Configure una interconexión del centro de datos del vPC de la capa 2 en un 7000 Series Switch del nexo

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Antecedentes
Configurar
Aislamiento FHRP
Interconexión dual de la VAINA L2/L3
VPC de múltiples capas para la agregación y DCI
Configuración adicional del aislamiento
Cifrado de MACSec
Verificación
Aislamiento FHRP
Aislamiento adicional
Cifrado de MACSec
Troubleshooting
Advertencias
Información Relacionada

Introducción

Este documento describe cómo configurar una interconexión del centro de datos de la capa 2 (L2) (DCI) con el uso de un canal del puerto virtual (vPC).

Prerrequisitos

Se asume que el vPC y el Hot Standby Routing Protocol (HSRP) están configurados ya en los dispositivos que se utilizan en los ejemplos proporcionados en este documento.

> Nota: El protocolo link aggregation control (LACP) se debe utilizar en el link del vPC, que actúa como el DCI.

> Consejo: El cifrado de MACSec requiere una licencia del Advanced Services LAN en las versiones antes de la versión 6.1(1) y tiene limitaciones linecard-específicas. Refiera a las guías de consulta y a las limitaciones para la sección de Cisco TrustSec de la **guía de configuración de seguridad de las 7000 Series NX-OS del nexo de Cisco, la versión 6.x** para la información adicional.

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- vPC
- HSRP
- Spanning-Tree Protocol (STP)
- Cifrado de MACSec (opcional)

Componentes Utilizados

La información en este documento se basa en un 7000 Series Switch del nexo de Cisco que funcione con la versión de software 6.2(8b).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

El propósito de un DCI es ampliar los VLA N específicos entre diversos centros de datos, que ofrece la adyacencia L2 para los servidores y los dispositivos del Almacenamiento conectado a la red (NAS) que son separados por las distancias grandes.

El vPC presenta la ventaja del aislamiento STP entre los dos sitios (ningún (BPDU) de la Unidad de bridge protocol data a través del vPC DCI), así que ninguna caída del sistema en un centro de datos no se propaga al centro de datos remotos porque los links redundantes todavía se proporcionan entre los centros de datos.

> Nota: El vPC se puede utilizar para interconectar un máximo de dos centros de datos. Si más de dos centros de datos deben ser interconectados, Cisco recomienda que usted utiliza la virtualización del transporte del recubrimiento (OTV).

Un EtherChannel del vPC DCI se configura típicamente con esta información en la mente:

- Primer aislamiento del protocolo de la redundancia de salto (FHRP): Prevenga el ruteo por debajo del nivel óptimo con el uso de un gateway dedicado para cada centro de datos. Las configuraciones varían al dependiente sobre la ubicación del gateway FHRP.

- Aislamiento STP: Como se mencionó anteriormente, esto previene la propagación de las

caídas del sistema a partir de un centro de datos a otro.

- Control de la tormenta de broadcast: Esto se utiliza para minimizar la cantidad de tráfico de broadcast entre los centros de datos.
- Cifrado de MACSec (opcional): Esto cifra el tráfico para prevenir la intrusión entre los dos recursos.

Configurar

Utilice la información que se describe en esta sección para configurar un L2 DCI con el uso de un vPC.

