ACI VMM統合のトラブルシューティング

内容

概要

このドキュメントでは、ACI Virtual Machine Manager(VM)統合(VMM)の説明とトラブルシューティングの手順について説明します。

背景説明

このドキュメントの内容は、『Troubleshooting Cisco Application Centric Infrastructure, Second Edition』のマニュアル、具体的には『VMM Integration - Overview, VMM Integration - vCenter Connectivity, VMM Integration - Host Dynamic Discovery』および『VMM Integration - Hypervisor Uplink Load Balancing』の章から抜粋しています。

Virtual Machine Managerの概要

ACIコントローラは、サードパーティの仮想マシンマネージャ(VMM)と統合できます。

これは、ファブリックのエンドツーエンドのネットワーキング設定とそれに接続するワークロードの運用を簡素化および自動化するACIの主要機能の1つです。ACIは、仮想マシン、ベアメタルサーバ、コンテナなど、複数のワークロードタイプに拡張できる単一のオーバーレイポリシーモデルを提供します。

この章では、特にVMware vCenter VMM統合に関連する一般的なトラブルシューティングシナリオに焦点を当てます。

読者は次の点を確認します。

- vCenter通信障害の調査。
- ホストおよびVMの動的検出プロセスと障害シナリオ。
- ハイパーバイザロードバランシングアルゴリズム。

vCenter接続

ロールベースアクセスコントロール(RBAC)

APICがvCenterコントローラとインターフェイスできるメカニズムは、特定のVMMドメインに関連付けられたユーザーアカウントによって異なります。vCenter上でAPICが正常に操作を実行できるようにするために、VMMドメインに関連付けられたvCenterユーザーに対して具体的な要件の概要を説明します。vCenterが、インベントリと構成のプッシュと取得、または管理対象インベントリ関連のイベントの監視とリスニングを行っているかどうかにかかわらず、この要件が適用されます。

このような要件に関する懸念を取り除く最も簡単な方法は、フルアクセスを持つ管理者vCenterアカウントを使用することです。ただし、ACI管理者がこのような自由を常に利用できるとは限りません。

ACIバージョン4.2以降のカスタムユーザアカウントの最小権限は次のとおりです。

- **アラーム** APICはフォルダに2つのアラームを作成します。1つはDVS用、もう1つはポートグループ用です。APICでEPGまたはVMMドメインポリシーが削除されるとアラームが発生しますが、VMが接続されているため、vCenterは対応するポートグループまたはDVSを削除できません。
- **分散スイッチ**
- **dvPortグループ**
- **フォルダ**

- **Network** APICは、ポートグループの追加または削除、ホスト/DVS MTUの設定、LLDP/CDP、LACPなどのネットワーク設定を管理します。
- **ホスト** 上記に加えてAVSを使用する場合、ユーザはAPICがDVSを作成するデータセンターのホスト権限が必要です。**Host.Configuration.Advanced settingsHost.Local operations.Reconfigure virtual machineHost.Configuration.Network configuration**これは、AVSおよび仮想レイヤ4 ~レイヤ7サービスVMの自動配置機能に必要です。AVSの場合、APICはVMKインターフェイスを作成し、OpFlexに使用されるVTEPポートグループに配置します。
- **仮想マシン** サービスグラフが使用されている場合は、仮想アプライアンスの仮想マシン権限も必要です。**仮想マシン。構成。デバイス設定の変更仮想マシン。構成。設定**

RBAC関連の問題のトラブルシューティング

RBACの問題は、VMMドメインの初期セットアップ中に最も多く発生しますが、初期セットアップがすでに行われた後にvCenter管理者がVMMドメインに関連付けられたユーザーアカウントのアクセス許可を変更した場合に発生することがあります。

症状は以下のように現れます。

- 新しいサービスを展開できない部分または完全な障害（DVSの作成、ポートグループの作成、一部のオブジェクトは正常に展開されるが、すべてではない）。
- 運用インベントリが不完全であるか、ACI管理者ビューに表示されません。
- サポートされていないvCenterの動作、または上記のいずれかのシナリオ（ポートグループの導入の失敗など）で発生した障害。
- vCenterコントローラはオフラインとして報告され、障害は接続またはクレデンシャル関連の問題があることを示します。

RBAC関連の問題のソリューション

上記のすべての権限が、VMMドメインで設定されているvCenterユーザに付与されていることを確認します。

もう1つの方法は、VMMドメイン設定で定義したのと同じクレデンシャルを使用してvCenterに直接ログインし、同様の操作（ポートグループの作成など）を試すことです。 ユーザがvCenterに直接ログインしている間に同じ操作を実行できない場合、ユーザに正しい権限が付与されないことは明らかです。

接続のトラブルシューティング

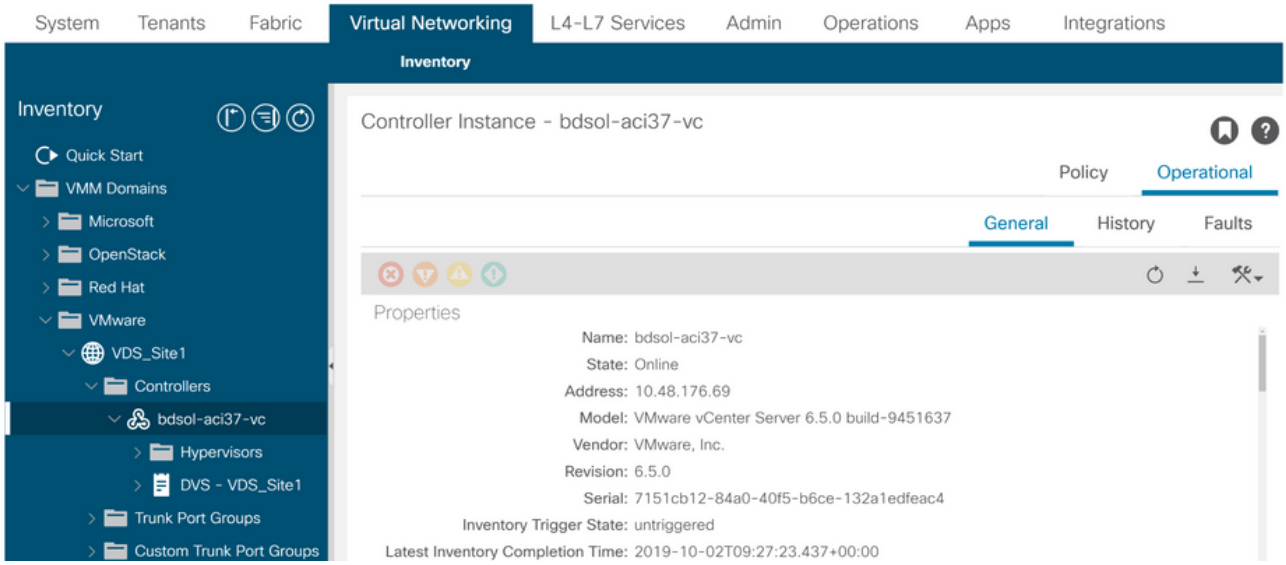
VMM接続に関連する問題をトラブルシューティングする際には、ACIがvCenterと通信する方法の基本的な動作の一部に注意することが重要です。

1つ目の最も適切な動作は、クラスタ内の1つのAPICのみが設定を送信し、任意の時点でインベントリを収集することです。このAPICは、このVMMドメインの**共有リーダー**と呼ばれます。ただし、複数のAPICが**vCenterイベント**をリッスンするのは、シャードリーダーが何らかの理由でイベントを見逃したシナリオを説明するためです。同じAPICの分散アーキテクチャに従い、特定のVMMドメインには、プライマリデータと機能を処理する1つのAPIC（この場合は共有リーダー）と、2つのレプリカ(VMMの場合は**フォロワー**)があります。 APIC間でVMMの通信と機能の処理を分散するには、任意の2つのVMMドメインに同じ共有リーダーまたは異なる共有リーダーを設

定できます。

vCenterの接続状態を確認するには、GUIで対象のVMMコントローラに移動するか、次に示すCLIコマンドを使用します。

VMWare VMMドメイン – vCenter接続状態




```
apic2# show vmware domain name VDS_Site1 vcenter 10.48.176.69
Name                          : bdsol-aci37-vc
Type                          : vCenter
Hostname or IP                : 10.48.176.69
Datacenter                    : Site1
DVS Version                   : 6.0
Status                        : online
Last Inventory Sync           : 2019-10-02 09:27:23
Last Event Seen               : 1970-01-01 00:00:00
Username                      : administrator@vsphere.local
Number of ESX Servers         : 2
Number of VMs                 : 2
Faults by Severity            : 0, 0, 0, 0
Leader                        : bdsol-aci37-apic1

Managed Hosts:
ESX              VMs       Adjacency   Interfaces
---------------  --------  ----------  ------------------------------------------------
10.48.176.66     1         Direct      leaf-101 eth1/11, leaf-102 eth1/11
10.48.176.67     1         Direct      leaf-301 eth1/11, leaf-302 eth1/11
```

VMMコントローラーがオフラインであると示された場合、次のようなエラーがスローされます。

```
Fault fltCompCtrlrConnectFailed
Rule ID:130
Explanation:
This fault is raised when the VMM Controller is marked offline. Recovery is in process.
Code: F0130
Message: Connection to VMM controller: hostOrIp with name name in datacenter rootContName in
domain: domName is failing repeatedly with error: [remoteErrMsg]. Please verify network
connectivity of VMM controller hostOrIp and check VMM controller user credentials are valid.
```

