安全防火墙FTD高内存（由于高访问列表元素计数）

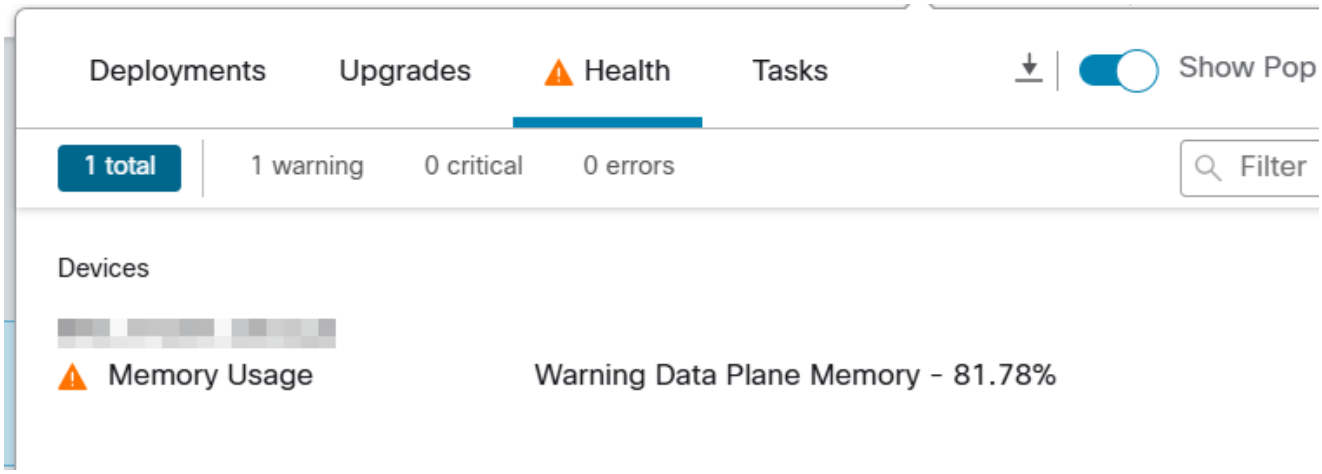
目录

问题

FTD显示超过80%的持续高数据平面内存利用率警报。在策略部署后，内存利用率仍保持在这一较高水平，因为策略部署显着增加了访问列表元素数量，数量超过平台可以容纳的数量。

在FTD高可用性配置中，此问题影响两台设备，但显示活动FTD上的内存使用率较高。

- FMC警报显示FTD的数据平面上的高内存使用率：



- FTD CLI还确认高内存使用率：

```
<#root>

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

Used memory:       11746269504 bytes (82%)


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

- access-list元素计数在FTD CLI中显示100万个或更多元素：

  <#root>

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

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

- 在FTD的FMC运行状况监控图中，与ACE部署相关的内存急剧增加：



- 在高可用性对等FTD上，内存使用可能会由于未清除内存而停滞在高水平上：

  <#root>

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

  Used memory:       11058725992 bytes (77%)


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

环境

- Cisco Firepower 2130威胁防御高可用性配置
- FTD软件版本：7.4.2
- FMC软件版本：7.6.2
- 高访问列表元素数量接近一百万或更多

分辨率

1.在FTD高可用性配置中，在预定时间内重新启动对等FTD，以清除以前可能已累积的保留内存存储。

2.重新启动后，请验证：

- 对等FTD正确重新同步到高可用性对。
- 内存利用率显示正常水平。
- FTD内存警报从FMC UI清除。

3.导航到设备>设备管理，然后点击FTD的编辑图标。

4.点击左上角附近的Device选项卡（FTD HA的Summary选项卡），向下滚动到Advanced Settings部分，然后单击Edit图标。

5.选中对象组搜索复选框以启用此功能，然后单击保存。

6.将配置更改部署到FTD HA对并监控运行状况监控器几分钟，以观察内存使用情况的更改。

<#root>

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

Used memory:        7388823784 bytes (52%)


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

其他注意事项

如果即使启用对象组搜索后，内存利用率也会成为持续的性能问题，请考虑以下优化策略：

- 使用FMC连接事件检查排名靠前的命中计数规则。
- 减少对大量受信任流量进行不必要的检查。
- 评估是否所有规则都需要入侵检测。
- 考虑升级到更高容量的Firepower平台（FPR4K或FPR9K系列）。

原因

高数据平面内存利用率是由于FTD上的保留内存和策略部署后增加的访问列表元素处理开销造成的。重要访问列表元素计数与内存利用率峰值直接相关。在不使用对象组搜索优化的情况下，显着增加的ACL处理要求有助于保持较高的内存使用率。

相关内容

- 使用FMC CLI计算访问列表元素(ACE)计数
- 思科安全防火墙管理中心设备配置指南7.4:访问控制规则的最佳实践
- 思科安全防火墙管理中心设备配置指南7.4:配置对象组搜索
- Firepower威胁防御的命令参考
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。