ルートサーバを使用したNexus EVPN-VXLANマルチサイトの設定

内容

はじめに

このドキュメントでは、ルートサーバ統合を使用して、Cisco Nexus 9000スイッチ上でEVPN/VXLANマルチサイト環境を設定および確認する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- マルチプロトコルラベルスイッチング(MPLS)レイヤ3 VPN
- マルチプロトコルボーダーゲートウェイプロトコル(MP-BGP)
- イーサネットVPN/仮想拡張LAN(EVPN/VXLAN)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Nexus 9000シリーズスイッチ（ラボ環境で使用される特定のモデル）
- 提示された例で設定されているソフトウェアおよびハードウェアのバージョン

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して

ください。

背景説明

データセンターは、あらゆるビジネス環境をサポートするために必要な処理能力、ストレージ、およびアプリケーションを備えたリソースプールです。

データセンターインフラストラクチャ設計を適切に計画することが重要です。このドキュメントでは、病院のネットワークなどの重要な要件と、それらの要件を満たす、またはそれを超える方法について説明します。

現代のITインフラストラクチャおよびデータセンターの展開には、ハイアベイラビリティ(HA)、より高速な拡張、常に高いパフォーマンスが必要です。

DC設計/アーキテクチャスペースの重要な要件には、次のようなものがあります。

- ポート密度はファブリックエクステンダ(FEX)によって向上します。
- コンピューティング能力は、ハードウェア仮想化(UCS)によって向上します。
- アクセスレイヤのアップリンク帯域幅は、ポートチャネルによって改善されます。
- シャーシレベルの冗長性はvPCによって向上します。
- ソフトウェア定義型ネットワーキング(SDN)ファブリックは、アプリケーションセントリックインフラストラクチャ(ACI)によって改善され、ファブリックのアンダーレイとオーバーレイを自動化します。
- Data Center Network Manager(DCNM)により、新しいサービスの迅速な導入とサポートが向上します。
- 長距離アプリケーションの帯域幅要件は、ダークファイバまたは波長サービスによって改善されます。

地理的冗長性と拡張性は、データセンター環境をスケールアウトするための重要な属性です。マルチサイトVXLAN/EVPNは、より優れたデータセンター相互接続(DCI)ソリューションの提供に役立ちます。

外部接続には、ネットワークの他の部分（インターネット、WAN、またはキャンパス）へのデータセンターの接続が含まれます。外部接続用に提供されるオプションはすべてマルチテナント対応で、外部ネットワークドメインへのレイヤ3(L3)転送に重点を置いています。

EVPNは次世代のオールインワンVPNソリューションです。これは、他の多くのVPNテクノロジーの役割を果たすだけでなく、より優れています。機能には、次のものがあります。

- レガシーネットワークとの統合
- 選択的なアドバタイズメント/拡張：レイヤ2(L2) – タイプ2ルートを持つ特定のVLAN/サブネットのみを拡張します。タイプ5のルートを持つ特定のL3ドメインのみにL3を拡張します。
- タイプ4ルートによる冗長グループの自動検出。
- エイリアス、アドレスの大量引き出し、タイプ1ルートによるスプリットホライズン(SH)マルチホーミング(MH)表示。
- タイプ3ルートによるマルチキャストトンネルエンドポイントおよびマルチキャスト(MCAST)トンネルタイプの自動検出。

その他の利点：

- データセンターとクラウド間でのワークロードバランシング
- 中断に対するプロアクティブな対応：ハリケーンや洪水などの災害が近づくリスクを軽減します。
- データセンターのメンテナンスと移行：計画されたイベントを一定期間にわたってスケジュールし、レガシーネットワークと統合します。
- バックアップと障害回復サービス(aaS)。

