Configurer une interconnexion de data center vPC de couche 2 sur un commutateur Nexus 7000

Table des matières

Introduction

Ce document décrit comment configurer une interconnexion de data center (DCI) de couche 2 (L2) avec l'utilisation d'un vPC (Virtual Port-Channel).

Conditions préalables

Il est supposé que vPC et le protocole HSRP (Hot Standby Routing Protocol) sont déjà configurés sur les périphériques utilisés dans les exemples fournis dans ce document.

Utilisez le protocole LACP (Link Aggregation Control Protocol) sur la liaison vPC, qui fait office de DCI.



Conseil : Le cryptage MACSec nécessite une licence de services avancés LAN dans les versions antérieures à la version 6.1(1) et présente des limitations spécifiques à la carte de ligne. Pour plus d'informations, reportez-vous à la section Guidelines and Limitations for Cisco TrustSec du Guide de configuration de la sécurité NX-OS de la gamme Cisco Nexus 7000, version 6.x.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- vPC
- HSRP
- Le protocole STP
- Cryptage MACSec (facultatif)

Composants utilisés

Les informations contenues dans ce document sont basées sur un commutateur de la gamme Cisco Nexus 7000 qui exécute la version logicielle 6.2(8b).

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

L'objectif d'un DCI est d'étendre des VLAN spécifiques entre différents data centers, ce qui offre une contiguïté de couche 2 pour les serveurs et les périphériques NAS (Network-Attached Storage) qui sont séparés par de grandes distances.

Le vPC présente l'avantage de l'isolation STP entre les deux sites (aucune unité BPDU (Bridge Protocol Data Unit) sur le vPC DCI), de sorte que toute panne dans un data center ne se propage pas au data center distant, car des liaisons redondantes sont toujours fournies entre les data centers.

Utilisez le vPC pour interconnecter un maximum de deux data centers. Si plus de deux data centers doivent être interconnectés, utilisez la virtualisation OTV (Overlay Transport Virtualization).

Un canal EtherChannel vPC DCI est généralement configuré avec ces informations à l'esprit :

- Isolation FHRP (First Hop Redundancy Protocol) : Empêchez le routage non optimal grâce à l'utilisation d'une passerelle dédiée pour chaque data center. Les configurations varient selon l'emplacement de la passerelle FHRP.
- Isolation STP : Comme mentionné précédemment, cela empêche la propagation des pannes d'un data center à un autre.
- Contrôle des tempêtes de diffusion : Cette option permet de réduire le trafic de diffusion entre les data centers.
- Cryptage MACSec (facultatif) : Le trafic est ainsi chiffré afin d'empêcher toute intrusion entre les deux sites.

Configurer

Utilisez les informations décrites dans cette section pour configurer un DCI de couche 2 avec

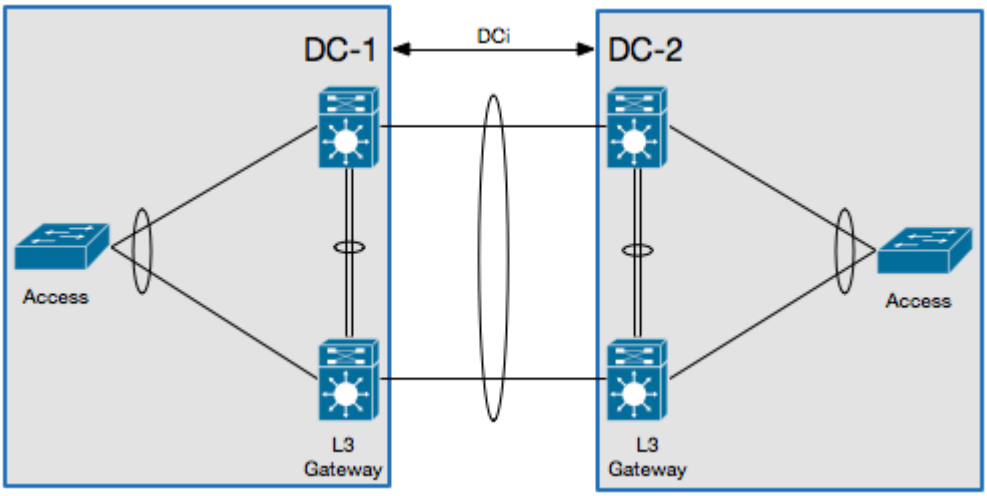
l'utilisation d'un vPC. Les clients enregistrés peuvent utiliser l'outil Command Lookup Tool pour obtenir plus d'informations sur les commandes utilisées ici.

Isolement FHRP

Cette section décrit deux scénarios pour lesquels l'isolation FHRP peut être implémentée.

Interconnexion double POD L2/L3

Voici la topologie utilisée dans ce scénario :



Dans ce scénario, la passerelle de couche 3 (L3) est configurée sur la même paire vPC et agit en tant que DCI. Pour isoler le HSRP, vous devez configurer une liste de contrôle d'accès au port (PACL) sur le canal de port DCI et désactiver les protocoles ARP (Gratuitous Address Resolution Protocol) (GARP) HSRP sur les interfaces virtuelles commutées (SVI) pour les VLAN qui se déplacent sur le DCI.

