

Informazioni e configurazione di Nexus 9000 vPC con best practice

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Descrizione e terminologia di vPC](#)

[Vantaggi tecnici di vPC](#)

[Vantaggi operativi e architetturali di vPC](#)

[Aspetti di ridondanza hardware e software vPC](#)

[Configurazione di vPC VPN VXLAN](#)

[Esempio di rete](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Configurazione peer fabric vPC](#)

[Esempio di rete](#)

[Verifica](#)

[Configura vPC fronte/retro](#)

[Esempio di rete](#)

[Configurazione di vPC a doppia faccia con vPC Fabric Peering](#)

[Esempio di rete](#)

[Risoluzione dei problemi](#)

[Procedure ottimali per ISSU con vPC](#)

[Consigli efficaci](#)

[Procedure ottimali per la sostituzione dello switch vPC](#)

[Controlli preliminari](#)

[Passi](#)

[Controllo post-convalida](#)

[Considerazioni su vPC per l'implementazione di VXLAN](#)

[Consigli efficaci](#)

[Informazioni correlate](#)

Introduzione

In questo documento vengono descritte le best practice per utilizzare i port-channel virtuali (vPC) sui dispositivi Cisco Nexus serie 9000 (9k) Switch.

Prerequisiti

Requisiti

- Richiesta licenza NX-OS per vPC
- La funzionalità vPC è inclusa nella licenza base del software NX-OS.

Questa licenza di base include anche i protocolli HSRP (Hot Standby Router Protocol), VRRP (Virtual Router Redundancy Protocol), LACP (Link Aggregation Control Protocol).

Le funzionalità di layer 3, ad esempio il protocollo OSPF (Open Shortest Path First) o il protocollo ISIS (Intermediate-System-to-Intermediate System), richiedono una licenza LAN_ENTERPRISE_SERVICES_PKG.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Nexus 93180YC-FX con versione 10.2(3)
- Cisco Nexus 93180YC-FX con versione 10.2(3)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

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.

vPC Fabric Peering fornisce una soluzione avanzata di accesso dual-homing senza il sovraccarico delle porte fisiche di scarico per vPC Peer Link.

Premesse

Il presente documento si applica a:

- Nexus 9k vPC
- vPC con Vxlan
- Peering fabric vPC
- vPC fronte/retro
- vPC virtuale a doppia faccia

Questo documento descrive anche le operazioni di aggiornamento del software in servizio (ISSU) relative a vPC e fornisce dettagli sui più recenti miglioramenti apportati al vPC (ripristino ritardato, timer dell'interfaccia NVE (Network Virtual Interface)).

Descrizione e terminologia di vPC

vPC è una tecnologia di virtualizzazione che presenta entrambi i dispositivi accoppiati Cisco Nexus serie 9000 come un nodo logico di layer 2 unico per l'accesso ai dispositivi o agli endpoint di layer 2.

vPC appartiene alla famiglia di tecnologie Multicassis EtherChannel (MCEC). Un canale di porta virtuale (vPC) consente ai collegamenti fisicamente connessi a due diversi dispositivi Cisco Nexus serie 9000 di apparire come un canale a porta singola per un terzo dispositivo.

Il terzo dispositivo può essere uno switch, un server o qualsiasi altro dispositivo di rete che supporti la tecnologia di aggregazione dei collegamenti.

Vantaggi tecnici di vPC

vPC offre i seguenti vantaggi tecnici:

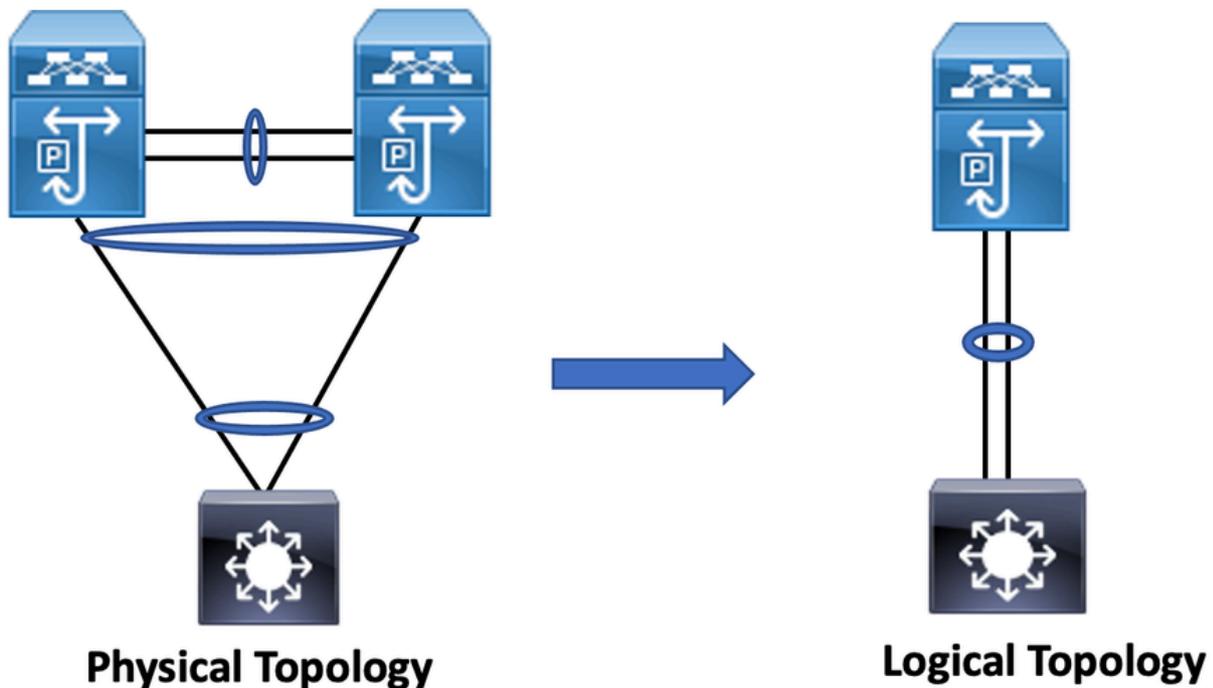
- Elimina le porte bloccate dallo Spanning Tree Protocol (STP).
- Utilizza tutta la larghezza di banda uplink disponibile.
- Consente ai server dual-homed di funzionare in modalità attivo-attivo.
- Convergenza rapida in caso di guasto del collegamento o del dispositivo.
- Offre due gateway predefiniti attivi/attivi per i server vPC. Sfrutta inoltre la gestione nativa di split-horizon/loop fornita dalla tecnologia di channeling delle porte: un pacchetto in entrata da un canale porta non può uscire immediatamente dallo stesso canale porta.

Vantaggi operativi e architetturali di vPC

vPC offre agli utenti i seguenti vantaggi operativi e architetturali immediati:

- Semplifica la progettazione della rete.

- Costruisce una rete di layer 2 estremamente resistente e robusta.
- Mobilità ininterrotta delle macchine virtuali e cluster ad alta disponibilità dei server.
- Aumenta la larghezza di banda del layer 2, aumentando la larghezza di banda bisettoriale.
- Aumenta le dimensioni della rete di livello 2.



Aspetti di ridondanza hardware e software vPC

vPC sfrutta gli aspetti di ridondanza hardware e software tramite i seguenti metodi:

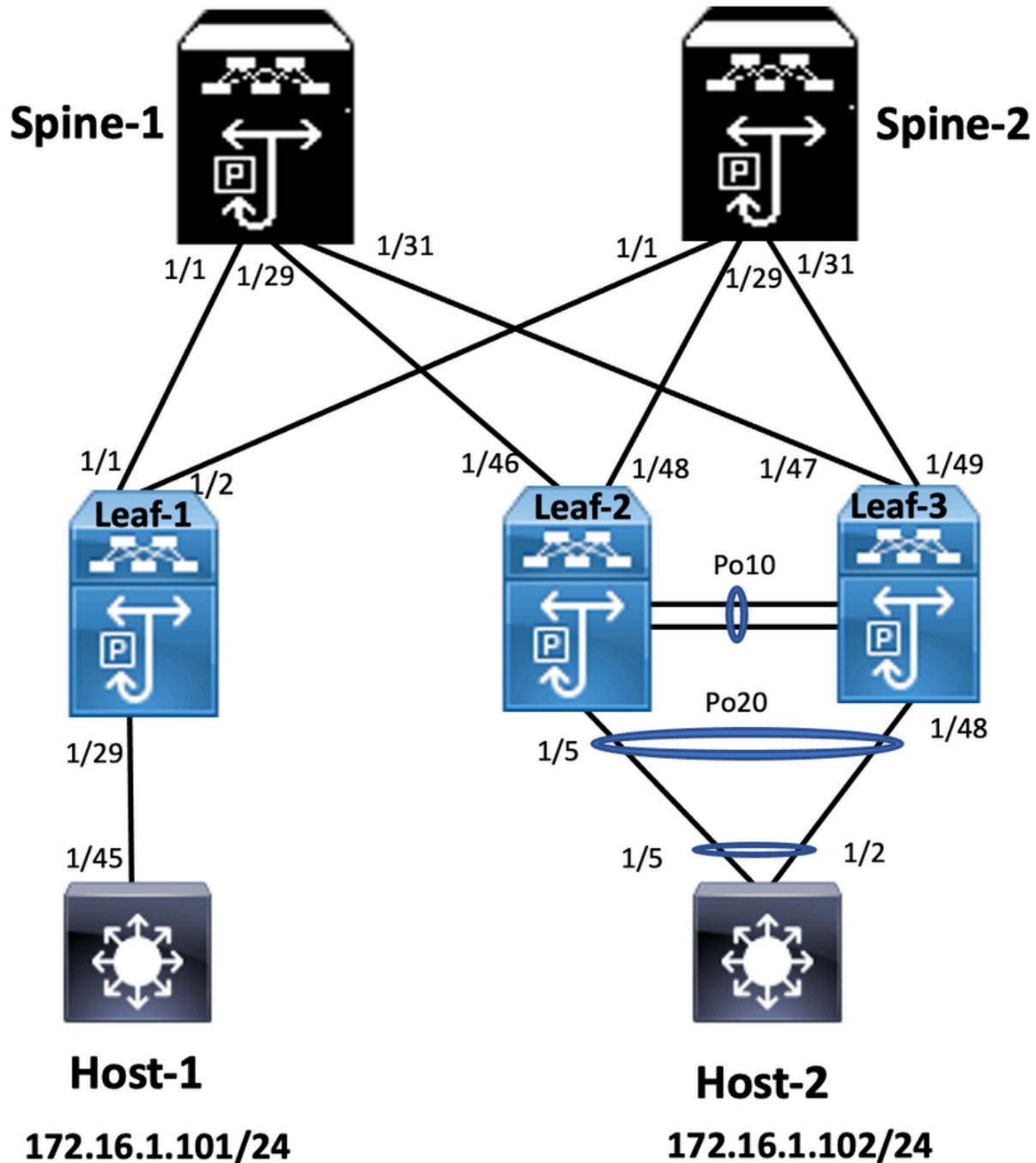
- vPC utilizza tutti i collegamenti membri del canale della porta disponibili in modo che in caso di errore di un singolo collegamento, l'algoritmo hash reindirizza tutti i flussi ai collegamenti disponibili.
- Il dominio vPC è composto da due dispositivi peer. Ogni dispositivo peer elabora metà del traffico proveniente dal livello di accesso. In caso di guasto di un dispositivo peer, l'altro dispositivo peer assorbe tutto il traffico con un impatto minimo sul tempo di convergenza.
- Ogni dispositivo peer nel dominio vPC esegue il proprio control plane ed entrambi i dispositivi funzionano in modo indipendente. Eventuali problemi del control plane rimangono locali per il dispositivo peer e non si propagano né influiscono sull'altro dispositivo peer.