設定

ネットワーク図

作成者が入力するプレースホルダコンテンツ

サイト1のリーフ1の設定

これは、サイト1のリーフ1の設定です。各コマンドは、重要な機能を有効にし、EVPN-VXLANマルチサイト動作に必要なインターフェイス、VRF、VLAN、およびルーティングプロトコルを設定します。

```
feature nxapi
cfs ipv4 distribute
nv overlay evpn
feature ospf
feature bgp
feature pim
feature fabric forwarding
feature interface-vlan
feature vn-segment-vlan-based
feature lacp
feature vpc
feature nv overlay
fabric forwarding anycast-gateway-mac 0000.1111.2222
ip pim rp-address 10.102.0.2 group-list 224.0.0.0/4
ip pim ssm range 232.0.0.0/8
ip igmp snooping vxlan
vlan 1,100,200,300-350,2001
vlan 100
vn-segment 4000100
vlan 200
vn-segment 4000200
vlan 301
vn-segment 4000301
vlan 302
vn-segment 4000302
vlan 303
vn-segment 4000303
vlan 350
name L3-VNI
vn-segment 4000999
vlan 2001
vn-segment 4000502
```

```
vrf context L3VNI4000999
vni 4000999
rd auto
address-family ipv4 unicast
route-target both auto
route-target both auto evpn
vrf context vrf_1
vni 4000501
rd auto
address-family ipv4 unicast
route-target both auto
route-target both auto evpn
vrf context vrf_2
vni 4000502
rd auto
address-family ipv4 unicast
route-target both auto
route-target both auto evpn
vpc domain 100
peer-switch
peer-keepalive destination 10.197.214.54 source 10.197.214.53
virtual peer-link destination 10.102.1.9 source 10.102.1.8 dscp 56
delay restore 150
peer-gateway
ip arp synchronize
interface Vlan100
no shutdown
mtu 9216
vrf member vrf_2
no ip redirects
ip address 192.168.100.254/24
no ipv6 redirects
fabric forwarding mode anycast-gateway
interface Vlan200
no shutdown
mtu 9216
vrf member vrf_2
no ip redirects
ip address 192.168.200.254/24
no ipv6 redirects
fabric forwarding mode anycast-gateway
interface Vlan301
no shutdown
mtu 9216
vrf member vrf_1
no ip redirects
ip address 172.16.11.254/24
no ipv6 redirects
fabric forwarding mode anycast-gateway
interface Vlan302
no shutdown
mtu 9216
vrf member vrf_1
no ip redirects
ip address 172.16.12.254/24
no ipv6 redirects
fabric forwarding mode anycast-gateway
interface Vlan303
no shutdown
mtu 9216
vrf member vrf_1
no ip redirects
```

```
ip address 172.16.13.254/24
no ipv6 redirects
fabric forwarding mode anycast-gateway
interface Vlan2001
no shutdown
mtu 9000
vrf member vrf_2
no ip redirects
ip forward
ipv6 address use-link-local-only
no ipv6 redirects
interface port-channel10
switchport
switchport mode trunk
switchport trunk allowed vlan 100,200,300-350,2001
spanning-tree port type network
vpc peer-link
interface port-channel100
switchport
switchport mode trunk
switchport trunk allowed vlan 100,200
mtu 9216
vpc 100
interface nve1
no shutdown
host-reachability protocol bgp
advertise virtual-rmac
source-interface loopback1
member vni 4000100
suppress-arp
mcast-group 231.0.0.1
member vni 4000200
suppress-arp
mcast-group 231.0.0.2
member vni 4000502
associate-vrf
interface Ethernet1/1
switchport
switchport mode trunk
switchport trunk allowed vlan 100,200
mtu 9216
channel-group 100
no shutdown
interface Ethernet1/2
mtu 9216
port-type fabric
medium p2p
ip address 192.168.17.12/24
ip ospf network point-to-point
ip router ospf 100 area 0.0.0.0
ip pim sparse-mode
no shutdown
interface loopback0
ip address 10.102.0.5/32
ip router ospf 100 area 0.0.0.0
ip pim sparse-mode
interface loopback1
ip address 10.102.1.8/32
ip address 10.201.201.201/32 secondary
ip router ospf 100 area 0.0.0.0
ip pim sparse-mode
router ospf 100
```

```
router-id 10.102.0.5
router bgp 100
router-id 10.102.0.5
log-neighbor-changes
address-family l2vpn evpn
advertise-pip
neighbor 10.102.0.2
remote-as 100
update-source loopback0
address-family ipv4 unicast
address-family ipv6 unicast
send-community
send-community extended
address-family l2vpn evpn
send-community
send-community extended
neighbor 10.102.0.3
remote-as 100
update-source loopback0
address-family ipv4 unicast
address-family ipv6 unicast
send-community
send-community extended
address-family l2vpn evpn
send-community
send-community extended
evpn
vni 4000100 l2
rd auto
route-target import auto
route-target export auto
vni 4000200 l2
rd auto
route-target import auto
route-target export auto
vni 4000301 l2
rd auto
route-target import auto
route-target export auto
vni 4000302 l2
rd auto
route-target import auto
route-target export auto
vni 4000303 l2
rd auto
route-target import auto
route-target export auto
```

