Entender e configurar o vPC Nexus 9000 com as melhores práticas

Contents

Introdução

Este documento descreve as melhores práticas a serem usadas para canais de porta virtuais (vPC) nos switches Cisco Nexus 9000 (9k) Series.

Pré-requisitos

Requisitos

- Requisito de licença do NX-OS para vPC
- O recurso vPC está incluído na licença básica do software NX-OS.

Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), Link Aggregation Control Protocol (LACP) também estão incluídos nesta licença básica.

Os recursos da camada 3, como o protocolo OSPF (Open Shortest Path First) ou o protocolo ISIS (Intermediate-System-to-Intermediate System), exigem a licença LAN_ENTERPRISE_SERVICES_PKG.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Nexus93180YC-FX que executa a versão 10.2(3)
- Cisco Nexus93180YC-FX que executa a versão 10.2(3)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer 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.

O vPC Fabric Peering fornece uma solução avançada de acesso dual-homing sem a sobrecarga

de portas físicas desperdiçadas para o vPC Peer Link.

Informações de Apoio

Este documento se aplica a:

- vPC Nexus 9k
- vPC com Vxlan
- Peering de estrutura vPC
- vPC com dois lados
- vPC virtual com dois lados

Este documento também aborda as operações de In-Service Software Upgrade (ISSU) relacionadas ao vPC e fornece detalhes sobre os aprimoramentos mais recentes do vPC (restauração de atraso, temporizadores de interface NVE).

Descrição e terminologia do vPC

O vPC é uma tecnologia de virtualização que apresenta ambos os dispositivos emparelhados Cisco Nexus 9000 Series como um nó lógico de camada 2 exclusivo para acessar dispositivos de camada ou endpoints.

O vPC pertence à família de tecnologia MCEC (Multichassis EtherChannel). Um canal de porta virtual (vPC) permite que os links fisicamente conectados a dois dispositivos Cisco Nexus 9000 Series diferentes apareçam como um canal de porta única para um terceiro dispositivo.

O terceiro dispositivo pode ser um switch, servidor ou qualquer outro dispositivo de rede que suporte a tecnologia de agregação de links.

Benefícios técnicos do vPC

O vPC oferece os seguintes benefícios técnicos:

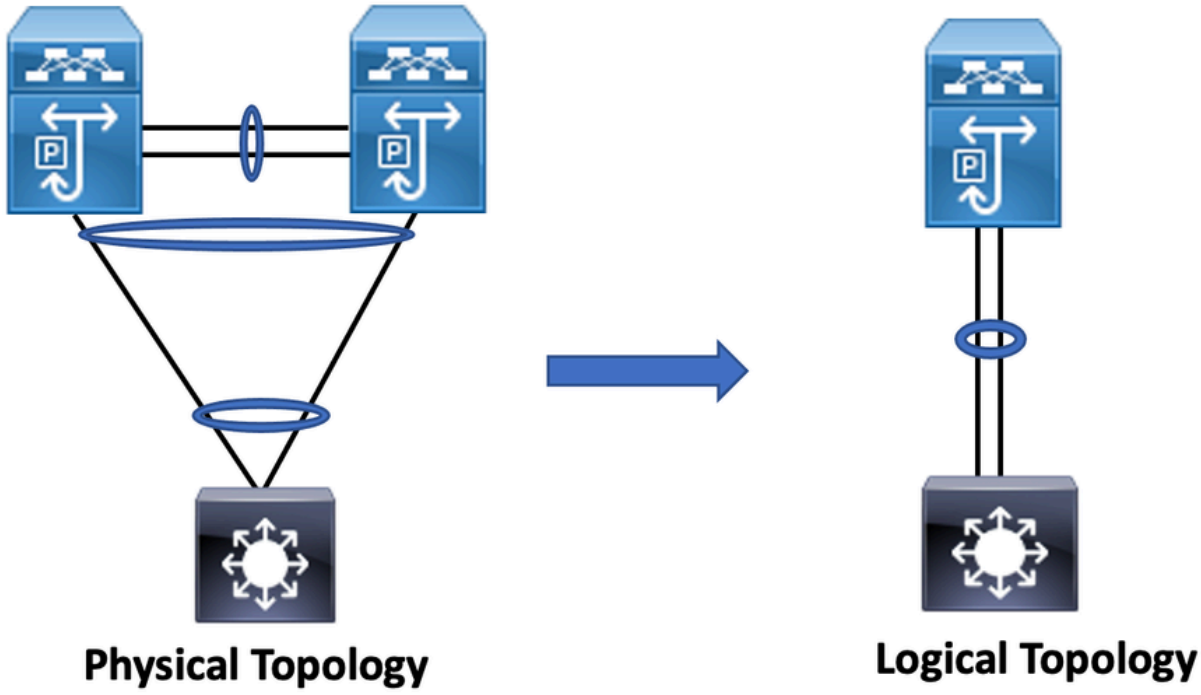
- Elimina as portas bloqueadas do Spanning Tree Protocol (STP).
- Usa toda a largura de banda de uplink disponível.
- Permite que servidores dual-homed operem no modo ativo-ativo.
- Fornece convergência rápida em caso de falha de link ou dispositivo.
- Oferece gateways padrão ativos/duplos ativos para servidores vPC. Também aproveita o gerenciamento nativo de split horizon/loop fornecido pela tecnologia de canalização de portas: um pacote chega e um canal de porta não pode sair imediatamente desse mesmo canal de porta.

