تكوين اتصال مركز البيانات من المستوى الثاني عبر الكمبيوتر الشخصي (vPC) على محول من السلسلة Nexus 7000

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
التكوين
عزل FHRP
الربط المزدوج L2/L3 POD
PC متعدد الطبقات للتجميع و DCI
تكوين عزل إضافي
تشفير MACSec
التحقق من الصحة
عزل FHRP
عزل إضافي
تشفير MACSec
استكشاف الأخطاء وإصلاحها
كافيتس
معلومات ذات صلة

المقدمة

يوضح هذا المستند كيفية تكوين اتصال مركز البيانات البيني (DCI) من الطبقة 2 (L2) باستخدام تقنية Virtual Port-Channel (vPC).

المتطلبات الأساسية

يفترض أنه تم تكوين بروتوكول vPC وبروتوكول التوجيه الاحتياطي الفعال (HSRP) بالفعل على الأجهزة التي يتم إستخدامها في الأمثلة الواردة في هذا المستند.

ملاحظة: يجب إستخدام بروتوكول التحكم في تجميع الارتباطات (LACP) على إرتباط vPC، الذي يعمل كمعرف فئة المورد (DCI).

تلميح: يتطلب تشفير MACec ترخيص خدمات LAN المتقدمة في الإصدارات قبل الإصدار 6.1(1) ولها قيود خاصة ببطاقة الخط. ارجع إلى قسم المبادئ التوجيهية والحدود الخاصة ببروتوكول Cisco TrustSec من **دليل تكوين أمان نظام التشغيل NX7000 Series من Cisco NX، الإصدار x.6** للحصول على معلومات إضافية.

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- vPC
- HSRP
- بروتوكول الشجرة الممتدة (STP)
- تشفير MACSec (إختياري)

المكونات المستخدمة

أسست المعلومة في هذا وثيقة على cisco Nexus 7000 sery مفتاح أن يركض برمجية صيغة 6.2(8b).

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

والغرض من معرف فئة المورد (DCI) هو توسيع شبكات VLAN معينة بين مراكز البيانات المختلفة، مما يوفر تجاور المستوى الثاني للخوادم وأجهزة التخزين المتصلة بالشبكة (NAS) التي يتم فصلها بمسافات كبيرة.

يقدم الكمبيوتر vPC ميزة عزل بروتوكول الشجرة المتفرعة (STP) بين الموقعين (لا توجد وحدة بيانات لبروتوكول الجسر (BPDU) عبر بطاقة DCI vPC)، وبالتالي لا يتم نشر أي أعطال في مركز البيانات عن بعد لمركز البيانات لأن الارتباطات المتكررة لا تزال متوفرة بين مراكز البيانات.

ملاحظة: يمكن إستخدام الكمبيوتر الشخصي vPC للربط بين مركزي بيانات كحد أقصى. إذا كان يجب ربط أكثر من مركزين للبيانات، فإن Cisco توصيك باستخدام المحاكاة الظاهرية للنقل العشوائي (OTV).

يتم تكوين قناة EtherChannel لمعرف فئة المورد (DCI) بشكل نموذجي مع وضع هذه المعلومات في الاعتبار:

- عملية عزل بروتوكول تكرار الخطوة الأولى (FHRP): منع التوجيه دون الأمثل باستخدام عبارة مخصصة لكل مركز بيانات. تختلف التكوينات باختلاف موقع بوابة FHRP.

- عزل بروتوكول الشجرة المتفرعة (STP): كما سبق ذكره، يؤدي ذلك إلى منع انتشار حالات انقطاع الاتصال من مركز بيانات إلى آخر.

- التحكم في سرعة البث: يتم إستخدام هذا الأمر لتقليل مقدار حركة مرور البث بين مراكز البيانات إلى الحد الأدنى.

- تشفير MACec (إختياري): يعمل هذا على تشفير حركة المرور لمنع التسلل بين المنفذين.

التكوين

أستخدم المعلومات الموضحة في هذا القسم لتكوين DCI من المستوى الثاني باستخدام vPC.

