Exemplo de configuração do recurso de recuperação automática do Nexus 7000 vPC

Contents

Introduction

Este documento descreve como configurar o recurso de recuperação automática do PortChannel (vPC) virtual no Nexus 7000.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Informações de Apoio

Por que precisamos da Recuperação Automática do vPC?

Há dois motivos principais para essa melhoria do vPC:

- Em uma interrupção de data center ou queda de energia, os dois pares de vPC que são compostos por switches Nexus 7000 estão desligados. Ocasionalmente, apenas um dos pares pode ser restaurado. Como o outro Nexus 7000 ainda está desligado, o link peer do vPC e o link peer-keepalive do vPC também estão desligados. Nesse cenário, o vPC não é ativado mesmo para o Nexus 7000 que já está ativado. Todas as configurações de vPC devem ser removidas do canal de porta nesse Nexus 7000 para que o canal de porta funcione. Quando o outro Nexus 7000 é ativado, você precisa fazer novamente alterações na configuração para incluir a configuração do vPC para todos os vPCs. Na versão 5.0(2) e posterior, você pode configurar o comando **reload restore** na configuração de domínio do vPC para resolver esse problema.
- Por alguma razão, o link par do vPC é desligado. Como o peer-keepalive do vPC ainda está ativo, o dispositivo peer secundário do vPC desliga todas as portas membro do vPC devido à detecção dupla ativa. Assim, todo o tráfego passa pelo switch principal do vPC. Por algum motivo, o switch principal do vPC também desliga. Esse problema de switch faz buracos negros no tráfego, já que os vPCs no dispositivo peer secundário ainda estão desligados porque detectou a detecção dual-ative antes do switch primário do vPC ser desligado.

Na versão 5.2(1) e posterior, o recurso de recuperação automática do vPC mescla esses dois aprimoramentos.

Configuração

A configuração da recuperação automática do vPC é simples. Você precisa configurar a recuperação automática no domínio vPC em ambos os pares do vPC.

Este é um exemplo de configuração:

No 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
```

No 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
```

Como a recuperação automática realmente funciona?

Esta seção discute cada comportamento mencionado na seção Informações de fundo separadamente. A suposição é que a recuperação automática do vPC é configurada e salva na configuração de inicialização nos switches S1 e S2.

1. Uma queda de energia desliga ambos os pares de vPC do Nexus 7000 simultaneamente e apenas um switch pode ser ligado.
   - S1 e S2 estão ativados. O vPC é formado corretamente com peer-link e peer-keepalive.
   - S1 e S2 desligam simultaneamente.
   - Agora apenas um switch pode ligar. Por exemplo, S2 é o único switch que liga.
   - O S2 aguarda o tempo limite de recuperação automática do vPC (o padrão é 240 segundos, que podem ser configurados com o comando **auto-recovery reload-delay x**, em que **x** é 240-3600 segundos) para verificar se o status de peer-link ou peer-keepalive do vPC é ativado. Se qualquer um desses links estiver ativado (status peer-link ou peer-keepalive), a recuperação automática não é acionada.

- Após o tempo limite, se ambos os links ainda estiverem desligados (link par e status de keepalive par), a recuperação automática do vPC será ativada e o S2 se tornará primário e iniciará para ligar seu vPC local. Como não há pares, a verificação de consistência é ignorada.
- Agora o S1 vem. No momento, o S2 mantém sua função principal e o S1 assume uma função secundária, uma verificação de consistência é realizada e ações apropriadas são tomadas.