Vantagens operacionais e arquitetônicas do vPC

O vPC oferece estas vantagens operacionais e arquitetônicas imediatas para os usuários:

- Simplifica o projeto da rede.

- Cria uma rede de Camada 2 altamente resiliente e robusta.
- Permite mobilidade perfeita de máquina virtual e clusters de alta disponibilidade de servidor.
- Dimensiona a largura de banda disponível da camada 2, aumentando a largura de banda bisseccional.
- Aumenta o tamanho da rede de Camada 2.



Aspectos de redundância de hardware e software do vPC

O vPC aproveita os aspectos de redundância de hardware e software através destes métodos:

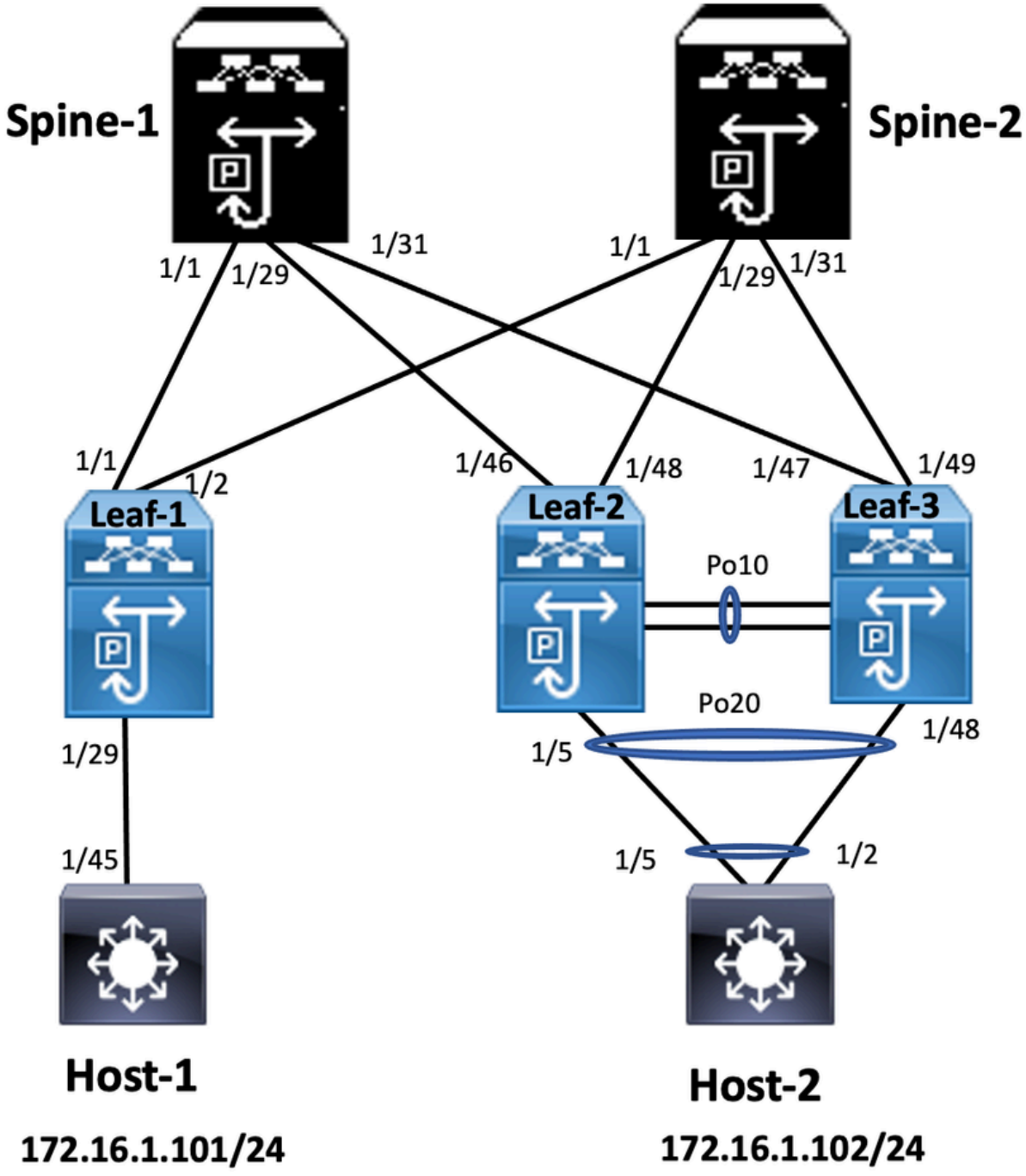
- O vPC usa todos os links de membro do canal de porta disponíveis para que, caso um link individual falhe, o algoritmo de hash redirecione todos os fluxos para os links disponíveis.
- O domínio vPC é composto de dois dispositivos pares. Cada dispositivo peer processa metade do tráfego vindo da camada de acesso. Caso um dispositivo de peer falhe, o outro dispositivo de peer absorve todo o tráfego com impacto mínimo no tempo de convergência.
- Cada dispositivo par no domínio vPC executa seu próprio plano de controle, e ambos os dispositivos funcionam independentemente. Quaisquer problemas potenciais do plano de controle permanecem locais ao dispositivo par e não propagam nem impactam o outro dispositivo par.