Da STP, vPC elimina le porte bloccate STP e utilizza tutta la larghezza di banda di uplink disponibile. Il protocollo STP viene utilizzato come meccanismo di sicurezza dagli errori e non determina il percorso L2 per i dispositivi collegati a vPC.

All'interno di un dominio vPC, un utente può connettere i dispositivi di accesso in diversi modi: Le connessioni vPC che sfruttano il comportamento attivo/attivo con la connettività port-channel, active/standby includono STP e il collegamento singolo senza STP eseguito sul dispositivo di accesso.

Configurazione di vPC VPN VXLAN

Esempio di rete



Nel diagramma, l'host si connette a una coppia di switch Nexus 9000 e include l'ID di dominio vPC, ma gli switch configurati dall'host non eseguono il vPC. Lo switch di accesso/host registra l'uplink come semplice canale porta senza che il vPC ne sia a conoscenza.

<#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-channel10
vpc peer-link
```

```
interface port-channel20
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-channel10
vpc peer-link
```

```
interface port-channel20
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
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

<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</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)#</pre>
---	---

<pre> 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> 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>
--	--

Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione.

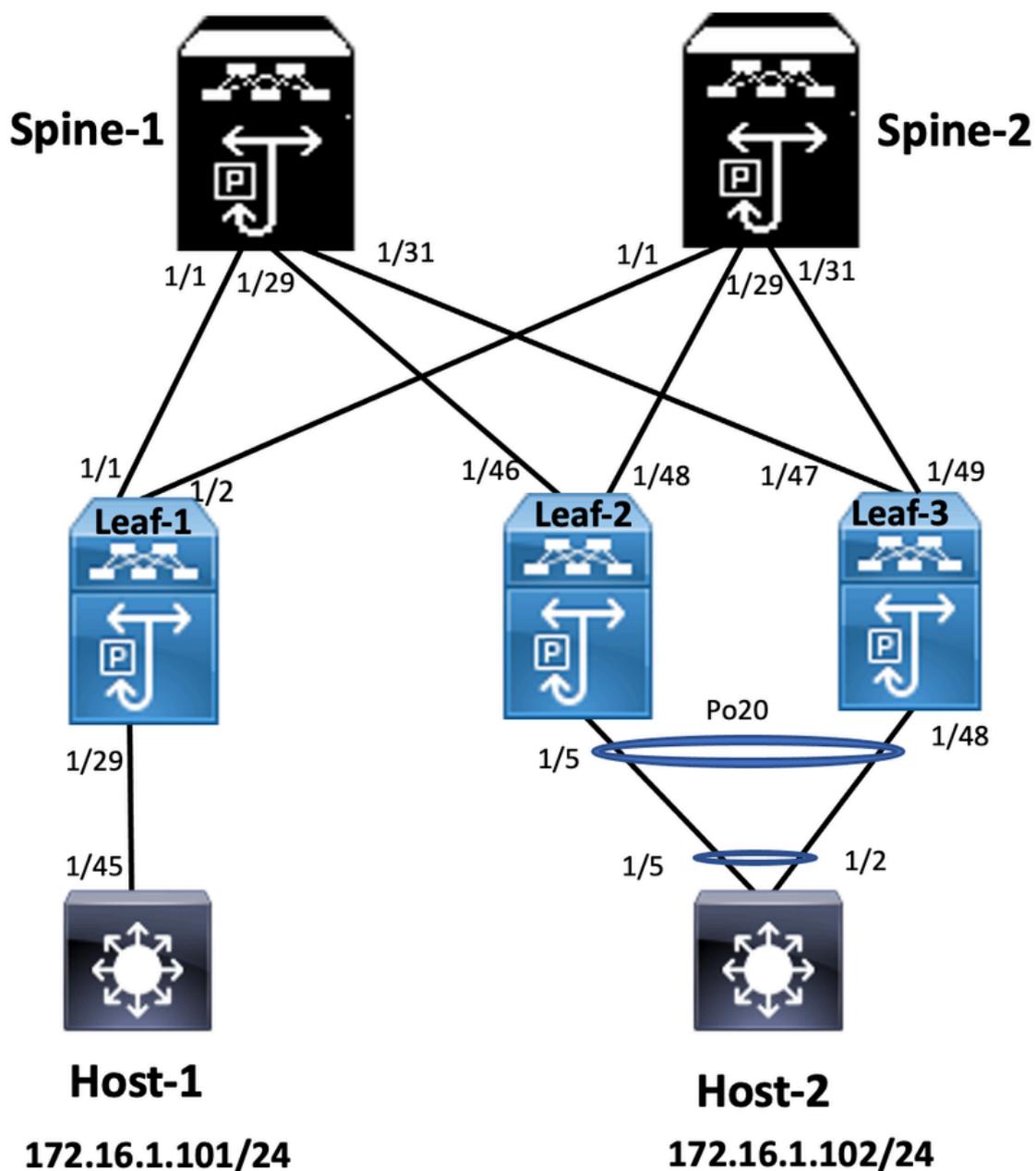
<pre> Leaf-2(config-if)# show vpc bri Legend: (*) - local vPC is down, forwarding via vPC peer-link vPC domain id : 1 Peer status : peer adjacency formed ok vPC keep-alive status : peer is alive Configuration consistency status : success Per-vlan consistency status : success Type-2 consistency status : 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 ----- 1 Po10 up 1-2,10 ----- vPC status ----- ----- Id Port Status Consistency Reason 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 ----- 1 Po10 up 1-2,10 ----- vPC status ----- ----- Id Port Status Consistency Reason Active vlans </pre>
--	--

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.

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.

Configurazione peer fabric vPC

Esempio di rete



<#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-channel10
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-channel10
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
```

Verifica

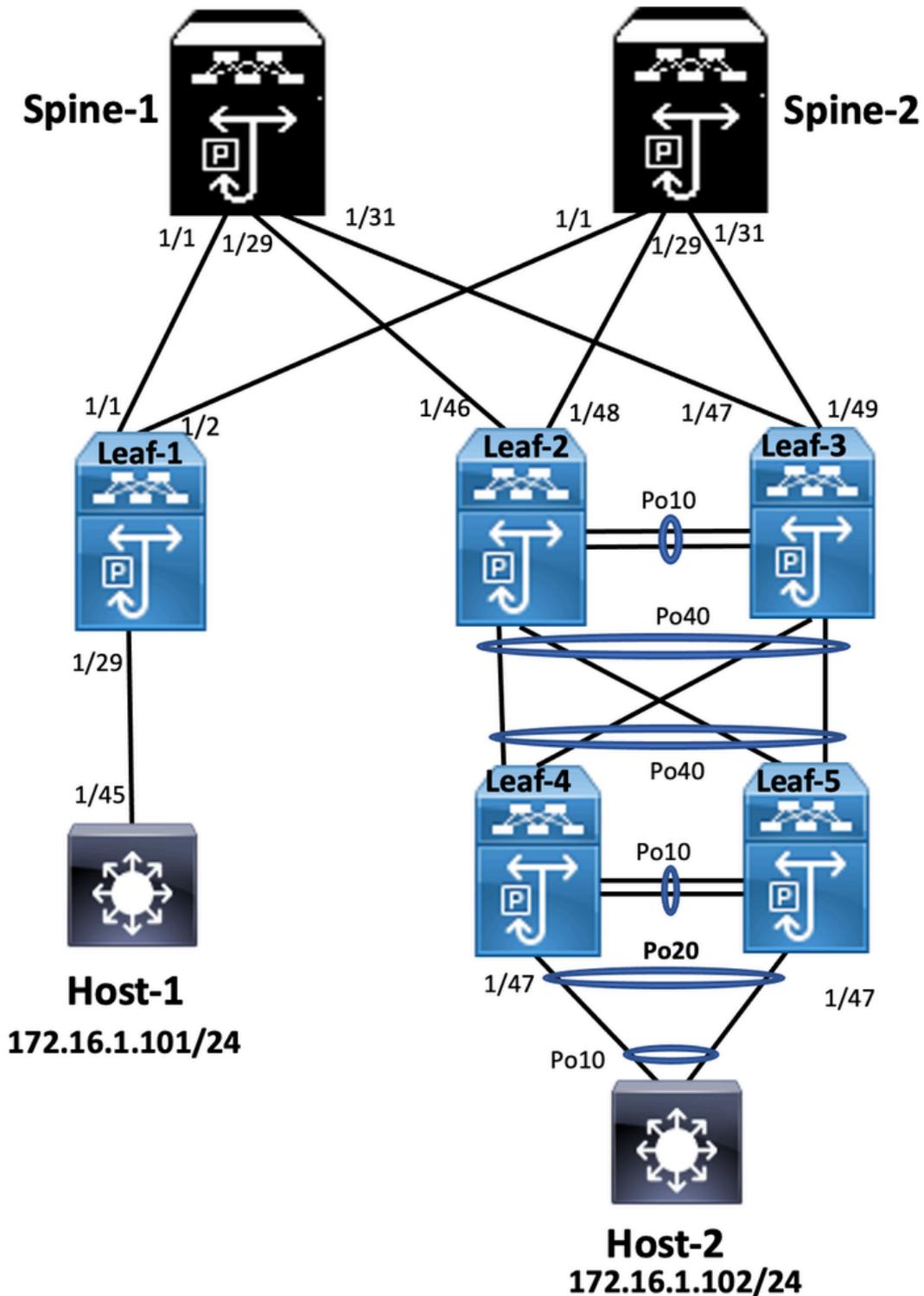
Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

