アクセスリスト要素数の増加によるファイアウォールFTDの高メモリの保護

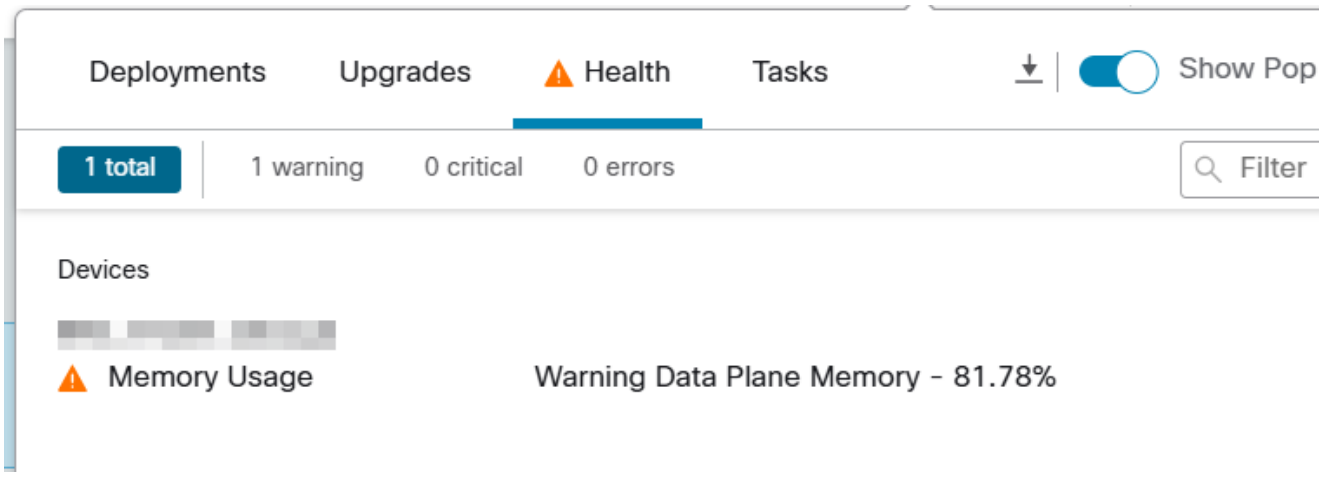
内容

問題

FTDでは、データプレーンのメモリ使用率が80 %を超えるアラートが継続的に表示されます。ポリシーを導入した後も、メモリ使用率はこの高いレベルにとどまり、アクセスリスト要素の数はプラットフォームが対応できる範囲を超えて大幅に増加しました。

FTDハイアベイラビリティ設定では、この問題は両方のユニットに影響しますが、アクティブなFTDのメモリ使用率が高くなります。

- FMCアラートでは、FTDのデータプレーンでメモリ使用量が高いことがわかります。



- FTD CLIでも、メモリの高使用率が確認されます。

```
<#root>

firepower# show memory
Free memory:        2590897856 bytes (18%)
Used memory:       11746269504 bytes (82%)

-------------      ------------------
Total memory:      14337167360 bytes (100%)
```

- access-list element countは、FTD CLIで100万以上の要素を示します。

<#root>

```
firepower# show access-list element-count
```

Total number of access-list elements: 3223691

- FTDのFMCヘルスモニタリンググラフでは、ACEの展開に関連するメモリが急激に増加しています。



- ハイアベイラビリティピアFTDでは、クリアされていないメモリが原因で、メモリ使用量が高いレベルでスタックする場合があります。

<#root>

```
firepower# failover exec standby show memory
Free memory:         3278441368 bytes (23%)
```

Used memory: 11058725992 bytes (77%)

```
-------------      -------------------
Total memory:       14337167360 bytes (100%)
```

環境

- ハイアベイラビリティ構成のCisco Firepower 2130 Threat Defense
- FTDソフトウェアバージョン：7.4.2
- FMCソフトウェアバージョン：7.6.2
- アクセスリストの要素の数が100万以上に近い

解決方法

1. FTD High Availability(HA)設定では、事前に計画した時間の間にピアFTDをリブートして、以前に蓄積した可能性がある保持されているメモリストアをクリアします。

2. リブート後、次の点を確認します。

- ピアFTDがハイアベイラビリティペアに適切に再同期されます。
- メモリ使用率が正常なレベルを示している。
- FTDメモリのアラートがFMC UIからクリアされます。

3. Devices > Device Managementに移動し、FTDのEditアイコンをクリックします。

4. 左上にあるDeviceタブ（FTD HAの場合はSummaryタブ）をクリックし、Advanced Settingsセクションまでスクロールダウンしてから、Editアイコンをクリックします。

5. Object Group Searchのボックスをチェックしてこの機能を有効にし、Saveをクリックします。

6. FTD HAペアに設定変更を導入し、ヘルスモニタを数分間監視してメモリ使用量の変化を監視します。

<#root>

```
firepower# show memory
Free memory:        6948343576 bytes (48%)
```

```
Used memory:        7388823784 bytes (52%)


-------------     --------------------------
Total memory:      14337167360 bytes (100%)
```

その他の考慮事項

オブジェクトグループ検索を有効にしてもメモリ使用率がパフォーマンス上の問題になる場合は、次のような最適化戦略を検討してください。

- FMC接続イベントを使用して上位ヒットカウントルールを確認しています。
- 大量の信頼できるトラフィックに対する不要なインスペクションを削減する。
- すべてのルールで侵入インスペクションが必要かどうかを評価する。
- 大容量のFirepowerプラットフォーム（FPR4KまたはFPR9Kシリーズ）へのプラットフォームアップグレードを検討しています。

原因

データプレーンメモリの高使用率は、FTDの保持メモリと、ポリシー導入後のアクセスリスト要素の処理オーバーヘッドの増加が組み合わさって発生します。重要なアクセスリスト要素の数は、メモリ使用率の急増と直接相関しています。オブジェクトグループ検索の最適化を行わずにACL処理要件を大幅に向上させると、メモリ使用量が継続的に増加します。

関連コンテンツ

- FMC CLIを使用したアクセスリスト要素(ACE)数の計算
- Cisco Secure Firewall Management Centerデバイス設定ガイド7.4：アクセスコントロールルールのベストプラクティス
- Cisco Secure Firewall Management Centerデバイス設定ガイド7.4：オブジェクトグループ検索の設定

- Firepower Threat Defenseのコマンドリファレンス
- 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。