Memoria FTD firewall sicura con alta capacità a causa di un numero elevato di elementi dell'elenco degli accessi

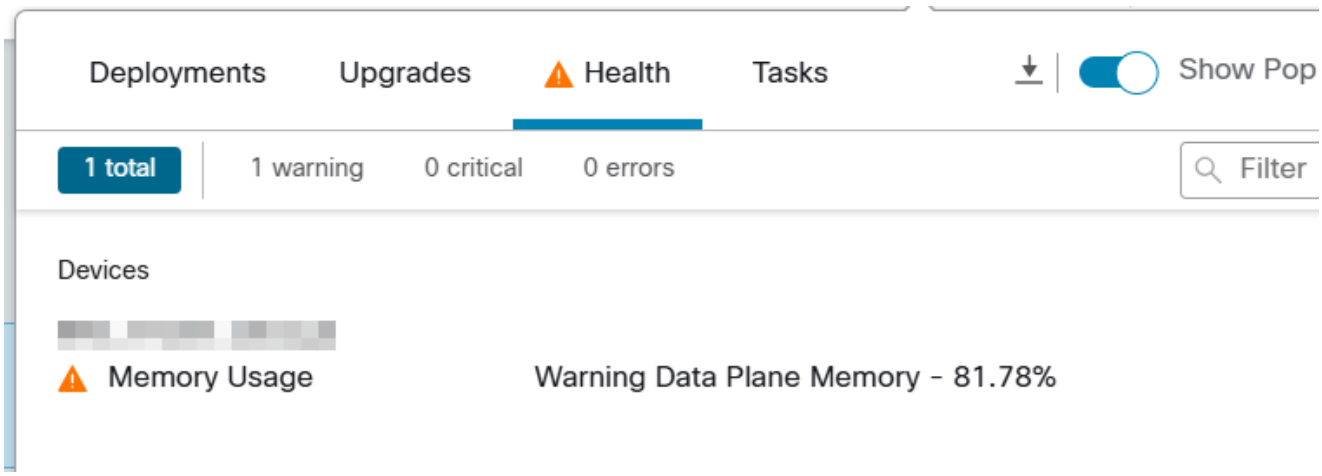
Sommario

Problema

FTD mostra un livello di utilizzo della memoria del piano dati elevato e persistente superiore all'80%. L'utilizzo della memoria rimane a questo livello elevato dopo le distribuzioni di policy che hanno aumentato in modo significativo il numero di elementi dell'elenco degli accessi di più di quanto la piattaforma possa supportare.

Nelle configurazioni ad alta disponibilità FTD, il problema influisce su entrambe le unità, ma mostra un maggiore utilizzo della memoria nell'FTD attivo.

- Gli allarmi FMC indicano un elevato utilizzo di memoria su Data Plane per FTD:



- Anche la CLI FTD conferma un elevato utilizzo della memoria:

<#root>

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

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

- Il conteggio degli elementi dell'elenco degli accessi mostra 1 milione o più elementi nella CLI FTD:

<#root>

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

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

- Nei grafici di monitoraggio dello stato FMC per FTD, c'è un forte aumento della memoria correlata alle installazioni ACE:



- In un FTD peer ad alta disponibilità, l'utilizzo della memoria può bloccarsi a un livello elevato a causa della memoria non cancellata:

<#root>

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

Used memory:       11058725992 bytes (77%)


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

Ambiente

- Cisco Firepower 2130 Threat Defense nella configurazione ad alta disponibilità
- Versione software FTD: 7.4.2
- Versione software FMC: 7.6.2
- Numero di elementi con elenco accessi elevato vicino a 1 milione o più

Risoluzione

1. Nelle configurazioni ad alta disponibilità FTD, riavviare l'FTD peer durante un tempo prepianificato per cancellare gli archivi di memoria conservati che avrebbero potuto essere accumulati in precedenza.

2. Dopo il riavvio, verificare che:

- L'FTD peer viene risincronizzato correttamente nella coppia Alta disponibilità.
- L'utilizzo della memoria mostra i livelli normali.
- L'avviso di memoria FTD viene cancellato dall'interfaccia utente di FMC.

3. Passare a Dispositivi > Gestione dispositivi e fare clic sull'icona Modifica per FTD.

4. Fare clic sulla scheda Device in alto a sinistra (scheda Summary per FTD HA) e scorrere verso il basso fino alla sezione Advanced Settings, quindi fare clic sull'icona Edit.

5. Selezionare la casella Ricerca gruppo di oggetti per abilitare questa funzione e fare clic su Salva.

6. Distribuire le modifiche della configurazione alla coppia FTD HA e monitorare lo stato del monitoraggio per alcuni minuti per osservare le modifiche dell'utilizzo della memoria.

<#root>

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

Used memory:        7388823784 bytes (52%)


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

Ulteriori considerazioni

Se l'utilizzo della memoria rappresenta un problema di prestazioni anche dopo l'abilitazione della ricerca del gruppo di oggetti, prendere in considerazione strategie di ottimizzazione quali:

- Esame delle prime regole di conteggio delle corrispondenze mediante gli eventi di connessione di FMC.
- Riduzione delle ispezioni non necessarie su volumi elevati di traffico affidabile.
- Valutare se tutte le regole richiedono l'ispezione delle intrusioni.
- È in considerazione l'upgrade della piattaforma a piattaforme Firepower di capacità superiore (serie FPR4K o FPR9K).

Causa

L'elevato utilizzo della memoria del piano dati è causato da una combinazione di memoria conservata sull'FTD e da un maggiore sovraccarico di elaborazione degli elementi dell'elenco degli accessi dopo le distribuzioni delle policy. I conteggi degli elementi dell'elenco accessi significativi sono correlati direttamente ai picchi di utilizzo della memoria. L'aumento significativo dei requisiti di elaborazione degli ACL senza l'ottimizzazione della ricerca del gruppo di oggetti contribuisce a un utilizzo elevato e costante della memoria.

Contenuto correlato

- Calcola il numero di elementi ACE (Access List Element) tramite CLI di FMC
- Guida alla configurazione dei dispositivi di Cisco Secure Firewall Management Center, 7.4: Procedure ottimali per le regole di controllo di accesso
- Guida alla configurazione dei dispositivi di Cisco Secure Firewall Management Center, 7.4: Configura ricerca gruppo di oggetti
- Guida di riferimento ai comandi per Firepower Threat Defense
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).