2. O link par do vPC é desligado primeiro e, em seguida, o par principal do vPC é desligado.
   - S1 e S2 estão ativados e o vPC é formado corretamente com peer-link e peer-keepalive.
   - Por algum motivo, o link peer do vPC é desligado primeiro.
   - Como o peer-keepalive do vPC ainda está ativo, ele detecta a detecção dual-ative. O S2 secundário do vPC desliga todos os vPCs locais.
   - Agora o S1 principal do vPC é desligado ou recarregado.
   - Essa interrupção também desliga o link peer-keepalive do vPC.
   - O S2 espera que três mensagens de peer keepalive consecutivas sejam perdidas. Por algum motivo, o link peer do vPC é ativado ou o S2 recebe uma mensagem de peer-keepalive e a recuperação automática não é ativada.
   - No entanto, se o peer-link permanecer desligado e três mensagens consecutivas de peer-keepalive forem perdidas, a recuperação automática do vPC será ativada.
   - O S2 assume a função de principal e ativa seu vPC local, que ignora a verificação de consistência.
   - Quando o S1 conclui o recarregamento, o S2 mantém sua função de primário e o S1 se torna secundário, uma verificação de consistência é executada e as ações apropriadas são tomadas.

   Note: Como explicado em ambos os cenários, o switch que cancela sua função de vPC com a recuperação automática de vPC continua a ser primário mesmo depois que o link par está ativado. O outro par assume a função de secundário e suspende seu próprio vPC até que uma verificação de consistência seja concluída.

Por exemplo:

S1 está desligado. O S2 torna-se o principal operacional conforme esperado. O peer-link e o peer-keepalive e todos os links vPC são desconectados do S1. S1 não está ligado. Como o S1 está completamente isolado, ele liga o vPC (embora os links físicos estejam inativos) devido à recuperação automática e assume a função de primário. Agora, se peer-link ou peer-keepalive estiverem conectados entre S1 e S2, S1 mantém a função de primary e S2 se torna secundário. Essa configuração faz com que o S2 suspenda seu vPC até que o peer-link e o peer-keepalive do vPC sejam ligados e a verificação de consistência seja concluída. Esse cenário faz com que o tráfego atinja um buraco negro, já que o vPC S2 é secundário e os links físicos S1 estão desativados.

Devo ativar a recuperação automática do vPC?

Éuma boa prática habilitar a recuperação automática no ambiente vPC.

Há uma pequena chance de que o recurso de recuperação automática do vPC possa criar um cenário dual-ative. Por exemplo, se você primeiro perder o peer-link e depois perder o peer-keepalive, você terá um cenário dual-ative.

Nessa situação, cada porta membro do vPC continua anunciando a mesma ID do Link Aggregation Control Protocol que fazia antes da falha dupla ativa.

Uma topologia vPC protege intrinsecamente de loops em caso de cenários dual-ative. Em um pior cenário, há quadros duplicados. Apesar disso, como um mecanismo de prevenção de loop, cada switch encaminha BPDUs (Bridge Protocol Data Units, Unidades de Dados de Protocolo de Bridge) com o mesmo ID de Bridge BPDU anterior à falha dupla do vPC.

Embora não seja intuitivo, ainda é possível e desejável continuar a encaminhar o tráfego da camada de acesso para a camada de agregação sem descartes para fluxos de tráfego atuais, desde que as tabelas do Address Resolution Protocol (ARP) já estejam preenchidas em ambos os peers do Cisco Nexus 7000 Series para todos os hosts necessários.

Se novos endereços MAC precisarem ser aprendidos pela tabela ARP, podem surgir problemas. Os problemas surgem porque a resposta ARP do servidor pode ser enviada por hash para um dispositivo Cisco Nexus 7000 Series e não para o outro, o que torna impossível o fluxo correto do tráfego.

Suponha, no entanto, que antes da falha na situação descrita, o tráfego foi distribuído igualmente para os dispositivos Cisco Nexus 7000 Series por um PortChannel correto e por uma configuração de Equal Cost Multipath (ECMP). Nesse caso, o tráfego de servidor para servidor e de cliente para servidor continua com a ressalva de que os hosts de conexão única conectados diretamente ao Cisco Nexus 7000 Series não poderão se comunicar (por falta do link de peer). Além disso, novos endereços MAC aprendidos em um Cisco Nexus 7000 Series não podem ser aprendidos no peer, porque isso faria com que o tráfego de retorno que chega no dispositivo Cisco Nexus 7000 Series do mesmo nível fosse inundado.

Consulte a página 19 do Cisco NX-OS Software Virtual PortChannel: Conceitos fundamentais para mais informação.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems