Configurez une interconnexion du centre de calculs de vpc de la couche 2 sur la gamme d'un Nexus 7000 commutent

Contenu

Introduction

Ce document décrit comment configurer une interconnexion de Data Center de la couche 2 (L2) (DCI) avec l'utilisation d'un Port canalisé virtuel (vpc).

Conditions préalables

On le suppose que le vpc et le protocole de routage de secours immédiat (HSRP) sont déjà configurés sur les périphériques qui sont utilisés dans les exemples fournis dans ce document.

> **Note**: Le Control Protocol d'agrégation de liaisons (LACP) devrait être utilisé sur le lien de vpc, qui agit en tant que DCI.

Conseil : Le chiffrement de MACSec exige un permis de Services avancés réseau local dans les versions avant la version 6.1(1) et a des limites de linecard-particularité. Référez-vous aux instructions et les limites pour la section de Cisco TrustSec du **guide de configuration de Sécurité de la gamme 7000 NX-OS de Cisco Nexus, libèrent 6.x** pour des informations supplémentaires.

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- vpc
- HSRP
- Protocole spanning-tree (STP)
- Cryptage de MACSec (facultatif)

Composants utilisés

Les informations dans ce document sont basées sur gamme 7000 de Cisco Nexus commutent que la version de logiciel de passages 6.2(8b).

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Le but d'un DCI est d'étendre la particularité VLAN entre différents centres de traitement des données, qui offre la contiguïté L2 pour les serveurs et les périphériques de stockage connecté au réseau (NAS) qui sont séparés par de grandes distances.

Le vpc présente l'avantage de l'isolation STP entre les deux sites (aucun Bridge Protocol Data Unit (BPDU) à travers le vpc DCI), ainsi aucune panne à un centre de traitement des données n'est propagée au centre de traitement des données distant parce que des liens redondants sont encore fournis entre les centres de traitement des données.

Note: Le vpc peut être utilisé afin d'interconnecter un maximum de deux centres de traitement des données. Si plus de deux centres de traitement des données doivent être interconnectés, Cisco recommande que vous utilisiez la virtualisation de transport de recouvrement (OTV).

Un EtherChannel de vpc DCI est typiquement configuré avec ces informations à l'esprit :

- D'abord isolation de Protocol de Redondance de saut (FHRP) : Empêchez le routage suboptimal avec l'utilisation d'une passerelle dédiée pour chaque centre de traitement des données. Les configurations varient la personne à charge sur l'emplacement de la passerelle FHRP.

- Isolation STP : Comme précédemment mentionné, ceci empêche la propagation des pannes d'un centre de traitement des données à l'autre.
- Contrôle de saturation de diffusion : Ceci est utilisé afin de réduire la quantité du trafic d'émission entre les centres de traitement des données.
- Cryptage de MACSec (facultatif) : Ceci chiffre le trafic afin d'empêcher l'intrusion entre les deux équipements.

Configurez

Utilisez les informations qui sont décrites dans cette section afin de configurer un L2 DCI avec l'utilisation d'un vpc.

> **Note**: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Isolation FHRP

Cette section décrit deux scénarios pour lesquels l'isolation FHRP peut être mise en application.

Double interconnexion de la ZONE L2/L3

C'est la topologie qui est utilisée dans ce scénario :