サイト1のリーフ2の設定

```
feature nxapi
feature sftp-server
cfs ipv4 distribute
nv overlay evpn
feature ospf
feature bgp
feature pim
```

```
feature fabric forwarding
feature interface-vlan
feature vn-segment-vlan-based
feature lacp
feature vpc
feature nv overlay
fabric forwarding anycast-gateway-mac 0000.1111.2222
ip pim rp-address 10.102.0.2 group-list 224.0.0.0/4
ip pim ssm range 232.0.0.0/8
vlan 1,100,200,300-350,2001
vlan 100
vn-segment 4000100
vlan 200
vn-segment 4000200
vlan 301
vn-segment 4000301
vlan 302
vn-segment 4000302
vlan 303
vn-segment 4000303
vlan 350
name L3-VNI
vn-segment 4000999
vlan 2001
vn-segment 4000502
vrf context L3VNI4000999
vni 4000999
rd auto
address-family ipv4 unicast
route-target both auto
route-target both auto evpn
vrf context vrf_1
vni 4000501
rd auto
address-family ipv4 unicast
route-target both auto
route-target both auto evpn
vrf context vrf_2
vni 4000502
rd auto
address-family ipv4 unicast
route-target both auto
route-target both auto evpn
vpc domain 100
peer-switch
peer-keepalive destination 10.197.214.53 source 10.197.214.54
virtual peer-link destination 10.102.1.8 source 10.102.1.9 dscp 56
delay restore 150
peer-gateway
ip arp synchronize
interface Vlan100
no shutdown
mtu 9216
vrf member vrf_2
no ip redirects
ip address 192.168.100.254/24
no ipv6 redirects
fabric forwarding mode anycast-gateway
interface Vlan200
no shutdown
mtu 9216
vrf member vrf_2
```

```
no ip redirects
ip address 192.168.200.254/24
no ipv6 redirects
fabric forwarding mode anycast-gateway
interface Vlan301
no shutdown
mtu 9216
vrf member vrf_1
no ip redirects
ip address 172.16.11.254/24
no ipv6 redirects
fabric forwarding mode anycast-gateway
interface Vlan302
no shutdown
mtu 9216
vrf member vrf_1
no ip redirects
ip address 172.16.12.254/24
no ipv6 redirects
fabric forwarding mode anycast-gateway
interface Vlan303
no shutdown
mtu 9216
vrf member vrf_1
no ip redirects
ip address 172.16.13.254/24
no ipv6 redirects
fabric forwarding mode anycast-gateway
interface Vlan2001
no shutdown
mtu 9000
vrf member vrf_2
no ip redirects
ip forward
ipv6 address use-link-local-only
no ipv6 redirects
interface port-channel10
switchport
switchport mode trunk
switchport trunk allowed vlan 100,200,300-350,2001
spanning-tree port type network
vpc peer-link
interface port-channel100
switchport
switchport mode trunk
switchport trunk allowed vlan 100,200
mtu 9216
vpc 100
interface nve1
no shutdown
host-reachability protocol bgp
advertise virtual-rmac
source-interface loopback1
member vni 4000100
suppress-arp
mcast-group 231.0.0.1
member vni 4000200
suppress-arp
mcast-group 231.0.0.2
member vni 4000502
associate-vrf
interface Ethernet1/1
```

```
switchport
switchport mode trunk
switchport trunk allowed vlan 100,200
mtu 9216
channel-group 100
no shutdown
interface Ethernet1/2
mtu 9216
port-type fabric
medium p2p
ip address 192.168.18.12/24
ip ospf network point-to-point
ip router ospf 100 area 0.0.0.0
ip pim sparse-mode
no shutdown
interface loopback0
ip address 10.102.0.8/32
ip router ospf 100 area 0.0.0.0
ip pim sparse-mode
interface loopback1
ip address 10.102.1.9/32
ip address 10.201.201.201/32 secondary
ip router ospf 100 area 0.0.0.0
ip pim sparse-mode
icam monitor scale
router ospf 100
router-id 10.102.0.8
router bgp 100
router-id 10.102.0.8
log-neighbor-changes
address-family l2vpn evpn
advertise-pip
neighbor 10.102.0.2
remote-as 100
update-source loopback0
address-family ipv4 unicast
address-family ipv6 unicast
send-community
send-community extended
address-family l2vpn evpn
send-community
send-community extended
neighbor 10.102.0.3
remote-as 100
update-source loopback0
address-family ipv4 unicast
address-family ipv6 unicast
send-community
send-community extended
address-family l2vpn evpn
send-community
send-community extended
evpn
vni 4000100 l2
rd auto
route-target import auto
route-target export auto
vni 4000200 l2
rd auto
route-target import auto
route-target export auto
vni 4000301 l2
```

```
rd auto
route-target import auto
route-target export auto
vni 4000302 l2
rd auto
route-target import auto
route-target export auto
vni 4000303 l2
rd auto
route-target import auto
route-target export auto
```

