安全防火牆FTD部署失敗

問題

在思科防火牆Firepower威脅防禦(FTD)上觀察到網路中斷和停機。 重複發生的事件導致拒絕流量（包括SNMP通訊），並需要重新啟動裝置和持續監控，以確定根本原因並降低進一步的影響。

環境

- Cisco Secure Firewall Firepower 1140裝置（影響任何FTD型號）
- FTD軟體版本：7.4.2.4（其他版本也受到影響）
- 動態的基於對象的存取控制原則(ACP)
- 頻繁的策略部署

解析

要解決思科安全防火牆FTD裝置上反複出現的故障轉移和策略部署問題，必須遵循一套全面的故障排除和補救步驟。所列的工作流程經過結構化處理，可清晰地分離和解釋每個步驟，包括監控、資料收集、診斷和升級指南。

1：使用資料包跟蹤器檢查路由和訪問目標流量。

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

2：使用FTD上的擷取，可以判斷輸入「by configured rule」時是否捨棄封包，即使流量存在有效的規則和路由。

```
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：檢查FTD消息日誌以查詢缺陷CSCwo78475的證據。

```
> 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 m
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：將這些日誌的時間戳與FTD中部署日誌的時間戳相匹配。

```
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在HA中，請容錯移轉至備用FTD，稍後檢查以確保流量復原。

6：如果在FTD中找到匹配的日誌和條件，裝置會受到缺陷的影響，可以升級到7.4.3。同時，部署可以限製為下班時間，以減少流量影響。

原因

觀察到的流量影響和策略部署問題的根本原因是影響FTD軟體的已知缺陷，特別是：

- 思科錯誤ID CSCwo78475：在具有動態對象的FTD裝置上部署策略期間，流量會命中不正確的訪問控制策略(ACP)規則。這可能導致拒絕合法流量，即使運行配置中存在正確的規則也是如此。已在版本7.4.3中修復。

相關內容

- 思科錯誤ID CSCwo78475:在具有動態對象的FTD上部署策略期間，流量會遇到不正確的ACP規則
- 思科技術支援與下載:思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。