VCとAPIC間の接続の問題をトラブルシューティングするには、次の手順を使用できます。

1.シャード・リーダーの特定

APICとvCenter間の接続の問題をトラブルシューティングする最初の手順は、特定のVMMドメインの共有リーダーであるAPICを理解することです。この情報を確認する最も簡単な方法は、任意のAPICで「show vmware domain name <domain>」コマンドを実行することです。

```
apic1# show vmware domain name VDS_Site1
Domain Name                         : VDS_Site1
Virtual Switch Mode                 : VMware Distributed Switch
Vlan Domain                         : VDS_Site1 (1001-1100)
Physical Interfaces                 : leaf-102 eth1/11, leaf-301 eth1/11, leaf-302 eth1/11,
                                    leaf-101 eth1/11
Number of EPGs                      : 2
Faults by Severity                  : 0, 0, 0, 0
LLDP override                       : RX: enabled, TX: enabled
CDP override                        : no
Channel Mode override               : mac-pinning
NetFlow Exporter Policy             : no
Health Monitoring                   : no

vCenters:
Faults: Grouped by severity (Critical, Major, Minor, Warning)
vCenter               Type      Datacenter            Status    ESXs   VMs    Faults
--------------------  --------  --------------------  --------  -----  -----  ---------------
10.48.176.69          vCenter   Site1                 online    2      2      0,0,0,0

APIC Owner:
Controller    APIC      Ownership
------------  --------  ---------------
bdsol-        apic1     Leader
aci37-vc
bdsol-        apic2     NonLeader
aci37-vc
bdsol-        apic3     NonLeader
aci37-vc
```

2. vCenterへの接続の確認

vCenterとアクティブに通信しているAPICを特定した後、pingなどのツールを使用してIP接続を確認します。

```
apic1# ping 10.48.176.69
PING 10.48.176.69 (10.48.176.69) 56(84) bytes of data.
64 bytes from 10.48.176.69: icmp_seq=1 ttl=64 time=0.217 ms
64 bytes from 10.48.176.69: icmp_seq=2 ttl=64 time=0.274 ms
64 bytes from 10.48.176.69: icmp_seq=3 ttl=64 time=0.346 ms
64 bytes from 10.48.176.69: icmp_seq=4 ttl=64 time=0.264 ms
64 bytes from 10.48.176.69: icmp_seq=5 ttl=64 time=0.350 ms
^C
--- 10.48.176.69 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4084ms
rtt min/avg/max/mdev = 0.217/0.290/0.350/0.052 ms
```

vCenterがIPアドレスではなくFQDNを使用して設定されている場合は、nslookupコマンドを使用して名前解決を確認できます。

```
apic1:~> nslookup bdsol-aci37-vc
Server: 10.48.37.150
Address: 10.48.37.150#53
Non-authoritative answer:
Name: bdsol-aci37-vc.cisco.com
```

```
Address: 10.48.176.69
```

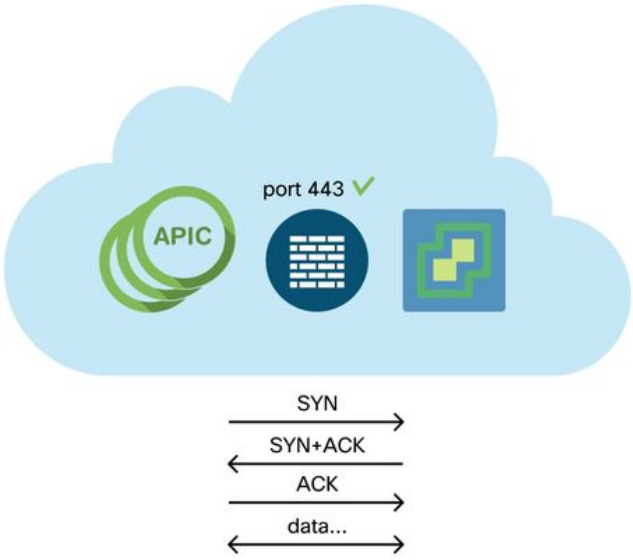
3. OOBまたはINBが使用されているかどうかを確認する

APICルーティングテーブルをチェックして、アウトオブバンドまたはインバンドのどちらが接続に適しているか、およびどのゲートウェイが使用されているかを確認します。

```
apic1# bash
admin@apic1:~> route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.48.176.1     0.0.0.0         UG    16     0        0 oobmgmt
```

4.すべてのAPICとvCenterの間（通信パス内のファイアウォールを含む）でポート443が許可されていることを確認します。

vCenter <-> APIC - HTTPS（TCPポート443）– 通信



APICからvCenterへの一般的なHTTPS到達可能性は、curlを使用してテストできます。

```
apic2# curl -v -k https://10.48.176.69
* Rebuilt URL to: https://10.48.176.69/*   Trying 10.48.176.69...
* TCP_NODELAY set
* Connected to 10.48.176.69 (10.48.176.69) port 443 (#0)
...
```

共有リーダーがnetstatコマンドを使用して、ポート443でTCP接続を確立していることを確認します。

```
apic1:~> netstat -tulaen | grep 10.48.176.69
tcp 0 0 10.48.176.57:40806 10.48.176.69:443 ESTABLISHED 600 13062800
```

5.パケットキャプチャの実行

可能であれば、トラフィックがいずれかのデバイスで送受信されているかどうかを識別するために、共有リーダーとvCenterの間のパスに沿ってパケットキャプチャを実行します。

VMwareインベントリ

次の表に、VMWare VDSパラメータの一覧を示し、APICでこれらを構成できるかどうかを指定します。

APICによって管理されるVMware VDSパラメータ

VMware VDS	デフォルト値	Cisco APICポリシーを使用して設定可能ですか。
[名前(Name)]	VMMドメイン名	はい（ドメインから取得）
説明	「APIC仮想スイッチ」	No
フォルダ名	VMMドメイン名	はい（ドメインから取得）
バージョン	vCenterによるサポートが最も高い	Yes
ディスカバリプロトコル	LLDP	Yes
アップリンクポートとアップリンク名	8	あり(Cisco APICリリース4.2(1)以降)
アップリンク名プレフィクス	アップリンク	あり(Cisco APICリリース4.2(1)以降)
最大MTU	9000	Yes
LACPポリシー	無効	Yes
ポート ミラーリング	0セッション	Yes
アラーム	2つのアラームをフォルダレベルで追加	No

次の表に、VMWare VDSポートグループのパラメータの一覧を示し、APICでこれらを構成できるかどうかを指定します。

APICによって管理されるVMWare VDSポートグループパラメーター

VMware VDSポートグループ	デフォルト値	APICポリシーを使用して設定可能
[名前(Name)]	テナント名 |アプリケーションプロファイル名 | EPG名	あり（EPGから派生）
ポートバインディング	静的結合	No
VLAN	VLANプールから取得	Yes
ロードバランシングアルゴリズム	APIC上のポートチャネルポリシーに基づいて導出	Yes
混合モード	Disabled	Yes
偽造された送信	Disabled	Yes
MACの変更	Disabled	Yes
すべてのポートをブロック	FALSE	No

VMwareインベントリのトラブルシューティング

インベントリ同期イベントは、APICがポリシーを動的に更新する必要があるvCenterイベントをAPICが認識できるようにするために発生します。vCenterとAPICの間で発生する可能性があるインベントリ同期イベントには、次の2種類があります。完全なインベントリ同期とイベントベースのインベントリ同期。APICとvCenter間の完全なインベントリ同期のデフォルトスケジュールは

24時間ごとですが、手動でトリガーすることもできます。イベントベースのインベントリ同期は通常、vMotionなどのトリガーされたタスクに関連付けられます。このシナリオでは、仮想マシンがあるホストから別のホストに移動し、それらのホストが2つの異なるリーフスイッチに接続されている場合、APICはVM移行イベントをリッスンし、オンデマンド導入の即時性のシナリオでは、ソースリーフのEPGをアンプログラムし、宛先リーフのEPGをプログラムします。

VMMドメインに関連付けられたEPGの導入の即時性によっては、vCenterからインベントリを取得できない場合に望ましくない結果が生じる可能性があります。インベントリが完了しなかったり、部分的であったりするシナリオでは、障害の原因となったオブジェクトを示す工ラーが常に発生します。

シナリオ1 – バッキングが無効な仮想マシン：

仮想マシンがあるvCenterから別のvCenterに移動された場合、または仮想マシンに無効なバッキング（古い/削除されたDVSへのポートグループの接続など）があると判断された場合、vNICに動作上の問題があることが報告されます。

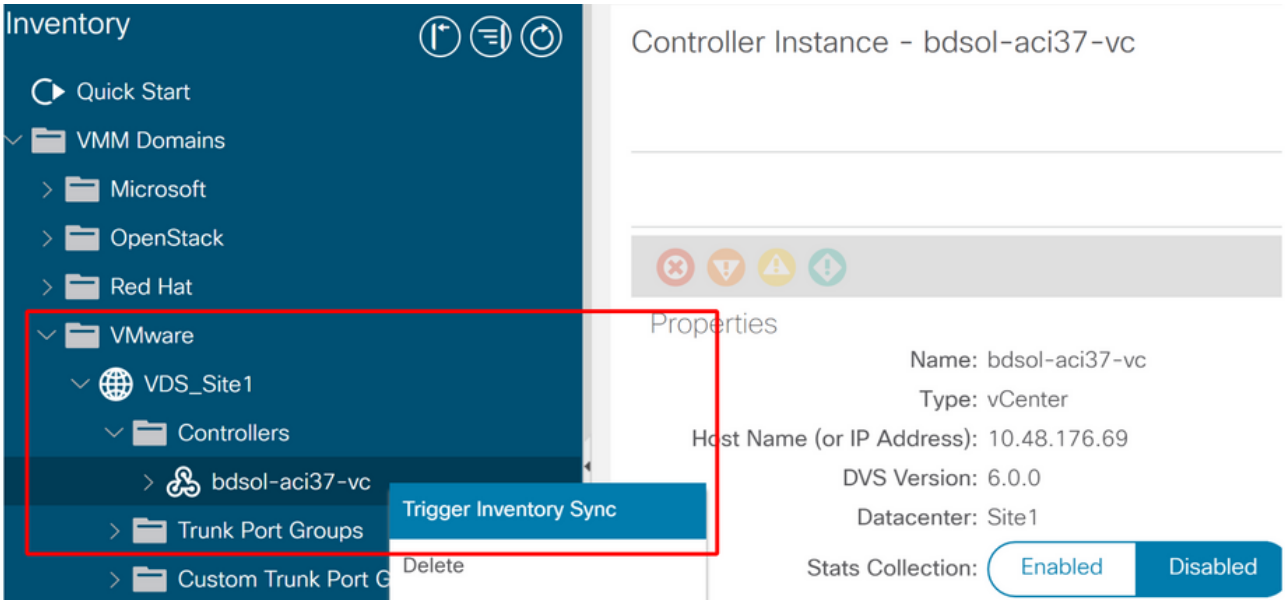
```
Fault fltCompVNicOperationalIssues
Rule ID:2842
Explanation:
This fault is raised when ACI controller failed to update the properties of a VNIC (e.g., it can
not find the EPG that the VNIC attached to).
Code: F2842
Message: Operational issues detected for VNic name on VM name in VMM controller: hostOrIp with
name name in datacenter rootContName in domain: domName due to error: issues.
Resolution:
Remediate the virtual machines indicated in the fault by assigning a valid port group on the
affected vNIC of the VM.
```

