Firewall seguro FTD memoria alta debido al alto recuento de elementos de la lista de acceso

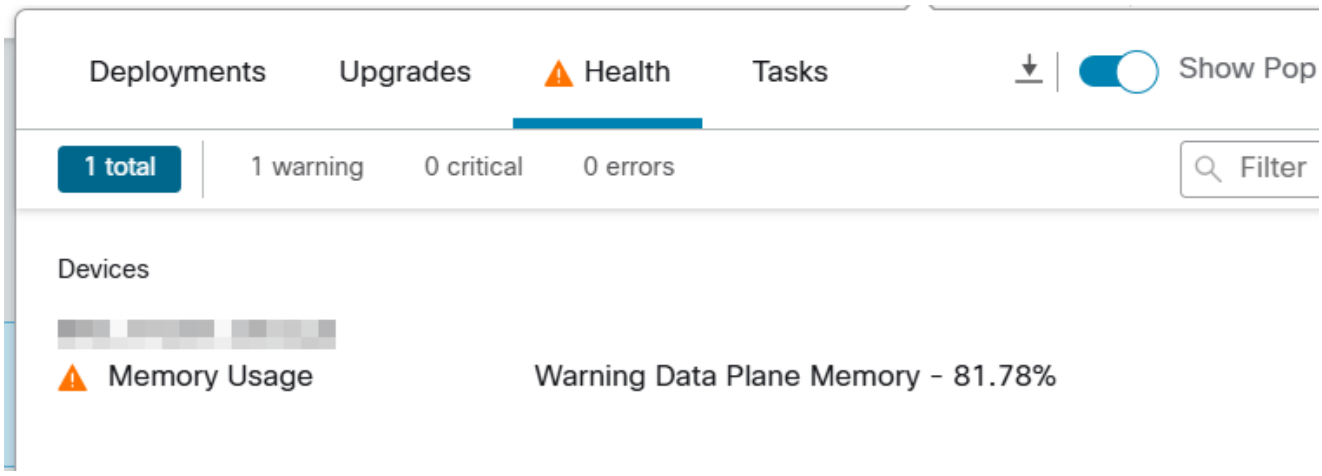
Contenido

Problema

El FTD muestra alertas persistentes de uso elevado de la memoria del plano de datos de más del 80%. La utilización de la memoria permanece en este nivel elevado después de las implementaciones de políticas que aumentaron significativamente los recuentos de elementos de listas de acceso en más de lo que puede admitir la plataforma.

En las configuraciones de alta disponibilidad de FTD, el problema afecta a ambas unidades, pero muestra un mayor uso de memoria en el FTD activo.

- Las alertas de FMC muestran un uso elevado de la memoria en el plano de datos para el FTD:



- La CLI de FTD también confirma un uso elevado de la memoria:

<#root>

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

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

- El recuento de elementos de la lista de acceso muestra 1 millón o más elementos en la CLI de FTD:

<#root>

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

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

- En los gráficos de supervisión de estado de FMC para el FTD, hay un aumento pronunciado de la memoria que se correlaciona con las implementaciones ACE:



- En un FTD de par de alta disponibilidad, el uso de memoria puede atascarse en un nivel alto debido a la memoria no borrada:

<#root>

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

Used memory:       11058725992 bytes (77%)


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

Entorno

- Cisco Firepower 2130 Threat Defense en configuración de alta disponibilidad
- Versión del software FTD: 7.4.2
- Versión del software FMC: 7.6.2
- Un elevado número de elementos de la lista de acceso se acerca a 1 millón o más

Resolución

1. En las configuraciones de alta disponibilidad de FTD, reinicie el FTD de peer durante un tiempo planificado previamente para borrar los almacenes de memoria retenida que podrían haberse acumulado previamente.

2. Después del reinicio, verifique que:

- El FTD de peer se vuelve a sincronizar correctamente en el par de alta disponibilidad.
- La utilización de la memoria muestra niveles normales.
- La alerta de memoria FTD se borra de la interfaz de usuario de FMC.

3. Navegue hasta Devices > Device Management y haga clic en el icono Edit para el FTD.

4. Haga clic en la pestaña Device cerca de la parte superior izquierda (pestaña Summary para FTD HA) y desplácese hacia abajo hasta la sección Advanced Settings, luego haga clic en el icono Edit.

5. Active la casilla de Búsqueda de Grupos de Objetos para activar esta función y haga clic en Guardar.

6. Implemente los cambios de configuración en el par FTD HA y supervise el monitor de estado durante varios minutos para observar los cambios de uso de memoria.

<#root>

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

Used memory:        7388823784 bytes (52%)


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

Consideraciones adicionales

Si la utilización de la memoria se convierte en un problema de rendimiento continuo incluso después de habilitar la búsqueda de grupos de objetos, considere estrategias de optimización como:

- Revisión de las principales reglas de recuento de visitas mediante los eventos de conexión FMC.
- Reducción de la inspección innecesaria en tráfico de confianza y de gran volumen.
- Evaluar si todas las reglas requieren inspección de intrusiones.
- Se está planteando actualizar la plataforma a plataformas Firepower de mayor capacidad (series FPR4K o FPR9K).

Causa

La elevada utilización de la memoria del plano de datos se debe a una combinación de memoria retenida en el FTD y a una mayor sobrecarga de procesamiento de elementos de lista de acceso después de las implementaciones de políticas. Los recuentos significativos de elementos de la lista de acceso se correlacionan directamente con los picos de utilización de memoria. Los requisitos de procesamiento de ACL significativamente mayores sin la optimización de Búsqueda de grupos de objetos contribuyen a un uso elevado y sostenido de la memoria.

Contenido relacionado

- Calcular el recuento de elementos de lista de acceso (ACE) mediante CLI de FMC
- Guía de configuración de dispositivos de Cisco Secure Firewall Management Center, 7.4: Prácticas recomendadas para las reglas de control de acceso
- Guía de configuración de dispositivos de Cisco Secure Firewall Management Center, 7.4: Configurar búsqueda de grupos de objetos
- Referencia de comandos para Firepower Threat Defence
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).