No STP, o vPC elimina as portas bloqueadas do STP e usa toda a largura de banda de uplink disponível. O STP é usado como um mecanismo à prova de falhas e não determina o caminho de L2 para dispositivos conectados ao vPC.

Dentro de um domínio vPC, um usuário pode conectar dispositivos de acesso de várias maneiras: As conexões com vPC que aproveitam o comportamento ativo/ativo com a conectividade de canal de porta, ativa/standby incluem STP e conexão única sem STP que é executada no dispositivo de acesso.

Configurar vPC EVPN VXLAN

Diagrama de Rede



No diagrama, o host se conecta a um par de switches Nexus 9000 e inclui o id de domínio do vPC, mas os switches configurados pelo host não executam o vPC sozinhos. O switch/host de acesso registra o uplink como um canal de porta simples sem conhecimento 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-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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

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	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)#

```
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)#
```

```
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)#
```

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

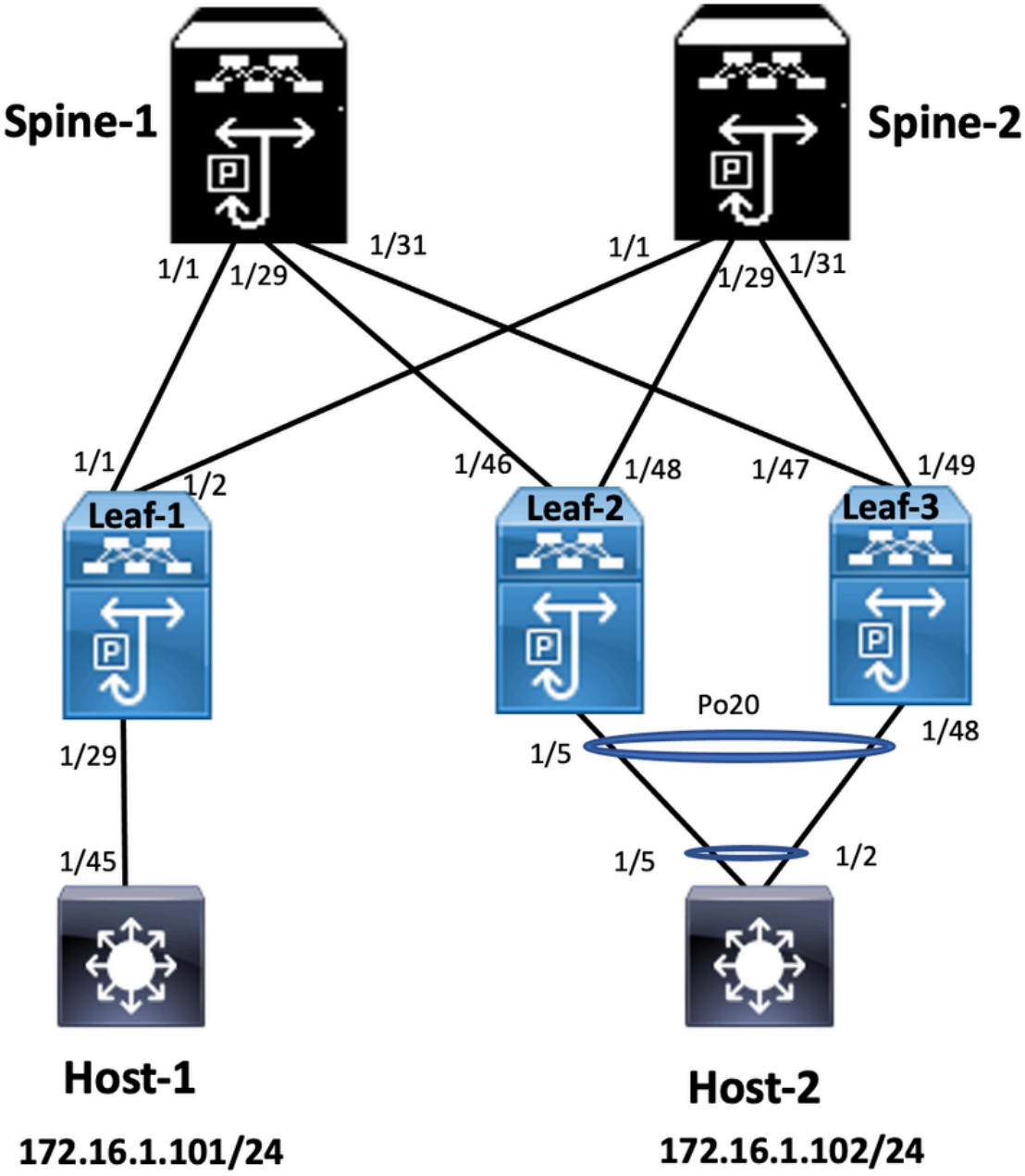
```
Leaf-2(config-if)# show vpc bri
Legend:
(*) - local vPC is down, forwarding via vPC
peer-link
vPC domain id : 1
Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : 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
----------------------------------------------------
-----------------------------
```

```
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 --------------- 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.	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.

Configurar o vPC Fabric Peering

Diagrama de Rede



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
```

Verificar

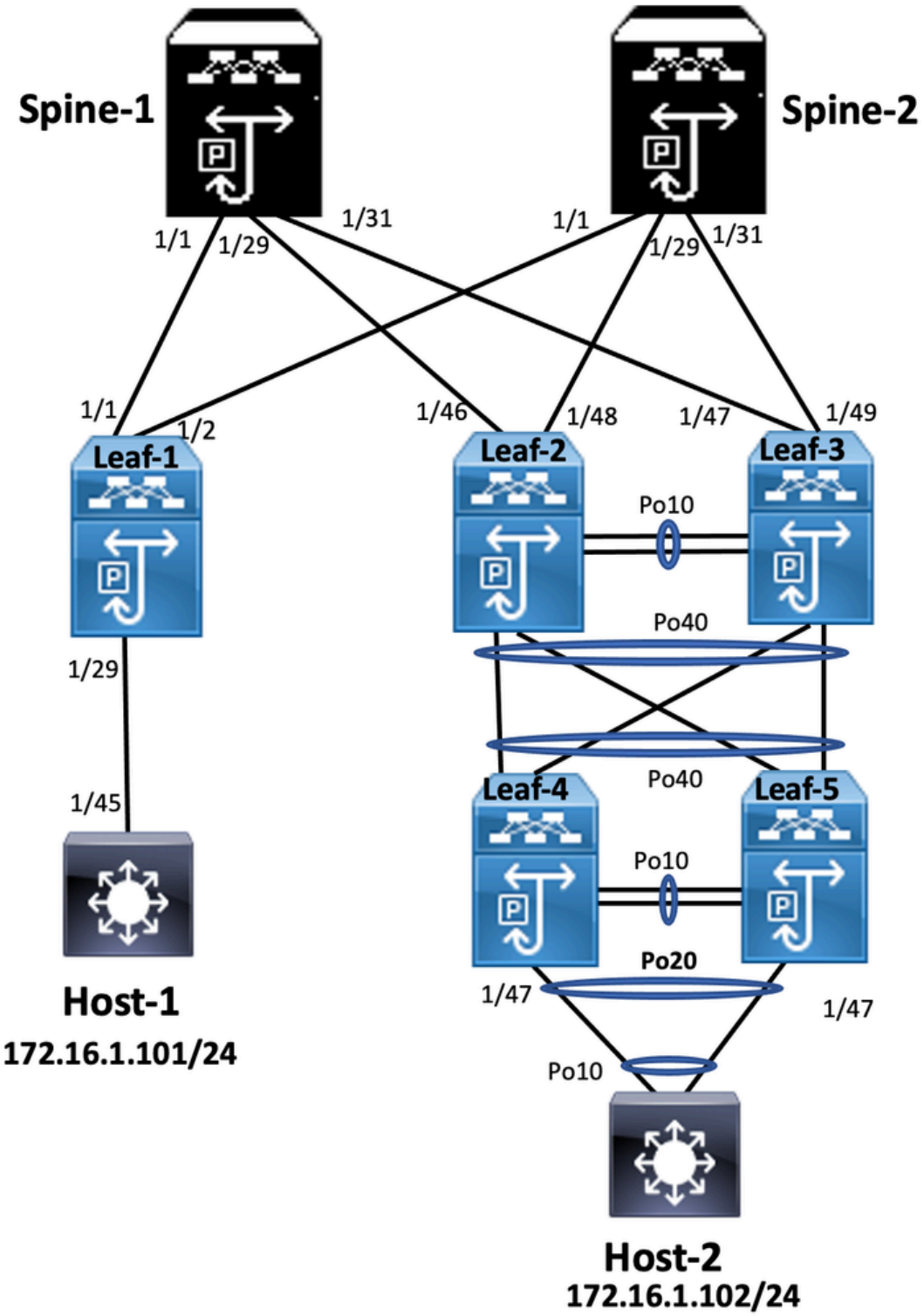
Use esta seção para confirmar se a sua configuração funciona corretamente.

```
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
```