Dans ce scénario, la passerelle de la couche 3 (L3) est configurée sur les mêmes paires de vpc et agit en tant que DCI. Afin d'isoler le HSRP, vous devez configurer une liste de contrôle d'accès de port (PACL) sur le Port canalisé DCI et désactiver des protocoles ARP gratuits de HSRP (ARPs) (GARPs) relatif aux interfaces virtuelles commutées (SVI) pour les VLAN qui se déplacent à travers 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
```

> **Note**: La configuration précédente peut également être utilisée avec des Commutateurs du Nexus 9000.

Vpc multicouche pour l'agrégation et le DCI

C'est la topologie qui est utilisée dans ce scénario :

Dans ce scénario, le DCI est isolé sur son propre contexte du périphérique virtuel L2 (volts continu), et la passerelle L3 est sur un périphérique de couche d'agrégation. Afin d'isoler le HSRP, vous devez configurer une liste de contrôle d'accès VLAN (VACL) cette des blocs le trafic de contrôle de HSRP et un filtre d'inspection ARP qui bloque le HSRP GARPs sur le L2 DCI volts continu.

Voici un 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 supplémentaire d'isolation

Cette section fournit un exemple de configuration cela :

- Permet seulement les VLAN qui sont nécessaires au centre de traitement des données distant à étendre.
- Isole le STP à chaque centre de traitement des données.
- Relâche le trafic d'émission qui dépasse 1% de toute la vitesse de liaison.

Voici l'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
```

Note: Le contrôle de tempête pour le trafic de multidiffusion peut également être configuré, mais il doit avoir le même pourcentage que le trafic d'émission.

Cryptage de MACSec

Note: La configuration qui est décrite dans cette section est facultative.

Employez ces informations afin de configurer le cryptage de 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>
```

Note: L'interface doit être agitée pour que l'autorisation de MACSec se produise.

Vérifiez

Utilisez les informations qui sont décrites dans cette section afin de confirmer que votre configuration fonctionne correctement.

Isolation FHRP

Sélectionnez la commande de **Br de show hsrp** dans le CLI afin de vérifier que la passerelle de HSRP est en activité aux deux centres de traitement des données :

```
!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)
```

Sélectionnez cette commande dans le CLI afin de vérifier le filtre d'ARP :

```
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 un résultat semblable à ceci apparaît, alors le GARPs entre les deux passerelles actives n'est pas correctement isolé.

Isolation supplémentaire

Sélectionnez la commande de **show spanning-tree root** dans le CLI afin de vérifier que la racine STP ne se dirige pas vers le Port canalisé DCI :

```
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
```

Sélectionnez cette commande dans le CLI afin de vérifier que le contrôle de tempête est correctement configuré :

```
N7K-A# show interface <DCI-Port-Channel> counters storm-control

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

Cryptage de MACSec

Sélectionnez cette commande dans le CLI afin de vérifier que le cryptage de MACSec est correctement configuré :

```
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
...
```

Dépannez

Il n'y a actuellement aucune information de dépannage spécifique disponible pour le FHRP ou les configurations supplémentaires d'isolation.

Pour la configuration de MACSec, si la clé pré-partagée n'est pas convenue des deux côtés du lien, vous voyez un résultat semblable à ceci quand vous sélectionnez la commande de **<DCI-Physical-Port> d'interface d'exposition** dans le CLI :

```
N7K-A# show interface <DCI-Physical-Port>
Ethernet3/41 is down (Authorization pending)
admin state is up, Dedicated Interface
```

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

Mises en garde

Note: Des mises en garde pour les produits connexes ne sont pas incluses.

Ces mises en garde sont liées à l'utilisation d'un DCI sur la gamme 7000 de Cisco Nexus commutent :

- ID de bogue Cisco CSCur69114 - *Filtre du HSRP PACL cassé - Des paquets sont inondés au domaine layer2*. Cette bogue est trouvée seulement dans la version de logiciel 6.2(10).
- ID de bogue Cisco CSCut75457 - *Filtre du HSRP VACL cassé*. Cette bogue est trouvée seulement dans les versions de logiciel 6.2(10) et 6.2(12).
- ID de bogue Cisco CSCut43413 - *DCi : Lien instable virtuel de MAC de HSRP par l'isolation PACL FHRP*. Cette bogue est due à une limitation matérielle.

Informations connexes

- Conceptions de Data Center : Interconnexion de Data Center
- Considérations d'introduction et de déploiement de technologie OTV
- Cisco a virtualisé des considérations de conception de mobilité de charge de travail
- Support et documentation techniques - Cisco Systems