シナリオ2:vCenter管理者がvCenter上のVMM管理オブジェクトを変更しました。

vCenterからAPICによって管理されるオブジェクトの変更はサポートされていません。vCenterでサポートされていない操作を実行すると、次の工ラーが表示されます。

```
Fault fltCompCtrlrUnsupportedOperation
Rule ID:133
Explanation:
This fault is raised when deployment of given configuration fails for a Controller.
Code: F0133
Message: Unsupported remote operation on controller: hostOrIp with name name in datacenter
rootContName in domain domName detected, error: [deployIssues]
Resolution:
If this scenario is encountered, try to undo the unsupported change in vCenter and then trigger
an 'inventory sync' manually.
```

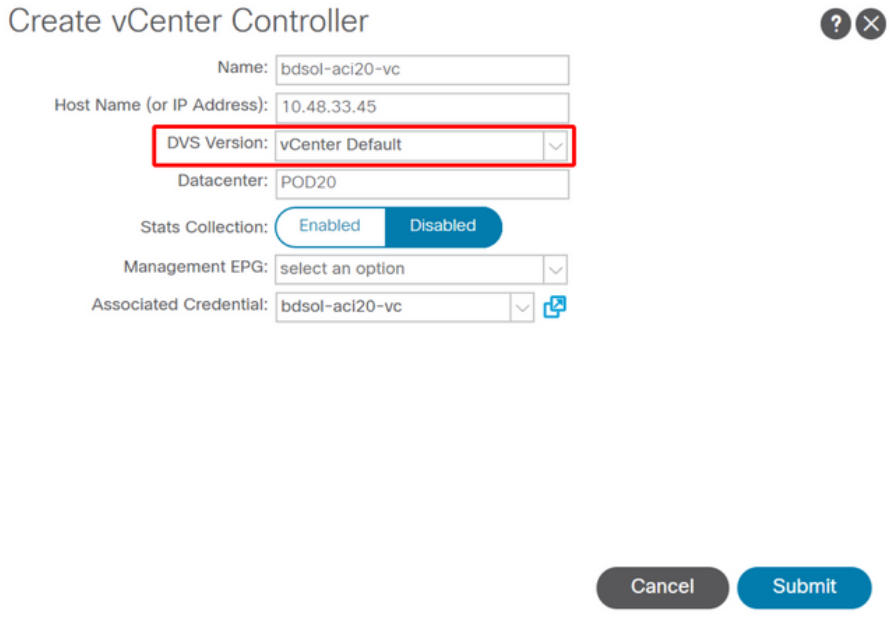
VMWare VMMドメイン – vCenterコントローラー – インベントリ同期のトリガー



VMware DVSバージョン

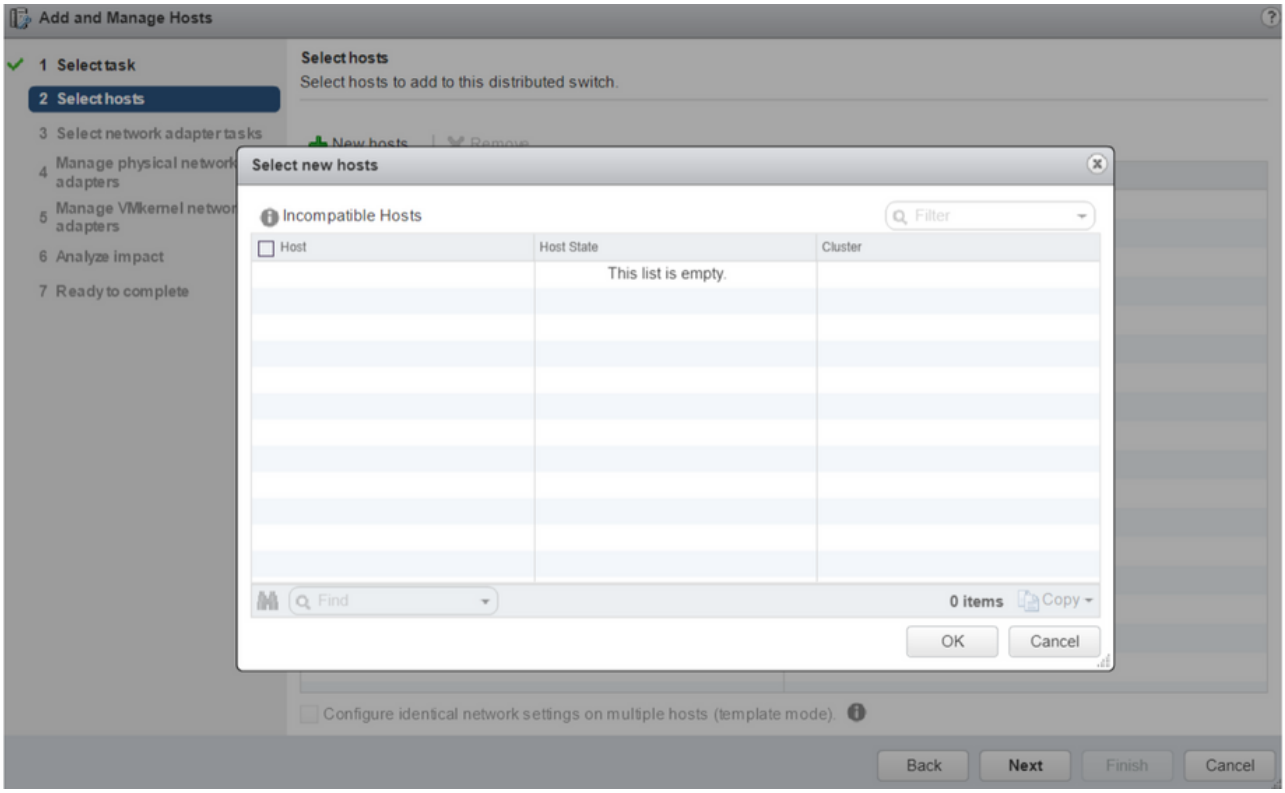
VMMドメインの一部として新しいvCenterコントローラを作成する場合、DVSバージョンのデフォルト設定では[vCenter Default]が使用されます。 これを選択すると、DVSバージョンがvCenterのバージョンで作成されます。

VMWare VMMドメイン – vCenterコントローラーの作成

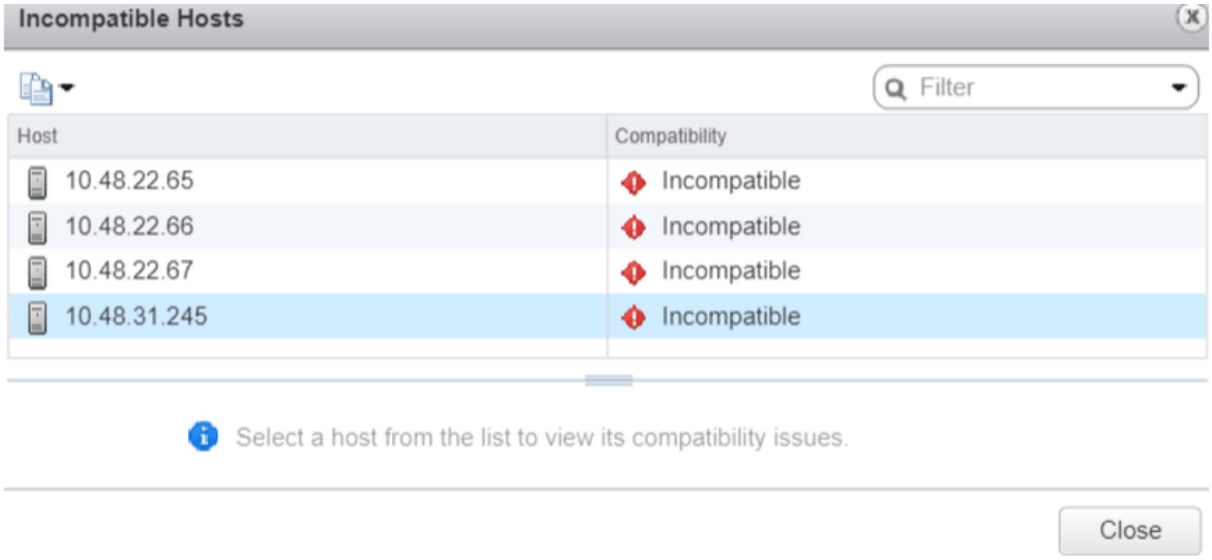


つまり、6.5を実行するvCenterと6.0を実行するESXiサーバの例では、APICがバージョン6.5のDVSを作成するため、vCenter管理者は6.0を実行するESXiサーバをACI DVSに追加できません。

