Konfigurieren eines Layer-2-vPC-Rechenzentrums-Interconnects auf einem Nexus-Switch der Serie 7000

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration eines Layer 2 (L2) Data Center Interconnects (DCI) mithilfe eines Virtual Port-Channels (vPC) beschrieben.

Voraussetzungen

Es wird davon ausgegangen, dass vPC und Hot Standby Routing Protocol (HSRP) bereits auf den Geräten konfiguriert sind, die in den in diesem Dokument enthaltenen Beispielen verwendet werden.

Verwenden Sie das Link Aggregation Control Protocol (LACP) für die vPC-Verbindung, die als DCI fungiert.

Tipp: Für die MACSec-Verschlüsselung ist eine LAN Advanced Services-Lizenz in Versionen vor Version 6.1(1) erforderlich, und sie unterliegt spezifischen Einschränkungen für Linecards. Weitere Informationen finden Sie im Abschnitt Richtlinien und Einschränkungen für Cisco TrustSec im Cisco Nexus 7000 Serie NX-OS Security Configuration Guide, Release 6.x.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- vPC
- HSRP
- Spanning Tree Protocol (STP)
- MACSec-Verschlüsselung (optional)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einem Cisco Nexus Switch der Serie 7000, auf dem die Softwareversion 6.2(8b) ausgeführt wird.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

Der Zweck eines DCI besteht in der Erweiterung spezifischer VLANs zwischen verschiedenen Rechenzentren, wodurch L2-Adjacency für Server und Network-Attached Storage (NAS)-Geräte bereitgestellt wird, die durch große Entfernungen voneinander getrennt sind.

Der vPC bietet den Vorteil der STP-Isolierung zwischen den beiden Standorten (keine Bridge Protocol Data Unit (BPDU) über den DCI-vPC), sodass Ausfälle in einem Rechenzentrum nicht an das Remote-Rechenzentrum weitergegeben werden, da zwischen den Rechenzentren weiterhin redundante Verbindungen bestehen.

Verwenden Sie den vPC, um maximal zwei Rechenzentren miteinander zu verbinden. Wenn mehr als zwei Rechenzentren miteinander verbunden werden müssen, verwenden Sie Overlay Transport Virtualization (OTV).

Ein DCI-vPC-EtherChannel wird in der Regel mit folgenden Informationen konfiguriert:

- First Hop Redundancy Protocol (FHRP)-Isolierung: Vermeiden Sie suboptimales Routing mit einem dedizierten Gateway für jedes Rechenzentrum. Die Konfigurationen variieren je nach Standort des FHRP-Gateways.
- STP-Isolierung: Wie bereits erwähnt, verhindert dies die Übertragung von Ausfällen von einem Rechenzentrum auf ein anderes.
- Broadcast-Sturmkontrolle: Dadurch wird der Broadcast-Datenverkehr zwischen den Rechenzentren minimiert.
- MACSec-Verschlüsselung (optional): Diese verschlüsselt den Datenverkehr, um ein Eindringen zwischen den beiden Einrichtungen zu verhindern.

Konfigurieren

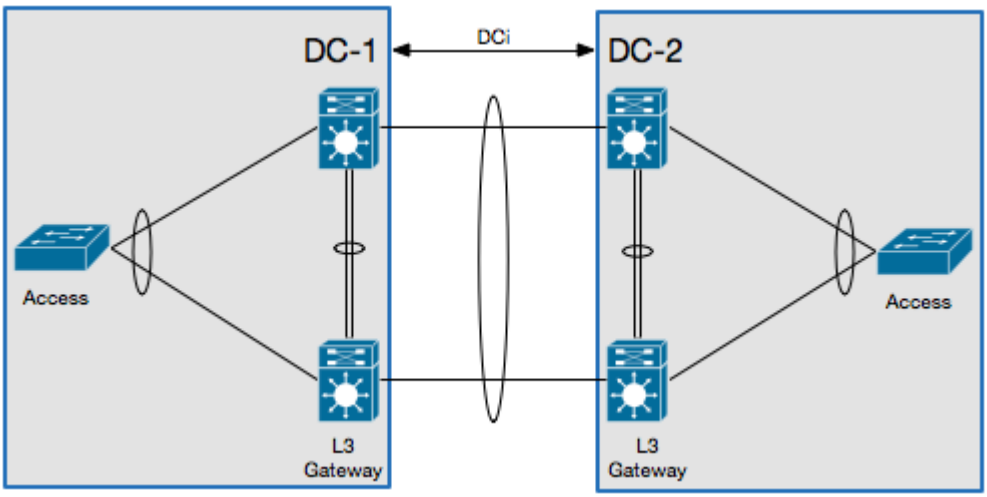
Verwenden Sie die in diesem Abschnitt beschriebenen Informationen, um eine L2-DCI unter Verwendung eines vPC zu konfigurieren. Registrierte Kunden können das Command Lookup Tool verwenden, um weitere Informationen zu den hier verwendeten Befehlen abzurufen.