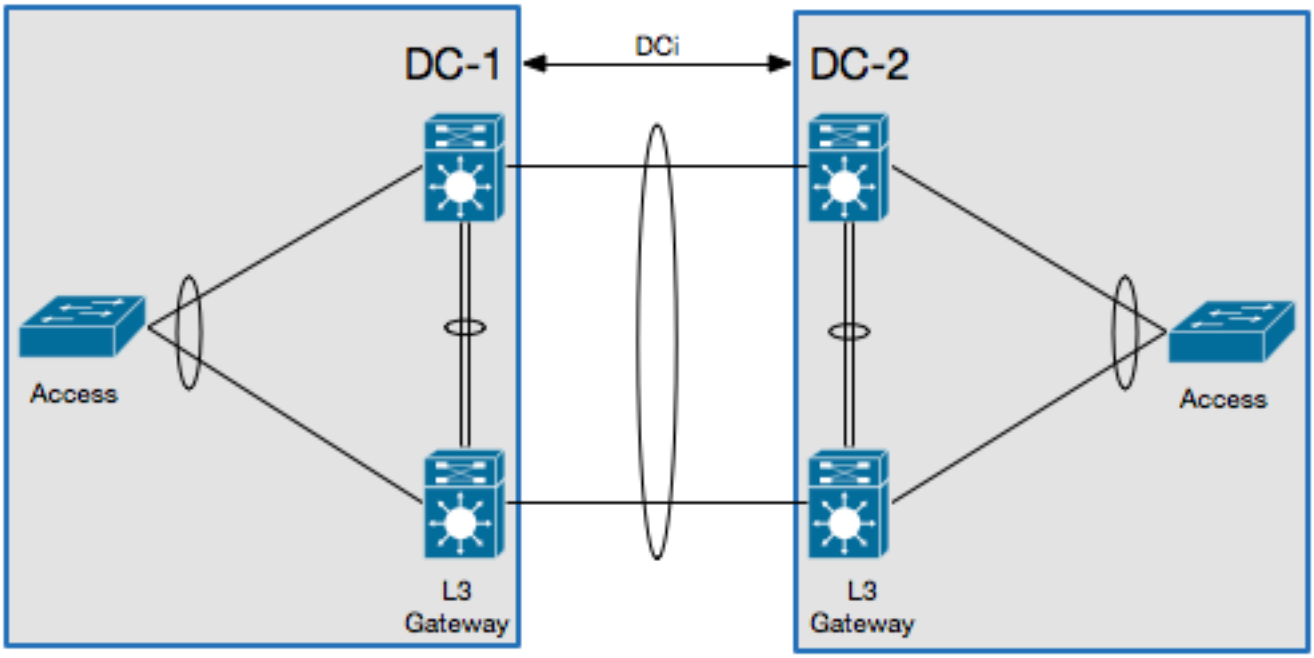
> Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Aislamiento FHRP

Esta sección describe dos escenarios para los cuales el aislamiento FHRP pueda ser implementado.

Interconexión dual de la VAINA L2/L3

Ésta es la topología que se utiliza en este escenario:



En este escenario, el gateway de la capa 3 (L3) se configura en los mismos pares del vPC y actúa como el DCI. Para aislar el HSRP, usted debe configurar una lista de control de acceso del puerto (PACL) en el canal del puerto DCI y inhabilitar los protocolos Protocolo de resolución de la dirección (ARP) gratuitos del HSRP (ARP) (GARP) en las interfaces virtuales conmutadas (SVI)

para los VLA N que se mueven a través del DCI.

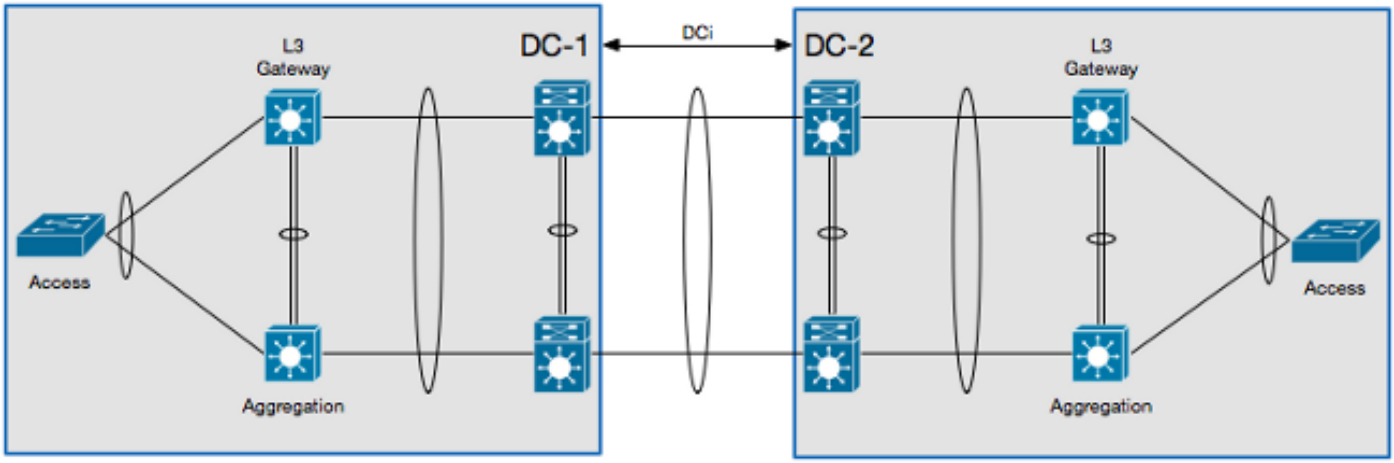
Aquí está un ejemplo de configuración:

```
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
```

Nota: La configuración previa se puede también utilizar con los 9000 Switch del nexo.