ドキュメントの簡潔さと読みやすさを考慮して、追加デバイスの完全な設定がソースコンテンツに含まれており、そこから参照できます。各設定は上記と同じ詳細構造に従い、必要な機能を有効にし、VLAN、VNI、VRF、インターフェイス、およびルーティングプロトコルを定義し、各デバイスの役割に応じてNVE、BGP EVPN、およびマルチサイト境界ゲートウェイ(BGP-BGP)パラメータを設定します。

確認

このセクションでは、EVPN-VXLANマルチサイト設定が動作していることを確認するための検証手順と出力例を示します。

手順1:pingを使用してエンドツーエンド接続を確認する

```
Host2# ping 192.168.200.103
PING 192.168.200.103 (192.168.200.103): 56 data bytes
64 bytes from 192.168.200.103: icmp_seq=0 ttl=254 time=1.21 ms
64 bytes from 192.168.200.103: icmp_seq=1 ttl=254 time=0.627 ms
64 bytes from 192.168.200.103: icmp_seq=2 ttl=254 time=0.74 ms
64 bytes from 192.168.200.103: icmp_seq=3 ttl=254 time=0.737 ms
64 bytes from 192.168.200.103: icmp_seq=4 ttl=254 time=0.542 ms
--- 192.168.200.103 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.542/0.771/1.21 ms
```