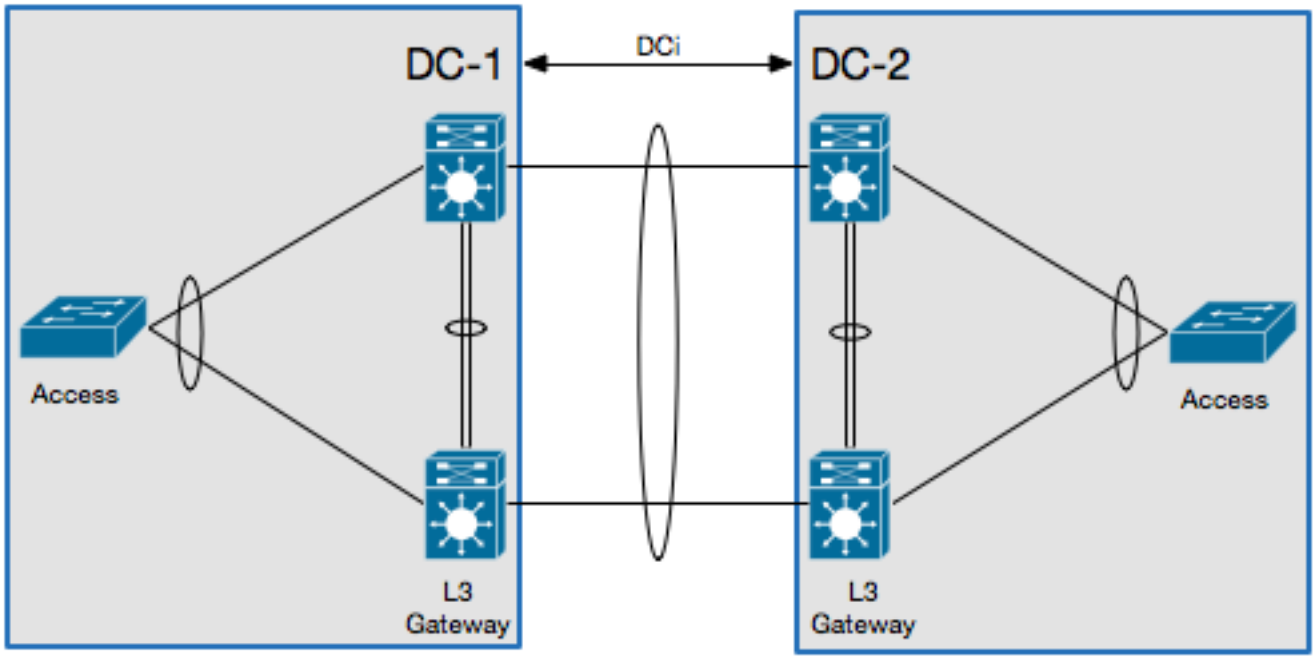
ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

عزل FHRP

يصف هذا القسم سيناريوهين يمكن تنفيذ عزل FHRP بشأنهما.

الربط المزدوج L2/L3 POD

هذه هي الطوبولوجيا المستخدمة في هذا السيناريو:



في هذا السيناريو، يتم تكوين بوابة الطبقة 3 (L3) على زوج vPC نفسه وتعمل كمعرف فئة المورد (DCI). لعزل HSRP، أنت ينبغي شكلت ميناء منفذ تحكم قائمة (PACL) على ال DCI ميناء-channel وأعجزت HSRP يتطلب عنوان بروتوكول (GARPs) (ARP) على ال يحول قارن فعلي (SVIs) ل VLANs أن ينتقل عبر ال DCI.

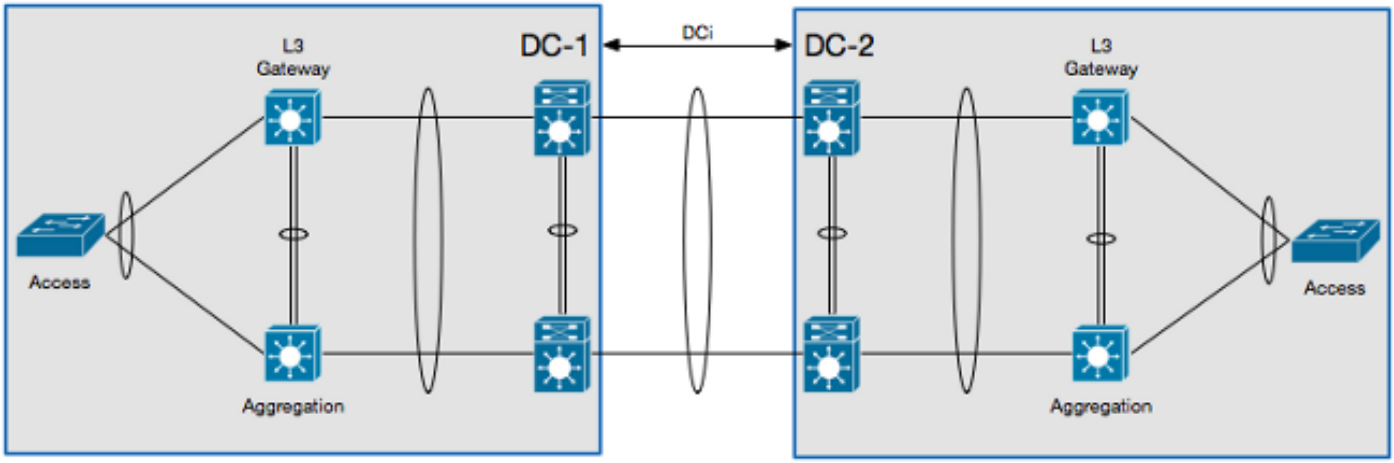
هنا مثال على التكوين:

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

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

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

ملاحظة: يمكن أيضا إستخدام التكوين السابق مع محولات Nexus 9000.

PC متعدد الطبقات للتجميع و DCI

هذه هي الطوبولوجيا المستخدمة في هذا السيناريو:



في هذا السيناريو، يتم عزل DCI على سياق الجهاز الظاهري (VDC) الخاص به من المستوى الثاني، وتكون بوابة L3 على جهاز طبقة تجميع. لعزل HSRP، يجب تكوين قائمة تحكم في الوصول إلى شبكة VLAN (VACL) التي تمنع حركة مرور التحكم في HSRP وعامل تصفية فحص ARP الذي يمنع HSRP GARP على L2 DCI VDC.

هنا مثال على التكوين:

```
ip access-list ALL_IPs
  permit ip any any 10
mac access-list ALL_MACs
  permit any any 10
ip access-list HSRP_IP
  permit udp any 224.0.0.2/32 eq 1985 10
  permit udp any 224.0.0.102/32 eq 1985 20
mac access-list HSRP_VMAC
  permit 0000.0c07.ac00 0000.0000.00ff any 10
  permit 0000.0c9f.f000 0000.0000.0fff any 20
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
  deny ip any mac 0000.0c07.ac00 ffff.ffff.ff00 10
  deny ip any mac 0000.0c9f.f000 ffff.ffff.f000 20
  permit ip any mac any 30

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

تكوين عزل إضافي

يقدم هذا القسم مثالا للتكوين الذي:

- يسمح فقط ال VLANs أن يكون احتجت في مركز البيانات بعيد أن يكون مددت.
- يعزل بروتوكول الشجرة المتفرعة (STP) في كل مركز بيانات.
- تسقط حركة مرور البث التي تتجاوز 1٪ من إجمالي سرعة الارتباط.

هنا مثال تشكيل:

```
<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
```

ملاحظة: يمكن أيضا تكوين التحكم في العواصف لحركة مرور البث المتعدد، ولكن يجب أن تحتوي على نفس النسبة المئوية لحركة مرور البث.

تشفير MACSec

ملاحظة: التكوين الموضح في هذا القسم إختياري.

أستخدم هذه المعلومات لتكوين تشفير 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
```

ملاحظة: يجب نفض الواجهة لإجراء تفويض MACec.

التحقق من الصحة

أستخدم المعلومات الموضحة في هذا القسم للتأكد من أن التكوين لديك يعمل بشكل صحيح.

عزل FHRP

دخلت **العرض hsrp br** أمر في ال CLI in order to دققت أن ال HSRP مدخل يكون نشط في كلا مركز معطيات:

```
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)
```

دخلت هذا أمر في ال CLI in order to دققت ال ARP مرشح:

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

إذا ظهرت مخرجات مماثلة لهذا، فلا يتم عزل GARPs بين العبارتين النشيطتين بشكل صحيح.

عزل إضافي

أدخل الأمر **show spanning-tree root** في واجهة سطر الأوامر (CLI) للتحقق من أن جذر بروتوكول الشجرة المتفرعة (STP) لا يشير إلى موجه أمر DCI port-channel:

```
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
```

أدخل هذا الأمر في واجهة سطر الأوامر (CLI) للتحقق من تكوين التحكم في العاصفة بشكل صحيح:

```
N7K-A# show interface

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

تشفير MACSec

أدخل هذا الأمر في واجهة سطر الأوامر (CLI) للتحقق من تكوين تشفير MACec بشكل صحيح:

```
N7K-A# show cts interface

: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
...
```

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليا معلومات محددة حول أستكشاف الأخطاء وإصلاحها لتكوينات FHRP أو تكوينات عزل إضافية.

لتكوين MACec، إذا لم يتم الاتفاق على المفتاح المشترك مسبقا على كلا جانبي الارتباط، سترى مخرجات مماثلة لهذا عند إدخال الأمر **show interface <dci-physical-port>** في واجهة سطر الأوامر:

```
N7K-A# show interface

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

ملاحظة: يجب أن يكون المفتاح نفسه على كلا جانبي الاتصال.

كافيتس

ملاحظة: لا يتم تضمين التنبيهات الخاصة بالمنتجات ذات الصلة.

تتصل هذه التحذيرات باستخدام DCI على المحول Cisco Nexus 7000 Series Switch:

- معرف تصحيح الأخطاء من Cisco CSCur69114 - *تعطل عامل تصفية حزم HSRP - يتم تدفق الحزم إلى مجال الطبقة 2*. يوجد هذا الخطأ فقط في الإصدار 6.2(10) من البرنامج.

- معرف تصحيح الأخطاء من Cisco CSCut75457 - *تم تعطيل عامل تصفية HSRP VACL*. يوجد هذا الخطأ فقط في إصدارات البرنامج 6.2(10) و 6.2(12).

- معرف تصحيح الأخطاء من *DCi: HSRP Virtual MAC Flapping* - Cisco CSCut43413 *من خلال FHRP Isolation PACL*. يرجع هذا الخطأ إلى حد في الجهاز.

معلومات ذات صلة

- تصميمات مركز البيانات: اتصال مركز البيانات الداخلي
- اعتبارات تقديم ونشر تقنية OTV
- اعتبارات تصميم إمكانية تنقل أحمال العمل الافتراضية من Cisco
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).