VPC de múltiples capas para la agregación y DCI

Ésta es la topología que se utiliza en este escenario:



En este escenario, el DCI se aísla en su propio contexto del dispositivo virtual L2 (VDC), y el gateway L3 está en un dispositivo de la capa de la agregación. Para aislar el HSRP, usted debe configurar un VLAN Access Control List (VACL) ese los bloques el tráfico de control del HSRP y un filtro de la inspección ARP que bloquee el HSRP GARP en el L2 DCI VDC.

Aquí está un ejemplo de configuración:

```
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>
```

Configuración adicional del aislamiento

Esta sección proporciona un ejemplo de configuración eso:

- Permite solamente los VLA N que son necesarios en el centro de datos remotos que se extenderá.
- Aísla el STP en cada centro de datos.
- Cae el tráfico de broadcast que excede el 1% de la velocidad del link total.

Aquí está el ejemplo de configuración:

```
 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
```

> Nota: El control de tormentas para el tráfico Multicast puede también ser configurado, pero debe tener el mismo porcentaje que el tráfico de broadcast.

Cifrado de MACSec

> Nota: La configuración que se describe en esta sección es opcional.

Utilice esta información para configurar el cifrado 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>
```

Nota: La interfaz se debe agitar para que la autorización de MACSec ocurra.

Verificación

Utilice la información que se describe en esta sección para confirmar que su configuración trabaja correctamente.

Aislamiento FHRP

Ingrese el comando del **Br del hsrp de la demostración** en el CLI para verificar que el gateway del HSRP es activo en ambos centros de datos:

```
!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)
```

Ingrese este comando en el CLI para verificar el filtro 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 aparece una salida similar a esto, después los GARP entre los dos gatewayes activos no se aíslan correctamente.

Aislamiento adicional

Ingrese el comando de la **raíz del árbol de expansión de la demostración** en el CLI para verificar que la raíz STP no señala hacia el canal del puerto 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
```

Ingrese este comando en el CLI para verificar que el control de tormentas está configurado correctamente:

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

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

Cifrado de MACSec

Ingrese este comando en el CLI para verificar que el cifrado de MACSec está configurado correctamente:

```
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
...
```

Troubleshooting

No hay actualmente información de Troubleshooting específica disponible para el FHRP o las configuraciones adicionales del aislamiento.

Para la configuración de MACSec, si la clave previamente compartida no se conviene en a ambos lados del link, usted ve una salida similar a esto cuando usted ingresa el comando del **<DCI-Physical-Port> de la interfaz de la demostración** en el CLI:

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

> Nota: La clave debe ser lo mismo a ambos lados de la conexión.

Advertencias

> Nota: Las advertencias para los Productos relacionados no son incluidas.

Estas advertencias se relacionan con el uso de un DCI en el 7000 Series Switch del nexo de Cisco:

- Id. de bug Cisco CSCur69114 - *Filtro del HSRP PACL roto - Los paquetes se inundan al dominio layer2*. Este bug se encuentra solamente en la versión de software 6.2(10).
- Id. de bug Cisco CSCut75457 - *Filtro del HSRP VACL roto*. Este bug se encuentra solamente en las versiones de software 6.2(10) y 6.2(12).

- Id. de bug Cisco CSCut43413 - *DCi: Cambio del MAC virtual HSRP con el aislamiento PACL FHRP*. Este bug es debido a una limitación del hardware.

Información Relacionada

- Diseños del centro de datos: Interconexión del centro de datos
- Introducción a la tecnología y consideraciones sobre la instrumentación OTV
- Cisco virtualizó los aspectos del diseño de la movilidad de la carga de trabajo
- Soporte Técnico y Documentación - Cisco Systems