APICマネージドDVS - vCenterホストの追加 – 空のリスト



APICマネージドDVS - vCenterホストの追加 – 互換性のないホスト



そのため、VMMドメインを作成するときは、必要なESXiサーバをDVSに追加できるように、正しい[DVS Version]を選択してください。

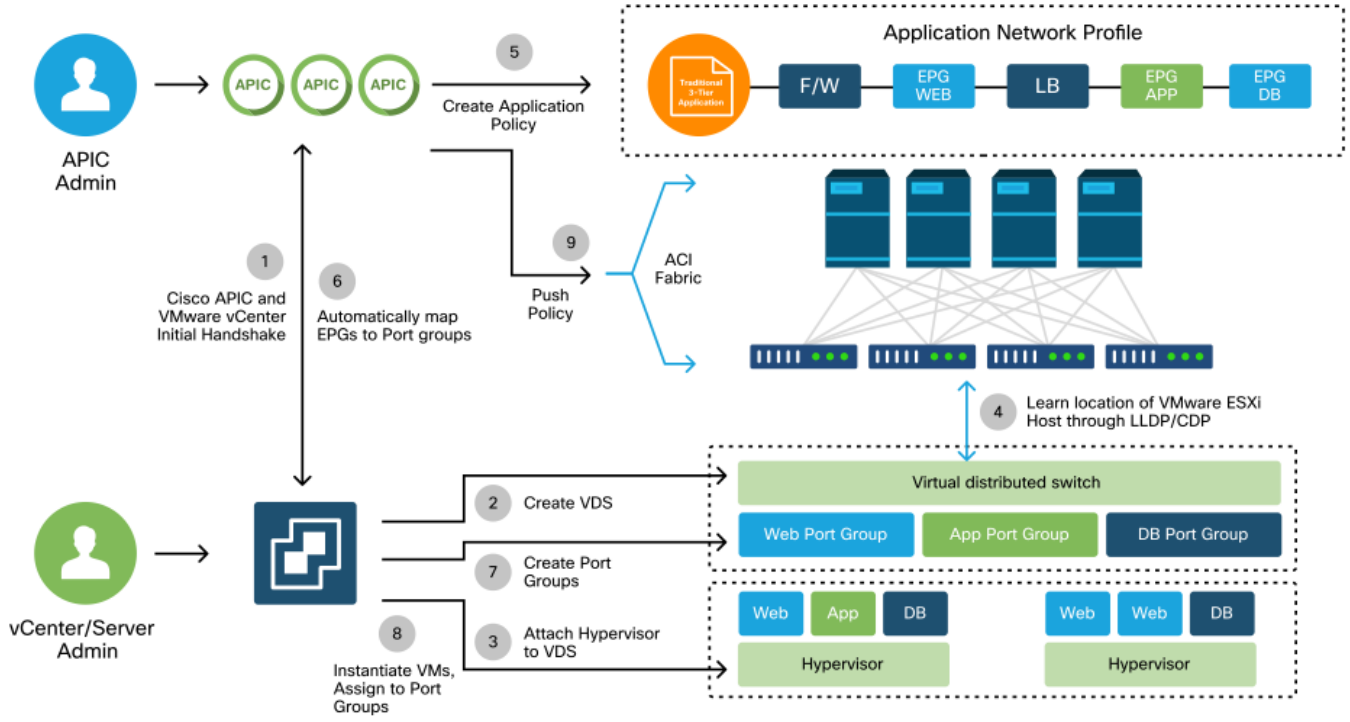
ホストの動的検出

ホスト/VMディスカバリプロセス

ACIでのVMM統合は、ファブリックがホストと適用可能な仮想マシンが接続されている場所を動的に検出してポリシーを効率的に展開できるという点で、手動プロビジョニングとは異なります。この動的なプロセスを通じて、VLAN、SVI、ゾーニングルールなどがノードに導入されると、ACIはリーフスイッチ上のハードウェアリソースの使用率を最適化できます。これは、ポリシーを必要とするエンドポイントが接続されている場合にのみ行われます。ネットワーク管理者にとって、使いやすさの観点から見た利点は、VMが自動接続されるVLAN/ポリシーをACIがプロビジ

ョニングすることです。ポリシーを展開する場所を決定するために、APICは複数のソースからの情報を使用します。次の図は、DVSベースのVMMドメインを使用する場合のホスト検出プロセスの基本手順の概要を示しています。

VMWare VMMドメイン – 導入ワークフロー



要するに、次の重要なステップは、次の場合に発生しています。

- LLDPまたはCDPは、ハイパーバイザとリーフスイッチ間で交換されます。
- ホストは隣接関係の情報をvCenterに報告します。
- vCenterがAPICに隣接情報を通知： APICはインベントリ同期によってホストを認識します。
- APICはポリシーをリーフポートにプッシュします。 これらの条件の詳細については、このセクション内の「解決の即時性」サブセクションを参照してください。
- vCenter隣接情報が失われると、APICはポリシーを削除できます。

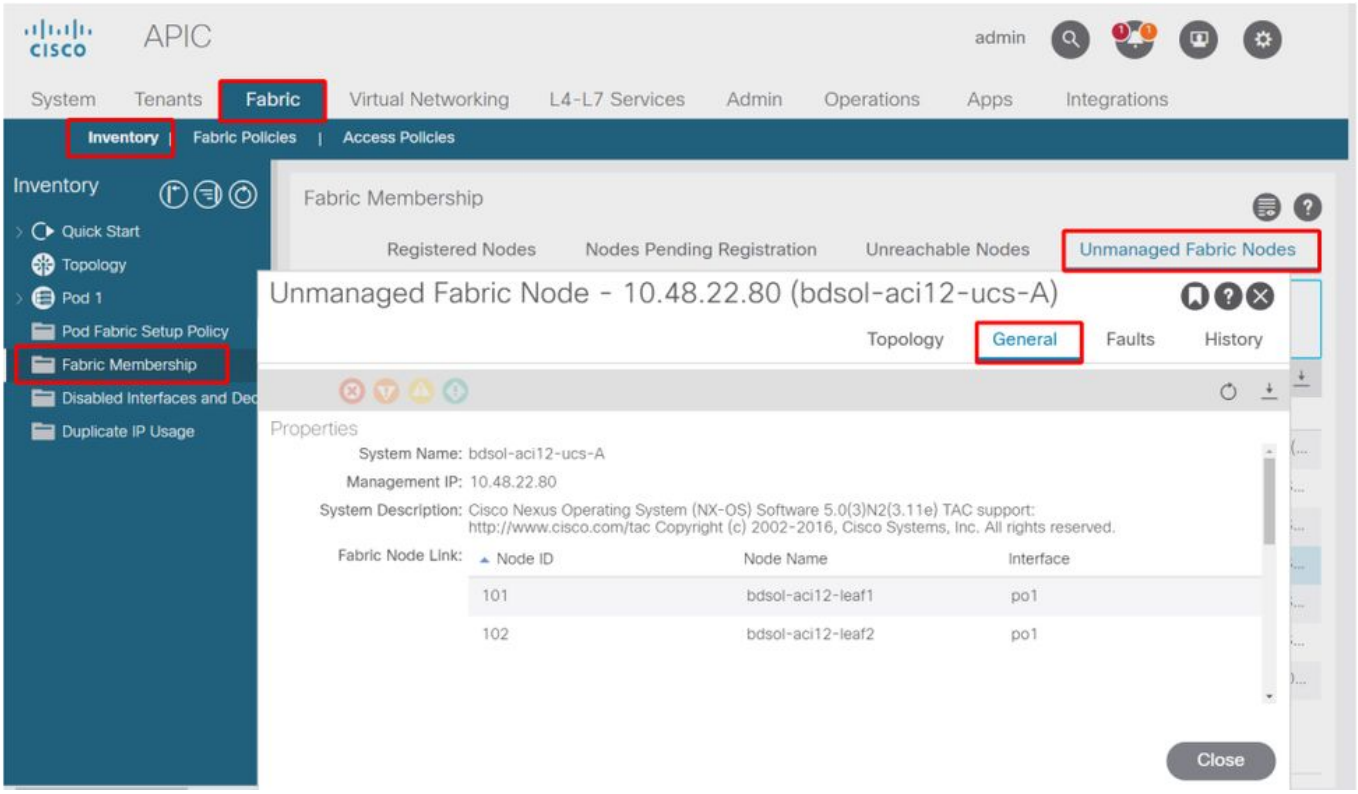
このように、CDP/LLDPは検出プロセスで重要な役割を果たします。CDP/LLDPが適切に設定され、両側で同じプロトコルが使用されていることを確認することが重要です。

ファブリックLooseNode/中間スイッチ：使用例

リーフスイッチとハイパーバイザの間に中間スイッチを持つブレードシャーシを使用した導入では、APICは隣接関係を「縫い合わせる」必要があります。このシナリオでは、中間スイッチがホストとは異なるプロトコル要件を持つ場合があるため、複数の検出プロトコルを使用できます。

ブレードサーバと中間スイッチ（ブレードシャーシスイッチなど）を使用した構成では、ACIは中間スイッチを検出し、その背後にあるハイパーバイザをマッピングする必要があります。ACIでは、中間スイッチをLooseNodeまたは「アンマネージドファブリックノード」と呼びます。 検出されたLooseNodesは、[Fabric] > [Inventory] > [Fabric Membership] > [Unmanaged Fabric Nodes]で確認できます。 GUIでこれらのタイプのサーバの1つに移動すると、ユーザはリーフから中間のスイッチからホストへのパスを表示できます。

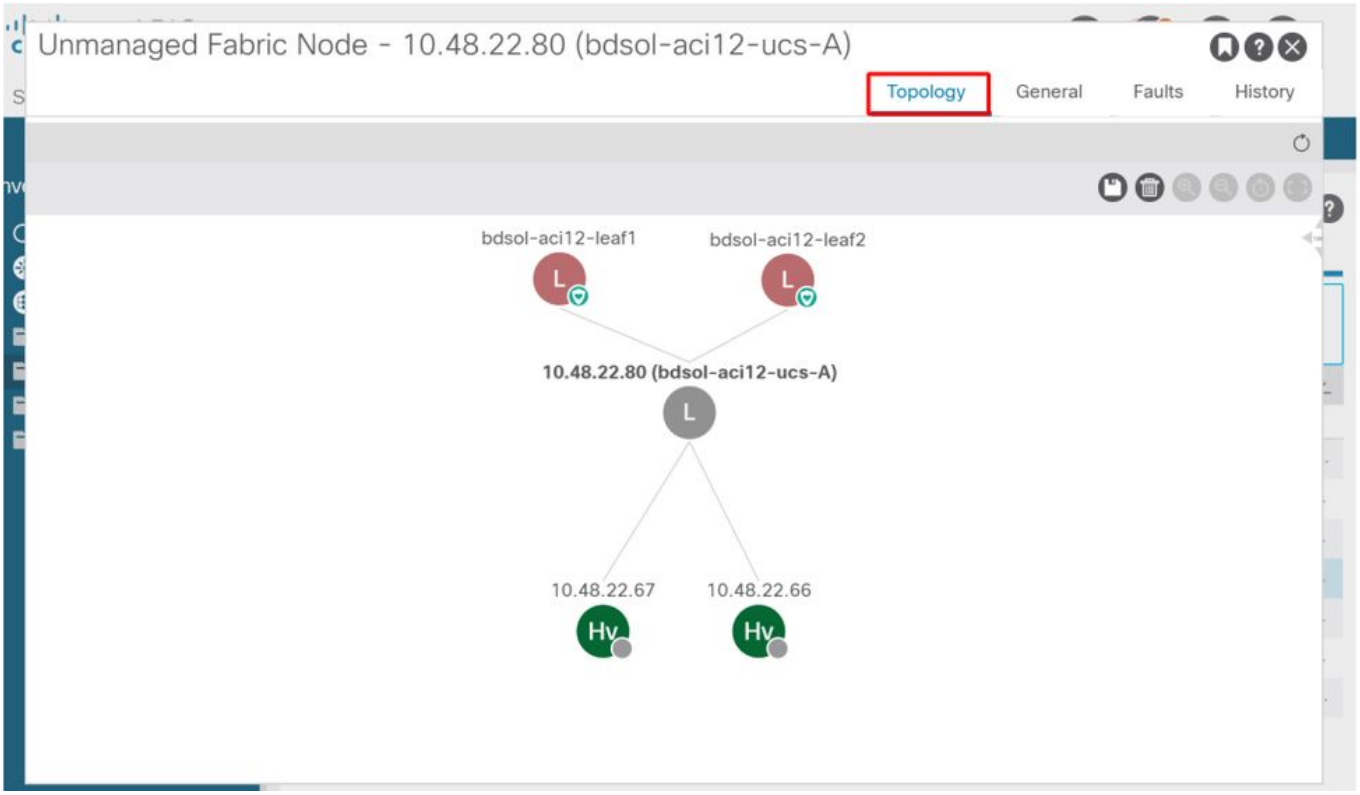
APIC UI：アンマネージドファブリックノード(LooseNodes)