Configurar vPC com Dois Lados

Diagrama de Rede



<#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-switch
  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
```

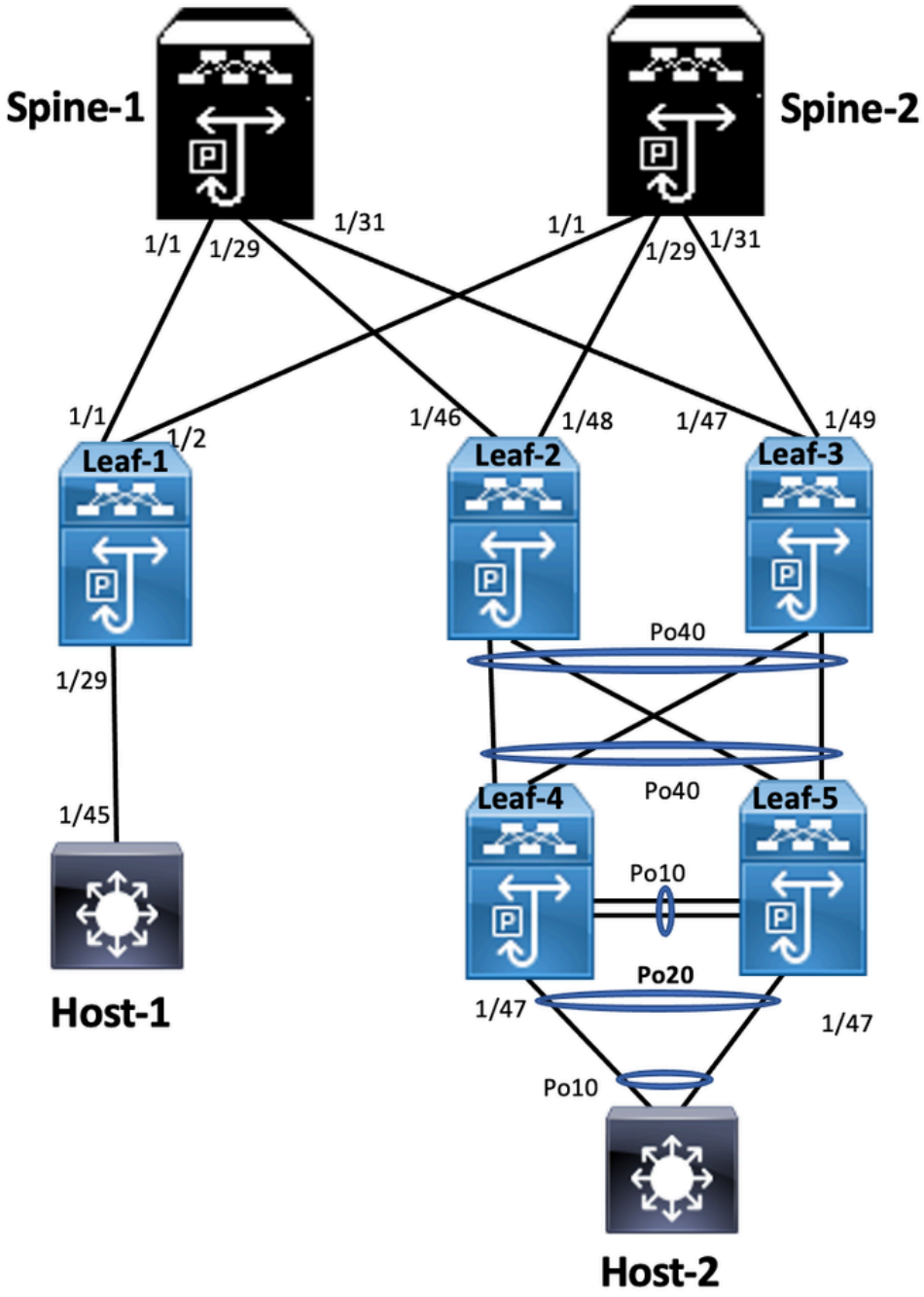
```
  vpc 40
```

Leaf-5

```
Leaf-5(config-if)# show running-config vpc
feature vpc

vpc domain 2
  peer-switch
  peer-keepalive destination 10.201.182.28 source 10.201.182.29
  peer-gateway

interface port-channel10
  vpc peer-link

interface port-channel20
  vpc 20

interface port-channel40
  vpc 40
```

Configurar vPC de dupla face com vPC Fabric Peering

Diagrama de Rede



No vPC de dois lados, ambos os switches Nexus 9000 executam o vPC. Cada par de vPCs dos switches Nexus 9000 é conectado ao par de vPC de agregação com um vPC exclusivo.

<#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 double-sided vPC.
```

Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

```
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
```

```
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
```

```
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<

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
```

```
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

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)#
```

```
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
---------------- ---- --- --------- -------- --
```

```
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
---------------- ---- --- --------- -------- --
------------------------------
```

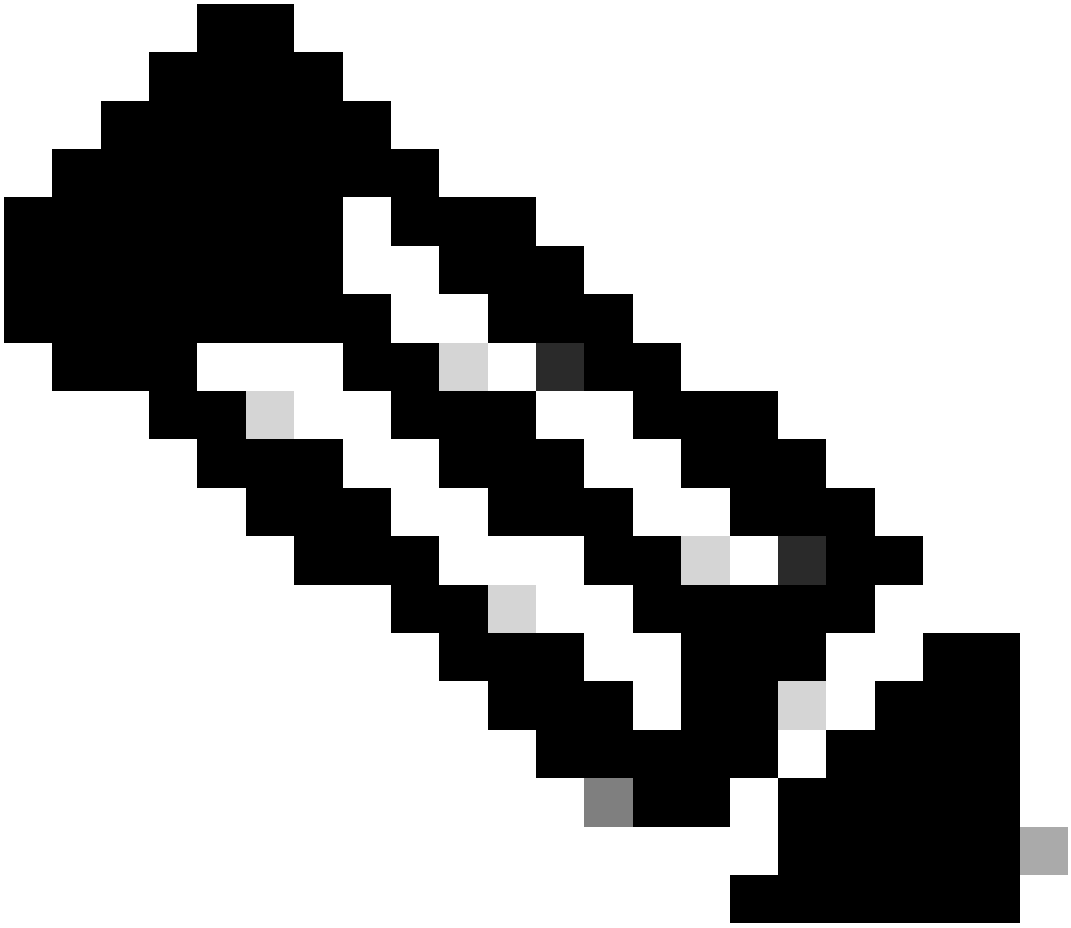
```
------------------------------
Eth1/47          Desg FWD 4         128.185
P2p

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
---------------- ---- --- --------- -------- --
------------------------------
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)#
```

```
Po10             Root FWD 4         128.4105
(vPC peer-link) Network P2p
Po40             Desg FWD 1         128.4135
(vPC) P2p

Leaf-3(config-if-range)#
```

Práticas recomendadas para ISSU com vPC

Esta seção descreve as práticas recomendadas para o upgrade de software sem interrupções, use o Cisco ISSU quando um domínio vPC estiver configurado. O recurso vPC System NX-OS Upgrade (ou Downgrade) vPC é totalmente compatível com o Cisco ISSU.

Em um ambiente vPC, o ISSU é o método recomendado para atualizar o sistema. O sistema vPC pode ser atualizado independentemente sem interrupção do tráfego. A atualização é serializada e deve ser executada uma de cada vez. O bloqueio de configuração durante o ISSU impede que ocorram atualizações síncronas em ambos os dispositivos pares do vPC (a configuração é bloqueada automaticamente em outro dispositivo par do vPC quando o ISSU é iniciado). Para executar a operação do ISSU, é necessário um único botão.



Note: O vPC com FEX (host vPC) também oferece suporte total ao ISSU. Não há perda de pacotes quando o domínio vPC atualizado tem FEX. O servidor com conexão dupla a 2 FEX diferentes através de um canal de porta padrão não está ciente de que a operação de atualização ocorre na rede.

<#root>

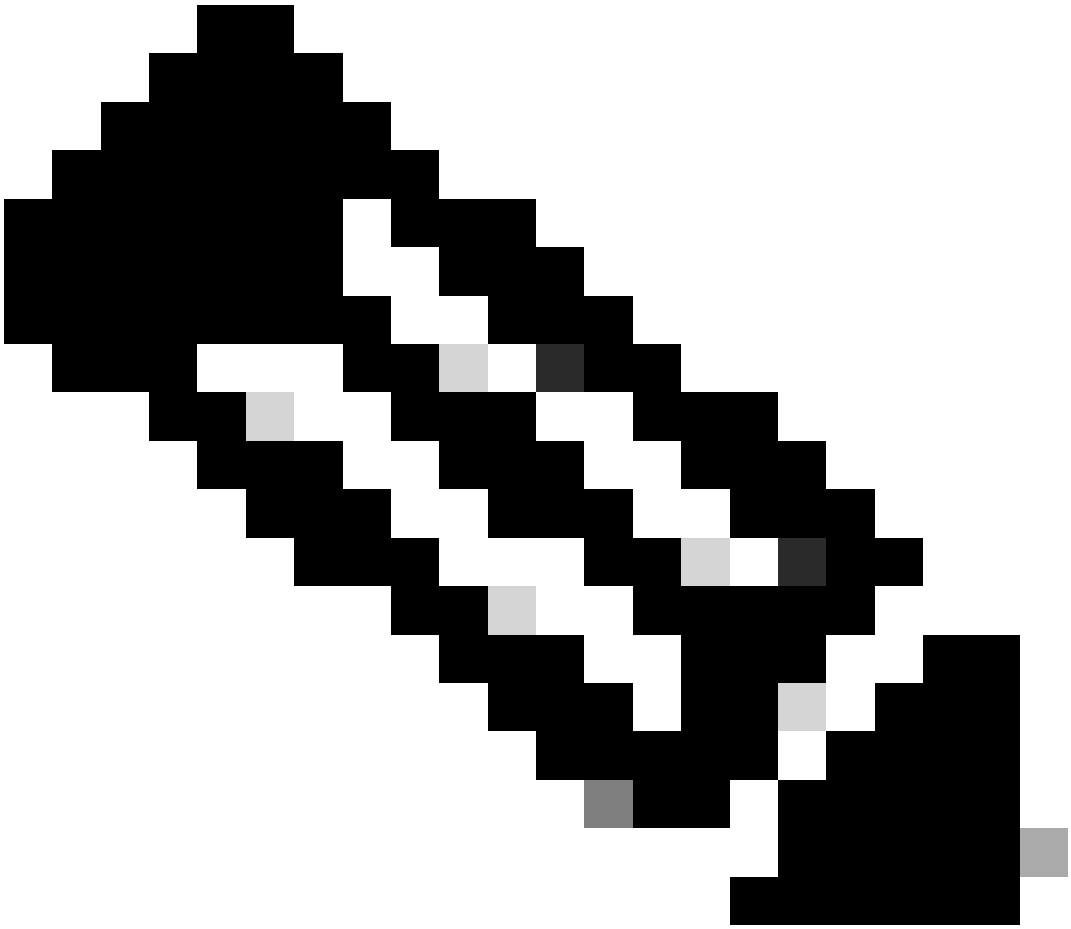
switch#install all nxos bootflash:

Recomendações fortes

O dispositivo par do vPC 1, 9K1 (carrega o código primeiro no dispositivo par do vPC primário ou secundário não tem importância) usa ISSU. Observe que outros dispositivos pares do vPC (9K2) têm sua configuração bloqueada para proteção contra qualquer operação no switch.

- Use o ISSU (In-Service Software Upgrade) para alterar a versão do código do NX-OS para o

domínio vPC. Execute a operação sequencialmente, um dispositivo vPC por vez.
- Consulte as notas de versão do NX-OS para selecionar corretamente a versão de código do NX-OS de destino com base no código do dispositivo (matriz de compatibilidade ISSU)



Note: O upgrade 9k1 de 7.x para 9.3.8/9.3.9 causou a inatividade da porta de 40g no vPC. Se o link par estiver conectado a 40 G, é recomendável atualizar ambos os switches para 9.3.8/9.3.9 para ativar 40G ou o caminho deve seguir: I7(7) - 9.3(1) - 9.3(9)

Práticas recomendadas durante a substituição do switch vPC

Pré-verificações

```
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
```

Etapas

1. Feche todas as portas membro do vPC uma por uma.
2. Desligue todas as portas órfãs.
3. Desligue todos os links físicos da Camada 3, um por um.
4. Desligue o link vPC Peer Keep Alive (PKA).
5. Desligue o link par do vPC.
6. Certifique-se de que todas as portas estejam desativadas no switch problemático.
7. Assegure-se de que o tráfego seja desviado para o switch redundante através de comandos compartilhados no 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. Verifique se o dispositivo de substituição está configurado com a imagem e a licença corretas.

```
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 o switch com a configuração de backup corretamente.
10. Se a recuperação automática estiver habilitada, desabilite-a durante a substituição.