Voici un exemple de configuration :

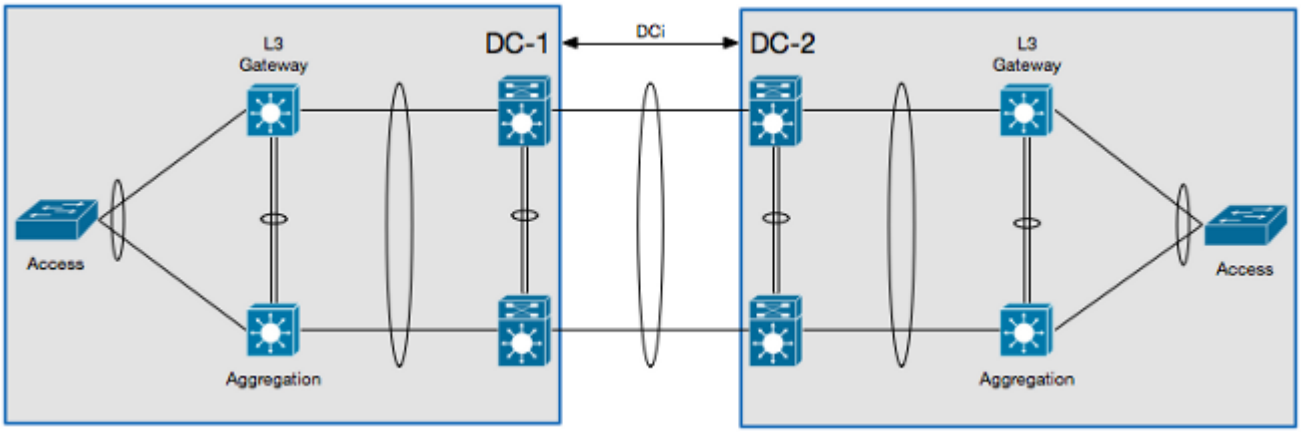
```
ip access-list DENY_HSRP_IP
  10 deny udp any 224.0.0.2/32 eq 1985
  20 deny udp any 224.0.0.102/32 eq 1985
  30 permit ip any any

interface <DCI-Port-Channel>
  ip port access-group DENY_HSRP_IP in

interface Vlan <x>
  no ip arp gratuitous hsrp duplicate
```

vPC multicouche pour agrégation et DCI

Voici la topologie utilisée dans ce scénario :



Dans ce scénario, le DCI est isolé sur son propre VDC (Virtual Device Context) de couche 2 et la passerelle de couche 3 se trouve sur un périphérique de couche d'agrégation. Pour isoler le HSRP, configurez une liste de contrôle d'accès VLAN (VACL) qui bloque le trafic de contrôle HSRP et un filtre d'inspection ARP qui bloque les GARP HSRP sur le VDC DCI L2. Exemple de configuration :

```
ip access-list ALL_IPs
  10 permit ip any any
mac access-list ALL_MACs
  10 permit any any
ip access-list HSRP_IP
  10 permit udp any 224.0.0.2/32 eq 1985
  20 permit udp any 224.0.0.102/32 eq 1985
mac access-list HSRP_VMAC
  10 permit 0000.0c07.ac00 0000.0000.00ff any
  20 permit 0000.0c9f.f000 0000.0000.0fff any
vlan access-map HSRP_Localization 10
        match ip address HSRP_IP
        match mac address HSRP_VMAC
        action drop
        statistics per-entry
vlan access-map HSRP_Localization 20
        match ip address ALL_IPs
        match mac address ALL_MACs
        action forward
        statistics per-entry
vlan filter HSRP_Localization vlan-list <DCI_Extended_VLANs>

feature dhcp

arp access-list HSRP_VMAC_ARP
  10 deny ip any mac 0000.0c07.ac00 ffff.ffff.ff00
  20 deny ip any mac 0000.0c9f.f000 ffff.ffff.f000
  30 permit ip any mac any
```

```
ip arp inspection filter HSRP_VMAC_ARP vlan <DCI_Extended_VLANs>
```

Configuration d'isolation supplémentaire

Cette section fournit un exemple de configuration qui :

- Autorise uniquement l'extension des VLAN nécessaires au data center distant
- Isole le STP au niveau de chaque data center
- Abandonne le trafic de diffusion qui dépasse 1 % de la vitesse totale de la liaison

Exemple de configuration :

```
 interface <DCI-Port-Channel>
  switchport trunk allowed vlan <DCI_Extended_VLANs>
  spanning-tree port type edge trunk
  spanning-tree bpdufilter enable
  storm-control broadcast level 1.0
```

Le contrôle des tempêtes pour le trafic de multidiffusion peut également être configuré, mais il doit avoir le même pourcentage que le trafic de diffusion.

Cryptage MACSec

La configuration décrite dans cette section est facultative.