LLDPまたはCDP検出が実施されている場合、ACIはこのようなLooseNodeのトポロジを特定できます。これは、中間スイッチのダウンストリームのハイパーバイザがVMM統合によって管理されており、リーフ自体がダウンストリームから中間スイッチに隣接関係を持つためです。

この概念を次の図に示します。

APIC UI – アンマネージドファブリックノードパス

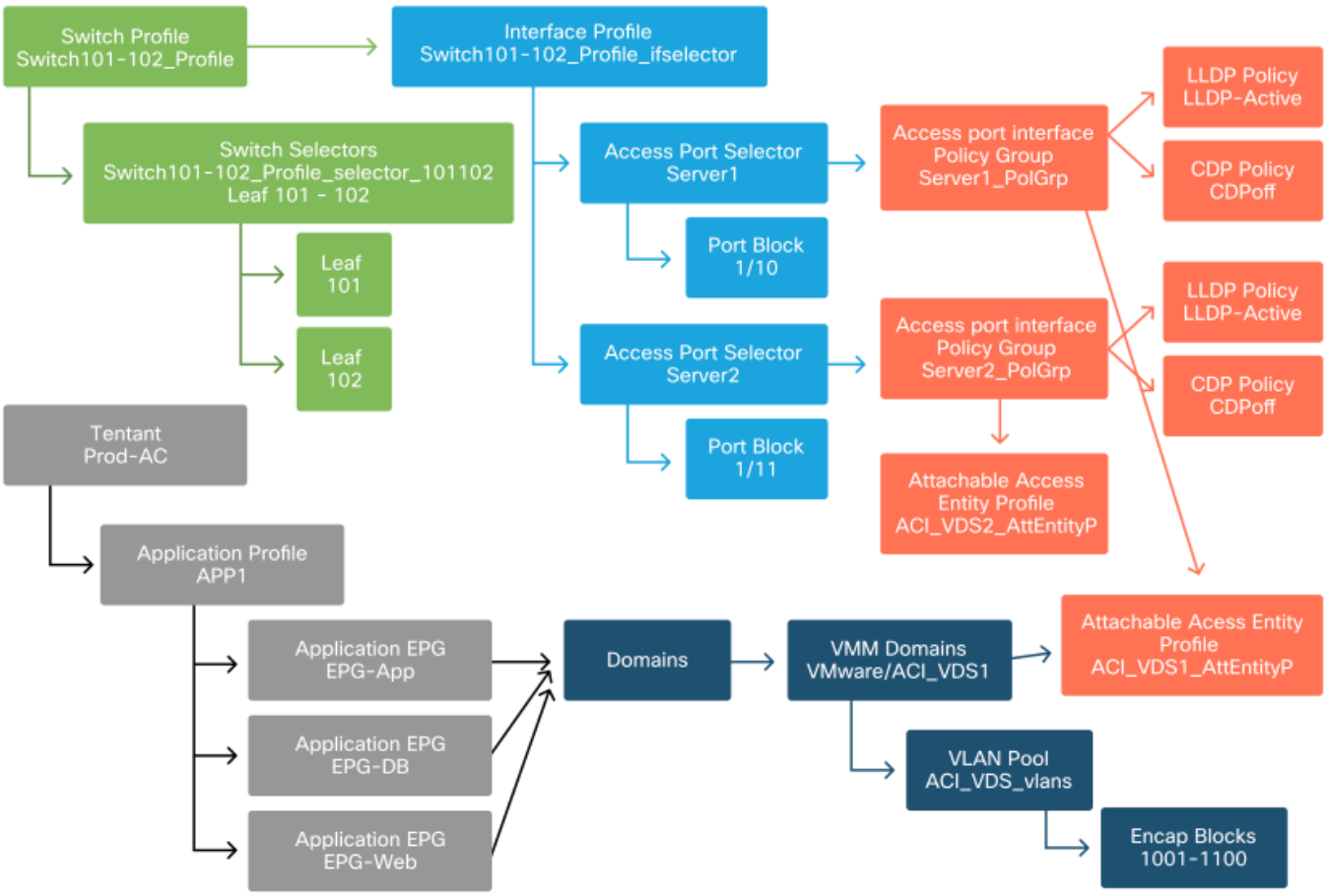


解決の即時性

vCenter/ESXiへの管理接続など、重要なサービスがVMM統合DVSを利用するシナリオでは、Pre-provision Resolution Immediacyを使用するのが賢明です。この設定では、ダイナミックホストディスカバリのメカニズムが削除され、代わりにポリシー/VLANがホスト側インターフェイスに静的にプログラムされます。この構成では、VMM VLANは常に、VMMドメインが参照するAEPに関連付けられたすべてのインターフェイスに展開されます。これにより、検出プロトコル関連の隣接関係イベントのために、重要なVLAN（管理など）がポートから削除される可能性がなくなります。

次の図を参照してください。

プロビジョニング前の導入例



ACI_VDS1 VMMドメインのEPGに対して事前プロビジョニングが設定されている場合、VLANはServer1のリンクに展開されますが、Server2のAEPにはACI_VDS1 VMMドメインが含まれないため、Server2のリンクには展開されません。

解決の即時性の設定をまとめるには、次の手順に従います。

- オンデマンド：ポリシーは、リーフとホスト、およびポートグループに接続されたVM間で隣接関係が確立されたときに展開されます。
- Immediate：リーフとホスト間で隣接関係が確立されると、ポリシーが展開されます。
- 事前プロビジョニング：ポリシーは、VMMドメインが含まれているAEPを使用してすべてのポートに展開されます。隣接関係は必要ありません。

トラブルシューティングのシナリオ

VMがデフォルトゲートウェイのARPを解決できない

このシナリオでは、VMM統合が設定され、DVSがハイパーバイザに追加されていますが、VMはACIのゲートウェイのARPを解決できません。VMがネットワーク接続できるようにするには、隣接関係が確立され、VLANが展開されていることを確認します。

まず、ユーザは、選択したプロトコルに応じて、リーフで「show lldp neighbors」または「show cdp neighbors」を使用して、リーフがホストを検出したことを確認できます。

```
Leaf101# show lldp neighbors
Capability codes:
 (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
 (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID            Local Intf      Hold-time  Capability  Port ID
bdsol-aci37-apic1     Eth1/1          120                    eth2-1
bdsol-aci37-apic2     Eth1/2          120                    eth2-1
bdsol-aci37-os1       Eth1/11         180        B           0050.565a.55a7
S1P1-Spine201         Eth1/49         120        BR          Eth1/1
S1P1-Spine202         Eth1/50         120        BR          Eth1/1
Total entries displayed: 5
```

