安全防火墙FTD部署失败

问题

在思科防火墙Firepower威胁防御(FTD)中观察到网络中断和停机。 重复发生的事件导致流量被拒绝，包括SNMP通信，并且需要重新启动设备并进行持续监控，以确定根本原因并降低进一步的影响。

环境

- 思科安全防火墙Firepower 1140设备（影响任何FTD型号）
- FTD软件版本：7.4.2.4（其他版本也受到影响）
- 基于对象的动态访问控制策略(ACP)
- 频繁的策略部署

分辨率

要解决思科安全防火墙FTD设备上反复出现的故障转移和策略部署问题，必须遵循一套全面的故障排除和补救步骤。所列的工作流程经过结构化处理，可提供每个步骤的明确分离和说明，包括监控、数据收集、诊断和升级指导。

1：使用数据包跟踪器检查路由和访问预期流量。

```
firepower# packet-tracer input INPUTNAMEIF tcp SRCIP 54321 DSTIP 443
firepower# packet-tracer input INPUTNAMEIF icmp SRCIP 8 0 DSTIP
```

2：使用FTD上的捕获来确定在条目“按配置的规则”丢弃数据包时是否丢弃数据包，即使该流量存在有效的规则和路由。

```
firepower# capture 1 interface INPUTIFNAME trace detail trace-count 1000 match ip host SRCIP host DSTIP
firepower# capture x type asp-drop all match ip host SRCIP host DSTIP
firepower# show capture
capture 1 type raw-data trace detail trace-count 1000 interface inside [Capturing - 31565 bytes]
  match ip 10.1.1.0 255.255.255.0 any
capture x type asp-drop all [Capturing - 31565 bytes]
  match ip 10.1.1.0 255.255.255.0 any
```

3：检查FTD消息日志以查找缺陷CSCwo78475的证据。

```
> expert
admin@FTD-1:~$ sudo su
Password:
root@FTD-1:/Volume/home/admin# cat /ngfw/var/log/messages | grep -E "New inspector|did not finish|swapp
Feb 10 18:35:03 FTD-device SF-IMS[28366]: New inspector is not initializing Identity API because it's a
Feb 10 18:35:03 FTD-device SF-IMS[28366]: New inspector has different policy groups or ABP name to ID ma
Feb 10 18:35:10 FTD-device SF-IMS[28366]: Reading the muster data snapshot did not finish in time: 4 se
Feb 10 18:36:22 FTD-device SF-IMS[28366]: Identity API state swapped
```

4：将这些日志的时间戳与FTD中部署日志的时间戳进行匹配。

```
Feb 10 18:34:45 FTD-device policy_apply.pl[18923]: INFO  Deployment type is NORMAL_DEPLOYMENT and devic
Feb 10 18:37:03 FTD-device policy_apply.pl[30894]: INFO  finalizeDeviceDeployment - sandbox = /var/cisc
```

5：如果FTD处于HA状态，请故障转移至备用FTD，然后检查该状态以确保流量恢复。

6：如果在FTD中找到匹配的日志和条件，设备会受到缺陷的影响，可以升级到7.4.3。同时，部署可以限制为非工作时间，以减少流量影响。

原因

观察到的流量影响和策略部署问题的根本原因是影响FTD软件的已知缺陷，特别是：

- Cisco Bug ID CSCwo78475：在具有动态对象的FTD设备上进行策略部署时，流量会遇到不正确的访问控制策略(ACP)规则。这可能会导致合法流量被拒绝，即使运行配置中存在正确的规则也是如此。已在版本7.4.3中修复。

相关内容

- 思科漏洞ID CSCwo78475:在带有动态对象的FTD上的策略部署期间，流量遇到不正确的ACP规则
- 思科技术支持和下载: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）。