Utilisez ces informations pour configurer le cryptage MACSec :

```
feature dot1x
feature cts

! MACSec requires 24 additional bytes for encapsulation.
interface <DCI-Port-Channel>
  mtu 1524

interface <DCI-Physical-Port>
  cts manual
    no propagate-sgt
    sap pmk <Preshared-Key>
```

Faites basculer l'interface pour que l'autorisation MACSec se produise.

Vérifier

Utilisez les informations décrites dans cette section pour vérifier que votre configuration fonctionne correctement.

Isolement FHRP

Entrez la commande show hsrp br dans la CLI pour vérifier que la passerelle HSRP est active dans les deux data centers :

<#root>

```
!DC-1
N7K-A#

show hsrp br


*:IPv6 group   #:group belongs to a bundle
                      P indicates configured to preempt.
                      |
 Interface   Grp  Prio P State    Active addr      Standby addr     Group addr
  Vlan10      10   120    Active   local            10.1.1.3         10.1.1.5
     (conf)

!DC-2
N7K-C#

show hsrp br


*:IPv6 group   #:group belongs to a bundle
                      P indicates configured to preempt.
                      |
 Interface   Grp  Prio P State    Active addr      Standby addr     Group addr
  Vlan10      10   120    Active   local            10.1.1.3         10.1.1.5
     (conf)
```

Entrez cette commande dans l'interface de ligne de commande pour vérifier le filtre ARP :

<#root>

```
N7K-D#

show log log | i DUP_VADDR
```

```
2015 Apr 10 21:16:45 N7K-A %ARP-3-DUP_VADDR_SRC_IP:  arp [7915]  Source address of
 packet received from 0000.0c9f.f00a on Vlan10(port-channel102) is duplicate of local
 virtual ip, 10.1.1.5
```

Si une sortie similaire à celle-ci apparaît, alors les GARP entre les deux passerelles actives ne sont pas correctement isolés.

Isolement supplémentaire

Entrez la commande show spanning-tree root dans la CLI pour vérifier que la racine STP ne pointe pas vers le canal de port DCI :

<#root>

N7K-A#

show spanning-tree root

```
                                        Root  Hello Max Fwd
Vlan                 Root ID            Cost  Time  Age Dly  Root Port
---------------- -------------------- ------- ----- --- ---  ----------------
VLAN0010          4106 0023.04ee.be01       0    2   20  15  This bridge is root
```

Entrez cette commande dans l'interface de ligne de commande pour vérifier que le contrôle des tempêtes est correctement configuré :

<#root>

N7K-A#

show interface <DCI-Port-Channel> counters storm-control

```
--------------------------------------------------------------------------------
Port        UcastSupp %     McastSupp %     BcastSupp %     TotalSuppDiscards
--------------------------------------------------------------------------------
Po103            100.00          100.00            1.00                     0
```

Cryptage MACSec

Entrez cette commande dans l'interface de ligne de commande pour vérifier que le cryptage

MACSec est correctement configuré :

<#root>

```
N7K-A#

show cts interface <DCI-Physical-Port>


CTS Information for Interface Ethernet3/41:
...
    SAP Status:             CTS_SAP_SUCCESS
      Version: 1
      Configured pairwise ciphers: GCM_ENCRYPT
      Replay protection: Enabled
      Replay protection mode: Strict
      Selected cipher: GCM_ENCRYPT
      Current receive SPI: sci:e4c7220b98dc0000 an:0
      Current transmit SPI: sci:e4c7220b98d80000 an:0
...
```

Dépannage

Aucune information de dépannage spécifique n'est actuellement disponible pour le protocole FHRP ou les configurations d'isolation supplémentaires.

Pour la configuration MACSec, si la clé pré-partagée n'est pas convenue des deux côtés de la liaison, vous voyez un résultat semblable à celui-ci quand vous entrez la commande show interface <DCI-Physical-Port> dans la CLI :

<#root>

```
N7K-A#

show interface <DCI-Physical-Port>


Ethernet3/41 is down (Authorization pending)
admin state is up, Dedicated Interface
```

La clé doit être identique des deux côtés de la connexion.

Mises en garde

Ces avertissements sont liés à l'utilisation d'un DCI sur le commutateur Cisco Nexus 7000. Les mises en garde relatives aux produits connexes ne sont pas incluses.

- ID de bogue Cisco CSCur69114 - Filtre PACL HSRP rompu - Les paquets sont diffusés vers le domaine de couche 2. Ce bogue se trouve uniquement dans la version 6.2(10) du logiciel.
- ID de bogue Cisco CSCut75457 - Filtre VACL HSRP rompu. Ce bogue se trouve uniquement dans les versions 6.2(10) et 6.2(12) du logiciel.
- ID de bogue Cisco CSCut43413 - DCi : HSRP Virtual MAC Flapping via FHRP Isolation PACL. Ce bogue est dû à une limitation matérielle.

Informations connexes

- Solutions Cisco
- Introduction à la technologie OTV et considérations de déploiement
- Considérations de conception de la mobilité des charges de travail virtualisées Cisco
- Documentation et assistance techniques

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.