トラブルシューティングの観点から必要な場合は、CLIとGUIの両方でESXi側から確認できます。

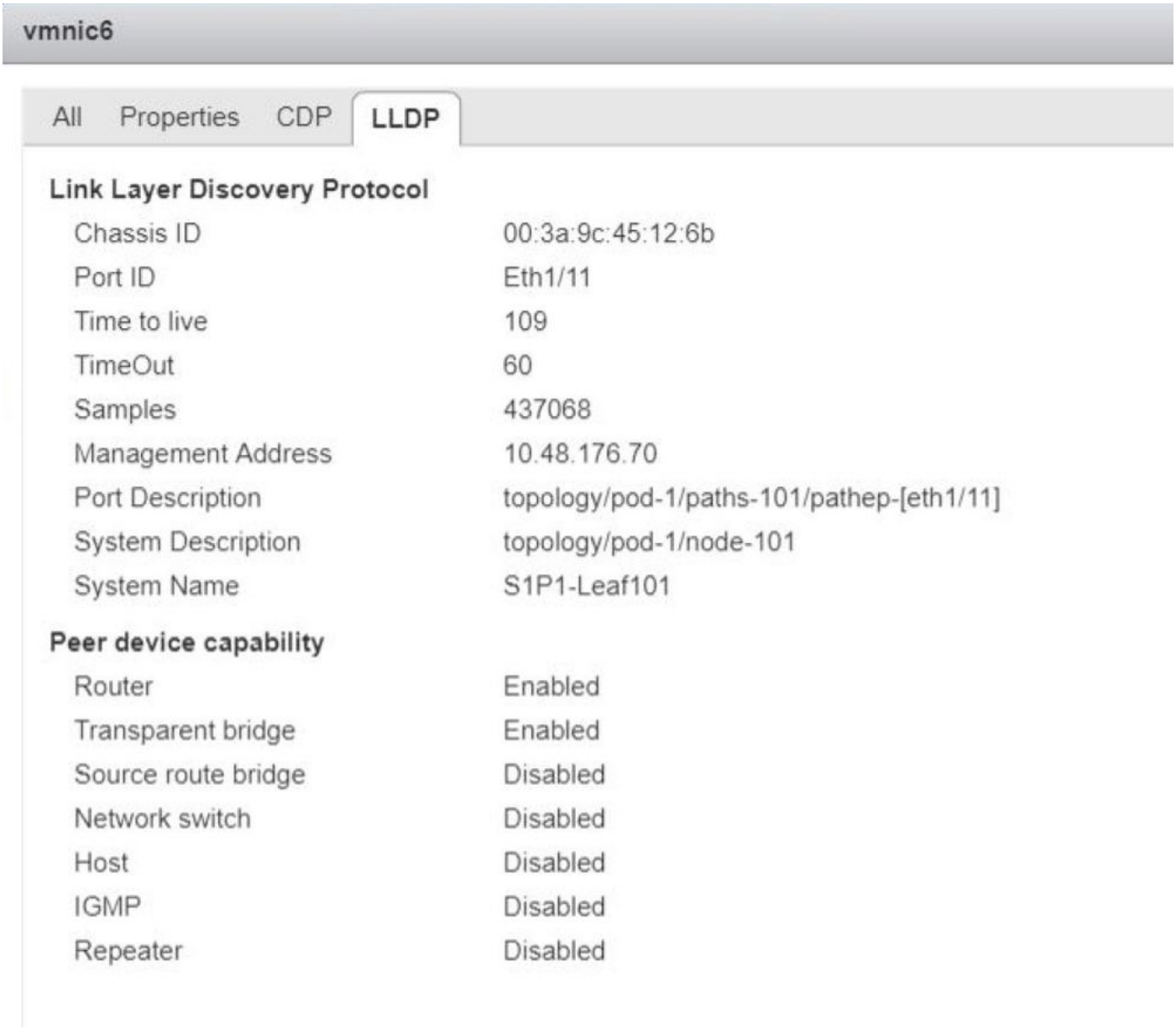
```
[root@host:~] esxcli network vswitch dvs vmware list
VDS_Site1
  Name: VDS_Site1
 ...
  Uplinks: vmnic7, vmnic6
  VMware Branded: true
  DVPort:
        Client: vmnic6
        DVPortgroup ID: dvportgroup-122
        In Use: true
        Port ID: 0

        Client: vmnic7
        DVPortgroup ID: dvportgroup-122
        In Use: true
        Port ID: 1

[root@host:~] esxcfg-nics  -l
Name    PCI          Driver      Link Speed     Duplex MAC Address       MTU    Description
vmnic6  0000:09:00.0 enic        Up   10000Mbps Full   4c:77:6d:49:cf:30 9000   Cisco Systems
Inc Cisco VIC Ethernet NIC
vmnic7  0000:0a:00.0 enic        Up   10000Mbps Full   4c:77:6d:49:cf:31 9000   Cisco Systems
Inc Cisco VIC Ethernet NIC

[root@host:~] vim-cmd hostsvc/net/query_networkhint --pnic-name=vmnic6 | grep -A2 "System Name"
              key = "System Name",
              value = "Leaf101"
           }
```

vCenter Web Client：ホスト – vmnic LLDP/CDP隣接関係の詳細

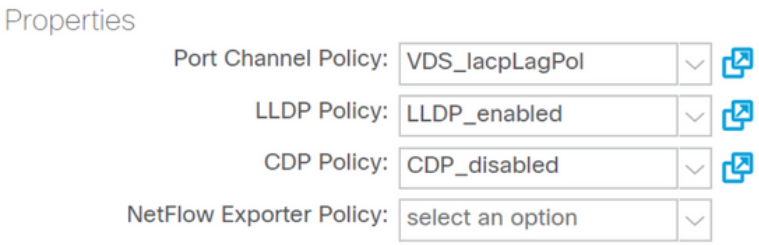


リーフLLDP隣接関係がESXiホストから見えない場合は、ESXi OSの代わりにLLDPDUを生成するように設定されたネットワークアダプタを使用していることが原因です。ネットワークアダプタでLLDPが有効になっており、すべてのLLDP情報を消費しているかどうかを確認してください。この場合は、アダプタ自体でLLDPを必ず無効にして、vSwitchポリシーによって制御されるようにします。

別の原因として、リーフとESXiハイパーバイザの間で使用される検出プロトコル間に不整合が存在することが考えられます。両端で同じディスカバリプロトコルを使用していることを確認します。

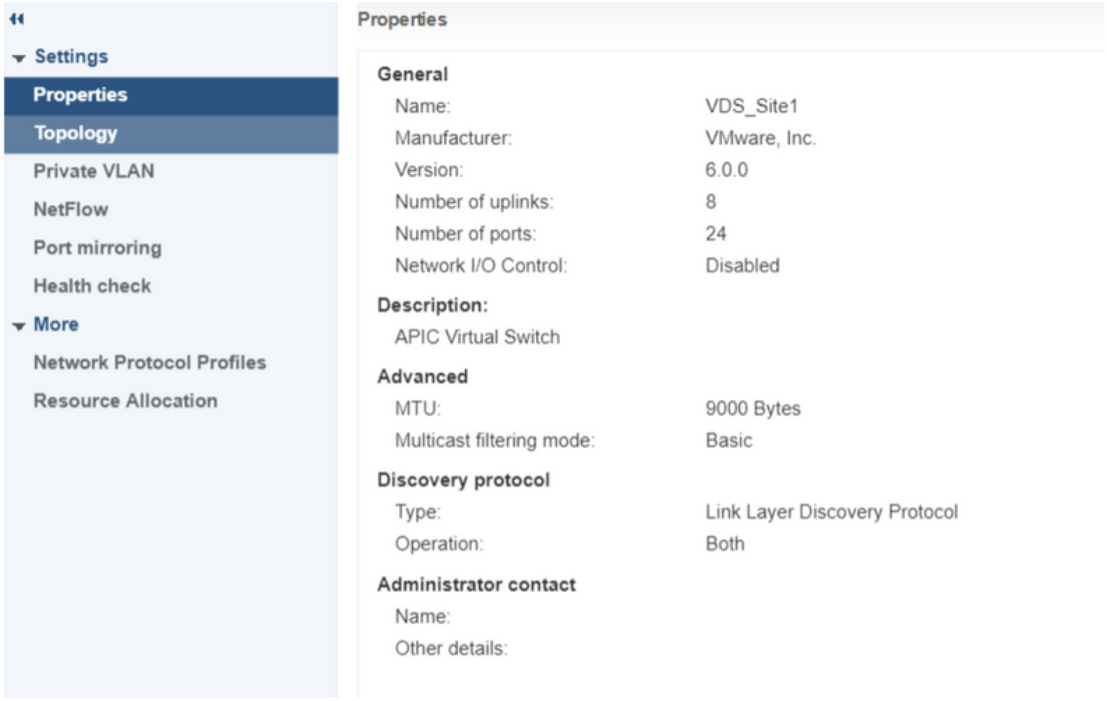
APIC UIでCDP/LLDP設定がACIとDVS間で一致しているかどうかを確認するには、[Virtual Networking] > [VMM Domains] > [VMWare] > [Policy] > [vSwitch Policy]に移動します。 LLDPポリシーとCDPポリシーは相互に排他的であるため、どちらか一方のみを有効にしてください。

APIC UI - VMWare VMMドメイン – vSwitchポリシー



vCenterで次の項目に移動します。[Networking] > [VDS] > [Configure]。

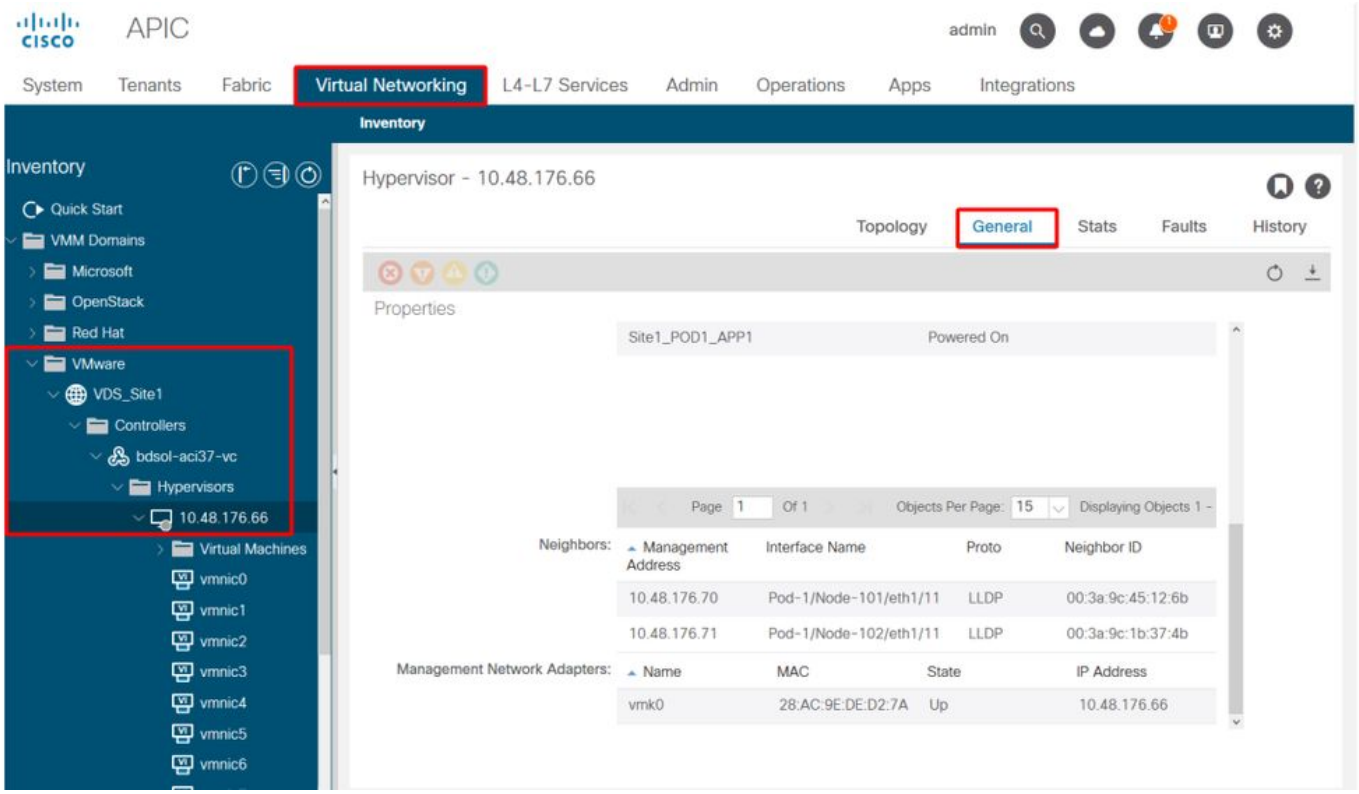
vCenter WebクライアントUI - VDSプロパティ



必要に応じてLLDP/CDP設定を修正します。

次に、APICが、[Virtual Networking] > [VMM Domains] > [VMWare] > [Policy] > [Controller] > [Hypervisor] > [General]の下で、UIのリーフスイッチに対するESXiホストのLLDP/CDPネイバーシップを確認することを検証します。