```
show vpc brief
show vpc role
show vpc virtual-peerlink vlan consistency
```

```
show vpc fabric-ports
show vpc consistency-para global
show nve interface nve 1 detail
```

Configura vPC fronte/retro

Esempio di rete



<#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-channel20
 vpc 20
```

```
interface port-channel40
 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-channel10
 vpc peer-link
```

```
interface port-channel20
 vpc 20
```

```
interface port-channel40
 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-channel10
 vpc peer-link
```

```
interface port-channel20
 vpc 20
```

```
interface port-channel40
 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
```

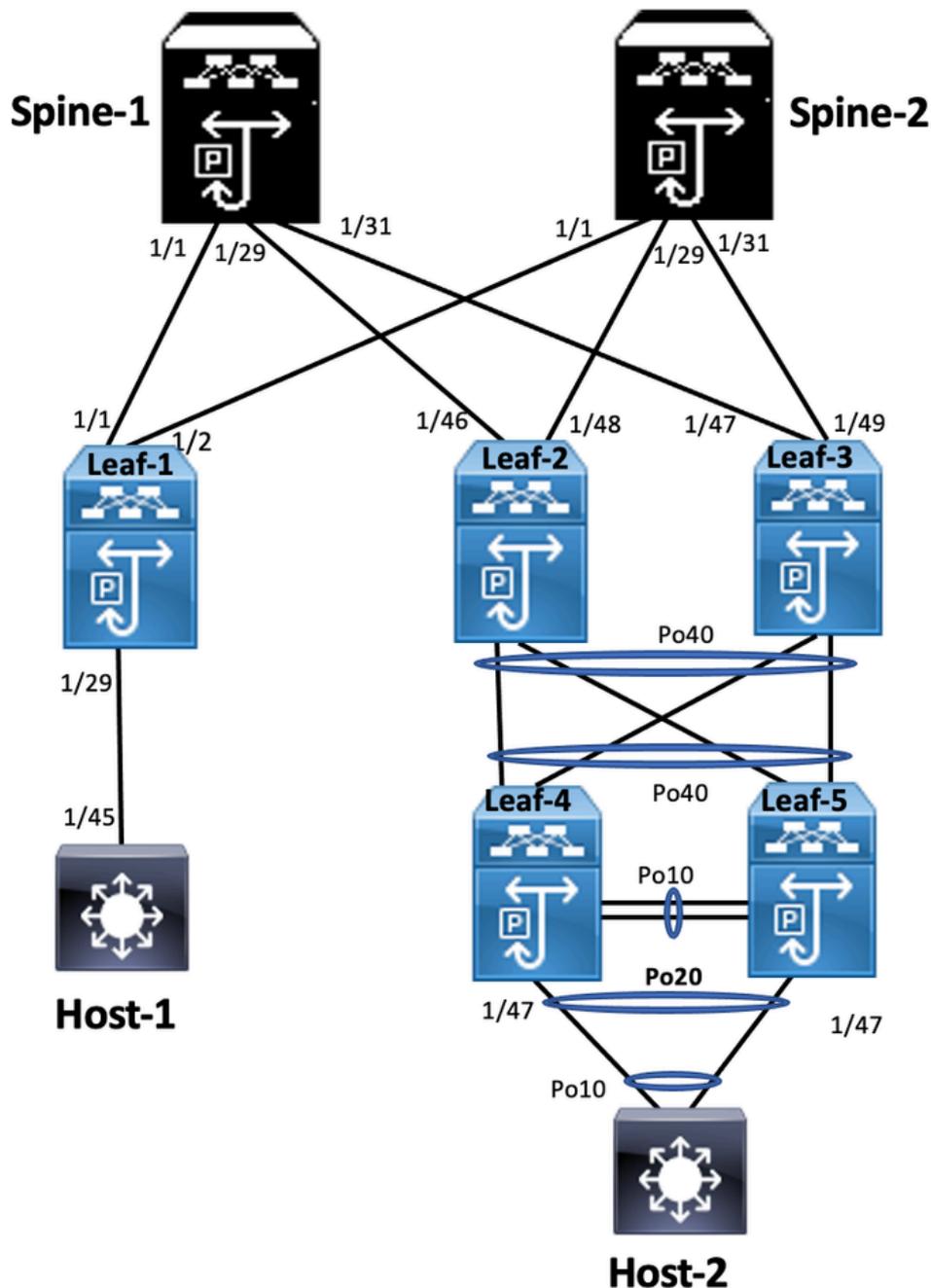
```
interface port-channel110  
vpc peer-link
```

```
interface port-channel120  
vpc 20
```

```
interface port-channel140  
vpc 40
```

Configurazione di vPC a doppia faccia con vPC Fabric Peering

Esempio di rete



In vPC a doppia faccia, entrambi gli switch Nexus 9000 eseguono vPC. Ogni coppia di switch Nexus 9000 vPC è collegata alla coppia di vPC di aggregazione con un unico vPC.

```
<#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-channel10
 vpc peer-link

interface port-channel20
 vpc 20

interface port-channel40
 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-channel10
 vpc peer-link

```

```

interface port-channel20
 vpc 20

```

```

interface port-channel40
 vpc 40

```

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

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

<pre> 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 </pre>	<pre> 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-channel40) 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 </pre>
---	---

<pre> Interface Role Sts Cost Prio.Nbr Type ----- Po10 Root FWD 4 128.4105 (vPC peer-link) Network P2p Po20 Desg FWD 1 128.4115 (vPC) P2p Po40 Root FWD 1 128.4135 (vPC) P2p 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< </pre>	<pre> Interface Role Sts Cost Prio.Nbr Type ----- Po10 Desg FWD 4 128.4105 (vPC peer-link) Network P2p Po20 Desg FWD 1 128.4115 (vPC) P2p Po40 Root FWD 1 128.4135 (vPC) P2p 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 </pre>
<pre> Interface Role Sts Cost Prio.Nbr Type ----- Po10 Root FWD 4 128.4105 (vPC peer-link) Network P2p Po20 Desg FWD 1 128.4115 (vPC) P2p Po40 Desg FWD 1 128.4135 (vPC) P2p </pre>	<pre> Interface Role Sts Cost Prio.Nbr Type ----- Po10 Desg FWD 4 128.4105 (vPC peer-link) Network P2p Po20 Desg FWD 1 128.4115 (vPC) P2p Po40 Desg FWD 1 128.4135 (vPC) P2p Leaf-5(config-if)# </pre>
<pre> Leaf-2(config-if-range)# show spanning-tree VLAN0001 Spanning tree enabled protocol rstp Root ID Priority 32769 Address 0023.04ee.be01 Cost 0 Port 0 () Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Bridge ID Priority 32769 (priority 32768 sys-id-ext 1) Address 003a.9c28.2cc7 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Interface Role Sts Cost Prio.Nbr Type ----- </pre>	<pre> Leaf-3(config-if-range)# show spanning-tree VLAN0010 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 Type ----- </pre>

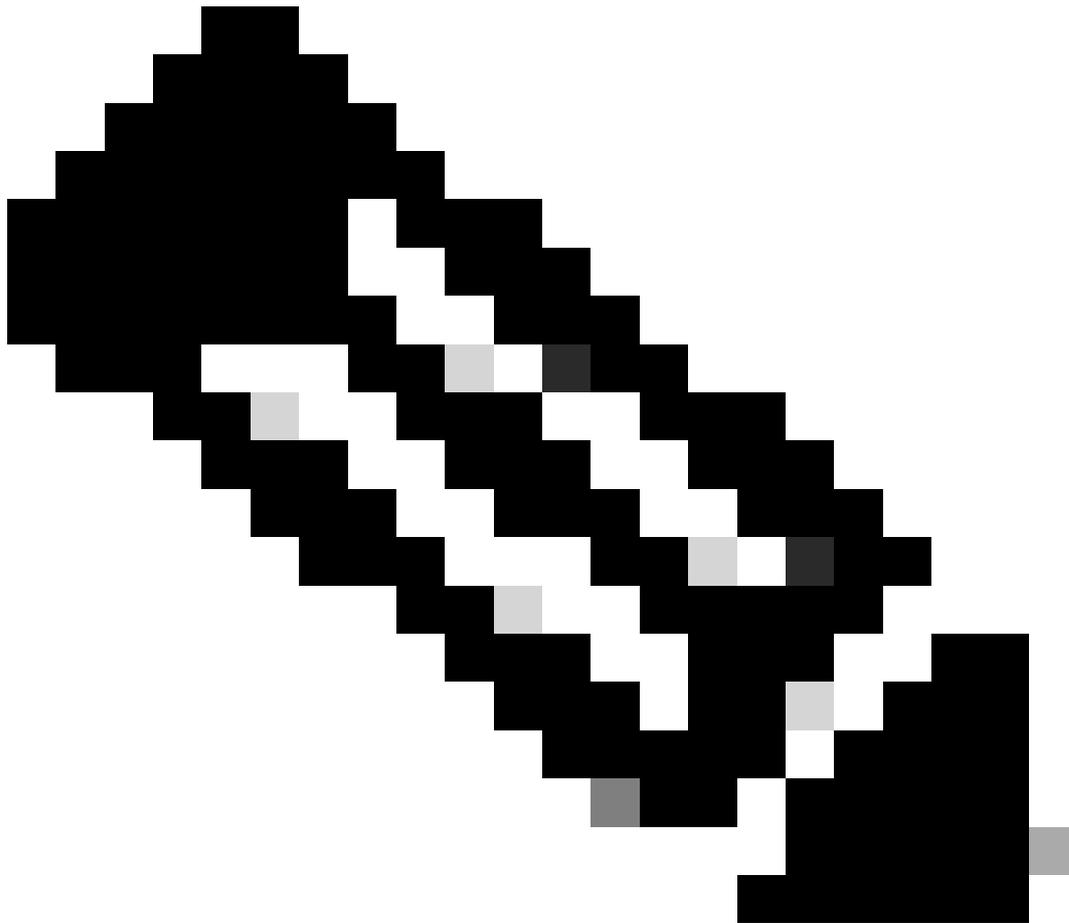
-----			-----		
Eth1/47	Desg FWD 4	128.185	Po10	Root FWD 4	128.4105
P2p			(vPC peer-link) Network P2p		
VLAN0010			Po40	Desg FWD 1	128.4135
Spanning tree enabled protocol rstp			(vPC) P2p		
Root ID	Priority	32778	Leaf-3(config-if-range)#		
	Address	0023.04ee.be01			
	This bridge is the root				
	Hello 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	
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)#					

Procedure ottimali per ISSU con vPC

In questa sezione vengono descritte le best practice per l'aggiornamento del software senza interruzioni. Usare Cisco IOS quando è configurato un dominio vPC. La funzione vPC System NX-OS Upgrade (o Downgrade) è completamente compatibile con Cisco ISSU.

