Veilige firewall FTD met hoog geheugen vanwege het hoge aantal toegangselementen

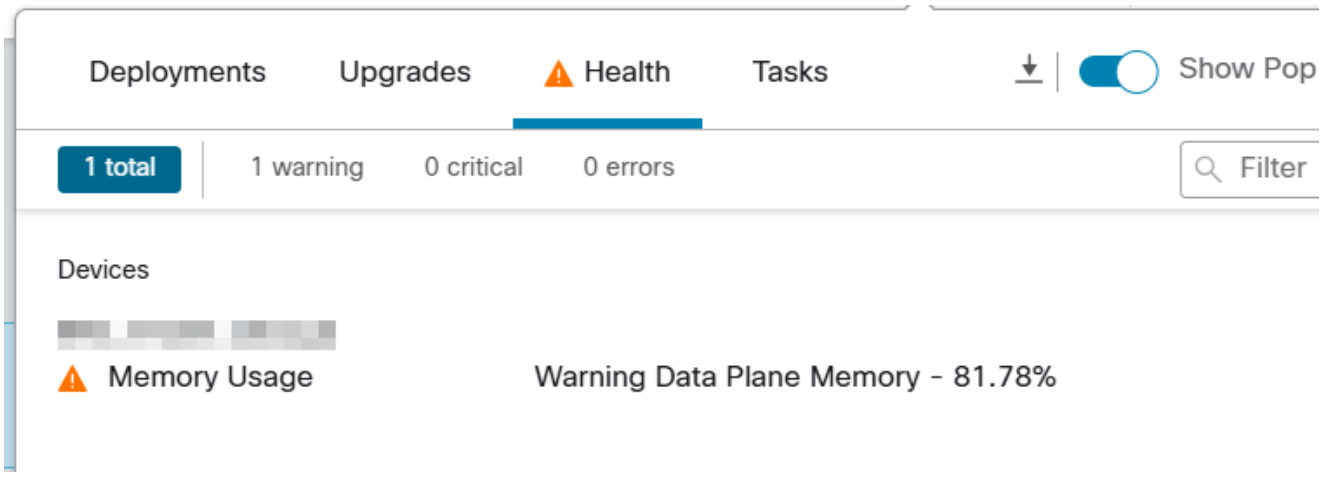
Inhoud

uitgifte

FTD toont aanhoudende hoge waarschuwingen voor het gebruik van het gegevensvlakgeheugen van meer dan 80%. Het geheugengebruik blijft op dit verhoogde niveau na beleidsimplementaties die het aantal toegangselementen aanzienlijk hebben verhoogd met meer dan wat het platform kan accommoderen.

In FTD-configuraties met hoge beschikbaarheid heeft het probleem gevolgen voor beide eenheden, maar toont het een hoger geheugengebruik op de actieve FTD.

- FMC-waarschuwingen tonen een hoog geheugengebruik op het gegevensvlak voor de FTD:



- De FTD CLI bevestigt ook een hoog geheugengebruik:

<#root>

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

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

- Het aantal elementen in de toegangslijst toont 1 miljoen of meer elementen in de FTD-CLI:

<#root>

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

Total number of access-list elements: 3223691

- In de FMC Health monitoring grafieken voor de FTD, is er een sterke toename van het geheugen correleert met ACE-implementaties:



- Op een peer FTD met hoge beschikbaarheid kan het geheugengebruik op een hoog niveau vastlopen vanwege ongewist geheugen:

<#root>

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

Used memory: 11058725992 bytes (77%)

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

milieu

- Cisco Firepower 2130 Threat Defense in configuratie met hoge beschikbaarheid
- FTD-softwareversie: 7.4.2
- FMC-softwareversie: 7.6.2
- Hoogwaardige toegangslijst telt bijna 1 miljoen of meer

resolutie

1. Start in FTD-configuraties met hoge beschikbaarheid de peer-FTD opnieuw op tijdens een vooraf geplande tijd om bewaarde geheugenopslagplaatsen te wissen die zich eerder hadden kunnen ophopen.

2. Controleer na het opnieuw opstarten of:

- De peer FTD synchroniseert correct opnieuw in het High Availability-paar.
- Het geheugengebruik vertoont normale niveaus.
- De FTD-geheugenwaarschuwing wordt gewist uit de FMC-gebruikersinterface.

3. Navigeer naar Apparaten > Apparaatbeheer en klik op het pictogram Bewerken voor de FTD.

4. Klik op het tabblad Apparaat linksboven (Overzicht tabblad voor FTD HA) en scroll omlaag naar de sectie Geavanceerde instellingen en klik vervolgens op het pictogram Bewerken.

5. Schakel het selectievakje voor Objectgroep zoeken in om deze functie in te schakelen en klik op Opslaan.

6. Implementeer de configuratiewijzigingen in het FTD HA-paar en bewaak de gezondheidsmonitor gedurende enkele minuten om veranderingen in het geheugengebruik te observeren.

<#root>

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

Used memory:        7388823784 bytes (52%)


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

Aanvullende overwegingen

Als geheugengebruik een blijvend prestatieprobleem wordt, zelfs na het inschakelen van Object Group Search, overweeg dan optimalisatiestrategieën zoals:

- Regels voor het tellen van de hoogste treffers bekijken met FMC Connection Events.
- Vermindering van onnodige inspectie van hoogvolume, vertrouwd verkeer.
- Evalueren of alle regels inbraakcontrole vereisen.
- Overweeg een platformupgrade naar Firepower-platforms met een hogere capaciteit (FPR4K- of FPR9K-reeks).

Oorzaak

Het hoge gebruik van het gegevensvlakgeheugen wordt veroorzaakt door een combinatie van het bewaarde geheugen op de FTD en een verhoogde overhead van de verwerking van elementen van de toegangslijst na beleidsimplementaties. Significante tellingen van toegangslijst-elementen correleren rechtstreeks met de pieken in het geheugengebruik. Dramatisch verhoogde ACL-verwerkingsvereisten zonder optimalisatie van objectgroep zoeken dragen bij aan duurzaam hoog geheugengebruik.

Gerelateerde inhoud

- Het aantal Access List Element (ACE) berekenen met behulp van FMC CLI
- Cisco Secure Firewall Management Center Device Configuration Guide, 7.4: Best practices

voor toegangscontroleregels

- Cisco Secure Firewall Management Center Device Configuration Guide, 7.4: Zoekopdracht in objectgroep configureren
- Command Reference voor Firepower Threat Defense
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.