在防火牆群集環境中排除LACP埠通道故障

問題

FTD裝置上的Port-channel1顯示操作狀態為Failed（失敗），未傳送或接收LACP PDU。此裝置是FTD叢集的一部分，而Port-channel1用作資料介面，因此當port-channel關閉時，會產生流量影響。

觀察到的具體症狀包括：

- LACP鄰居資訊，顯示合作夥伴系統ID為0,0-0-0-0-0-0，埠號為0x0。
- Partner Oper Key和Port State顯示為0x0。
- LACP計數器在防火牆機箱上未遞增。
- 介面顯示「掛起（無LACP PDU）」狀態。
- 在相鄰交換機上，只有LACP傳送計數器增加。LACP Recv計數器不增加。

受影響裝置的LACP鄰居輸出顯示：

<#root>

```
device(fxos)#
```

show lacp neighbor

```
Flags:  S - Device is sending Slow LACPDUs F - Device is sending Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode
port-channel1 neighbors
Partner's information
            Partner               Partner                     Partner
Port        System ID             Port Number     Age         Flags
Eth1/2
```

0,0-0-0-0-0-0

0x0

```
             5022089     SP
            LACP Partner           Partner                     Partner
            Port Priority          Oper Key                    Port State
            0                      0x0                         0x0
Partner's information
            Partner                Partner                     Partner
Port        System ID              Port Number     Age         Flags
Eth1/3

0,0-0-0-0-0-0



0x0

            4895677     SP
            LACP Partner           Partner                     Partner
            Port Priority          Oper Key                    Port State
            0                      0x0                         0x0
```

在防火牆上，埠通道成員的LACP傳送/接收計數器不會增加：

```
<#root>

device#

connect fxos


device(fxos)#

show lacp counters


                    LACPDUs         Marker      Marker Response    LACPDUs
Port              Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
--------------------------------------------------------------------------
port-channel1
Ethernet1/4      11413   13114       0       0       0       0       0

<-- the LACP counters do not increase
```

連線埠通道介面及其子介面處於關閉/關閉狀態：

```
<#root>

#
```

show interface ip brief

```
Interface                  IP-Address      OK?           Method Status      Protocol
Internal-Control0/0        unassigned      YES           unset  up          up
Internal-Data0/0           unassigned      YES           unset  up          up
Internal-Data0/1           unassigned      YES           unset  up          up
Internal-Data0/2           169.254.1.1     YES           unset  up          up
Internal-Data0/3           unassigned      YES           unset  up          up
Internal-Data0/4           unassigned      YES           unset  down        up
Port-channel1              unassigned      YES           unset
```

down down

```
Port-channel1.90           192.0.2.15      YES           CONFIG
```

down down

```
Port-channel1.102          192.0.2.130     YES           CONFIG
```

down down

```
...
```

交換機側日誌表明交換機正在傳輸LACP但未接收合作夥伴LACP PDU，埠處於掛起狀態：

<#root>

```
Apr  2 18:44:20.614: %LINEPROTO-5-UPDOWN: Line protocol on Interface TwentyFiveGigE2/0/25, changed stat
Apr  2 18:44:25.452: %ETC-5-L3DONTBNDL2: Twe2/0/25
```

suspended

```
: LACP currently not enabled on the remote port.
Apr  2 18:44:36.318: %ETC-5-L3DONTBNDL2: Twe2/0/25
```

suspended

```
: LACP currently not enabled on the remote port.
Apr  3 02:17:06.798: %LINK-5-UPDOWN: Interface TwentyFiveGigE2/0/25, changed state to down
Apr  3 02:17:26.722: %LINK-5-UPDOWN: Interface TwentyFiveGigE2/0/25, changed state to up
Apr  3 02:17:35.915: %ETC-5-L3DONTBNDL2: Twe2/0/25 suspended: LACP currently not enabled on the remote
Apr  3 02:23:22.255: %LINK-5-UPDOWN: Interface TwentyFiveGigE2/0/25, changed state to down
Apr  3 02:23:43.886: %LINK-5-UPDOWN: Interface TwentyFiveGigE2/0/25, changed state to up
Apr  3 02:23:53.808: %ETC-5-L3DONTBNDL2: Twe2/0/25 suspended: LACP currently not enabled on the remote
```

環境

- 軟體版本:FTD 7.6.2。其他軟體版本（包括ASA）也可能會受到影響。
- 使用埠通道進行資料介面的FTD群集配置。
- 連線到上游交換機基礎設施的啟用LACP的埠通道。

解析

解決方法涉及確定受影響的FTD裝置因埠通道介面運行狀況檢查失敗而離開集群。在裝置上禁用集群時，所有資料介面都設計為關閉，從而使LACP PDU停止，並導致交換機側掛起和資料流影響。

已執行的診斷步驟

步驟 1:收集來自Cisco Firepower裝置和上游交換機的調試和支援捆綁包

從FXOS機箱收集多個故障排除存檔、LACP調試檔案、核心檔案和TS（故障排除）檔案進行分析。

步驟 2:驗證交換機行為和LACP狀態

交換機工程師確認交換機正在傳送LACP PDU，但沒有從Firepower裝置接收合作夥伴PDU。

步驟 3:分析LACP內部狀態轉換

分析表明，由於缺少夥伴PDU，介面進入暫停狀態，LACP計數器未增加。

提示：檢查「show cluster history」命令輸出和防火牆LINA系統日誌，確定群集失敗的原因。

在本示例中，裝置由於資料介面故障而退出集群：

```
<#root>

#

show cluster history

CONTROL_NODE          CONTROL_NODE          Event: Control node unit-1-1 is quitting
                                            due to interface health check
                                            failure on Port-channel1,
                                            1 times. Rejoin will be attempted
                                            after 5 min.
20:44:31 CEST Apr 2 2026
CONTROL_NODE          DISABLED              Client progression done
```

復原程式

步驟 1:在受影響的FTD裝置上重新啟用群集

```
<#root>

#

cluster enable
```

此命令使裝置重新加入群集、啟動資料介面、恢復LACP PDU並恢復Port-channel1功能。

步驟 2:檢驗LACP恢復

重新啟用集群後，LACP PDU恢復，Port-channel1在防火牆和交換機端均恢復正常運行。

原因

根本原因是導致FTD裝置離開集群的埠通道介面運行狀況檢查故障。在FTD裝置上禁用集群時，所有資料介面設計為管理性關閉，這將停止LACP PDU傳輸，並導致上游交換機掛起埠通道介面。

這種行為是意料之中的。

Cisco錯誤ID CSCwo09449已歸檔以增強產品的可維護性。

相關內容

- 思科錯誤ID CSCwo09449 - FXOS:禁用集群時，過時的TX和RX LACP計數器和掛起的資料埠通道

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）。