APIC UI - VMWare VMMドメイン – ハイパーバイザの詳細



これが期待値を示している場合、ユーザはホストに向かうポートにVLANが存在することを確認できます。

```
S1P1-Leaf101# show vlan encap-id 1035

 VLAN Name                             Status    Ports
 ---- -------------------------------- --------- -------------------------------

 12   Ecommerce:Electronics:APP        active    Eth1/11

 VLAN Type  Vlan-mode
 ---- ----- ----------
 12   enet  CE
```

APICプッシュDVSに接続されたvCenter/ESXi管理VMK

vCenterまたはESXiの管理トラフィックでVMM統合DVSを利用する必要があるシナリオでは、ダイナミック隣接関係のアクティブ化と必要なVLANのアクティブ化で行う作業が停滞しないように、特別な注意が必要です。

vCenterは通常、VMM統合が設定される前に構築されるため、物理ドメインとスタティックパスを使用して、vCenter VMのカプセル化VLANがリーフスイッチで常にプログラムされていることを確認することが重要です。これにより、VMM統合が完全に設定される前に、vCenter VMのカプセル化VLANを使用できます。VMM統合をセットアップした後でも、このEPGの可用性を常に保証するために、このスタティックパスを設定したままにすることをお勧めします。

ESXiハイパーバイザの場合、Cisco.comの「Cisco ACI Virtualization Guide」に従って、vDSに移行する際には、VMKインターフェイスが接続されるEPGが、解決の即時性が[Pre-provision]に設定された状態で導入されていることを確認することが重要です。これにより、ESXiホストのLLDP/CDP検出に依存することなく、リーフスイッチでVLANが常にプログラムされるようになります。

LooseNodeの背後で検出されないホスト隣接関係

LooseNode検出の問題の一般的な原因は次のとおりです。

- CDP/LLDPが有効になっていない CDP/LLDPは、中間スイッチ、リーフスイッチ、およびESXiホスト間で交換する必要がありますCisco UCSの場合、これはvNICのネットワーク制御ポリシーによって実現されます
- LLDP/CDPネイバーの管理IPを変更すると、接続が切断されます vCenterはLLDP/CDP隣接関係で新しい管理IPを認識しますが、APICは更新しません手動インベントリ同期をトリガーして修正する
- VMM VLANが中間スイッチに追加されていない APICはサードパーティ製のブレード/中間スイッチをプログラムしません。4.1(1)リリースで使用可能なCisco UCSM統合アプリケーション(ExternalSwitch)。VLANは、ACIリーフノードに接続されたアップリンクとホストに接続されたダウンリンクに設定およびトランキングする必要があります

F606391 – ホスト上の物理アダプタの隣接関係がない

次のエラーが表示される場合：

```
Affected Object: comp/prov-VMware/ctrlr-[DVS-DC1-ACI-LAB]-DVS1/hv-host-104
Fault delegate: [FSM:FAILED]: Get LLDP/CDP adjacency information for the physical adapters on
the host: bdsol-aci20-os3 (TASK:ifc:vmmmgr:CompHvGetHpNicAdj)
```

「VMがデフォルトゲートウェイのARPを解決できない」の項のワークフローを確認してください。これは、CDPとLLDPの隣接関係が存在しないことを意味します。これらの隣接関係は、エンドツーエンドで確認する必要があります。

ハイパーバイザアップリンクロードバランシング

ESXiなどのハイパーバイザをACIファブリックに接続する場合、通常は複数のアップリンクに接続されます。実際には、ESXiホストを少なくとも2台のリーフスイッチに接続することをお勧めします。これにより、障害シナリオやアップグレードの影響を最小限に抑えることができます。

ハイパーバイザ上で実行されるワークロードがアップリンクを使用する方法を最適化するために、VMware vCenterの構成では、ハイパーバイザのアップリンクに向けてVMによって生成されるトラフィックに対して複数のロードバランシングアルゴリズムを設定できます。

正しい接続を確立するには、すべてのハイパーバイザとACIファブリックを同じロードバランシングアルゴリズム設定に合わせることが重要です。そうしないと、ACIファブリックで断続的なトラフィックフローのドロップとエンドポイントの移動が発生する可能性があります。

これは、次のような過剰なアラートによってACIファブリックで確認できます。

```
F3083 fault
ACI has detected multiple MACs using the same IP address 172.16.202.237.
MACs: Context: 2981888. fvCEps:
uni/tn-BSE_PROD/ap-202_Voice/epg-VLAN202_Voice/cep-00:50:56:9D:55:B2;
uni/tn-BSE_PROD/ap-202_Voice/epg-VLAN202_Voice/cep-00:50:56:9D:B7:01;
or
[F1197][raised][bd-limits-exceeded][major][sys/ctx-[vxlan-2818048]/bd-[vxlan-16252885]/fault-
F1197]
Learning is disabled on BD Ecommerce:BD01
```

この章では、ACIへのVMWare ESXiホスト接続について説明しますが、ほとんどのハイパーバイ

ザに適用できます。

ラックサーバ

ESXiホストがACIファブリックに接続する様々な方法を見ると、ESXiホストは2つのグループ、スイッチ依存、およびスイッチ独立のロードバランシングアルゴリズムに分けられます。

スイッチに依存しないロードバランシングアルゴリズムは、特定のスイッチ設定が必要ない場所に接続する方法です。スイッチ依存のロードバランシングでは、スイッチ固有の設定が必要です。

