Mémoire élevée FTD du pare-feu sécurisé en raison du nombre élevé d'éléments de la liste d'accès

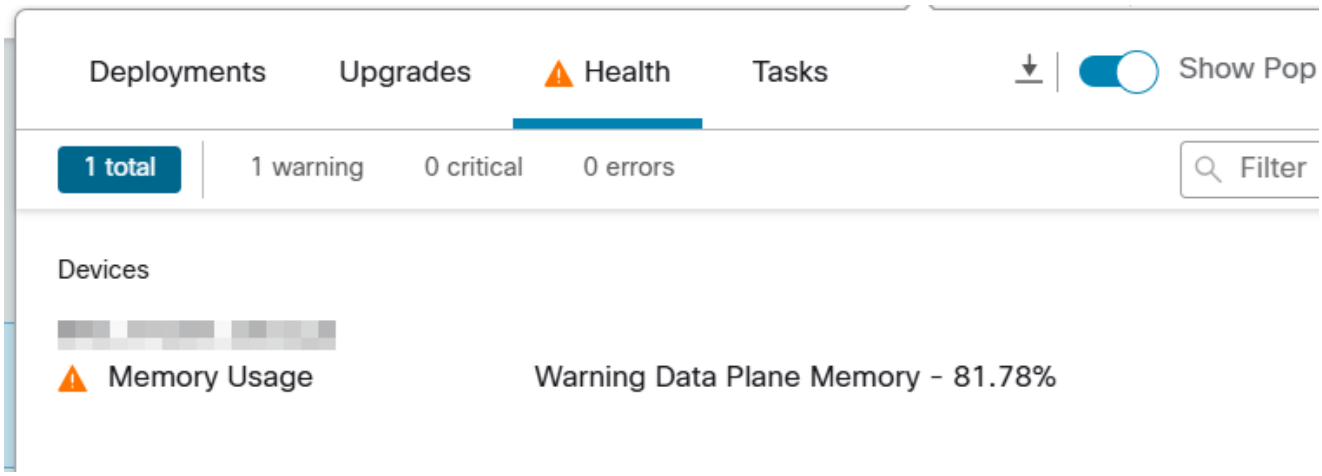
Table des matières

Problème

FTD indique des alertes persistantes d'utilisation élevée de la mémoire du plan de données de plus de 80 %. L'utilisation de la mémoire reste à ce niveau élevé après les déploiements de politiques qui ont considérablement augmenté le nombre d'éléments de liste d'accès par rapport à ce que la plate-forme peut accueillir.

Dans les configurations FTD High Availability, le problème affecte les deux unités, mais indique une utilisation de la mémoire plus élevée sur le FTD actif.

- Les alertes FMC indiquent une utilisation élevée de la mémoire sur le plan de données pour le FTD :



- L'interface de ligne de commande FTD confirme également une utilisation élevée de la mémoire :

<#root>

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

```
Used memory:       11746269504 bytes (82%)

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

- Le nombre d'éléments de la liste d'accès affiche 1 million d'éléments ou plus dans l'interface de ligne de commande FTD :

<#root>

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

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

- Dans les graphiques de surveillance de l'état de santé FMC pour le FTD, il y a une forte augmentation de la mémoire corrélée avec les déploiements ACE :



- Sur un FTD homologue à haute disponibilité, l'utilisation de la mémoire peut rester bloquée à un niveau élevé en raison d'une mémoire non effacée :

<#root>

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

Used memory:       11058725992 bytes (77%)

-------------      ------------------
```

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

Environnement

- Cisco Firepower 2130 - Défense contre les menaces dans une configuration haute disponibilité
- Version du logiciel FTD : 7.4.2
- Version du logiciel FMC : 7.6.2
- Les éléments de liste d’accès élevés comptent pour près d’un million ou plus

Résolution

1. Dans les configurations de haute disponibilité FTD, redémarrez le FTD homologue pendant une période préplanifiée pour effacer les magasins de mémoire conservés qui auraient pu s'être accumulés auparavant.

2. Après le redémarrage, vérifiez que :

- Le FTD homologue se resynchronise correctement dans la paire haute disponibilité.
- L'utilisation de la mémoire affiche des niveaux normaux.
- L'alerte de mémoire FTD disparaît de l'interface utilisateur FMC.

3. Accédez à Périphériques > Gestion des périphériques et cliquez sur l'icône Edit pour le FTD.

4. Cliquez sur l'onglet Device en haut à gauche (onglet Summary pour FTD HA) et faites défiler jusqu'à la section Advanced Settings, puis cliquez sur l'icône Edit.

5. Cochez la case Object Group Search pour activer cette fonctionnalité et cliquez sur Save.

6. Déployez les modifications de configuration sur la paire FTD HA et surveillez le moniteur d'état pendant plusieurs minutes pour observer les modifications d'utilisation de la mémoire.

<#root>

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

Used memory:        7388823784 bytes (52%)


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

Autres facteurs à considérer

Si l'utilisation de la mémoire devient un problème de performances permanent même après l'activation de la recherche de groupe d'objets, envisagez des stratégies d'optimisation telles que :

- Examen des principales règles de comptage des occurrences à l'aide des événements de connexion FMC.
- Réduction des inspections inutiles sur le trafic fiable à volume élevé.
- Évaluer si toutes les règles nécessitent une inspection des intrusions.
- Envisager une mise à niveau de la plate-forme vers des plates-formes Firepower de capacité supérieure (séries FPR4K ou FPR9K).

Motif

L'utilisation élevée de la mémoire du plan de données est due à une combinaison de mémoire conservée sur le FTD et d'une surcharge accrue du traitement des éléments de liste d'accès après les déploiements de politiques. Le nombre significatif d'éléments de liste d'accès est directement corrélé avec les pics d'utilisation de la mémoire. Des exigences de traitement ACL considérablement accrues sans optimisation de la recherche de groupe d'objets contribuent à une utilisation élevée et durable de la mémoire.

Autres informations utiles

- Calculer le nombre d'éléments de liste d'accès à l'aide de FMC CLI
- Guide de configuration des périphériques Cisco Secure Firewall Management Center, 7.4 : Meilleures pratiques pour les règles de contrôle d'accès
- Guide de configuration des périphériques Cisco Secure Firewall Management Center, 7.4 : Configurer la recherche de groupes d'objets
- Référence des commandes Firepower Threat Defense
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.