Ejemplo de Configuración de la Función Nexus 7000 vPC Auto-Recovery

Contenido

Introducción

Este documento describe cómo configurar la función de recuperación automática de PortChannel virtual (vPC) en el Nexus 7000.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

¿Por qué necesitamos la recuperación automática de vPC?

Hay dos razones principales para esta mejora de vPC:

- En caso de interrupción del Data Center o interrupción de la alimentación, ambos pares vPC que se componen de switches Nexus 7000 están apagados. En ocasiones, sólo se puede restaurar uno de los pares. Dado que el otro Nexus 7000 aún está desactivado, el enlace de par vPC y el enlace de par-keepalive vPC también están desactivados. En esta situación, el vPC no se enciende ni siquiera para el Nexus 7000 que ya está encendido. Todas las configuraciones de vPC deben eliminarse del canal de puerto en ese Nexus 7000 para que funcione el canal de puerto. Cuando se enciende el otro Nexus 7000, debe volver a realizar cambios en la configuración para incluir la configuración de vPC para todos los vPC. En la versión 5.0(2) y posteriores, puede configurar el comando **reload restore** bajo la configuración del dominio vPC para solucionar este problema.
- Por alguna razón, el enlace de par vPC se apaga. Dado que la señal de mantenimiento de par vPC sigue activa, el dispositivo de par secundario vPC desactiva todos sus puertos de miembro vPC debido a la detección de doble actividad. Por lo tanto, todo el tráfico pasa por el switch principal vPC. Por alguna razón, el switch principal vPC también se apaga. Este problema del switch hace que el tráfico quede atascado, ya que los vPC del dispositivo de par secundario siguen apagados porque detectaron detección dual-activa antes de que el switch principal vPC se apagara.

En la versión 5.2(1) y posteriores, la función de recuperación automática de vPC combina estas dos mejoras.

Configuración

La configuración de la recuperación automática de vPC es sencilla. Debe configurar la recuperación automática en el dominio vPC en ambos pares vPC.

Este es un ejemplo de configuración:

En el 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
```

En el 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
```

¿Cómo funciona realmente la recuperación automática?

Esta sección trata por separado cada comportamiento mencionado en la sección Información de fondo. Se supone que la recuperación automática de vPC está configurada y guardada en la configuración de inicio en ambos switches S1 y S2.

1. Una interrupción de la alimentación apaga simultáneamente a los pares vPC Nexus 7000 y solo se puede encender un switch.
   - S1 y S2 están activados. vPC se ha formado correctamente con peer-link y peer-keepalive activado.
   - Tanto S1 como S2 se apagan simultáneamente.
   - Ahora sólo un switch puede encenderse. Por ejemplo, S2 es el único switch que se enciende.

- S2 espera el tiempo de espera de recuperación automática de vPC (el valor predeterminado es 240 segundos que se pueden configurar con el comando **auto-recovery reload-delay x**, donde **x** es 240-3600 segundos) para verificar si se enciende el estado vPC peer-link o peer-keepalive. Si alguno de estos links está activado (estado de peer-link o de peer-keepalive), la recuperación automática no se activa.
- Después del tiempo de espera, si ambos links aún están desactivados (peer-link y estado de keepalive de peer), la recuperación automática de vPC habilita y S2 se convierte en primario y se inicia para encender su vPC local. Puesto que no hay pares, se omite la comprobación de coherencia.
- Ahora viene S1. En este momento, S2 conserva su función principal y S1 desempeña un papel secundario, se realiza una comprobación de coherencia y se toman las medidas adecuadas.

