

Exemple de configuration de la fonctionnalité de récupération automatique vPC Nexus 7000

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer la fonctionnalité de récupération automatique PortChannel (vPC) virtuelle sur le Nexus 7000.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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.

Informations générales

Pourquoi avons-nous besoin de la récupération automatique vPC ?

Cette amélioration de vPC s'explique principalement par deux raisons :

- En cas de panne de data center ou de coupure de courant, les deux homologues vPC composés des commutateurs Nexus 7000 sont éteints. Parfois, un seul des homologues peut être restauré. Comme l'autre Nexus 7000 est toujours désactivé, la liaison homologue vPC et la liaison homologue keepalive vPC sont également désactivées. Dans ce scénario, le vPC n'est pas activé même pour le Nexus 7000 qui est déjà activé. Toutes les configurations vPC doivent être supprimées du port-channel sur ce Nexus 7000 pour que le port-channel fonctionne. Lorsque l'autre Nexus 7000 est activé, vous devez à nouveau modifier la configuration pour inclure la configuration vPC pour tous les vPC. Dans les versions 5.0(2) et ultérieures, vous pouvez configurer la commande **reload restore** sous la configuration du domaine vPC pour résoudre ce problème.
- Pour une raison quelconque, la liaison homologue vPC s'éteint. Puisque le keepalive d'homologue vPC est toujours actif, le périphérique homologue secondaire vPC désactive tous ses ports membres vPC en raison de la détection de la double activité. Ainsi, tout le trafic passe par le commutateur principal vPC. Pour une raison quelconque, le commutateur principal vPC s'éteint également. Ce problème de commutateur crée des trous noirs dans le trafic depuis que les vPC sur le périphérique homologue secondaire sont toujours éteints, car il a détecté une détection double-active avant que le commutateur principal vPC ne s'éteigne.

Dans les versions 5.2(1) et ultérieures, la fonctionnalité de récupération automatique vPC fusionne ces deux améliorations.

Configuration

La configuration de la récupération automatique vPC est simple. Vous devez configurer la récupération automatique sous le domaine vPC sur les deux homologues vPC.

Voici un exemple de configuration:

Sur le commutateur 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

```

Sur le commutateur 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

```

Comment fonctionne la récupération automatique ?

Cette section traite séparément de chaque comportement mentionné dans la section Informations générales. L'hypothèse est que la récupération automatique vPC est configurée et enregistrée dans la configuration de démarrage sur les commutateurs S1 et S2.

1. Une coupure de courant arrête simultanément les deux homologues vPC du Nexus 7000 et un seul commutateur est capable de s'allumer.
 - S1 et S2 sont tous deux activés. vPC est formé correctement avec peer-link et peer-keepalive on.
 - S1 et S2 s'éteignent simultanément.
 - Aujourd'hui, un seul commutateur peut être mis sous tension. Par exemple, S2 est le seul commutateur sous tension.
 - S2 attend le délai de récupération automatique vPC (la valeur par défaut est 240 secondes qui peuvent être configurées avec la commande **auto-recovery reload-delay x**, où x est de

240 à 3 600 secondes) afin de vérifier si l'état peer-link ou peer-keepalive vPC est activé. Si l'une de ces liaisons est activée (état peer-link ou peer-keepalive), la récupération automatique n'est pas déclenchée.

- Après le délai d'attente, si les deux liaisons sont toujours désactivées (peer-link et peer-keepalive status), la récupération automatique vPC active et S2 devient primaire et démarre afin de mettre sous tension son vPC local. Comme il n'y a pas d'homologues, la vérification de cohérence est ignorée.
- Maintenant S1 est activé. À ce stade, S2 conserve son rôle principal et S1 joue un rôle secondaire, une vérification de cohérence est effectuée et des mesures appropriées sont prises.

