Memória Alta de FTD de Firewall Seguro Devido à Contagem Alta de Elementos da Lista de Acesso

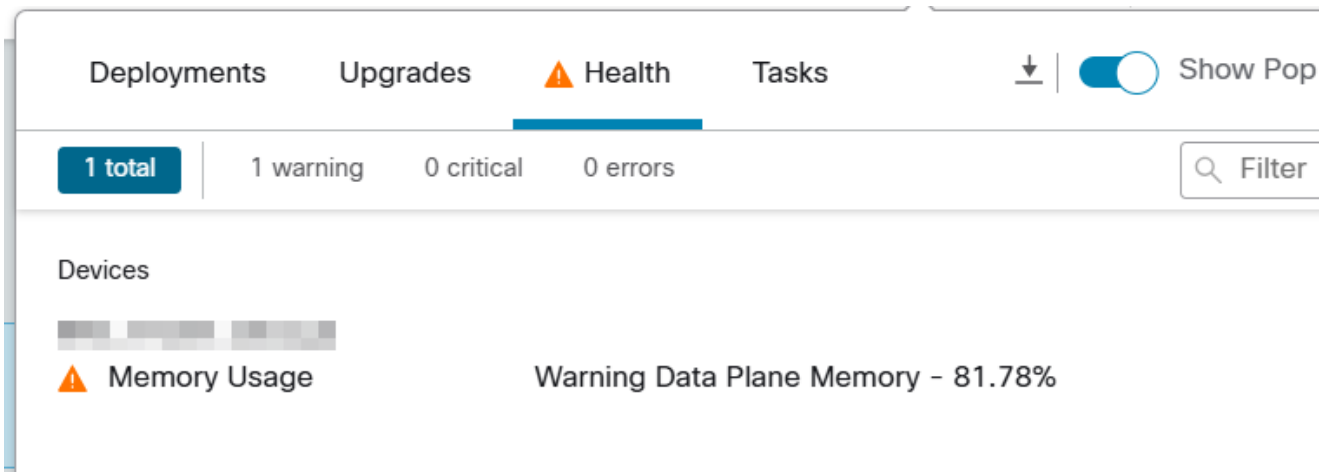
Contents

Problema

O FTD mostra alertas de utilização de memória de plano de dados alto persistentes de mais de 80%. A utilização de memória permanece nesse nível elevado após as implantações de política que aumentaram significativamente as contagens de elementos da lista de acesso em mais do que a plataforma pode acomodar.

Em configurações de alta disponibilidade de FTD, o problema afeta ambas as unidades, mas mostra maior uso de memória no FTD ativo.

- Os alertas do FMC mostram alto uso de memória no plano de dados para o FTD:



- A CLI do FTD também confirma o alto uso de memória:

<#root>

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

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

- A contagem de elementos da lista de acesso mostra 1 milhão ou mais de elementos na CLI de FTD:

<#root>

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

Total number of access-list elements: 3223691

- Nos gráficos de monitorização da saúde do FMC para o FTD, verifica-se um aumento acentuado da memória em correlação com as implantações de ACE:



- Em um FTD de peer de alta disponibilidade, o uso da memória pode ficar preso em um nível alto devido à memória não limpa:

<#root>

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

Used memory: 11058725992 bytes (77%)

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

Ambiente

- Defesa contra ameaças do Cisco Firepower 2130 em configuração de alta disponibilidade
- Versão do software FTD: 7.4.2
- Versão do software FMC: 7.6.2
- Contagens de elementos de listas de acesso altas perto de 1 milhão ou mais

Resolução

1. Em configurações de Alta Disponibilidade de FTD, reinicialize o FTD par durante um tempo pré-planejado para limpar os armazenamentos de memória retida que poderiam ter sido acumulados anteriormente.

2. Após a reinicialização, verifique se:

- O FTD par ressincroniza corretamente no par de alta disponibilidade.
- A utilização de memória mostra níveis normais.
- O alerta de memória FTD é apagado da interface do usuário do FMC.

3. Navegue até Devices > Device Management e clique no ícone Edit do FTD.

4. Clique na guia Dispositivo perto do canto superior esquerdo (guia Resumo para HA FTD) e role para baixo até a seção Configurações avançadas e clique no ícone Editar.

5. Marque a caixa de Pesquisa de Grupo de Objetos para ativar esse recurso e clique em Salvar.

6. Implante as alterações de configuração no par FTD HA e monitore o monitor de integridade por vários minutos para observar as alterações de uso de memória.

<#root>

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

Used memory:        7388823784 bytes (52%)


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

Outras considerações

Se a utilização de memória se tornar uma preocupação de desempenho sustentada mesmo após a habilitação da Pesquisa de Grupo de Objetos, considere estratégias de otimização como:

- Revisão das principais regras de contagem de ocorrências usando os eventos de conexão do FMC.
- Redução de inspeção desnecessária em tráfego confiável de alto volume.
- Avaliar se todas as regras exigem inspeção de intrusão.
- Considerar a atualização da plataforma para plataformas Firepower de maior capacidade (séries FPR4K ou FPR9K).

Causa

A alta utilização da Memória do Plano de Dados é causada por uma combinação de memória retida no FTD e sobrecarga de processamento de elemento de lista de acesso aumentada após as implantações de política. As contagens significativas de elementos da lista de acesso estão diretamente correlacionadas aos picos de utilização de memória. Os requisitos de processamento de ACL drasticamente aumentados sem a otimização da pesquisa de grupo de objetos contribuem para o uso sustentado de alta memória.

Conteúdo relacionado

- Calcule a contagem de elementos da lista de acesso (ACE) usando a CLI do FMC

- Guia de configuração de dispositivos do Cisco Secure Firewall Management Center, 7.4: Práticas recomendadas para regras de controle de acesso
- Guia de configuração de dispositivos do Cisco Secure Firewall Management Center, 7.4: Configurar Pesquisa de Grupo de Objetos
- Referência de comandos do Firepower Threat Defense
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.