Esempio di configurazione della funzionalità di ripristino automatico di Nexus 7000 vPC

Sommario

Introduzione

Questo documento descrive come configurare la funzione di ripristino automatico di PortChannel (vPC) virtuale su Nexus 7000.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Perché è necessario il ripristino automatico di vPC?

Le ragioni principali di questo miglioramento vPC sono due:

- In caso di interruzione dell'alimentazione o di interruzione dell'alimentazione del centro dati, entrambi i peer vPC costituiti da switch Nexus 7000 sono spenti. Occasionalmente, solo uno dei peer può essere ripristinato. Poiché l'altro Nexus 7000 è ancora disattivato, anche il collegamento peer vPC e il collegamento peer-keepalive vPC sono disattivati. In questo scenario, il vPC non è disponibile nemmeno per il Nexus 7000 che è già attivo. Tutte le configurazioni vPC devono essere rimosse dal canale della porta su Nexus 7000 per far funzionare il canale della porta. Quando si accende l'altro Nexus 7000, è necessario apportare nuovamente le modifiche alla configurazione per includere la configurazione vPC per tutti i vPC. Nella release 5.0(2) e successive, è possibile configurare il comando **reload restore** nella configurazione del dominio vPC per risolvere il problema.
- Per qualche motivo, il collegamento peer vPC si spegne. Poiché vPC peer-keepalive è ancora attivo, il dispositivo peer secondario vPC spegne tutte le porte membro vPC a causa del rilevamento della doppia attività. Di conseguenza, tutto il traffico passa attraverso lo switch primario vPC. Per qualche motivo, anche lo switch primario vPC si spegne. Questo problema relativo allo switch causa dei buchi neri nel traffico poiché i vPC sul dispositivo peer secondario sono ancora spenti perché ha rilevato il rilevamento dual-active prima dello spegnimento dello switch primario vPC.

Nella release 5.2(1) e successive, la funzione di ripristino automatico di vPC unisce questi due miglioramenti.

Configurazione

La configurazione del ripristino automatico di vPC è semplice. È necessario configurare il ripristino automatico nel dominio vPC su entrambi i peer vPC.

Di seguito viene riportata una configurazione di esempio:

On Switch S1

```
S1 (config)# vpc domain
S1(config-vpc-domain)# auto-recovery
S1# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link
vPC domain id                     : 1
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : primary
Number of vPCs configured         : 5
Peer Gateway                      : Enabled
Peer gateway excluded VLANs       : -
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Enabled (timeout = 240 seconds)
```

```
vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     1-112,114-120,800,810

vPC status
----------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
10   Po40   up     success     success                    1-112,114-1
                                                         20,800,810
```

On Switch S2

```
S2 (config)# vpc domain 1
S2(config-vpc-domain)# auto-recovery
S2# show vpc
Legend:
              (*) - local vPC is down, forwarding via vPC peer-link
vPC domain id                     : 1
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : secondary
Number of vPCs configured         : 5
Peer Gateway                      : Enabled
Peer gateway excluded VLANs       : -
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Enabled (timeout = 240 seconds)

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     1-112,114-120,800,810

vPC status ----------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
40   Po40   up     success     success                    1-112,114-1
                                                         20,800,810
```

Come funziona il ripristino automatico?

In questa sezione vengono descritti separatamente i comportamenti descritti nella sezione Informazioni di base. Si presume che il ripristino automatico di vPC sia configurato e salvato nella configurazione di avvio su entrambi gli switch S1 e S2.

1. Un'interruzione dell'alimentazione causa la disattivazione simultanea di entrambi i peer Nexus 7000 vPC e l'accensione di un solo switch.
   - S1 e S2 sono entrambi attivi. vPC è formato correttamente con peer-link e peer-keepalive attivati.
   - S1 e S2 si spengono contemporaneamente.
   - Ora è possibile accendere un solo switch. Ad esempio, S2 è l'unico interruttore che si accende.

- S2 attende il timeout di ripristino automatico di vPC (l'impostazione predefinita è 240 secondi, configurabile con il comando **auto-recovery reload-delay x**, dove **x** è 240-3600 secondi) per verificare se il collegamento peer vPC o lo stato peer-keepalive sono attivi. Se uno di questi collegamenti è attivo (stato peer-link o peer-keepalive), il ripristino automatico non viene attivato.
- Dopo il timeout, se entrambi i collegamenti sono ancora disattivati (stato peer-link e peer-keepalive), il ripristino automatico di vPC si attiva e S2 diventa primario e si avvia per accendere il vPC locale. Poiché non sono presenti peer, il controllo di coerenza viene ignorato.
- Ora S1 si accende. A questo punto, S2 mantiene il suo ruolo primario e S1 assume un ruolo secondario, viene eseguita una verifica di coerenza e vengono intraprese le azioni appropriate.

2. Il collegamento peer vPC si spegne prima e poi il peer vPC principale si spegne.
   - S1 e S2 sono entrambi attivi e vPC è formato correttamente con peer-link e peer-keepalive attivi.
   - Per qualche motivo, vPC peer-link va in primo piano.
   - Poiché vPC peer-keepalive è ancora attivo, rileva il rilevamento dual-active. Il vPC secondario S2 disattiva tutti i vPC locali.
   - A questo punto, l'S1 principale vPC si spegne o si ricarica.
   - Questa interruzione disattiva anche il collegamento peer-keepalive vPC.
   - S2 attende la perdita di tre messaggi peer-keepalive consecutivi. Per qualche motivo, il collegamento peer vPC si attiva oppure S2 riceve un messaggio peer-keepalive e il ripristino automatico non è abilitato.
   - Tuttavia, se il collegamento peer rimane disattivato e si perdono tre messaggi peer-keepalive consecutivi, il ripristino automatico vPC viene attivato.
   - S2 assume il ruolo di primario e abilita il vPC locale, ignorando la verifica di coerenza.
   - Quando S1 completa il ricaricamento, S2 mantiene il suo ruolo primario e S1 diventa secondario, viene eseguita una verifica di coerenza e vengono intraprese le azioni appropriate.

   Nota: Come spiegato in entrambi gli scenari, lo switch che rimuove il ruolo vPC con il ripristino automatico vPC continua a essere il dispositivo principale anche dopo l'attivazione del collegamento peer. L'altro peer assume il ruolo di secondario e sospende il proprio vPC fino al completamento di un controllo di coerenza.

Ad esempio:

S1 è spento. S2 diventa il principale operativo come previsto. Peer-link e peer-keepalive e tutti i collegamenti vPC sono disconnessi da S1. S1 non è acceso. Poiché S1 è completamente isolato, accende il vPC (anche se i collegamenti fisici sono inattivi) a causa del ripristino automatico e assume il ruolo di primario. Ora, se il peer-link o il peer-keepalive sono connessi tra S1 e S2, S1 mantiene il ruolo di primario e S2 diventa secondario. In base a questa configurazione, S2 sospende il proprio vPC finché non vengono accesi sia vPC peer-link che peer-keepalive e non viene completata la verifica di coerenza. Questo scenario causa il traffico verso il buco nero poiché il vPC S2 è secondario e i collegamenti fisici S1 sono disattivati.

È consigliabile abilitare il ripristino automatico di vPC?

Èbuona norma abilitare il ripristino automatico nell'ambiente vPC.

Èpossibile che la funzione di ripristino automatico di vPC crei uno scenario a doppia attività. Ad esempio, se prima si perde il collegamento peer e poi si perde il collegamento peer-keepalive, si avrà uno scenario a doppia attività.

In questo caso, ogni porta membro di vPC continua a pubblicizzare lo stesso ID del protocollo di controllo dell'aggregazione dei collegamenti che aveva prima del guasto dual-active.

Una topologia vPC protegge intrinsecamente dai loop in caso di scenari dual-attivi. Nello scenario peggiore, sono presenti frame duplicati. Tuttavia, come meccanismo di prevenzione dei loop, ciascuno switch inoltra le BDPU (Bridge Protocol Data Unit) con lo stesso ID BPDU Bridge utilizzato prima del guasto dual-active del vPC.

Anche se non intuitivo, è comunque possibile e desiderabile continuare a inoltrare il traffico dal livello di accesso al livello di aggregazione senza perdite per i flussi di traffico correnti, a condizione che le tabelle Address Resolution Protocol (ARP) siano già popolate su entrambi i peer Cisco Nexus serie 7000 per tutti gli host necessari.

Se è necessario apprendere nuovi indirizzi MAC dalla tabella ARP, potrebbero verificarsi dei problemi. I problemi si verificano perché la risposta ARP dal server potrebbe essere sottoposta a hashing su un dispositivo Cisco Nexus serie 7000 e non sull'altro, il che rende impossibile il corretto flusso del traffico.

Si supponga, tuttavia, che prima del guasto nella situazione appena descritta il traffico sia stato equamente distribuito a entrambi i dispositivi Cisco Nexus serie 7000 tramite una corretta configurazione PortChannel e Equal Cost Multipath (ECMP). In questo caso, il traffico tra server e tra client e server continua con l'avvertenza che gli host single-attached connessi direttamente a Cisco Nexus serie 7000 non saranno in grado di comunicare (per la mancanza del collegamento peer). Inoltre, i nuovi indirizzi MAC appresi su un Cisco Nexus serie 7000 non possono essere appresi sul peer, perché questo causerebbe l'inondazione del traffico di ritorno che arriva sul dispositivo Cisco Nexus serie 7000 peer.

Fare riferimento alla pagina 19 di Cisco NX-OS Software Virtual PortChannel: Concetti fondamentali per ulteriori informazioni.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems