

Explicación y configuración del vPC de Nexus 9000 con las prácticas recomendadas

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Descripción y terminología de vPC](#)

[Ventajas técnicas de vPC](#)

[Ventajas arquitectónicas y operativas de vPC](#)

[Aspectos de redundancia de hardware y software vPC](#)

[Configuración de vPC EVPN VXLAN](#)

[Diagrama de la red](#)

[Verificación](#)

[Troubleshoot](#)

[Configuración del Fabric Peering vPC](#)

[Diagrama de la red](#)

[Verificación](#)

[Configuración de vPC de doble cara](#)

[Diagrama de la red](#)

[Configuración de vPC de doble cara con Fabric Peering vPC](#)

[Diagrama de la red](#)

[Troubleshoot](#)

[Prácticas recomendadas para ISSU con vPC](#)

[Recomendaciones enérgicas](#)

[Prácticas recomendadas durante la sustitución del switch vPC](#)

[Comprobaciones previas](#)

[Pasos](#)

[Comprobación posterior a la validación](#)

[Consideraciones sobre vPC para la implementación de VXLAN](#)

[Recomendaciones enérgicas](#)

[Información Relacionada](#)

Introducción

Este documento describe las mejores prácticas para utilizar canales de puerto virtuales (vPC) en los switches de Cisco Nexus de la serie 9000 (9k).

Prerequisites

Requirements

- Requisitos de licencia de NX-OS para vPC
- La función vPC se incluye en la licencia de software NX-OS básica.

El protocolo de router con espera en caliente (HSRP), el protocolo de redundancia de router virtual (VRRP) y el protocolo de control de agregación de enlaces (LACP) también se incluyen en esta licencia básica.

Las funciones de capa 3, como el protocolo OSPF (Open Shortest Path First) o el protocolo ISIS (Intermediate-System-to-Intermediate System), requieren una licencia LAN_ENTERPRISE_SERVICES_PKG.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Nexus93180YC-FX que ejecuta la versión 10.2(3)
- Cisco Nexus93180YC-FX que ejecuta la versión 10.2(3)

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

| Terms | Meaning |
|-------------------------|--|
| vPC | The combined port-channel between the vPC peers and the downstream device. A vPC is a L2 port type: switchport mode trunk or switchport mode access. |
| vPC peer device | A vPC switch (one of a Cisco Nexus 9000 Series pair). |
| vPC Domain | Domain containing the 2 peer devices. Only 2 peer devices max can be part of the same vPC domain. |
| vPC Member port | One of a set of ports (that is. Port-channels) that form a vPC (or port-channel member of a vPC). |
| vPC Peer-link | Link used to synchronize the state between vPC peer devices. It must be a 10-Gigabit Ethernet Link. vPC peer-link is a L2 trunk carrying vPC VLAN. |
| vPC Peer-keepalive link | The keepalive link between vPC peer devices; this link is used to monitor the liveness of the peer device. |
| vPC VLAN | VLAN carried over the peer-link. |

El análisis de estructuras vPC proporciona una solución de acceso de doble reposición mejorada sin la sobrecarga de los puertos físicos de desecho para el enlace de par vPC.

Antecedentes

Este documento se aplica a:

- Nexus 9000 vPC
- vPC con Vxlan
- Fabric Peering vPC
- vPC de doble cara
- vPC virtual de doble cara

Este documento también trata las operaciones de actualización de software en funcionamiento (ISSU) relacionadas con vPC y ofrece detalles sobre las últimas mejoras de vPC (retraso en la restauración, temporizadores de interfaz virtual de red (NVE)).

Descripción y terminología de vPC

vPC es una tecnología de virtualización que presenta los dos dispositivos emparejados Nexus de Cisco serie 9000 como un nodo lógico de capa 2 exclusivo para acceder a los terminales o dispositivos de capa 2.

vPC pertenece a la familia de tecnologías Multichassis EtherChannel (MCEC). Un canal de puerto virtual (vPC) permite que los enlaces que están conectados físicamente a dos dispositivos Cisco Nexus serie 9000 diferentes aparezcan como un único canal de puerto para un tercer dispositivo.

El tercer dispositivo puede ser un switch, un servidor o cualquier otro dispositivo de red compatible con la tecnología de agregación de enlaces.

Ventajas técnicas de vPC

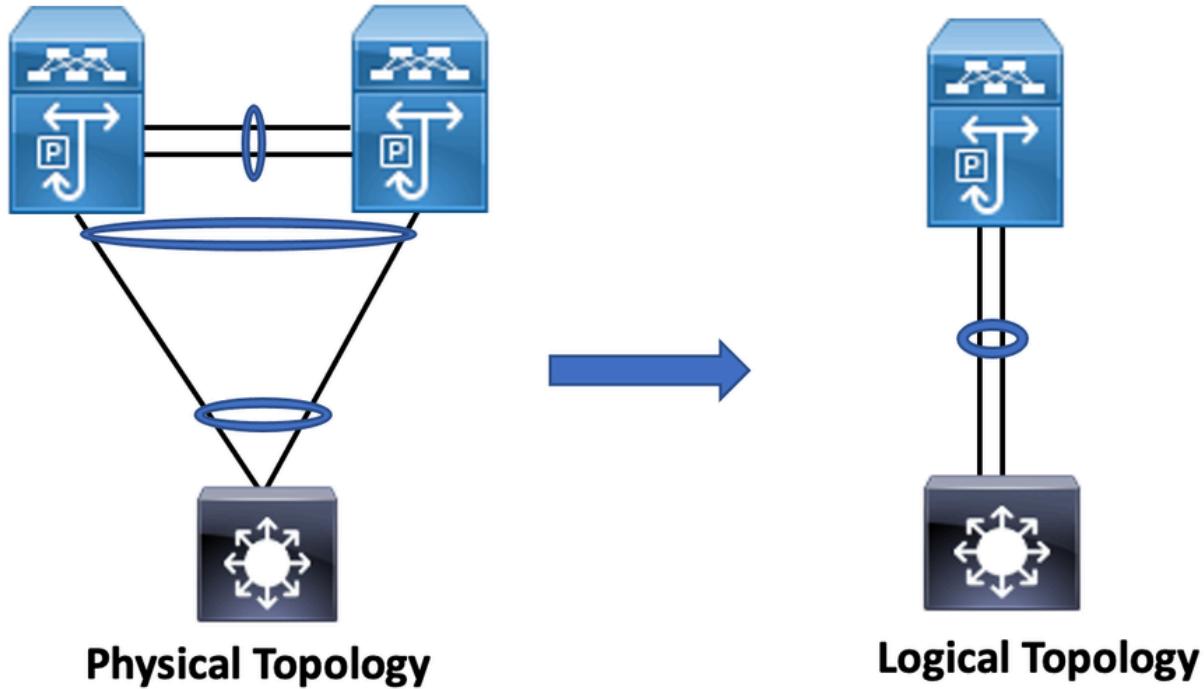
vPC proporciona estas ventajas técnicas:

- Elimina los puertos bloqueados por el protocolo de árbol de extensión (STP).
- Utiliza todo el ancho de banda de enlace ascendente disponible.
- Permite que los servidores doblemente conectados funcionen en modo activo-activo.
- Proporciona convergencia rápida ante fallos de enlaces o dispositivos.
- Ofrece gateways predeterminados duales activo/activo para servidores vPC. También aprovecha la gestión nativa de split horizon/loop proporcionada por la tecnología de canalización de puertos: un paquete viene cuando un canal de puerto no puede salir inmediatamente de ese mismo canal de puerto.

Ventajas arquitectónicas y operativas de vPC

vPC ofrece estas ventajas operativas y arquitectónicas inmediatas para los usuarios:

- Simplifica el diseño de red.
- Crea una red de capa 2 sólida y muy resistente.
- Permite una movilidad de máquinas virtuales sin problemas y clústeres de alta disponibilidad de servidores.
- Amplía el ancho de banda disponible de capa 2 y aumenta el ancho de banda biseccional.
- Aumenta el tamaño de la red de capa 2.



Aspectos de redundancia de hardware y software vPC

vPC aprovecha los aspectos de redundancia de hardware y software a través de estos métodos:

- vPC utiliza todos los enlaces de miembro de canal de puerto disponibles para que, en caso de que un enlace individual falle, el algoritmo hash redirija todos los flujos a los enlaces disponibles.
- El dominio vPC se compone de dos dispositivos del mismo nivel. Cada dispositivo par procesa la mitad del tráfico que proviene de la capa de acceso. En caso de que un dispositivo par falle, el otro dispositivo par absorbe todo el tráfico con un impacto mínimo en el tiempo de convergencia.
- Cada dispositivo par del dominio vPC ejecuta su propio plano de control y ambos dispositivos funcionan de forma independiente. Cualquier problema potencial del plano de control permanece local en el dispositivo par y no se propaga ni afecta al otro dispositivo par.

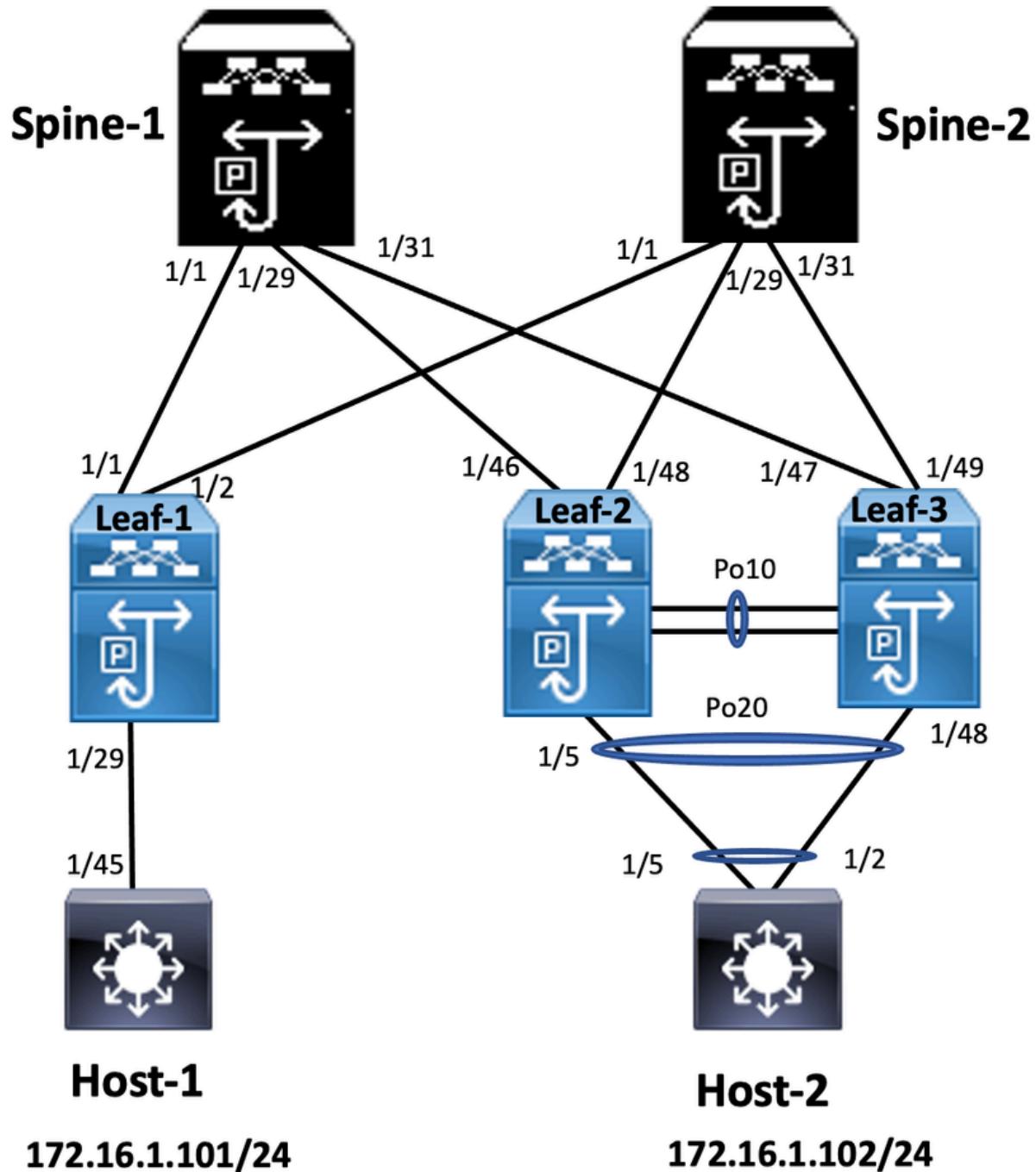
Desde STP, vPC elimina los puertos bloqueados STP y utiliza todo el ancho de banda de enlace ascendente disponible. STP se utiliza como mecanismo de seguridad contra fallos y no dicta la ruta L2 para los dispositivos conectados a vPC.

En un dominio vPC, un usuario puede conectar dispositivos de acceso de varias formas: Las

conexiones conectadas a vPC que aprovechan el comportamiento activo/activo con canal de puerto, la conectividad activo/en espera incluyen STP y un único adjunto sin STP que se ejecuta en el dispositivo de acceso.

Configuración de vPC EVPN VXLAN

Diagrama de la red



En el diagrama, el host se conecta a un par de switches Nexus 9000 que incluyen una ID de dominio de vPC, pero los switches configurados por el host no ejecutan vPC por sí mismos. El

switch/host de acceso registra el enlace ascendente como un canal de puerto simple sin conocimientos de vPC.

<#root>

Leaf-1

```
vlan 2
vn-segment 10002
vlan 10
vn-segment 10010
route-map PERMIT-ALL permit 10
vrf context test
vni 10002
rd auto
address-family ipv4 unicast
route-target both auto
route-target both auto evpn

interface nve1
no shutdown
host-reachability protocol bgp
source-interface loopback1
member vni 10002 associate-vrf
member vni 10010
suppress-arp
mcast-group 239.1.1.1

interface Loopback0
ip address 10.1.1.1/32
ip router ospf 100 area 0.0.0.0
ip pim sparse-mode
no shutdown

interface Loopback1
ip address 10.2.1.1/32
ip router ospf 100 area 0.0.0.0
ip pim sparse-mode
no shutdown
```

Leaf-2

```
vlan 2
vn-segment 10002
vlan 10
vn-segment 10010
route-map PERMIT-ALL permit 10
vrf context test
vni 10002
rd auto
address-family ipv4 unicast
route-target both auto
route-target both auto evpn

interface nve1
no shutdown
host-reachability protocol bgp
advertise virtual-rmac
```

```

source-interface loopback1
member vni 10002
associate-vrf member
vni 10010
suppress-arp
mcast-group 239.1.1.1

interface loopback1
ip address 10.2.1.4/32
ip address 10.2.1.10/32 secondary
ip router ospf 100 area 0.0.0.0
ip pim sparse-mode
icam monitor scale

interface loopback0
ip address 10.1.1.4/32
ip router ospf 100 area 0.0.0.0
ip pim sparse-mode
no shutdown

Leaf-2(config-if)# show run vpc
feature vpc

vpc domain 1
peer-switch
peer-keepalive destination 10.201.182.26 source 10.201.182.25
peer-gateway
ip arp synchronize

interface port-channel110
vpc peer-link

interface port-channel120
vpc 20

```

Leaf-3

```

vlan 2
vn-segment 10002
vlan 10
vn-segment 10010
route-map PERMIT-ALL permit 10
vrf context test
vni 10002
rd auto
address-family ipv4 unicast
route-target both auto
route-target both auto evpn

interface nve1
no shutdown
host-reachability protocol bgp
advertise virtual-rmac
source-interface loopback1
member vni 10002
associate-vrf member
vni 10010
suppress-arp
mcast-group 239.1.1.1

interface loopback1

```

```

ip address 10.2.1.3/32
ip address 10.2.1.10/32 secondary
ip router ospf 100 area 0.0.0.0
ip pim sparse-mode
icam monitor scale

interface loopback0
ip address 10.1.1.3/32
ip router ospf 100 area 0.0.0.0
ip pim sparse-mode

Leaf-3(config-if)# show run vpc
feature vpc

vpc domain 1
peer-switch
peer-keepalive destination 10.201.182.25 source 10.201.182.26
peer-gateway
ip arp synchronize

interface port-channel110
vpc peer-link

interface port-channel120
vpc 20

```

spine-1

```

interface loopback0
ip address 10.3.1.1/32
ip router ospf 100 area 0.0.0.0
ip pim sparse-mode

```

Host-1

```

interface Vlan10
no shutdown
vrf member test
ip address 172.16.1.101/25

```

Host-2

```

interface Vlan10
no shutdown
vrf member test
ip address 172.16.1.102/25

```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

| | |
|---|---|
| <pre>ip interface Status for VRF "test"(3) Interface ip Address Interface Status Vlan10 172.16.1.102 protocol-up/link-up/admin- up HOST-B(config)# ping 172.16.1.101 vrf test PING 172.16.1.101 (172.16.1.101): 56 data bytes 64 bytes from 172.16.1.101: icmp_seq=0 ttl=254 time=1.326 ms 64 bytes from 172.16.1.101: icmp_seq=1 ttl=254 time=0.54 ms 64 bytes from 172.16.1.101: icmp_seq=2 ttl=254 time=0.502 ms 64 bytes from 172.16.1.101: icmp_seq=3 ttl=254 time=0.533 ms 64 bytes from 172.16.1.101: icmp_seq=4 ttl=254 time=0.47 ms --- 172.16.1.101 ping statistics --- 5 packets transmitted, 5 packets received, 0.00% packet loss round-trip min/avg/max = 0.47/0.674/1.326 ms HOST-B(config)# </pre> | <pre>IP Interface Status for VRF "test"(3) interface IP Address Interface Status Vlan10 172.16.1.101 protocol-up/link-up/admin- up Host-A(config-if)# Host-A(config-if)# ping 172.16.1.102 vrf test PING 172.16.1.102 (172.16.1.102): 56 data bytes 64 bytes from 172.16.1.102: icmp_seq=0 ttl=254 time=1.069 ms 64 bytes from 172.16.1.102: icmp_seq=1 ttl=254 time=0.648 ms 64 bytes from 172.16.1.102: icmp_seq=2 ttl=254 time=0.588 ms 64 bytes from 172.16.1.102: icmp_seq=3 ttl=254 time=0.521 ms 64 bytes from 172.16.1.102: icmp_seq=4 ttl=254 time=0.495 ms --- 172.16.1.102 ping statistics --- 5 packets transmitted, 5 packets received, 0.00% packet loss round-trip min/avg/max = 0.495/0.664/1.069 ms Host-A(config-if)# </pre> |
|---|---|

Troubleshoot

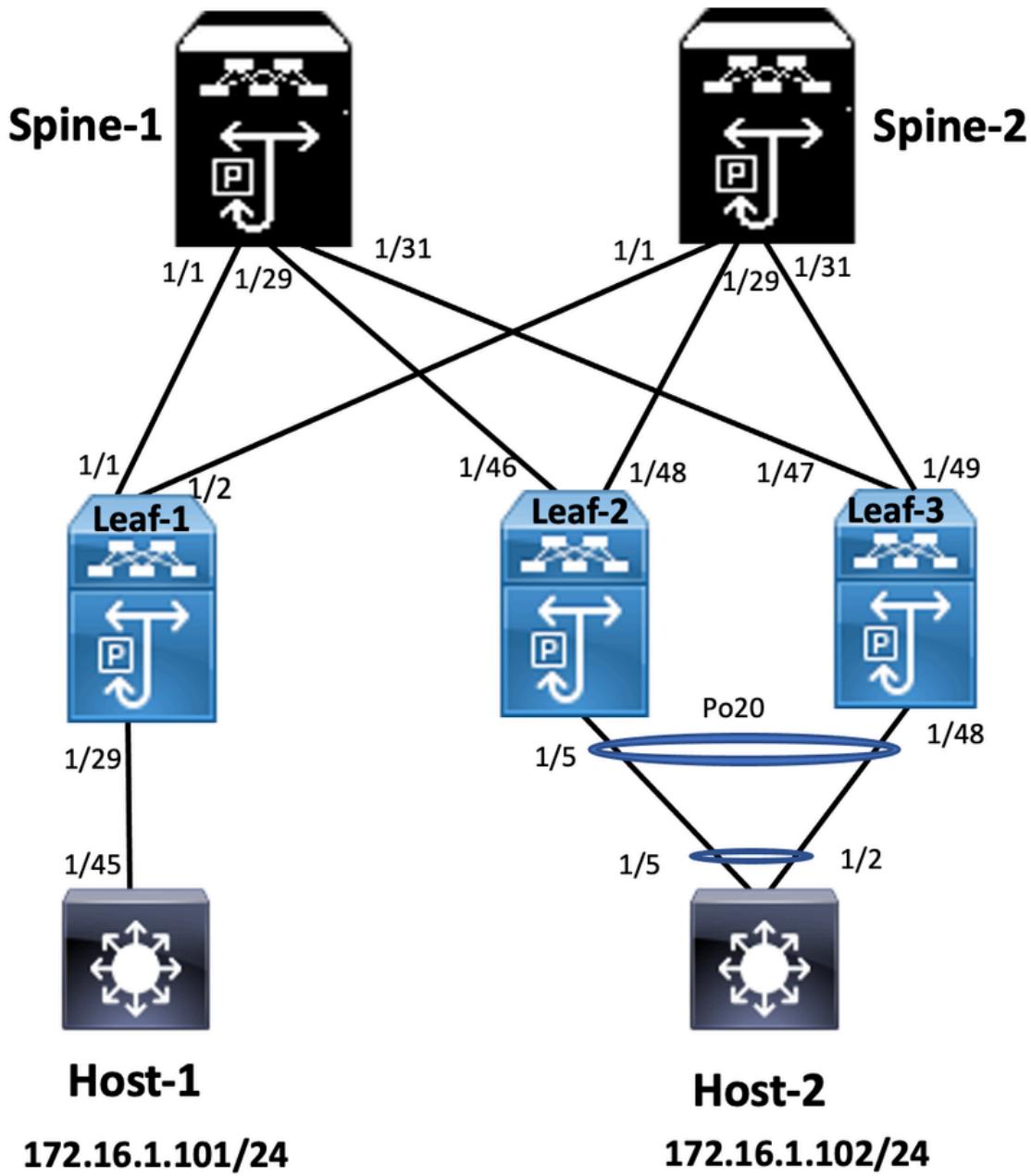
En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

| | |
|---|---|
| <pre>Leaf-2(config-if)# show vpc bri Legend: (*) - local vPC is down, forwarding via vPC peer-link vPC domain id : 1 Peer status : peer adjacency formed ok vPC keep-alive status : peer is alive Configuration consistency status : success Per-vlan consistency status : success Type-2 consistency status : success vPC role : primary Number of vPCs configured : 1 Peer Gateway : Enabled Dual-active excluded VLANs : - Graceful Consistency Check : Enabled Auto-recovery status : Disabled Delay-restore status : Timer is off.(timeout = 30s) Delay-restore SVI status : Timer is off.(timeout = 10s) Delay-restore Orphan-port status : Timer is off.(timeout = 0s) Operational Layer3 Peer-router : Disabled Virtual-peerlink mode : Disabled vPC Peer-link status ----- id Port Status Active vlans -- ----- --</pre> | <pre>Leaf-3(config-if)# show vpc bri Legend: (*) - local vPC is down, forwarding via vPC peer-link vPC domain id : 1 Peer status : peer adjacency formed ok vPC keep-alive status : peer is alive Configuration consistency status : success Per-vlan consistency status : success Type-2 consistency status : success vPC role : secondary Number of vPCs configured : 1 Peer Gateway : Enabled Dual-active excluded VLANs : Graceful Consistency Check : Enabled Auto-recovery status : Disabled Delay-restore status : Timer is off.(timeout = 30s) Delay-restore SVI status : Timer is off.(timeout = 10s) Delay-restore Orphan-port status : Timer is off.(timeout = 0s) Operational Layer3 Peer-router : Disabled Virtual-peerlink mode : Disabled vPC Peer-link status ----- id Port Status Active vlans -- ----- --</pre> |
|---|---|

| | |
|--|--|
| <pre> ----- 1 Po10 up 1-2,10 vPC status ----- ----- Id Port Status Consistency Reason Active vlans ----- 20 Po20 up success success 1-2,10 Please check "show vpc consistency-parameters vpc <vpc-num>" for the consistency reason of down vpc and for type-2 consistency reasons for any vpc. </pre> | <pre> ----- 1 Po10 up 1-2,10 vPC status ----- ----- Id Port Status Consistency Reason Active vlans ----- 20 Po20 up success success 1-2,10 Please check "show vpc consistency-parameters vpc <vpc-num>" for the consistency reason of down vpc and for type-2 consistency reasons for any vpc. </pre> |
|--|--|

Configuración del Fabric Peering vPC

Diagrama de la red



```
<#root>
```

```
Leaf-2
```

```
Leaf-2(config-vpc-domain)# show run vpc
feature vpc

vpc domain 1
peer-switch
peer-keepalive destination 10.201.182.26
virtual peer-link destination 10.1.1.3 source 10.1.1.4 dscp 56
peer-gateway
ip arp synchronize

interface port-channel110
vpc peer-link

interface Ethernet1/46
```

```
mtu 9216
port-type fabric
ip address 192.168.2.1/24
ip ospf network point-to-point
ip router ospf 100 area 0.0.0.0
ip pim sparse-mode
no shutdown
```

Leaf-3

```
Leaf-3(config-vpc-domain)# show run vpc
feature vpc

vpc domain 1
peer-switch
peer-keepalive destination 10.201.182.25
virtual peer-link destination 10.1.1.4 source 10.1.1.3 dscp 56

peer-gateway
ip arp synchronize

interface port-channel110
vpc peer-link

interface Ethernet1/47
mtu 9216
port-type fabric
ip address 192.168.1.1/24
ip ospf network point-to-point
ip router ospf 100 area 0.0.0.0
ip pim sparse-mode
no shutdown
```

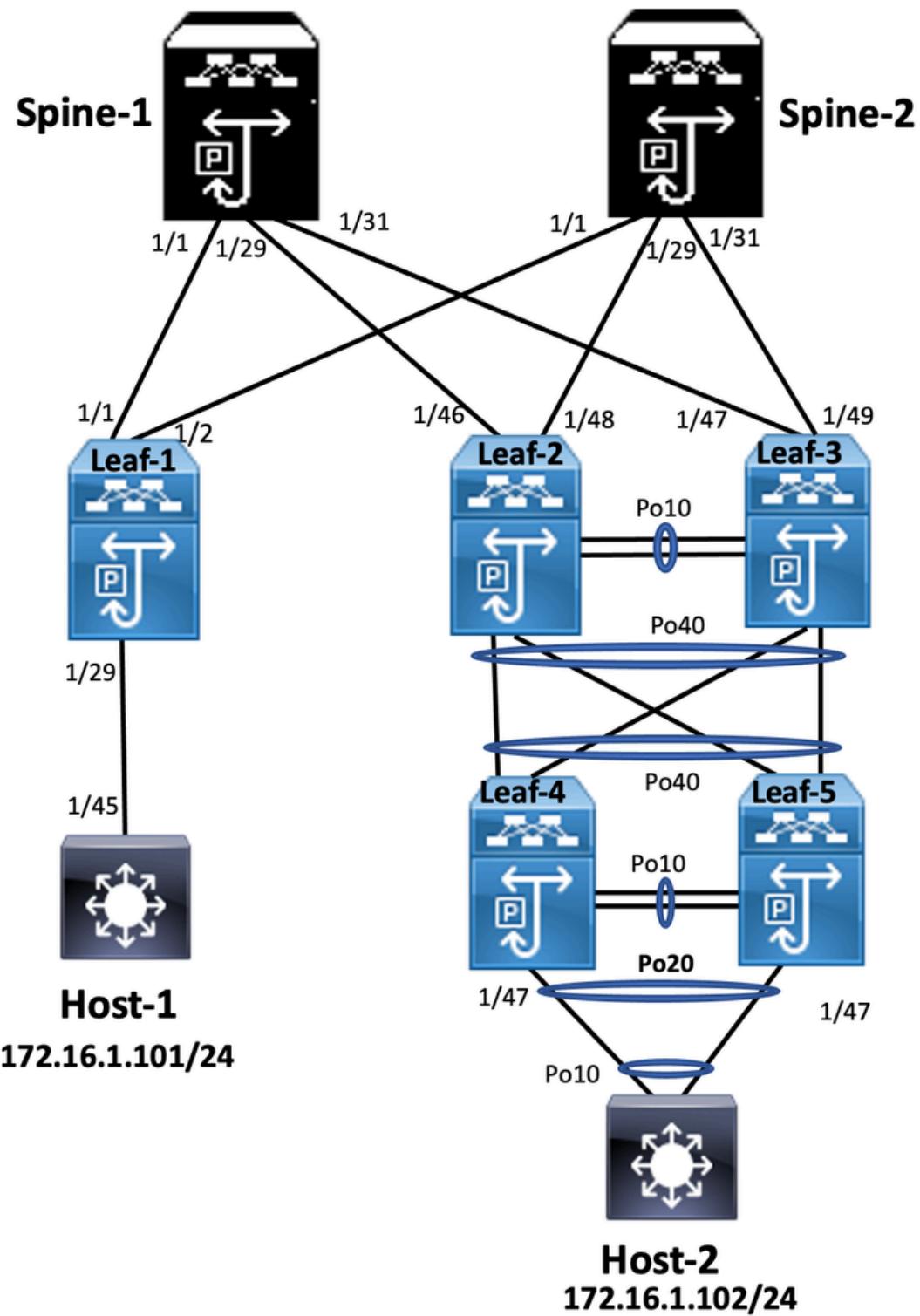
Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

```
show vpc brief
show vpc role
show vpc virtual-peerlink vlan consistency
show vpc fabric-ports
show vpc consistency-global
show nve interface nve 1 detail
```

Configuración de vPC de doble cara

Diagrama de la red



```
<#root>
```

```
Leaf-2
```

```
Leaf-2(config-if-range)# show run vpc
feature vpc
```

```
vpc domain 1
peer-switch
peer-keepalive destination 10.201.182.26 source 10.201.182.25
peer-gateway
```

```
ip arp synchronize  
  
interface port-channel10  
  vpc peer-link  
  
interface port-channel120  
  vpc 20  
  
interface port-channel140  
  vpc 40
```

Leaf-3

```
Leaf-3(config-if-range)# show run vpc  
feature vpc  
  
vpc domain 1  
peer-switch  
peer-keepalive destination 10.201.182.25 source 10.201.182.26  
peer-gateway  
ip arp synchronize  
  
interface port-channel110  
  vpc peer-link  
  
interface port-channel120  
  vpc 20  
  
interface port-channel140  
  vpc 40
```

Leaf-4

```
Leaf-4(config-if)# show run vpc  
feature vpc  
  
vpc domain 2  
peer-keepalive destination 10.201.182.29 source 10.201.182.28  
peer-gateway  
  
interface port-channel110  
  vpc peer-link  
  
interface port-channel120  
  vpc 20  
  
interface port-channel140  
  vpc 40
```

Leaf-5

```
Leaf-5(config-if)# show running-config vpc  
feature vpc  
  
vpc domain 2  
peer-keepalive destination 10.201.182.28 source 10.201.182.29  
peer-gateway
```

```
interface port-channel110
```

```
  vpc peer-link
```

```
interface port-channel120
```

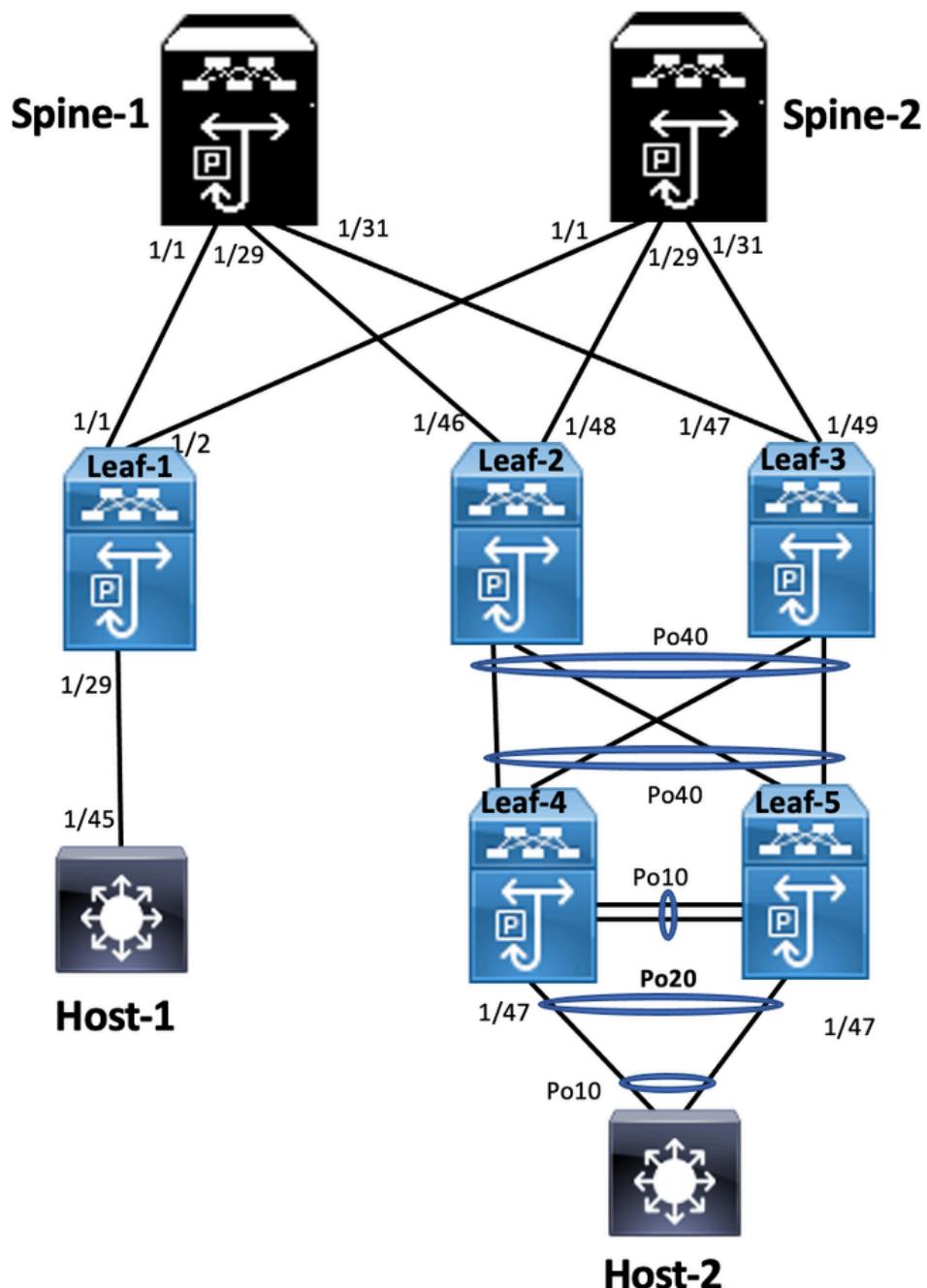
```
  vpc 20
```

```
interface port-channel140
```

```
  vpc 40
```

Configuración de vPC de doble cara con Fabric Peering vPC

Diagrama de la red



En vPC de doble cara, ambos switches Nexus 9000 ejecutan vPC. Cada par vPC de switches Nexus 9000 se conecta al par vPC de agregación con un vPC único.

<#root>

Leaf-2

```
Leaf-2(config-if-range)# show run vpc
feature vpc

vpc domain 1
  peer-switch
  peer-keepalive destination 10.201.182.26
  virtual peer-link destination 10.1.1.3 source 10.1.1.4 dscp 56
  peer-gateway
  ip arp synchronize

interface port-channel110
  vpc peer-link

interface port-channel120
  vpc 20

interface port-channel140
  vpc 40
```

Leaf-3

```
Leaf-3(config-if-range)# show run vpc
feature vpc

vpc domain 1
  peer-switch
  peer-keepalive destination 10.201.182.25
  virtual peer-link destination 10.1.1.4 source 10.1.1.3 dscp 56
  peer-gateway
  ip arp synchronize

interface port-channel110
  vpc peer-link

interface port-channel120
  vpc 20

interface port-channel140
  vpc 40
```

Leaf-4 and Leaf-5 configuration is similar as in double-sided vPC.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

```

Leaf-4(config-if)# show spanning-tree

VLAN0010
  Spanning tree enabled protocol rstp
    Root ID  Priority 32778
              Address 0023.04ee.be01
              Cost 5
              Port 4105 (port-channel10)
              Hello Time 2 sec Max Age 20
              sec Forward Delay 15 sec

```

```

    Bridge ID Priority 32778 (priority 32768
sys-id-ext 10)
              Address 0023.04ee.be02
              Hello Time 2 sec Max Age 20
              sec Forward Delay 15 sec

```

| Interface Type | Role | Sts | Cost | Prio.Nbr |
|----------------------|------|-----|------|----------|
| Po10 (vPC peer-link) | Root | FWD | 4 | 128.4105 |
| Po20 (vPC) P2p | Desg | FWD | 1 | 128.4115 |
| Po40 (vPC) P2p | Root | FWD | 1 | 128.4135 |

```

VLAN0020
  Spanning tree enabled protocol rstp
    Root ID  Priority 32788
              Address 0023.04ee.be02
              This bridge is the root
              Hello Time 2 sec Max Age 20
              sec Forward Delay 15 sec

```

```

    Bridge ID Priority 32788 (priority 32768
sys-id-ext 20)
              Address 0023.04ee.be02
              Hello Time 2 sec Max Age 20
              sec Forward Delay 15 sec<

```

| Interface Type | Role | Sts | Cost | Prio.Nbr |
|----------------------|------|-----|------|----------|
| Po10 (vPC peer-link) | Root | FWD | 4 | 128.4105 |
| Po20 (vPC) P2p | Desg | FWD | 1 | 128.4115 |
| Po40 (vPC) P2p | Desg | FWD | 1 | 128.4135 |

```
Leaf-2(config-if-range)# show spanning-tree
```

```

Leaf-5(config-if)# show spanning-tree

VLAN0010
  Spanning tree enabled protocol rstp
    Root ID  Priority 32778
              Address 0023.04ee.be01
              Cost 1
              Port 4135 (port-channel140)
              Hello Time 2 sec Max Age 20
              sec Forward Delay 15 sec
    Bridge ID Priority 32778 (priority 32768
sys-id-ext 10)
              Address 0023.04ee.be02
              Hello Time 2 sec Max Age 20
              sec Forward Delay 15 sec
  Interface      Role Sts Cost      Prio.Nbr
  Type

VLAN0020
  Spanning tree enabled protocol rstp
    Root ID  Priority 32788
              Address 0023.04ee.be02
              This bridge is the root
              Hello Time 2 sec Max Age 20
              sec Forward Delay 15 sec
    Bridge ID Priority 32788 (priority 32768
sys-id-ext 20)
              Address 0023.04ee.be02
              Hello Time 2 sec Max Age 20
              sec Forward Delay 15 sec
  Interface      Role Sts Cost      Prio.Nbr
  Type

Leaf-5(config-if)#
```

```
Leaf-3(config-if-range)# show spanning-tree
```

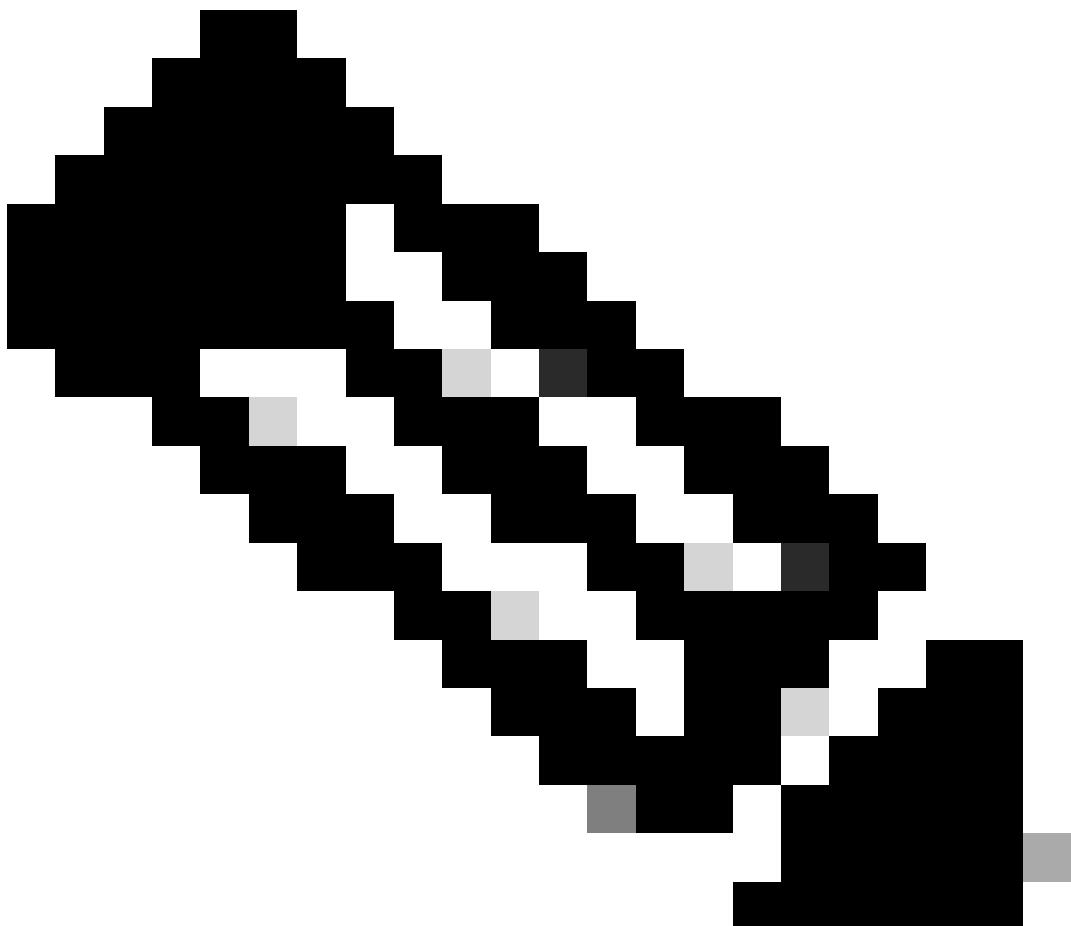
| | |
|--|--|
| VLAN0001 | VLAN0010 |
| Spanning tree enabled protocol rstp | Spanning tree enabled protocol rstp |
| Root ID Priority 32769 | Root ID Priority 32778 |
| Address 0023.04ee.be01 | Address 0023.04ee.be01 |
| Cost 0 | This bridge is the root |
| Port 0 () | Hello Time 2 sec Max Age 20 |
| Hello Time 2 sec Max Age 20 | sec Forward Delay 15 sec |
| sec Forward Delay 15 sec | Bridge ID Priority 32778 (priority 32768 sys-id-ext 10) |
| Bridge ID Priority 32769 (priority 32768 sys-id-ext 1) | Address 0023.04ee.be01 |
| Address 003a.9c28.2cc7 | Hello Time 2 sec Max Age 20 |
| Hello Time 2 sec Max Age 20 | sec Forward Delay 15 sec |
| sec Forward Delay 15 sec | Interface Role Sts Cost Prio.Nbr |
| Interface Role Sts Cost Prio.Nbr | Type |
| Eth1/47 Desg FWD 4 128.185 | Po10 Root FWD 4 128.4105 (vPC peer-link) Network P2p |
| P2p | Po40 Desg FWD 1 128.4135 (vPC) P2p |
| VLAN0010 | Leaf-3(config-if-range)# |
| Spanning tree enabled protocol rstp | |
| Root ID Priority 32778 | |
| Address 0023.04ee.be01 | |
| This bridge is the root | |
| Hello Time 2 sec Max Age 20 | |
| sec Forward Delay 15 sec | |
| Bridge ID Priority 32778 (priority 32768 sys-id-ext 10) | |
| Address 0023.04ee.be01 | |
| Hello Time 2 sec Max Age 20 | |
| sec Forward Delay 15 sec | |
| Interface Role Sts Cost Prio.Nbr | |
| Interface Role Sts Cost Prio.Nbr | Type |
| Po10 Desg FWD 4 128.4105 (vPC peer-link) Network P2p | |
| Po40 Desg FWD 1 128.4135 (vPC) P2p | |
| Eth1/47 Desg FWD 4 128.185 P2p | |
| Leaf-2(config-if-range)# | |

Prácticas recomendadas para ISSU con vPC

En esta sección se describen las prácticas recomendadas para la actualización de software sin interrupciones; utilice Cisco ISSU cuando se configure un dominio vPC. La función de actualización (o downgrade) de vPC System NX-OS es totalmente compatible con Cisco ISSU.

En un entorno vPC, ISSU es el método recomendado para actualizar el sistema. El sistema vPC

se puede actualizar de forma independiente sin interrumpir el tráfico. La actualización se serializa y debe ejecutarse de uno en uno. El bloqueo de configuración durante ISSU evita que se produzcan actualizaciones síncronas en ambos dispositivos de par vPC (la configuración se bloquea automáticamente en otro dispositivo de par vPC cuando se inicia ISSU). Para realizar el funcionamiento de ISSU, se necesita 1 solo botón.



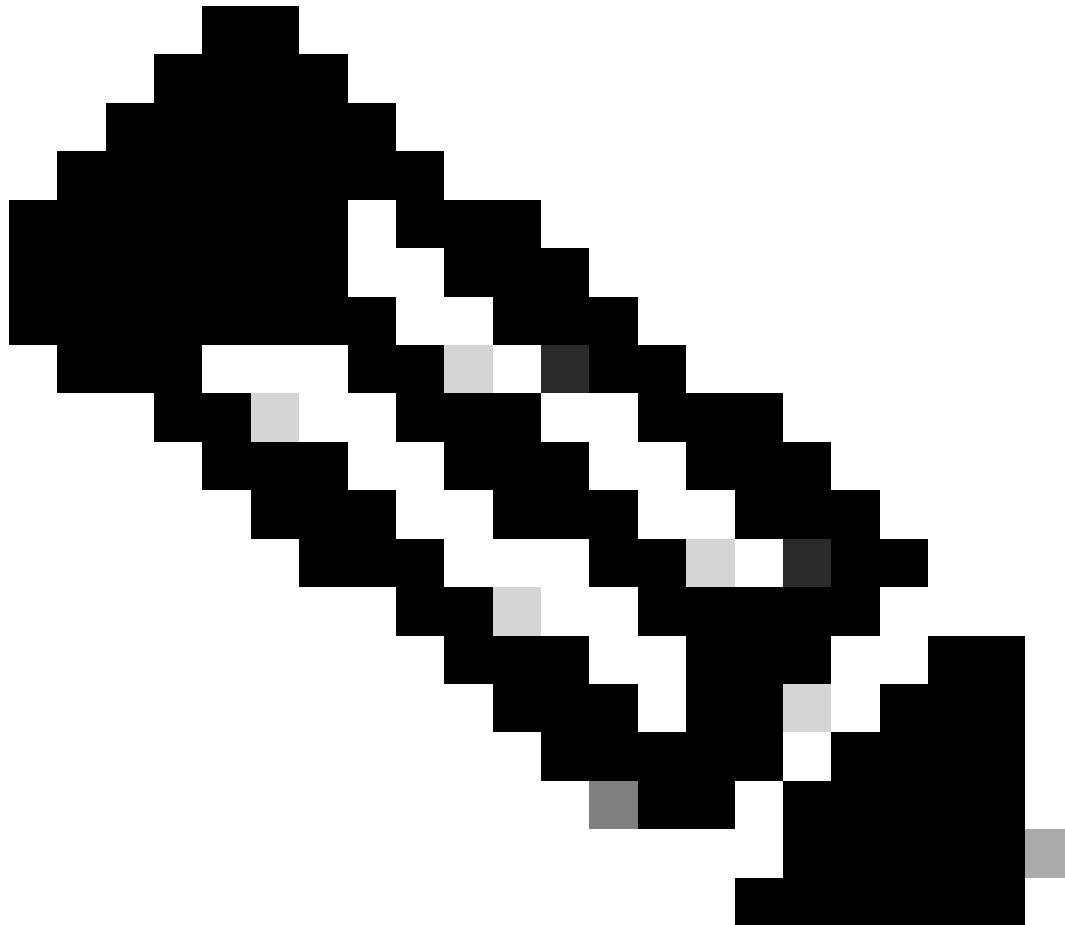
Nota: vPC con FEX (vPC host) también es totalmente compatible con ISSU. No hay pérdida de paquetes cuando el dominio vPC actualizado tiene FEX. El servidor de conexión dual a 2 FEX diferentes a través de un canal de puerto estándar no es consciente de que la operación de actualización tiene lugar en la red.

```
<#root>  
switch#install all nxos bootflash:
```

Recomendaciones energéticas

Dispositivo par vPC 1, 9K1 (carga el código primero en el dispositivo par vPC principal o secundario no tiene importancia) utilice ISSU. Tenga en cuenta que la configuración de otro dispositivo par vPC (9K2) está bloqueada para proteger frente a cualquier operación del switch.

- Utilice ISSU (actualización de software en funcionamiento) para cambiar la versión de código de NX-OS para el dominio vPC. Realice la operación de forma secuencial, un vPC por dispositivo a la vez.
 - Consulte las notas de la versión de NX-OS para seleccionar correctamente la versión de código de NX-OS objetivo en función del código del dispositivo (matriz de compatibilidad ISSU)
-



Nota: La actualización 9k1 de 7.x a 9.3.8/9.3.9 provocó la caída del puerto 40g en vPC. Si el enlace de par está conectado con 40 G, se recomienda actualizar ambos switches a 9.3.8/9.3.9 para activar 40 G o la ruta debe seguir: I7(7) - 9.3(1) - 9.3(9).

Prácticas recomendadas durante la sustitución del switch vPC

Comprobaciones previas

```
show version  
show module  
show spanning-tree summary  
show vlan summary  
show ip interface brief  
show port-channel summary  
show vpc  
show vpc brief  
show vpc role  
show vpc peer-keepalives  
show vpc statistics peer-keepalive  
show vpc consistency-parameters global  
show vpc consistency-parameters interface port-channel<>  
show vpc consistency-parameters vlans  
show run vpc all  
show hsrp brief  
show hsrp  
show run hsrp  
show hsrp interface vlan
```

```
Show vrrp  
Show vrrp brief  
Show vrrp interface vlan
```

```
Show run vrrp
```

Pasos

1. Cierre todos los puertos miembro de vPC uno por uno.
2. Cierre todos los puertos huérfanos.
3. Cierre todos los links físicos de Capa 3 uno por uno.
4. Cierre el enlace de mantenimiento activo de par (PKA) de vPC.
5. Apague el enlace par vPC.
6. Asegúrese de que todos los puertos estén inactivos en el switch problemático.
7. Asegúrese de que el tráfico se desvía al switch redundante a través de comandos compartidos en el switch redundante.

```
show vpc  
show vpc statistics  
show ip route vrf all summary  
show ip mroute vrf all summary  
show ip interface brief  
show interface status  
show port-channel summary  
show hsrp brief  
Show vrrp brief
```

8. Asegúrese de que el dispositivo de sustitución esté configurado con la imagen y la licencia correctas.

```
show version
show module
show diagnostic results module all detail
show license
show license usage
show system internal mts buffer summary/detail
show logging logfile
show logging nvram
```

9. Configure el switch con la configuración de respaldo correctamente.

10. Si la recuperación automática está activada, desactívela durante la sustitución.

```
Leaf-2(config)# vpc domain 1
Leaf-2(config-vpc-domain)# no auto-recovery
Leaf-2(config-if)# show vpc bri
Legend:
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id : 1
Peer status : peer adjacency formed ok □
vPC keep-alive status : peer is alive □
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role : primary
Number of vPCs configured : 1
Peer Gateway : Enabled
Dual-active excluded VLANs : -□Graceful Consistency Check : Enabled□
Auto-recovery status : Disabled□
Delay-restore status : Timer is off. (timeout = 30s)□
Delay-restore SVI status : Timer is off (timeout = 10s)□
Delay-restore Orphan-port status : Timer is off.(timeout = 0s)
Operational Layer3 Peer-router : Disabled
Virtual-peerlink mode : Disabled
```

11. Asegúrese de que el bit persistente esté establecido en False.

```
Leaf-5(config-vpc-domain)# show sys internal vpcm info all | i i stick
OOB Peer Version: 2 OOB peer was alive: TRUE Sticky Master: FALSE
```

12. Si el bit persistente está establecido en True, vuelva a configurar la prioridad de rol de vPC. Esto significa volver a aplicar la configuración original para la prioridad de rol.

- Dominio vPC 1 <== 1 es el número de dominio vPC mencionado en el switch original

- role priority 2000 <== ejemplo: si 2000 es la prioridad de rol de vPC establecida en el switch original

13. Active las interfaces estrictamente en este orden:

1. Abra el enlace de mantenimiento de conexiones entre pares.
2. Active el enlace de par vPC.
3. Confirme que la función vPC se ha establecido correctamente.
4. Abra el resto de las interfaces en los switches uno por uno en este orden:
 1. Puertos de miembro de vPC
 2. Puertos huérfanos (puertos no vPC)
 3. Interfaz física de capa 3

Comprobación posterior a la validación

```
show version
show module
show diagnostics result module all detail
show environment
show license usage
show interface status
show ip interface brief
show interface status err-disabled
show cdp neighbors
show redundancy status
show spanning-tree summary
show port-channel summary
show vpc
show vpc brief
show vpc role
show vpc peer-keepalives
show vpc statistics peer-keepalive
show vpc consistency-parameters global
show vpc consistency-parameters interface port-channel11
show vpc consistency-parameters v1ans
show hsrp brief
show vrrp brief
```

Consideraciones sobre vPC para la implementación de VXLAN

- En vPC VXLAN, se recomienda aumentar el temporizador de la interfaz vlan de restauración con retraso en la configuración vPC, si se amplía el número de SVI. Por ejemplo, si hay 1000 VNIs con 1000 SVIs, se recomienda aumentar el temporizador de la interfaz de restauración de retraso-vlan a 45 segundos.

```
<#root>
switch(config-vpc-domain)#
      delay restore interface-vlan 45
```

- Para vPC, la interfaz de bucle invertido tiene dos direcciones IP: la dirección IP principal y la secundaria.
 - La dirección IP principal es única y la utilizan los protocolos de capa 3.
 - La dirección IP secundaria en loopback es necesaria porque la interfaz NVE la utiliza para la dirección IP VTEP. La dirección IP secundaria debe ser la misma en ambos pares vPC.
- El temporizador de mantenimiento NVE debe ser superior al temporizador de restauración con retraso de vPC.

```
Leaf-2(config-if-range)# show nve interface nve 1 detail
Interface: nve1, State: Up, encapsulation: VXLAN
VPC Capability: VPC-VIP-Only [notified]
Local Router MAC: 003a.9c28.2cc7
Host Learning Mode: Control-Plane
Source-Interface: loopback1 (primary: 10.1.1.41.1.4, secondary: 10.1.1.10)
Source Interface State: Up
Virtual RMAC Advertisement: Yes
NVE Flags:
Interface Handle: 0x49000001
Source Interface hold-down-time: 180
Source Interface hold-up-time: 30
Remaining hold-down time: 0 seconds
Virtual Router MAC: 0200.1401.010a
Interface state: nve-intf-add-complete
Fabric convergence time: 135 seconds
Fabric convergence time left: 0 seconds
```

- Para conocer las prácticas recomendadas, habilite la recuperación automática en su entorno vPC. Aunque es poco frecuente, existe la posibilidad de que la función de recuperación automática de vPC le sitúe en un escenario activo dual.
- La función de switch de par vPC permite que un par de dispositivos de par vPC aparezcan como una única raíz de protocolo de árbol de extensión en la topología de capa 2 (tienen el mismo ID de puente). El switch de par vPC se debe configurar en ambos dispositivos de par vPC para que estén operativos. El comando es el siguiente:

```
N9K(config-vpc-domain)# peer-switch
```

- La puerta de enlace par vPC permite que un dispositivo par vPC actúe como puerta de enlace activa para los paquetes dirigidos a la otra MAC del router del dispositivo par. Mantiene el reenvío del tráfico local al dispositivo par vPC y evita el uso del enlace par. El tráfico y la funcionalidad no se ven afectados cuando se activa la función de puerta de enlace par-a-par.

```
N9k-1(config)# vpc domain 1  
N9k-1(config-vpc-domain)# peer-gateway
```

- Se ha introducido el comando peer-router de capa 3 que permite el routing a través de vPC.

```
N9k-1(config)# vpc domain 1  
N9k-1(config-vpc-domain)# layer3 peer-router  
N9K-1(config-vpc-domain)# exit  
  
N9K-1# sh vpc  
Legend:(*)  
- Local vPC is down, forwarding via vPC peer-link  
vPC domain id : 100  
Peer status : peer adjacency formed ok  
vPC keep-alive status : peer is alive  
Configuration consistency status : success  
Per-vlan consistency status : success  
Type-2 consistency status : success  
vPC role : secondary, operational primary  
Number of vPCs configured : 2  
Peer Gateway : Enabled  
Peer gateway excluded VLANs : -  
Peer gateway excluded bridge-domains : -  
Dual-active excluded VLANs and BDs : -  
Graceful Consistency Check : Enabled  
Auto-recovery status : Enabled (timeout = 240 seconds)  
Operational Layer3 Peer-router : Enabled
```

Recomendaciones energéticas

- La gateway de par debe estar habilitada antes que el router de par de capa 3.
- Ambos pares vPC deben tener configurado un router de par de capa 3 para que surta efecto.
- Habilite Supress-arp como práctica recomendada mientras que la dirección IP multicast para VXLAN.
- Utilice una dirección IP de bucle invertido independiente para el control y el plano de datos en el fabric de vPC VXLAN.
- En vPC con MSTP, la prioridad de puente debe ser la misma en ambos pares vPC.
- Para obtener los mejores resultados de convergencia, ajuste con precisión la restauración de retraso de vPC y los temporizadores de retención de la interfaz NVE.

Información Relacionada

- [Documentación de los switches Nexus serie 9000](#)
- [Guía de configuración de las interfaces NX-OS de Cisco Nexus 9000 Series, versión 9.3\(x\)](#)
- [Guía de escalabilidad verificada de Cisco Nexus serie 9000 NX-OS, versión 9.2\(1\)](#): incluye números de escalabilidad de vPC (CCO)

- [Versiones recomendadas de Cisco NX-OS para los switches Nexus de Cisco serie 9000](#)
- [Notas de la versión de switches Nexus serie 9000](#)
- [Guía de configuración de NX-OS VXLAN para Nexus de Cisco serie 9000, versión 9.2\(x\)](#) - sección sobre análisis de estructuras vPC
- [Ejemplo de Configuración de Configuración de EVPN Vxlan IPV6 Overlay](#)
- [Guía de diseño y configuración: Prácticas recomendadas para los canales de puerto virtuales \(vPC\) en los switches Nexus de Cisco serie 7000:](#) la teoría de vPC N7k y N9k es similar y esta referencia incluye información adicional sobre las prácticas recomendadas
- [Configuración y verificación de vPC virtual de doble cara](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).