In un ambiente vPC, il metodo consigliato per l'aggiornamento del sistema è ISSU. Il sistema vPC può essere aggiornato in modo indipendente senza interruzione del traffico. L'aggiornamento è serializzato e deve essere eseguito uno alla volta. Il blocco della configurazione durante l'ISSU impedisce l'esecuzione di aggiornamenti sincroni su entrambi i dispositivi peer vPC (la configurazione viene bloccata automaticamente su altri dispositivi peer vPC all'avvio dell'ISSU). Per eseguire l'operazione ISSU, è necessaria una singola manopola.



Nota: Anche vPC con FEX (host vPC) supporta completamente IOS. Quando il dominio vPC aggiornato presenta FEX, la perdita di pacchetti è pari a zero. Il server dual-attached a 2 FEX diversi tramite un canale della porta standard non è in grado di rilevare l'aggiornamento in rete.

<#root>

switch#install all nxos bootflash:

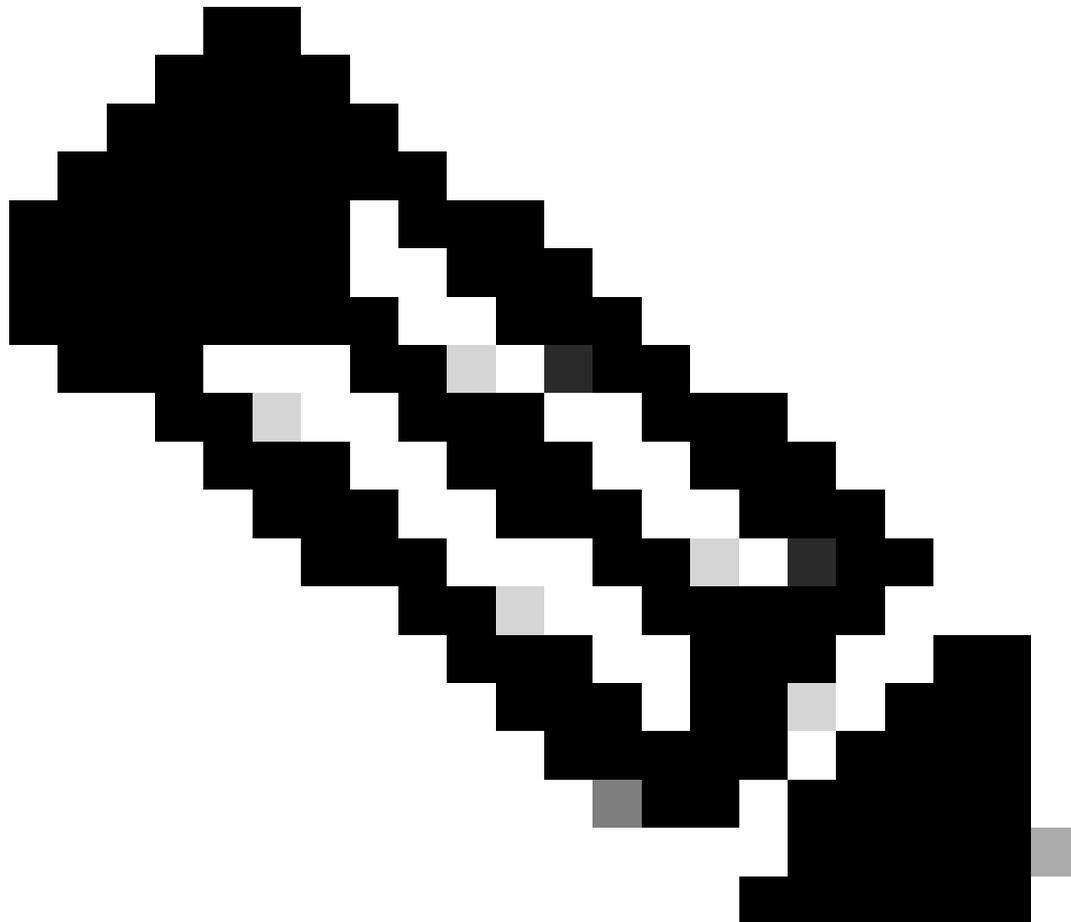
Consigli efficaci

Dispositivo peer vPC 1, 9K1 (carica il codice prima sul dispositivo peer vPC primario o secondario non ha importanza) utilizza ISSU. Si noti che la configurazione di un altro dispositivo peer vPC (9K2) è bloccata per proteggerlo da qualsiasi operazione sullo switch.

- Utilizzare ISSU (In-Service Software Upgrade) per modificare la versione del codice NX-OS

per il dominio vPC. Eseguire l'operazione in sequenza, un dispositivo peer vPC alla volta.

- Consultare le note sulla versione di NX-OS per selezionare correttamente la versione di destinazione del codice NX-OS in base al codice del dispositivo (matrice di compatibilità ISSU)
-



Nota: L'aggiornamento di 9k1 da 7.x a 9.3.8/9.3.9 ha causato un abbassamento della porta 40g su vPC. Se il collegamento peer è collegato a 40 GB, si consiglia di aggiornare entrambi gli switch a 9.3.8/9.3.9 per portare 40G su o il percorso deve seguire: I7(7) - 9.3(1) - 9.3(9).