2. La liaison homologue vPC s'éteint d'abord, puis l'homologue vPC principal s'éteint.

- S1 et S2 sont tous deux actifs et vPC est formé correctement avec peer-link et peer-keepalive sur.
- Pour une raison quelconque, la liaison homologue vPC démarre en premier.
- Comme le keepalive d'homologue vPC est toujours actif, il détecte la détection de double activité. Le vPC secondaire S2 désactive tous ses vPC locaux.
- Le commutateur S1 principal vPC s'éteint ou se recharge.
- Cette panne désactive également la liaison de veille homologue vPC.
- S2 attend la perte de trois messages de keepalive d'homologue consécutifs. Pour une raison quelconque, soit la liaison homologue vPC est activée, soit S2 reçoit un message de keepalive homologue, et la récupération automatique n'est pas activée.
- Cependant, si la liaison homologue reste désactivée et que trois messages de keepalive homologue consécutifs sont perdus, la récupération automatique vPC est activée.
- S2 assume le rôle de principal et active son vPC local qui contourne le contrôle de cohérence.
- Lorsque S1 termine le rechargement, S2 conserve son rôle de principal et S1 devient secondaire, une vérification de cohérence est effectuée et des mesures appropriées sont prises.

Note: Comme expliqué dans les deux scénarios, le commutateur qui ne suspend pas son rôle vPC avec la récupération automatique vPC continue de rester principal même après la liaison homologue. L'autre homologue joue le rôle de secondaire et suspend son propre vPC jusqu'à ce qu'une vérification de cohérence soit terminée.

Exemple :

S1 est hors tension. S2 devient la principale opérationnelle comme prévu. Peer-link et peer-keepalive et toutes les liaisons vPC sont déconnectées de S1. S1 n'est pas sous tension. Comme S1 est complètement isolé, il met le vPC sous tension (bien que les liaisons physiques soient en panne) en raison de la récupération automatique et joue le rôle de principal. Maintenant, si peer-link ou peer-keepalive sont connectés entre S1 et S2, S1 conserve le rôle de principal et S2 devient secondaire. Cette configuration entraîne la suspension de son vPC par S2 jusqu'à ce que la liaison homologue et le keepalive vPC soient tous deux sous tension et que la vérification de cohérence soit terminée. Ce scénario entraîne un trou noir du trafic, car le vPC de S2 est secondaire et les liaisons physiques de S1 sont désactivées.

Dois-je activer la récupération automatique vPC ?

Il est recommandé d'activer la récupération automatique dans votre environnement vPC.

Il est peu probable que la fonctionnalité de récupération automatique vPC crée un scénario de double activité. Par exemple, si vous avez d'abord perdu le peer-link, puis que vous avez perdu le peer-keepalive, vous aurez un scénario de double-activité.

Dans ce cas, chaque port membre vPC continue d'annoncer le même ID de protocole de contrôle d'agrégation de liaisons qu'avant la défaillance de la double activité.

Une topologie vPC protège intrinsèquement des boucles en cas de scénarios biactifs. Dans le pire des cas, il y a des trames en double. Malgré cela, en tant que mécanisme de prévention des boucles, chaque commutateur transfère des unités de données de protocole de pont (BPDU) avec le même ID de pont BPDU qu'avant la défaillance biactive vPC.

Bien qu'il ne soit pas intuitif, il est toujours possible et souhaitable de continuer à transférer le trafic de la couche d'accès à la couche d'agrégation sans perte pour les flux de trafic actuels, à condition que les tables ARP (Address Resolution Protocol) soient déjà remplies sur les deux homologues de la gamme Cisco Nexus 7000 pour tous les hôtes nécessaires.

Si de nouvelles adresses MAC doivent être apprises par la table ARP, des problèmes peuvent survenir. Les problèmes surviennent parce que la réponse ARP du serveur peut être hachée sur un périphérique de la gamme Cisco Nexus 7000 et non sur l'autre, ce qui empêche le trafic de circuler correctement.

Supposons toutefois qu'avant la défaillance décrite ci-dessus, le trafic était distribué de manière égale aux deux périphériques de la gamme Cisco Nexus 7000 par un PortChannel correct et par une configuration ECMP (Equal Cost Multipath). Dans ce cas, le trafic serveur à serveur et client à serveur continue avec la mise en garde que les hôtes à connexion unique connectés directement à la gamme Cisco Nexus 7000 ne pourront pas communiquer (faute de liaison homologue). En outre, les nouvelles adresses MAC apprises sur un commutateur Cisco Nexus 7000 ne peuvent pas être apprises sur l'homologue, car cela provoquerait une inondation du trafic de retour qui arrive sur le périphérique homologue Cisco Nexus 7000.

Reportez-vous à la page 19 du [logiciel Cisco NX-OS Virtual PortChannel : Concepts fondamentaux](#) pour plus d'informations.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [Support et documentation techniques - Cisco Systems](#)