

Dépannage d'une défaillance Port-Channel LACP dans un environnement de cluster de pare-feu

Problème

Port-channel1 sur un appareil FTD a indiqué un état opérationnel Échec, sans aucune unité de données de protocole LACP en cours d'envoi ou de réception. Le périphérique faisait partie d'un cluster FTD et Port-channel1 a été utilisé comme interface de données, ce qui a eu un impact sur le trafic lorsque le port-channel est tombé en panne.

Les symptômes spécifiques observés étaient les suivants :

- Informations sur le voisin LACP indiquant l'ID système partenaire 0,0-0-0-0-0-0 avec le numéro de port 0x0.
- Clé d'opération du partenaire et état du port indiquant 0x0.
- Les compteurs LACP n'augmentent pas sur le châssis du pare-feu.
- Interfaces affichant l'état « Suspendu (pas de PDU LACP) ».
- Sur le commutateur adjacent, seuls les compteurs LACP envoyés augmentent. Les compteurs de réception LACP n'augmentent pas.

Le résultat du voisin LACP du périphérique affecté a montré :

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

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

0x0

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

Sur le pare-feu, les compteurs LACP Sent/Recv n'augmentent pas pour les membres de port-channel :

```
<#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
```

L'interface port-channel et ses sous-interfaces sont à l'état down/down :

```
<#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
```

```
...
```

Les journaux côté commutateur indiquaient que le commutateur transmettait le protocole LACP mais ne recevait pas les unités de données de protocole LACP partenaires, les ports étant suspendus :

```
<#root>
```

```
Apr 2 18:44:20.614: %LINEPROTO-5-UPDOWN: Line protocol on Interface TwentyFiveGigE2/0/25, changed state to down  
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-L3DONTBNL2: 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-L3DONTBNL2: Twe2/0/25 suspended: LACP currently not enabled on the remote

Environnement

- Version du logiciel: FTD 7.6.2. D'autres versions logicielles, y compris ASA, peuvent également être affectées.
- Configuration de cluster FTD avec interfaces de données utilisant un Port-channel.
- Port-channel compatible LACP se connectant à l'infrastructure de commutation en amont.

Résolution

La résolution impliquait l'identification que l'unité FTD affectée avait quitté le cluster en raison d'une défaillance de contrôle d'intégrité de l'interface Port Channel. Lorsque la mise en grappe a été désactivée sur l'unité, toutes les interfaces de données ont été arrêtées par conception, ce qui a arrêté les unités d'alimentation LACP et provoqué une suspension côté commutateur et un impact sur le trafic.

Étapes de diagnostic effectuées

Étape 1: Collecter les offres de débogage et de support à la fois du périphérique Cisco Firepower et du commutateur en amont

Plusieurs archives de dépannage, fichiers de débogage LACP, fichiers principaux et fichiers TS (dépannage) ont été collectés à partir du châssis FXOS pour analyse.

Étape 2: Valider le comportement du commutateur et l'état LACP

L'ingénieur du commutateur a confirmé que le commutateur envoyait des unités de données de protocole LACP mais ne recevait pas d'unités de données de protocole partenaires du périphérique Firepower.

Étape 3: Analyser les transitions d'état internes LACP

L'analyse a montré que les interfaces sont passées à l'état suspendu en raison de PDU partenaires manquantes, les compteurs LACP n'étant pas incrémentés.



Conseil : Vérifiez le résultat de la commande « show cluster history » et les syslogs LINA du pare-feu pour déterminer la raison de la défaillance du cluster.

Dans cet exemple, le périphérique a quitté le cluster en raison d'une défaillance de l'interface de données :

```
<#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
```

Procédure De Recouvrement

Étape 1: Réactiver le clustering sur l'unité FTD concernée

```
<#root>
```

```
#
```

```
cluster enable
```

Cette commande a permis à l'unité de rejoindre le cluster, d'activer les interfaces de données, de reprendre les unités de données de protocole LACP et de restaurer la fonctionnalité Port-channel1.

Étape 2: Vérifier la récupération LACP

Après la réactivation du clustering, les PDU LACP ont repris et Port-channel1 est revenu à un fonctionnement normal du côté du pare-feu et du commutateur.

Motif

La cause principale était un échec du contrôle d'intégrité de l'interface Port-channel qui a entraîné le retrait de l'unité FTD du cluster. Lorsque la mise en grappe est désactivée sur une unité FTD, toutes les interfaces de données sont administrativement désactivées par conception, ce qui arrête la transmission des PDU LACP et entraîne la suspension des interfaces port-channel par le commutateur en amont.

Ce comportement est attendu.

L'ID de bogue Cisco CSCwo09449 a été enregistré pour améliorer la facilité de maintenance du produit.

Autres informations utiles

- ID de bogue Cisco [CSCwo09449](#) - FXOS : Compteurs LACP TX et RX obsolètes et canaux de port de données suspendus lorsque le clustering est désactivé

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.