手順2：追加のpingを使用したL2およびL3の到達可能性の確認

```
Host2# ping 192.168.100.103
PING 192.168.100.103 (192.168.100.103): 56 data bytes
64 bytes from 192.168.100.103: icmp_seq=0 ttl=254 time=1.195 ms
64 bytes from 192.168.100.103: icmp_seq=1 ttl=254 time=0.613 ms
64 bytes from 192.168.100.103: icmp_seq=2 ttl=254 time=0.575 ms
64 bytes from 192.168.100.103: icmp_seq=3 ttl=254 time=0.522 ms
64 bytes from 192.168.100.103: icmp_seq=4 ttl=254 time=0.534 ms
--- 192.168.100.103 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.522/0.687/1.195 ms
```

```
Host2# ping 192.168.100.100
PING 192.168.100.100 (192.168.100.100): 56 data bytes
64 bytes from 192.168.100.100: icmp_seq=0 ttl=254 time=1.029 ms
64 bytes from 192.168.100.100: icmp_seq=1 ttl=254 time=0.561 ms
64 bytes from 192.168.100.100: icmp_seq=2 ttl=254 time=0.579 ms
64 bytes from 192.168.100.100: icmp_seq=3 ttl=254 time=0.511 ms
64 bytes from 192.168.100.100: icmp_seq=4 ttl=254 time=0.496 ms
--- 192.168.100.100 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.496/0.635/1.029 ms
```

```
HOST_3(config)# ping 192.168.100.100
PING 192.168.100.100 (192.168.100.100): 56 data bytes
64 bytes from 192.168.100.100: icmp_seq=0 ttl=254 time=1.319 ms
64 bytes from 192.168.100.100: icmp_seq=1 ttl=254 time=0.77 ms
64 bytes from 192.168.100.100: icmp_seq=2 ttl=254 time=0.505 ms
64 bytes from 192.168.100.100: icmp_seq=3 ttl=254 time=0.542 ms
64 bytes from 192.168.100.100: icmp_seq=4 ttl=254 time=0.486 ms
--- 192.168.100.100 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.486/0.724/1.319 ms
```

ステップ3:ARPテーブルの確認

```
device# show ip arp
Flags: * - Adjacencies learnt on non-active FHRP router
+ - Adjacencies synced via CFSoE
# - Adjacencies Throttled for Glean
CP - Added via L2RIB, Control plane Adjacencies
PS - Added via L2RIB, Peer Sync
RO - Re-Originated Peer Sync Entry
D - Static Adjacencies attached to down interface

IP ARP Table for context default
Total number of entries: 8
Flags
```

手順4:MACアドレステーブルを確認する

```
device# show mac address-table
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,
+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan

VLAN    MAC Address       Type    age     Secure  NTFY    Ports
---------+-----------------+--------+---------+------+----+------------------
```

手順5:BGP EVPNルートの確認

```
device# show bgp l2vpn evpn
BGP routing table information for VRF default, address family L2VPN EVPN
BGP table version is 3291, Local Router ID is 10.102.0.5
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best
Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist, I-inject
Origin codes: i - IGP, e - EGP, ? - incomplete, | - multipath, & - backup, 2 - best2
Network Next Hop Metric LocPrf Weight Path
*>i[2]:[0]:[0]:[48]:[6c8b.d3fe.df3b]:[32]:[192.168.100.104]/27 210. 100. 100. 1 100 0 300 200 i
...
```

ステップ6:vPCステータスの確認

```
device# show vpc brief
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
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 = 150s)
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           : Enabled
vPC Peer-link status
id  Port    Status Active vlans
1   Po10    up     100,200,300-350,2001
vPC status
Id  Port    Status Consistency Reason   Active vlans
100 Po100   up     success    success   100,200
```

トラブルシュート

このセクションでは、EVPN-VXLANマルチサイト設定をトラブルシューティングするためのコマンドとアプローチについて説明します。

手順1:ARPテーブルの確認

```
device# show ip arp
Flags: * - Adjacencies learnt on non-active FHRP router
+ - Adjacencies synced via CFSoE
# - Adjacencies Throttled for Glean
CP - Added via L2RIB, Control plane Adjacencies
PS - Added via L2RIB, Peer Sync
RO - Re-Originated Peer Sync Entry
D - Static Adjacencies attached to down interface

IP ARP Table for context default
Total number of entries: 8
Flags
```

手順2:MACアドレステーブルを確認する

```
device# show mac address-table
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,
+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan

VLAN     MAC Address       Type     age      Secure  NTFY    Ports
---------+-----------------+--------+---------+------+----+------------------
```

ステップ3:BGP EVPNの確認

```
device# show bgp l2vpn evpn
```

手順4:vPCステータスの確認

```
device# show vpc brief
```

ステップ5:Cisco CLIアナライザの使用

Cisco CLI アナライザ (登録ユーザ専用) は、特定の show コマンドをサポートします。show コマンド出力の分析を表示するには、Cisco CLI アナライザを使用します。

関連情報

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。