Procedure ottimali per la sostituzione dello switch vPC

Controlli preliminari

```
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
```

Passi

1. Arrestare tutte le porte membro vPC una alla volta.
2. Chiudere tutte le porte orfane.
3. Chiudere tutti i collegamenti fisici di layer 3 uno alla volta.
4. Arrestare il collegamento vPC Peer Keep Alive (PKA).
5. Arrestare il collegamento peer vPC.
6. Verificare che tutte le porte siano inattive sullo switch con problemi.
7. Verificare che il traffico venga indirizzato allo switch ridondante tramite comandi condivisi sullo switch ridondante.

```
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. Accertarsi che il dispositivo sostitutivo sia configurato con l'immagine e la licenza corrette.

```
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. Configurare correttamente lo switch con la configurazione di backup.

10. Se il ripristino automatico è abilitato, disabilitarlo durante la sostituzione.

```
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. Assicurarsi che il bit Sticky sia impostato su 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. Se il bit di Sticky è impostato su True, riconfigurare la priorità del ruolo vPC. Ciò significa riapplicare la configurazione originale per la priorità del ruolo.

- vPC domain 1 <== 1 è il numero di dominio vPC indicato sullo switch originale
- role priority 2000 <== esempio: se 2000 è impostato come priorità del ruolo vPC sullo switch originale

13. Visualizzare le interfacce in modo rigoroso nel seguente ordine:

1. Attivare il collegamento keep-alive peer.
2. Attivare il collegamento peer vPC.
3. Confermare che il ruolo vPC sia stato stabilito correttamente.

4. Visualizzare il resto delle interfacce sugli switch uno per uno nell'ordine seguente:
 1. porte membro vPC
 2. Porte orfane (porte non vPC)
 3. Interfaccia fisica di layer 3

Controllo post-convalida

```
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-channel1
show vpc consistency-parameters vlans
show hsrp brief
show vrrp brief
```

Considerazioni su vPC per l'implementazione di VXLAN

- Sulla VXLAN vPC, si consiglia di aumentare il timer dell'interfaccia vlan di ripristino ritardato nella configurazione vPC, se il numero di SVI è stato aumentato. Ad esempio, se sono presenti 1000 VNI con 1000 SVI, si consiglia di aumentare il timer dell'interfaccia vlan di ripristino ritardato a 45 secondi.

```
<#root>
```

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

```
delay restore interface-vlan 45
```

- Per vPC, l'interfaccia di loopback dispone di due indirizzi IP: l'indirizzo IP primario e l'indirizzo IP secondario.
 - L'indirizzo IP primario è univoco e viene utilizzato dai protocolli di layer 3.
 - L'indirizzo IP secondario sul loopback è necessario perché l'interfaccia NVE

lo utilizza per l'indirizzo IP VTEP. L'indirizzo IP secondario deve essere lo stesso in entrambi i peer vPC.

- Il timer di attesa NVE deve essere superiore al timer di ripristino ritardato 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
```

- Per le procedure ottimali, abilitare il ripristino automatico nell'ambiente vPC. Sebbene raro, la funzione di ripristino automatico di vPC può offrire la possibilità di un doppio scenario attivo.
- La funzionalità vPC Peer-Switch consente a una coppia di dispositivi peer vPC di apparire come una singola radice Spanning Tree Protocol nella topologia di layer 2 (hanno lo stesso ID bridge). Per diventare operativi, i dispositivi peer vPC devono essere configurati su entrambi. Il comando è:

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

- vPC Peer-Gateway consente a un dispositivo peer vPC di fungere da gateway attivo per i pacchetti indirizzati all'altro MAC router del dispositivo peer. Mantiene l'inoltro del traffico locale al dispositivo peer vPC ed evita l'uso del collegamento peer. L'attivazione della funzionalità Peer-Gateway non influisce sul traffico e sulla funzionalità.

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

- È stato introdotto il comando layer3 peer-router che abilita il routing sul 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
```

Consigli efficaci

- Il gateway peer deve essere abilitato prima del router peer di layer 3.
- Per rendere effettivi entrambi i peer vPC, è necessario che il router peer di layer 3 sia configurato.
- Abilitare Suppress-arp come procedura ottimale quando si usa l'indirizzo IP multicast per la VXLAN.
- Usa indirizzo IP di loopback separato per controllo e piano dati nel fabric VXLAN vPC.
- In vPC con MSTP, la priorità del bridge deve essere la stessa su entrambi i peer vPC.
- Per ottenere risultati di convergenza ottimali, regolare con precisione i timer di ripristino posticipato vPC e di arresto interfaccia NVE.

Informazioni correlate

- [Documentazione sugli switch Nexus serie 9000](#)
- [Guida alla configurazione delle interfacce NX-OS sui Cisco Nexus serie 9000, versione 9.3\(x\)](#)
- [Guida alla scalabilità Cisco Nexus serie 9000 NX-OS Verified, versione 9.2\(1\)](#) - include i numeri di scalabilità vPC (CCO)
- [Versioni Cisco NX-OS consigliate per gli switch Cisco Nexus serie 9000](#)
- [Note sulla release degli switch Nexus serie 9000](#)
- [Guida alla configurazione di VXLAN per Cisco Nexus serie 9000 NX-OS, versione 9.2\(x\)](#) - sezione su vPC Fabric Peering
- [Esempio di configurazione della sovrimpressione IPV6 di EVPN Vxlan](#)
- [Guida alla progettazione e alla configurazione: Best Practices for Virtual Port Channels \(vPC\) sugli switch Cisco Nexus serie 7000](#) - La teoria dei VPC N7k e N9k è simile e questa guida di riferimento include informazioni aggiuntive sulle best practice

- [Configurazione e verifica di vPC virtuali su due lati](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).