FHRP-Isolierung

In diesem Abschnitt werden zwei Szenarien beschrieben, in denen die FHRP-Isolierung implementiert werden kann.

Dual-L2/L3-POD-Verbindung

In diesem Szenario wird die folgende Topologie verwendet:



In diesem Szenario wird das Layer 3 (L3)-Gateway auf demselben vPC-Paar konfiguriert und fungiert als DCI. Um das HSRP zu isolieren, müssen Sie eine Port Access Control List (PACL) auf dem DCI-Port-Channel konfigurieren und HSRP Gratis Address Resolution Protocols (ARPs) (GARPs) auf den Switched Virtual Interfaces (SVIs) für die VLANs deaktivieren, die über den DCI verschoben werden.

Nachfolgend finden Sie ein Beispiel für eine Konfiguration:

```
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

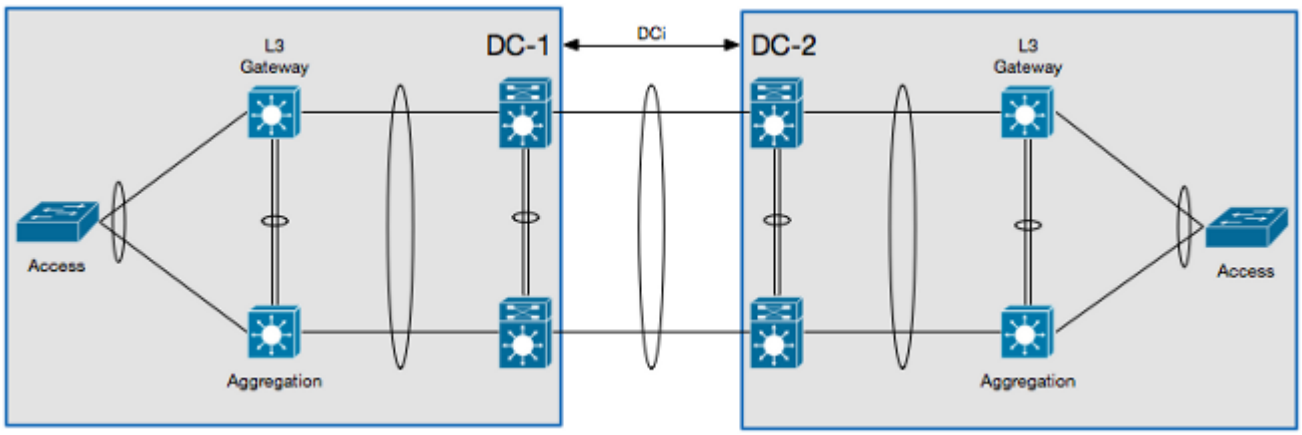
interface <DCI-Port-Channel>
  ip port access-group DENY_HSRP_IP in

interface Vlan <x>
```

```
  no ip arp gratuitous hsrp duplicate
```

Multilayer vPC für Aggregation und DCI

In diesem Szenario wird die folgende Topologie verwendet:



In diesem Szenario wird die DCI in ihrem eigenen L2 Virtual Device Context (VDC) isoliert, und das L3-Gateway befindet sich auf einem Aggregation Layer-Gerät. Um das HSRP zu isolieren, konfigurieren Sie eine VLAN Access Control List (VACL), die den HSRP-Steuerungsdatenverkehr blockiert, und einen ARP-Inspektionsfilter, der die HSRP-GARPs im L2 DCI-VDC blockiert. Beispielkonfiguration:

```
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>
```

Zusätzliche Isolationskonfiguration

In diesem Abschnitt finden Sie ein Beispiel für eine Konfiguration, die:

- Ermöglicht die Erweiterung nur der VLANs, die im Remote-Rechenzentrum benötigt werden
- Isolierung des STP in jedem Rechenzentrum
- Sendet Datenverkehr, der 1 % der Gesamtverbindungsgeschwindigkeit übersteigt.

Beispielkonfiguration:

```
 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
```

Die Sturmkontrolle für Multicast-Datenverkehr kann ebenfalls konfiguriert werden, muss jedoch denselben Prozentsatz wie der Broadcast-Datenverkehr aufweisen.

MACSec-Verschlüsselung

Die in diesem Abschnitt beschriebene Konfiguration ist optional.

Verwenden Sie diese Informationen, um die MACSec-Verschlüsselung zu konfigurieren:

```
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>
```

Setzen Sie eine Markierung für die Schnittstelle, damit eine MACSec-Autorisierung erfolgt.

Überprüfung

Verwenden Sie die in diesem Abschnitt beschriebenen Informationen, um sicherzustellen, dass Ihre Konfiguration ordnungsgemäß funktioniert.

FHRP-Isolierung

Geben Sie den Befehl show hsrp br in die CLI ein, um zu überprüfen, ob das HSRP-Gateway in beiden Rechenzentren aktiv ist:

<#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)
```

Geben Sie den folgenden Befehl in die CLI ein, um den ARP-Filter zu überprüfen:

<#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
```

Tritt eine ähnliche Ausgabe auf, werden die GARPs zwischen den beiden aktiven Gateways nicht richtig isoliert.

Zusätzliche Isolierung

Geben Sie den Befehl show spanning-tree root in die CLI ein, um zu überprüfen, ob der STP-Root nicht auf den DCI-Port-Channel zeigt:

<#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
```

Geben Sie den folgenden Befehl in die CLI ein, um zu überprüfen, ob die Sturmkontrolle ordnungsgemäß konfiguriert ist:

<#root>

N7K-A#

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

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

MACSec-Verschlüsselung

Geben Sie diesen Befehl in die CLI ein, um zu überprüfen, ob die MACSec-Verschlüsselung ordnungsgemäß konfiguriert ist:

<#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
...
```

Fehlerbehebung

Derzeit stehen keine spezifischen Informationen zur Fehlerbehebung für das FHRP oder zusätzliche Isolationskonfigurationen zur Verfügung.

Wenn bei der MACSec-Konfiguration der Pre-Shared Key auf beiden Seiten der Verbindung nicht vereinbart wurde, wird eine ähnliche Ausgabe angezeigt, wenn Sie den Befehl show interface <DCI-Physical-Port> in die CLI eingeben:

<#root>

```
N7K-A#

show interface <DCI-Physical-Port>


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

Der Schlüssel muss auf beiden Seiten der Verbindung gleich sein.

Hinweise

Diese Vorbehalte beziehen sich auf die Verwendung eines DCI auf einem Cisco Nexus Switch der Serie 7000. Rückstände für verwandte Produkte sind nicht enthalten.

- Cisco Bug-ID CSCur69114 - HSRP PACL Filter Broken - Pakete werden an die Layer-2-Domäne geflutet. Dieser Fehler wurde nur in der Softwareversion 6.2(10) gefunden.
- Cisco Bug-ID CSCut75457 - HSRP VACL-Filter beschädigt. Dieser Fehler wurde nur in den Softwareversionen 6.2(10) und 6.2(12) gefunden.
- Cisco Bug-ID CSCut43413 - DCi: HSRP Virtual MAC Flapping über FHRP Isolation PACL. Dieser Fehler ist auf eine Hardwarebeschränkung zurückzuführen.

Zugehörige Informationen

- Cisco Lösungen
- OTV-Technologie - Einführung und Bereitstellung
- Cisco Virtualized Workload Mobility - Überlegungen zum Design
- Technischer Support und Dokumentation

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.