Sicherer Firewall-FTD-Speicher aufgrund hoher Anzahl von Zugriffslistenelementen

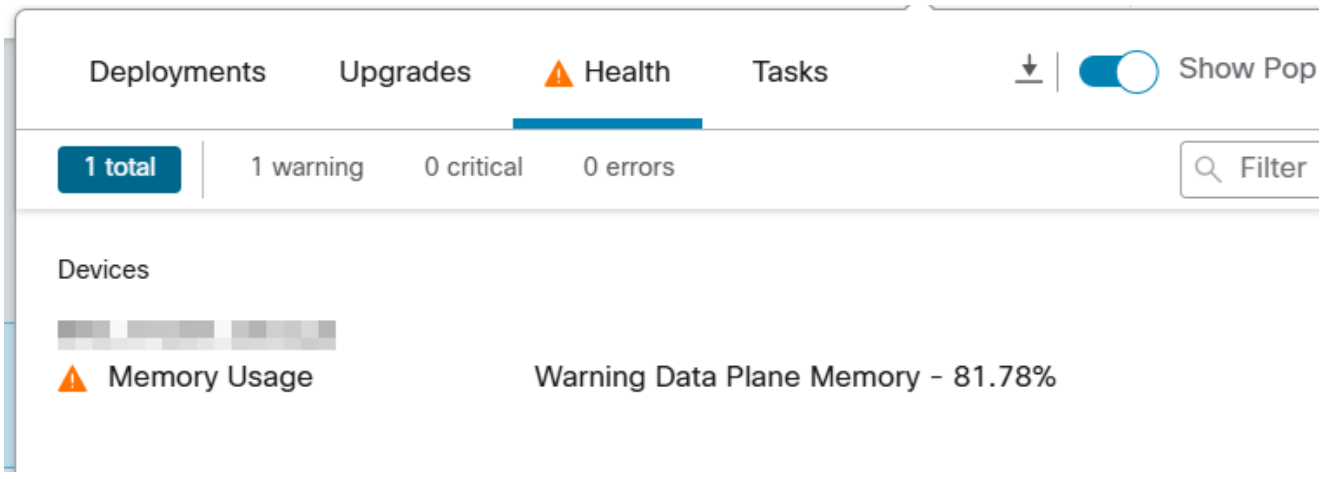
Inhalt

Problem

FTD zeigt anhaltende hohe Warnungen bei der Auslastung des Datenebenenspeichers von mehr als 80 %. Die Speichernutzung bleibt auf diesem erhöhten Niveau, nachdem Richtlinien bereitgestellt wurden, die die Anzahl der Zugriffslistenelemente deutlich erhöht haben, um mehr als die Plattform aufnehmen kann.

In FTD-Hochverfügbarkeitskonfigurationen betrifft das Problem beide Geräte, zeigt jedoch eine höhere Speichernutzung auf dem aktiven FTD an.

- FMC-Warnungen zeigen hohe Speichernutzung auf Datenebene für FTD:



- Die FTD-CLI bestätigt auch eine hohe Speichernutzung:

<#root>

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

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

- Die Anzahl der Zugriffslistenelemente zeigt 1 Million oder mehr Elemente in der FTD-CLI an:

  <#root>

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

  Total number of access-list elements: 3223691
  ```

- In den FMC-Diagnosediagrammen für die FTD ist ein starker Anstieg des Arbeitsspeichers zu verzeichnen, der mit ACE-Bereitstellungen korreliert:



- Bei einem Hochverfügbarkeits-Peer-FTD kann die Speichernutzung aufgrund von nicht gelöschtem Speicher auf hohem Niveau hängen bleiben:

  <#root>

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

  Used memory:        11058725992 bytes (77%)


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

Umwelt

- Cisco FirePOWER 2130 Threat Defense in hochverfügbarer Konfiguration
- FTD-Softwareversion: 7.4.2
- FMC-Softwareversion: 7.6.2
- Hohe Anzahl von Zugriffslistenelementen liegt bei etwa 1 Million oder mehr

Auflösung

1. Starten Sie in FTD-Hochverfügbarkeitskonfigurationen den Peer-FTD während eines vorab geplanten Zeitraums neu, um die zuvor angesammelten Speicher zu löschen.

2. Überprüfen Sie nach dem Neustart Folgendes:

- Die Peer-FTD führt eine ordnungsgemäße Neusynchronisierung mit dem Hochverfügbarkeitspaar durch.
- Die Speichernutzung zeigt normale Pegelstände an.
- Die FTD-Speicherwarnung wird von der FMC-Benutzeroberfläche gelöscht.

3. Navigieren Sie zu Geräte > Geräteverwaltung, und klicken Sie für das FTD auf das Symbol Bearbeiten.

4. Klicken Sie auf die Registerkarte Gerät oben links (Registerkarte Übersicht für FTD HA), scrollen Sie nach unten zum Abschnitt Erweiterte Einstellungen, und klicken Sie dann auf das Symbol Bearbeiten.

5. Aktivieren Sie das Kontrollkästchen Objektgruppensuche, um dieses Feature zu aktivieren, und klicken Sie auf Speichern.

6. Stellen Sie die Konfigurationsänderungen am FTD HA-Paar bereit, und überwachen Sie den Health Monitor einige Minuten, um die Änderungen der Speichernutzung zu beobachten.

<#root>

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

Used memory:        7388823784 bytes (52%)


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

Zusätzliche Überlegungen

Wenn die Speichernutzung auch nach Aktivierung der Objektgruppensuche zu einem nachhaltigen Problem für die Leistung wird, sollten Sie Optimierungsstrategien in Betracht ziehen, wie z. B.:

- Überprüfen der Regeln für die maximale Trefferanzahl mithilfe von FMC-Verbindungsereignissen
- Reduzierung unnötiger Prüfungen für vertrauenswürdigen Datenverkehr mit hohem Volumen.
- Bewertung, ob alle Regeln eine Intrusion Inspection erfordern.
- Plattformaktualisierung auf Firepower-Plattformen mit höherer Kapazität (FPR4K- oder FPR9K-Serie) in Erwägung gezogen.

Ursache

Die hohe Auslastung des Datenebenenspeichers wird durch eine Kombination aus beibehaltenem Speicher auf dem FTD und einem erhöhten Verarbeitungsaufwand für Zugriffslistenelemente nach der Bereitstellung von Richtlinien verursacht. Eine signifikante Anzahl von Zugriffslistenelementen korreliert direkt mit den Spitzenwerten der Speichernutzung. Erheblich gestiegene Anforderungen an die ACL-Verarbeitung ohne Optimierung der Objektgruppensuche tragen zu einer dauerhaft hohen Speichernutzung bei.

Verwandte Inhalte

- Berechnen der Anzahl von Access List-Elementen (ACE) mithilfe der FMC-CLI
- Konfigurationsanleitung für Cisco Secure Firewall Management Center-Geräte, 7.4: Best Practices für Zugriffskontrollregeln
- Konfigurationsanleitung für Cisco Secure Firewall Management Center-Geräte, 7.4: Objektgruppensuche konfigurieren
- Befehlsreferenz für Firepower Threat Defense
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.