2. vPC peer-link se apaga primero y después se apaga el par vPC principal.
   - S1 y S2 están activados y vPC se ha formado correctamente con peer-link y peer-keepalive activado.
   - Por alguna razón, el enlace de par vPC se apaga primero.
   - Dado que vPC peer-keepalive aún está activado, detecta detección dual-activa. El vPC secundario S2 apaga todos sus vPC locales.
   - Ahora el vPC principal S1 se apaga o se recarga.
   - Esta interrupción también desactiva el enlace de keepalive del par vPC.
   - S2 espera que se pierdan tres mensajes consecutivos de mantenimiento de peer. Por alguna razón, se enciende el enlace de par vPC o S2 recibe un mensaje de señal de mantenimiento de par y la recuperación automática no se habilita.
   - Sin embargo, si el link de peer permanece desactivado y se pierden tres mensajes consecutivos de keepalive de peer, la recuperación automática de vPC se habilita.
   - S2 asume la función de primario y habilita su vPC local que omite la verificación de consistencia.
   - Cuando S1 completa la recarga, S2 conserva su función de primario y S1 se convierte en secundario, se realiza una verificación de consistencia y se toman las medidas apropiadas.

   Nota: Como se explica en ambos escenarios, el switch que deja de suspender su función de vPC con la recuperación automática de vPC sigue siendo principal incluso después de que el link de par esté encendido. El otro par asume el rol secundario y suspende su propio vPC hasta que se complete una verificación de consistencia.

Por ejemplo:

S1 está apagado. S2 se convierte en el principal operativo como se esperaba. Peer-link y peer-keepalive y todos los links vPC se desconectan de S1. S1 no está encendido. Dado que S1 está completamente aislado, enciende el vPC (aunque los enlaces físicos están inactivos) debido a la recuperación automática y asume el papel de primario. Ahora, si el link de peer o el keepalive de peer están conectados entre S1 y S2, S1 mantiene el rol de primario y S2 se convierte en secundario. Esta configuración hace que S2 suspenda su vPC hasta que se enciendan tanto vPC peer-link como peer-keepalive y se complete la verificación de consistencia. Esta situación hace que el tráfico sea un agujero negro, ya que el vPC S2 es secundario y los links físicos S1 están apagados.

¿Debo habilitar la recuperación automática de vPC?

Es una buena práctica habilitar la recuperación automática en su entorno vPC.

Existe una pequeña posibilidad de que la función de recuperación automática de vPC cree un escenario de doble actividad. Por ejemplo, si perdió primero el link de par y luego perdió el keepalive de par, tendrá un escenario activo dual.

En esta situación, cada puerto miembro de vPC continúa anunciando el mismo ID de Link Aggregation Control Protocol que hizo antes de la falla dual-active.

Una topología vPC protege intrínsecamente de los loops en caso de situaciones de doble actividad. En el peor de los casos, hay tramas duplicadas. A pesar de esto, como mecanismo de prevención de loops, cada switch reenvía unidades de datos de protocolo de puente (BPDU) con el mismo ID de puente BPDU que antes de la falla de doble actividad de vPC.

Aunque no es intuitivo, todavía es posible y deseable continuar reenviando el tráfico desde la capa de acceso a la capa de agregación sin descartes para los flujos de tráfico actuales, siempre que las tablas de protocolo de resolución de direcciones (ARP) ya estén rellenadas en ambos pares Nexus de Cisco serie 7000 para todos los hosts necesarios.

Si la tabla ARP necesita aprender nuevas direcciones MAC, pueden surgir problemas. Los problemas se deben a que la respuesta ARP del servidor puede ser dañada a un dispositivo Cisco Nexus serie 7000 y no a otro, lo que hace imposible que el tráfico fluya correctamente.

Suponga, sin embargo, que antes de la falla en la situación descrita, el tráfico se distribuyó de la misma manera a los dispositivos Cisco Nexus serie 7000 mediante un PortChannel correcto y mediante una configuración ECMP (Equal Cost Multipath). En este caso, el tráfico de servidor a servidor y de cliente a servidor continúa con la advertencia de que los hosts conectados de forma individual conectados directamente a Cisco Nexus serie 7000 no podrán comunicarse (por falta del enlace de par). Además, las nuevas direcciones MAC aprendidas en un Cisco Nexus serie 7000 no se pueden aprender en el par, ya que esto causaría que el tráfico de retorno que llega en el dispositivo Cisco Nexus serie 7000 del mismo nivel se inunde.

Consulte la página 19 del Virtual PortChannel del software Cisco NX-OS: Conceptos fundamentales para obtener más información.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems