Pruner.plプロセスからのFTD High CPU Coreアラート

お問い合わせ内容

FMCでは、管理対象の複数のFTDデバイスに対して高CPU使用率のアラートが頻繁に生成され、ファイアウォールのパフォーマンスと安定性に関する問題が発生します。特に、FMCヘルスモニタでは、特定のコアで長時間にわたりCPUコアのスパイクが繰り返し発生しており、内部のPruner.plバックグラウンドプロセスが特定のコアの過剰なCPUを継続的に消費しています。これらの重大なCPUアラートがFMCに表示されても、ユーザが目に見えるトラフィックへの影響は見られず、FTD全体の安定性は影響を受けません。

環境

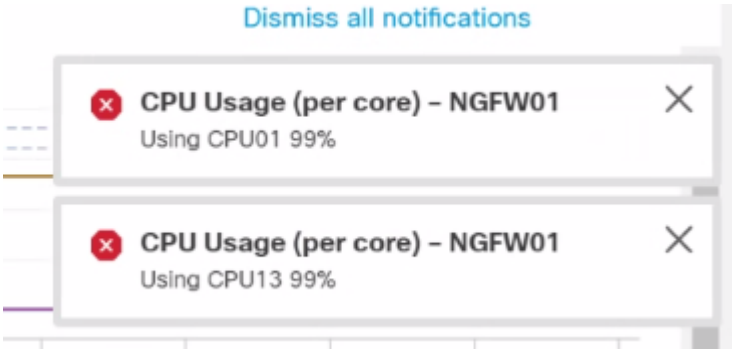
- FTDソフトウェアバージョン：7.2.5（7.2.6より前のすべてのバージョンで仮想モデルとハードウェアモデルの両方に影響）
- Firepower Management Center(FMC)で管理されるデバイス

解決策

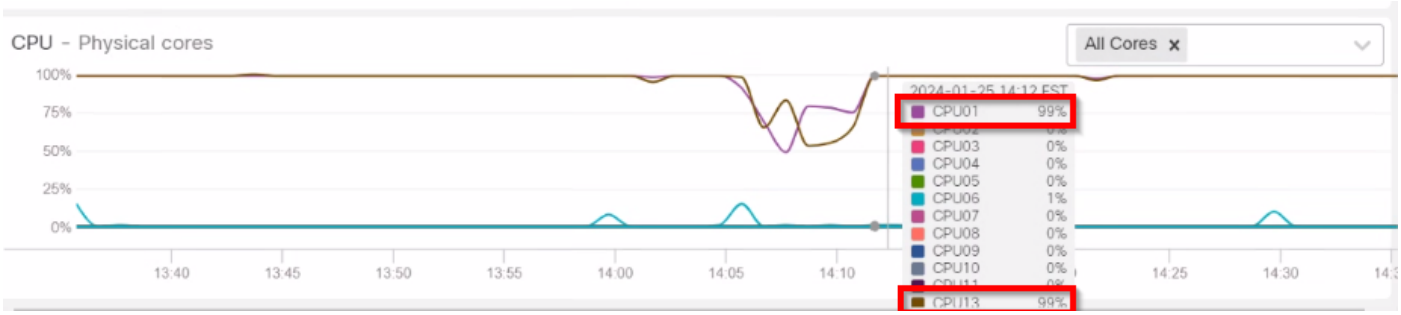
この問題を解決するには、該当するFTD不具合を、特定されたデバイスの修正が含まれているソフトウェアバージョンにアップグレードする必要があります。

トラブルシューティングと分析の手順

1: FTD Health MonitorのグラフのCPU使用率パターンを経時的に調べて、問題の範囲とタイミングを特定します。この分析により、全体的なCPUとメモリの使用率が通常の動作範囲内に留まっているにもかかわらず、特定のコアでCPUコアのスパイクが繰り返し発生していることがわかります。



inline_image_0.png (インラインイメージ_0.png)



inline_image_1.pngファイル

```
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:FTD CLIを分析し、影響を受けるFTDからのバンドルをトラブルシューティングして、高いCPU使用率の根本原因を特定します。

3：収集したデータを確認し、どのプロセスがCPUリソースを過剰に消費しているかを特定します。top.logファイルの分析により、Pruner.plプロセスが特定のコアで一貫して高いCPUを使用しており、問題のパターンが特定の時間枠に始まっていることが確認されました。

```
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/
```

ログには、空の0バイトの「*snort-unified.log」ファイルの数も多く表示されます。これは、Pruner.plが頻繁に実行される主な理由です。

```
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
```

ソフトウェアアップグレードソリューション

1：該当するすべてのFTDデバイスを、CSCwh79095に対する修正が取り込まれたソフトウェアバージョンにアップグレードします。推奨される最小バージョンは次のとおりです。

- FTD 7.2.7（7.2.xトレインの最小修正バージョン）
- FTD 7.4.1以降（推奨アップグレードパス）

2：アップグレード後、FMCヘルスアラートを監視して次のことを確認します。

- コアあたりのCPU使用率は安定している
- Pruner.plまたは同様のバックグラウンドプロセスでは、新しいクリティカルアラームは生成されません
- Pruner.plプロセスのCPU高使用率のアラートが発生しなくなりました

予防とベストプラクティス

次の推奨事項を実装して、同様の問題を防止します。

- 古いコードトレインを長期間実行することは避け、バグ修正とセキュリティアップデートの恩恵を受けるために推奨リリースへの定期的なアップグレードを計画する
- メジャーアップグレードの前に、シスコのリリースノートを確認し、現在のバージョンと対象バージョンの既知の不具合について不具合検索を実行します
- システムの安定性を確保するため、アップグレード後もFMCヘルスアラートのモニタリングを継続
- リリースノートに記載されているアップグレードに関する特別な考慮事項を確認します。

原因

CPU高使用率のアラートは、Cisco Bug ID CSCwh79095として特定されたFTD 7.2.5のソフトウェア不具合が原因で発生します。この不具合は、空の0バイトsnort-unified.logファイルが原因で、内部のPruner.plバックグラウンドプロセスによって特定のコアのCPUが過剰に消費されます。これにより、FMCで継続的な高CPUアラームがトリガーされます。重要なのは、この状態がデータプレーントラフィック転送やデバイスの全体的な安定性に影響を与えないことです。管理インターフェイスで重要なCPUアラートを生成するだけです。この問題は、CSCwe66384（Pruner.plおよびディスクマネージャの高CPU使用率で明らかなディスクの問題がない）やCSCwf80946（FTD：過剰なシステムCPUコアを使用するプルーナプロセスとFMC HMアラートの生成）などの、関連する重複するバグです。

関連コンテンツ

- Cisco Bug ID CSCwh79095：ゼロのバイトを含む過剰な数のsnort統合ログファイルをSnortが生成する（7.2.7、7.4.1、7.6.0で修正）
- Cisco Bug ID CSCwf77994：瞬間的な高使用率を実行しているFTDデバイスシステムコアのCPU使用率が非常に高い場合のアラート（7.2.9、7.4.1、7.6.0で修正）
- FTD/FMCリリースノートおよび推奨リリースドキュメント
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。