Alertas de Núcleo de CPU Alto FTD do Processo Pruner.pl

Problema

O FMC gera alertas frequentes de alta utilização da CPU para vários dispositivos FTD gerenciados e levanta preocupações sobre o desempenho e a estabilidade do firewall. Especificamente, o monitor de integridade do FMC mostra picos repetidos do núcleo da CPU em núcleos específicos durante períodos prolongados, com o processo em segundo plano Pruner.pl interno consumindo consistentemente CPU excessiva para os núcleos especificados. Apesar desses alertas críticos de CPU aparecerem no FMC, nenhum impacto de tráfego visível ao usuário é observado e a estabilidade geral do FTD permanece inalterada.

Ambiente

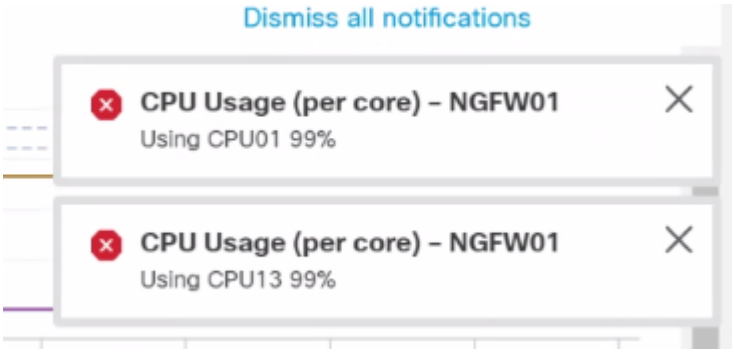
- Versão do software FTD: 7.2.5 (afeta modelos virtuais e de hardware em todas as versões anteriores à 7.2.6)
- Dispositivos gerenciados pelo Firepower Management Center (FMC)

Resolução

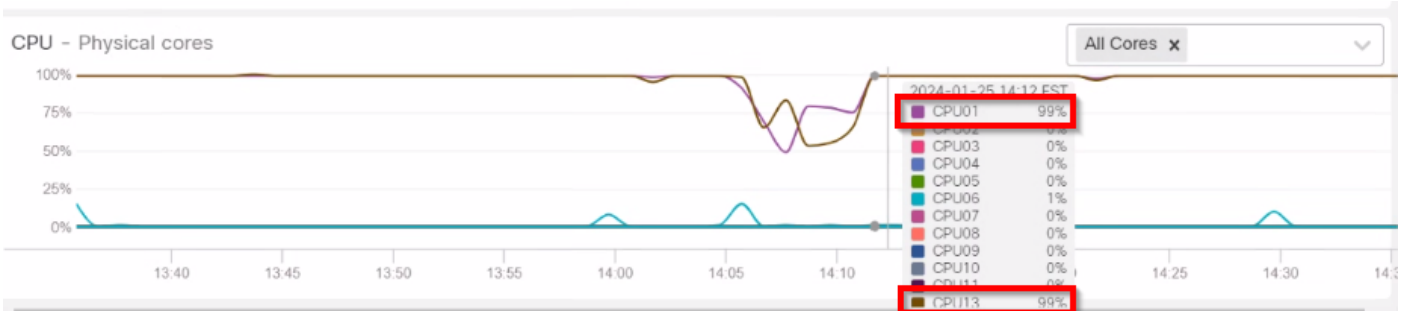
A resolução envolve a atualização dos dispositivos FTD afetados para uma versão de software que contenha a correção para o defeito identificado.

Etapas de Solução de Problemas e Análise

1: Examine os padrões de utilização da CPU nos gráficos do Monitor de integridade de FTD ao longo do tempo para identificar o escopo e a temporização do problema. A análise revela repetidos picos no núcleo da CPU em núcleos específicos que ocorrem, enquanto a utilização geral da CPU e da memória permaneceu dentro dos intervalos operacionais normais.



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: Analise a CLI do FTD e solucione problemas de pacotes do FTD afetado para identificar a causa raiz da alta utilização da CPU.

3: Revise os dados coletados para identificar quais processos estão consumindo recursos excessivos da CPU. A análise dos arquivos top.log confirmou que o processo Pruner.pl estava consistentemente usando alta CPU em determinados núcleos, com o padrão de problemas começando em torno de um período de tempo 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/
```

Os logs também mostram uma contagem alta de arquivos vazios, de 0-byte"*snort-unified.log", que são a principal razão para a execução de Pruner.pl com tanta frequência.

```
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
```

Solução de atualização de software

1: Atualize todos os dispositivos FTD afetados para uma versão de software que contenha a correção para CSCwh79095. As versões mínimas recomendadas são:

- FTD 7.2.7 (versão de correção mínima no trem 7.2.x)
- FTD 7.4.1 ou posterior (caminho de atualização recomendado)

2: Após a atualização, monitorizar os alertas de saúde do CVP para confirmar que:

- A utilização da CPU por núcleo permanece estável
- Nenhum alarme crítico novo é acionado para Pruner.pl ou processos de segundo plano semelhantes
- Alertas altos de CPU para o processo Pruner.pl não ocorrem mais

Prevenção e práticas recomendadas

Implemente essas recomendações para evitar problemas semelhantes:

- Evite executar treinamentos de código mais antigos a longo prazo e planeje atualizações periódicas para versões recomendadas para se beneficiar de correções de bugs e atualizações de segurança
- Antes das principais atualizações, revise as notas de versão da Cisco e procure defeitos conhecidos nas versões atual e desejada
- Continuar a monitorar os alertas de integridade do FMC após as atualizações para garantir a estabilidade do sistema
- Revisar quaisquer considerações especiais de upgrade documentadas nas notas de versão

Causa

Os alertas altos de CPU são causados por um defeito de software no FTD 7.2.5, identificado como Cisco Bug ID CSCwh79095. Esse defeito se deve a arquivos snort-unified.log vazios, de 0 bytes, que faz com que o processo em segundo plano Pruner.pl interno consuma CPU excessiva em núcleos específicos. Isso aciona alarmes persistentes de alta CPU no FMC. É importante observar que essa condição não afeta o encaminhamento de tráfego do plano de dados ou a estabilidade geral do dispositivo; gera apenas alertas críticos de CPU na interface de gerenciamento. O problema está relacionado a bugs duplicados, incluindo CSCwe66384 (Pruner.pl e alta CPU do gerenciador de disco sem problemas óbvios de disco) e CSCwf80946 (FTD: Processamento da impressora usando excesso de núcleos de CPU do sistema e gerando alertas FMC HM).

Conteúdo relacionado

- Cisco Bug ID CSCwh79095 - O Snort está gerando um número excessivo de arquivos de log unificados pelo Snort com zero bytes (Corrigido em: 7.2.7, 7.4.1, 7.6.0)
- ID de bug Cisco CSCwf77994 - Alertas de alta utilização de alto uso crítico falso para núcleos de sistema de dispositivos FTD executando alto uso instantâneo (Corrigido em: 7.2.9, 7.4.1, 7.6.0)
- Notas de versão do FTD/FMC e documentação das versões recomendadas
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.