

Fehlerbehebung bei LACP-Port-Channel-Fehlern in einer Firewall-Cluster-Umgebung

Problem

Für Port-channel1 einer FTD-Appliance wurde der Betriebsstatus als Failed (Ausgefallen) angezeigt, und es wurden keine LACP PDUs gesendet oder empfangen. Das Gerät war Teil eines FTD-Clusters, und Port-channel1 wurde als Datenschnittstelle verwendet, was sich bei einem Ausfall des Port-Channels negativ auf den Datenverkehr auswirkte.

Zu den beobachteten spezifischen Symptomen gehören:

- Für LACP-Nachbarinformationen wird die Partnersystem-ID als 0,0-0-0-0-0-0 mit der Portnummer 0x0 angezeigt.
- Partner Oper Key und Port State werden als 0x0 angezeigt.
- LACP-Zähler werden im Firewall-Chassis nicht inkrementiert.
- Schnittstellen mit dem Status "Suspendiert (keine LACP PDU)"
- Auf dem benachbarten Switch werden nur die Zähler für gesendete LACPs erhöht. Die LACP Recv-Zähler werden nicht erhöht.

Die Ausgabe des LACP-Nachbarn vom betroffenen Gerät ergab Folgendes:

```
<#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
```

Port	Partner System ID	Partner Port Number	Age	Partner 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

Auf der Firewall werden die LACP Sent/Recv-Zähler für die Port-Channel-Mitglieder nicht erhöht:

<#root>

device#

connect fxos

device(fxos)#

show lacp counters

Port	LACPDUs		Marker		Marker Response		LACPDUs	
	Sent	Recv	Sent	Recv	Sent	Recv	Pkts	Err

port-channel1								
Ethernet1/4	11413	13114	0	0	0	0	0	0

<-- the LACP counters do not increase

Die Port-Channel-Schnittstelle und ihre Subschnittstellen befinden sich im Down-/Down-Status:

```
<#root>
```

```
#
```

```
show interface ip brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Internal-Contro10/0	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
```

```
...
```

Aus Switch-seitigen Protokollen ging hervor, dass der Switch LACP sendete, aber keine Partner-LACP-PDUs empfing, wobei die Ports ausgesetzt wurden:

```
<#root>
```

```
Apr 2 18:44:20.614: %LINEPROTO-5-UPDOWN: Line protocol on Interface TwentyFiveGigE2/0/25, changed state to
```

```
Apr 2 18:44:25.452: %ETC-5-L3DONTBNL2: Twe2/0/25
```

```
suspended
```

```
: LACP currently not enabled on the remote port.
```

```
Apr 2 18:44:36.318: %ETC-5-L3DONTBNL2: 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
```

Umwelt

- Software-Version: FTD 7.6.2. Andere Softwareversionen, einschließlich ASA, können ebenfalls betroffen sein.
- FTD-Cluster-Konfiguration mit Datenschnittstellen unter Verwendung eines Port-Channels.
- LACP-fähiger Port-Channel zur Verbindung mit der Upstream-Switch-Infrastruktur.

Auflösung

Bei der Lösung wurde festgestellt, dass die betroffene FTD-Einheit den Cluster aufgrund eines Fehlers bei der Statusprüfung der Port-Channel-Schnittstelle verlassen hatte. Wenn das Clustering auf dem Gerät deaktiviert wurde, wurden alle Datenschnittstellen vom Design her ausgeschaltet, wodurch LACP PDUs gestoppt wurden und die Switch-seitige Aussetzung und Beeinträchtigung des Datenverkehrs verursacht wurden.

Durchgeführte Diagnoseschritte

Schritt 1: Sammeln von Debug- und Support-Paketen vom Cisco FirePOWER-Gerät und vom Upstream-Switch

Mehrere Fehlerbehebungsarchive, LACP-Debugdateien, Core-Dateien und TS-Dateien (Fehlerbehebung) wurden aus dem FXOS-Chassis zur Analyse gesammelt.

Phase 2: Validierung des Switch-Verhaltens und des LACP-Status

Der Switch-Techniker bestätigte, dass der Switch LACP-PDUs sendete, aber keine Partner-PDUs vom FirePOWER-Gerät empfing.

Schritt 3: Analyse der internen LACP-Zustandsübergänge

Die Analyse zeigte, dass die Schnittstellen aufgrund fehlender Partner-PDUs in einen ausgesetzten Zustand versetzt wurden, ohne dass die LACP-Zähler inkrementiert wurden.



Tipp: Überprüfen Sie die Befehlsausgabe "show cluster history" (Clusterverlauf anzeigen) und die LINA-Syslogs der Firewall, um den Grund für den Clusterausfall zu ermitteln.

In diesem Beispiel hat das Gerät den Cluster aufgrund eines Datenschnittstellenfehlers beendet:

```
<#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
```

Wiederherstellungsverfahren

Schritt 1: Erneutes Aktivieren von Clustering auf der betroffenen FTD-Einheit

```
<#root>
```

```
#
```

```
cluster enable
```

Dieser Befehl führte dazu, dass die Einheit wieder dem Cluster beitrug, Datenschnittstellen

aktiviert, LACP PDUs wieder aufgenommen und die Port-channel1-Funktionalität wiederhergestellt wurde.

Phase 2: Überprüfung der LACP-Wiederherstellung

Nach der erneuten Aktivierung des Clustering-Vorgangs wurden die LACP PDUs wieder aufgenommen, und Port-channel1 kehrte auf Firewall- und Switch-Seite zum Normalbetrieb zurück.

Ursache

Die Ursache war ein Fehler bei der Statusprüfung der Port-Channel-Schnittstelle, der dazu führte, dass die FTD-Einheit den Cluster verließ. Wenn Clustering auf einer FTD-Einheit deaktiviert ist, werden alle Datenschnittstellen administrativ abgeschaltet, wodurch die LACP PDU-Übertragung gestoppt wird und der Upstream-Switch veranlasst wird, die Port-Channel-Schnittstellen auszusetzen.

Dieses Verhalten wird erwartet.

Cisco Bug-ID [CSCwo09449](#) wurde eingereicht, um die Benutzerfreundlichkeit des Produkts zu verbessern.

Verwandte Inhalte

- Cisco Bug-ID [CSCwo09449](#) - FXOS: Veraltete TX- und RX-LACP-Zähler und ausgesetzte Daten-Port-Channels, wenn Clustering deaktiviert ist

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.