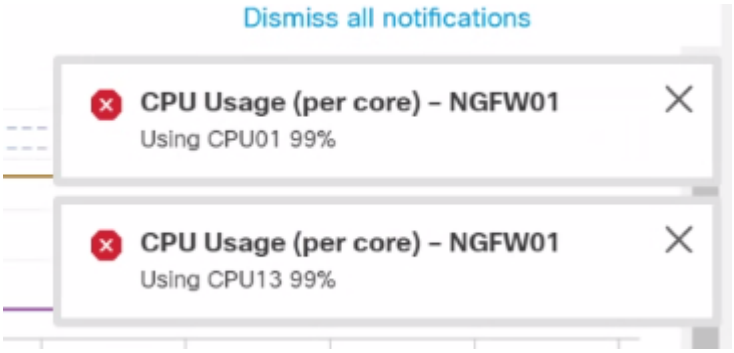
- Versión del software FTD: 7.2.5 (afecta tanto a los modelos virtuales como a los modelos de hardware en todas las versiones anteriores a la 7.2.6)
- Dispositivos administrados por Firepower Management Center (FMC)

Resolución

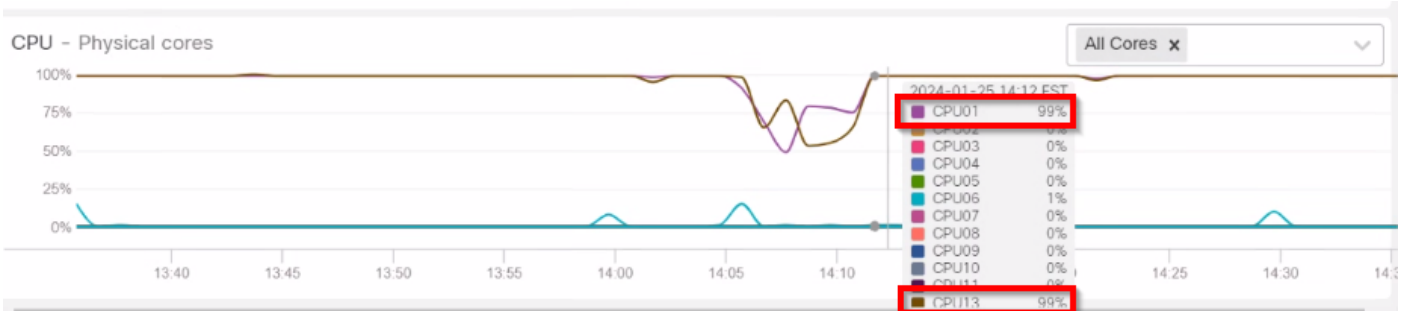
La resolución implica la actualización de los dispositivos FTD afectados a una versión de software que contenga la corrección del defecto identificado.

Pasos de solución de problemas y análisis

1: Examine los patrones de utilización de la CPU en los gráficos de FTD Health Monitor a lo largo del tiempo para identificar el alcance y el tiempo del problema. El análisis revela que se producen repetidos picos de núcleo de CPU en núcleos específicos, mientras que el uso general de la CPU y la memoria se mantuvo dentro de los rangos operativos normales.



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: Analice la CLI de FTD y resuelva problemas de paquetes del FTD afectado para identificar la causa raíz del uso elevado de la CPU.

3: Revise los datos recopilados para identificar qué procesos consumen demasiados recursos de la CPU. El análisis de los archivos top.log confirmó que el proceso Pruner.pl utilizaba de forma sistemática una CPU alta en determinados núcleos, y que el patrón de problemas empezaba en un período de tiempo específico.

```
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/
```

Los registros también muestran una alta cantidad de archivos vacíos, 0-byte"*snort-unified.log" que son la razón principal por la que Pruner.pl se ejecuta tan a menudo.

```
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
```

Solución de actualización de software

1: Actualice todos los dispositivos FTD afectados a una versión de software que contenga la corrección para CSCwh79095. Las versiones mínimas recomendadas son:

- FTD 7.2.7 (versión fija mínima en tren 7.2.x)
- FTD 7.4.1 o posterior (ruta de actualización recomendada)

2: Después de la actualización, supervise las alertas de estado de FMC para confirmar que:

- La utilización de la CPU por núcleo permanece estable
- No se generan nuevas alarmas críticas para Pruner.pl o procesos de fondo similares
- Ya no se producen alertas de CPU altas para el proceso Pruner.pl

Prevención y mejores prácticas

Aplique estas recomendaciones para evitar problemas similares:

- Evite ejecutar programas de formación de código antiguos a largo plazo y planifique actualizaciones periódicas a las versiones recomendadas para beneficiarse de correcciones de errores y actualizaciones de seguridad
- Antes de realizar actualizaciones importantes, revise las notas de la versión de Cisco y realice búsquedas de errores en busca de defectos conocidos en las versiones actual y final
- Seguir supervisando las alertas de estado de FMC después de las actualizaciones para garantizar la estabilidad del sistema
- Revise las consideraciones especiales de actualización documentadas en las notas de la versión

Causa

Las alertas de CPU altas son causadas por un defecto de software en FTD 7.2.5 identificado como Id. de bug de Cisco CSCwh79095. Este defecto se debe a archivos vacíos, snort-unified.log de 0 bytes que hace que el proceso interno en segundo plano Pruner.pl consuma una CPU excesiva en núcleos específicos. Esto activa alarmas persistentes de CPU altas en FMC. Es importante destacar que esta condición no afecta al reenvío de tráfico del plano de datos ni a la estabilidad general del dispositivo; solo genera alertas críticas de CPU en la interfaz de administración. El problema se relaciona con errores duplicados, incluidos CSCwe66384 (Pruner.pl y el administrador de discos con una CPU alta sin problemas obvios de disco) y CSCwf80946 (FTD: Proceso de recorte mediante núcleos de CPU del sistema excesivos y generación de alertas de HM de FMC).

Contenido relacionado

- Cisco Bug ID CSCwh79095 - Snort que genera un número excesivo de archivos de registro unificados con snort con cero bytes (corregido en: 7.2.7, 7.4.1 y 7.6.0)
- ID de bug de Cisco CSCwf77994 - Alertas críticas falsas de CPU altas para núcleos del sistema de dispositivos FTD que ejecutan un uso elevado instantáneo (fijo en: 7.2.9, 7.4.1 y 7.6.0)
- Documentación de las notas de la versión de FTD/FMC y de las versiones recomendadas
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).