```
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. Certifique-se de que o bit Sticky esteja definido como 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 o bit Sticky for definido como True, reconfigure a prioridade da função vPC. Isso significa reaplicar a configuração original para a prioridade de função.
    - O domínio vPC 1 <== 1 é o número de domínio vPC mencionado no switch original
    - role priority 2000 <== exemplo: se 2000 for uma prioridade de função vPC definida no switch original
13. Ative as interfaces estritamente nesta ordem:
    1. Ative o link de peer keep-alive.
    2. Ative o link par do vPC.
    3. Confirme se a função vPC foi estabelecida corretamente.

4. Ative o restante das interfaces nos switches, uma a uma, nesta ordem:
    1. Portas membro vPC
    2. Portas órfãs (portas não vPC)
    3. Interface física de Camada 3

Verificação pós-validação

```
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
```

Considerações sobre vPC para implantação de VXLAN

- Na vPC VXLAN, é recomendável aumentar o temporizador de interface vlan de restauração de atraso na configuração vPC, se o número de SVIs for aumentado. Por exemplo, se houver 1.000 VNIs com 1.000 SVIs, é recomendável aumentar o atraso do temporizador de restauração interface-vlan para 45 segundos.

  <#root>

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

- Para vPC, a interface de loopback tem dois endereços IP: o endereço IP primário e o endereço IP secundário.
    - O endereço IP primário é exclusivo e é usado pelos protocolos da camada

3.
    - O endereço IP secundário no loopback é necessário porque a interface NVE o utiliza para o endereço IP VTEP. O endereço IP secundário deve ser o mesmo em ambos os pares do vPC.
- O temporizador de retenção NVE precisa ser maior que o temporizador de restauração de atraso 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 as práticas recomendadas, habilite a recuperação automática no ambiente do vPC. Embora raro, há uma chance de que o recurso de recuperação automática do vPC possa colocar você em um cenário ativo duplo.
- O recurso Peer-Switch vPC permite que um par de dispositivos pares vPC apareça como uma única raiz de Spanning Tree Protocol na topologia da Camada 2 (eles têm o mesmo ID de bridge). O peer-switch vPC deve ser configurado em ambos os dispositivos pares vPC para se tornar operacional. O comando é:

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

- O vPC Peer-Gateway permite que um dispositivo de peer do vPC atue como gateway ativo para pacotes endereçados ao roteador MAC de outro dispositivo de peer. Ele mantém o encaminhamento de tráfego local para o dispositivo de peer do vPC e evita o uso do link de peer. Não há impacto no tráfego e na funcionalidade quando ele ativa o recurso Peer-Gateway.

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

- Foi introduzido o comando peer-router da camada 3, que permite o roteamento através do 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
```

Recomendações fortes

- Peer-gateway deve ser habilitado antes do peer-router de Camada 3.
- Ambos os pares do vPC devem ter o peer-router da camada 3 configurado para entrar em vigor.
- Habilite Supress-arp como uma prática recomendada enquanto multicast ip address for VXLAN.
- Use um endereço ip de loopback separado para controle e dataplane na estrutura vPC VXLAN.
- No vPC com MSTP, a prioridade de bridge deve ser a mesma em ambos os pares do vPC.
- Para obter os melhores resultados de convergência, ajuste fino da restauração de atraso do vPC e temporizadores de retenção da interface NVE.

Informações Relacionadas

- Documentação dos switches Nexus 9000 Series
- Guia de configuração das interfaces Cisco Nexus 9000 Series NX, versão 9.3(x)
- Cisco Nexus 9000 Series NX-OS Verified Scalability Guide, versão 9.2(1) - inclui números de escalabilidade do vPC (CCO)
- Versões recomendadas do Cisco NX-OS para switches Cisco Nexus 9000 Series
- Notas da versão dos switches Nexus 9000 Series
- Guia de configuração do Cisco Nexus 9000 Series NX-OS VXLAN, versão 9.2(x) - seção

sobre vPC Fabric Peering

- Exemplo de Configuração de Sobreposição de IPV6 EVPN Vxlan
- Guia de design e configuração: As Melhores formas de aprendizado para os Virtual Port Channels (vPC) nos switches Cisco Nexus 7000 Series - a teoria do vPC N7k e N9k é similar e esta referência abrange informações adicionais sobre as melhores formas de aprendizado
- Configurar e verificar o vPC virtual de dupla face

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.