vSwitchポリシーが、次の表に示す「ACIアクセスポリシーグループ」の要件に従っているかどうかを確認してください。

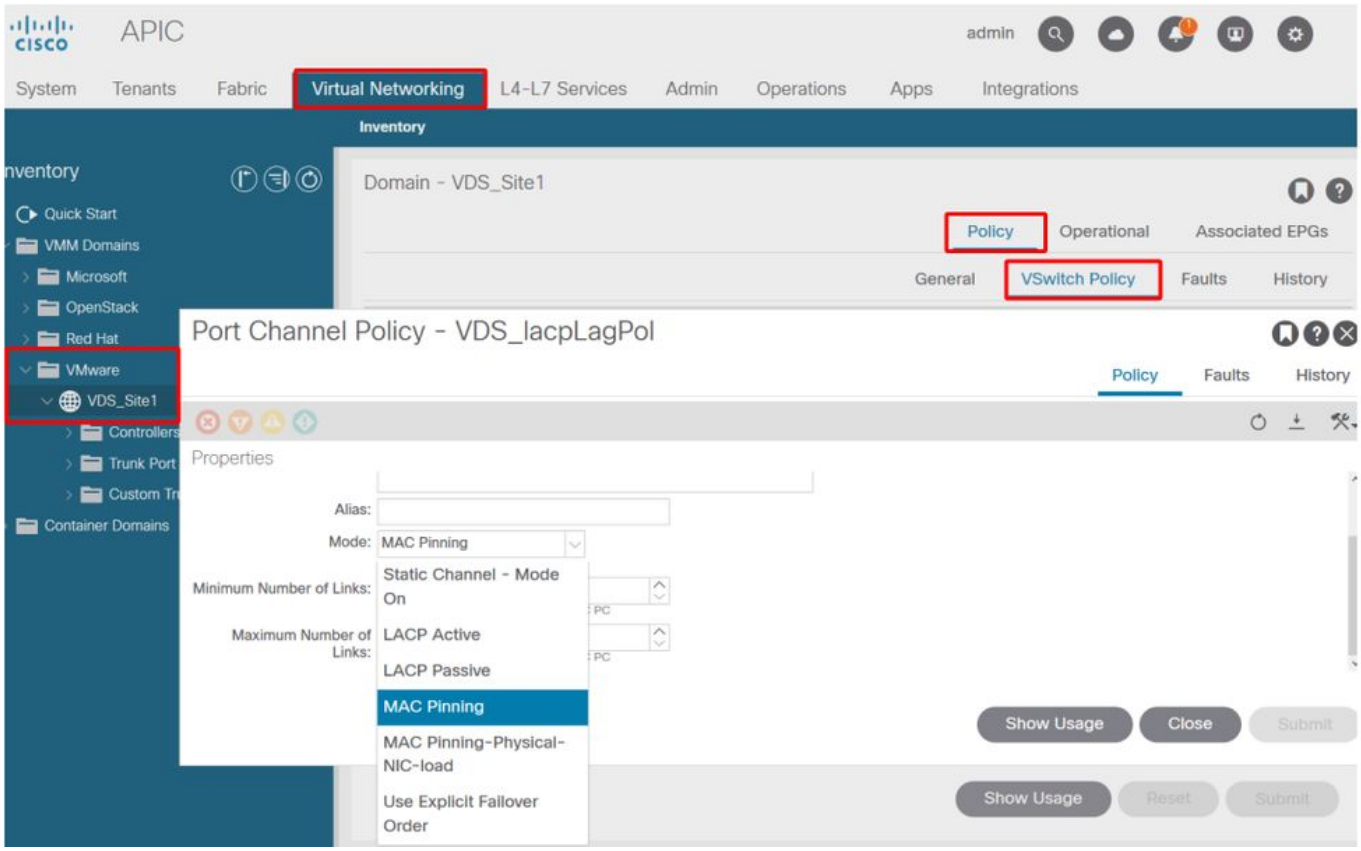
チーミングおよびACI vSwitchポリシー

VMwareチーミングおよびフェールオーバーモード	ACI vSwitchポリシー	説明	ACIアクセスポリシーグループ：ポートチャネルが必要
発信仮想ポートに基づくルート	MACピニング	スイッチの仮想ポートIDに基づいてアップリンクを選択します。仮想スイッチは、仮想マシンまたはVMKernelアダプタのアップリンクを選択すると、この仮想マシンまたはVMKernelアダプタの同じアップリンクを介してトラフィックを常に転送します。	No
送信元MACハッシュに基づくルート	適用外	送信元MACアドレスのハッシュに基づいてアップリンクを選択する	適用外
明示的なフェールオーバー順序	明示的なフェールオーバーモードの使用	アクティブアダプタのリストから、フェールオーバー検出基準を通過する最も高い順序のアップリンクを常に使用します。このオプションでは、実際のロードバランシングは実行されません。	No
リンク集約(LAG) - IPハッシュベース	スタティックチャネル – モードオン	各パケットの送信元と宛先のIPアドレスのハッシュに基づいてアップリンクを選択します。非IPパケットの場合、スイッチはこれらのフィールドのデータを使用してハッシュを計算します。IPベースのチーミングでは、ACI側でポートチャネル/VPCが「mode on」に設定されている必要があります。	Yes（チャネルモードを「on」に設定）
リンク集約(LAG):LACP	LACPアクティブ/パッシブ	選択したハッシュに基づいてアップリンクを選択します（20種類のハッシュオプションを使用できます）。LACPベースのチーミングでは、ACI側でポートチャネル/VPCがLACPを有効にして設定されている必要があります。ACIで拡張Lagポリシーを作成し、それをVSwitchポリシーに適用します。	Yes（チャネルモードを「LACP Active/Passive」に設定）

物理NIC負荷(LBT)に基づくルート	MACピニング：Physical-NIC-load	分散ポートグループまたは分散ポートで使用できます。ポートグループまたはポートに接続されている物理ネットワークアダプタの現在の負荷に基づいてアップリンクを選択します。アップリンクが75 %以上のビジー状態が30秒間続くと、ホストのvSwitchは仮想マシントラフィックの一部を空き容量のある物理アダプタに移動します。	No

vSwitchポリシーの一部としてポートチャネルポリシーを検証する方法については、次のスクリーンショットを参照してください。

ACI vSwitchポリシー：ポートチャネルポリシー



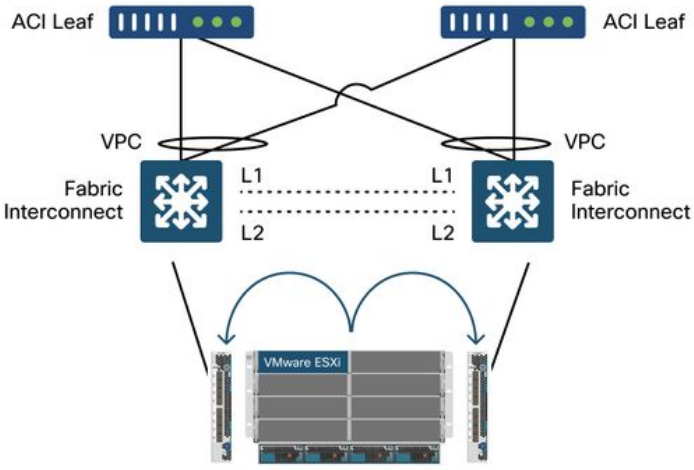
注:VMwareネットワーキング機能の詳細については、vSphereネットワーキング(https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.networking.doc/GUID-D34B1ADD-B8A7-43CD-AA7E-2832A0F7EE76.html)を参照してください。

Cisco UCS Bシリーズユースケース

Cisco UCS Bシリーズサーバを使用する際は、シャーシ内でユニファイドデータプレーンを持たないUCSファブリックインターコネクト(FI)に接続することに注意してください。この使用例は、同様のトポロジを採用する他のベンダーにも同様に適用されます。このため、ACIリーフスイッチ側とvSwitch側で使用されるロードバランシング方式が異なる場合があります。

ACIを使用したUCS FIトポロジを次に示します。

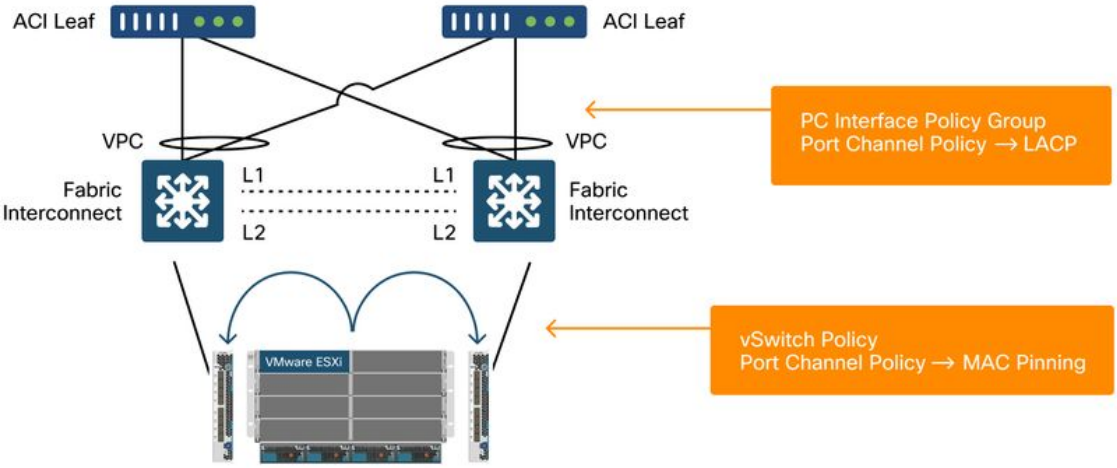
Cisco UCS FIとACIリーフスイッチ – トポロジ



重要な注意事項：

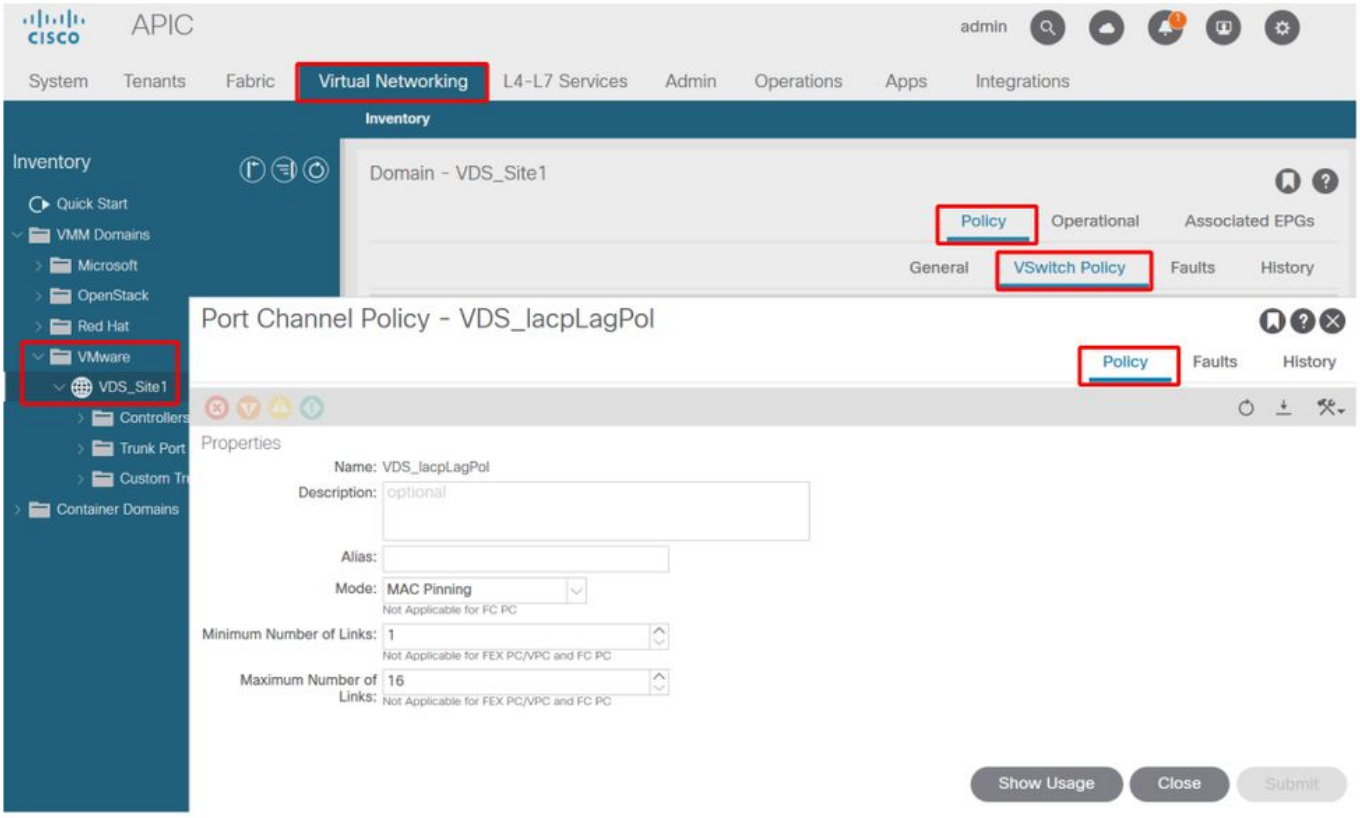
- 各Cisco UCS FIには、ACIリーフスイッチへのポートチャネルがあります。
- UCS FIは、ハートビートの目的でのみ直接接続されます（データプレーンには使用されません）。
- 各ブレードサーバのvNICは、特定のUCS FIに固定されるか、UCSファブリックフェールオーバー（アクティブ – スタンバイ）を使用してFIの1つに向かうパスを使用します。
- ESXiホストのvSwitchでIPハッシュアルゴリズムを使用すると、UCS FIでMACフラップが発生します。

これを正しく設定するには、次の手順を実行します。



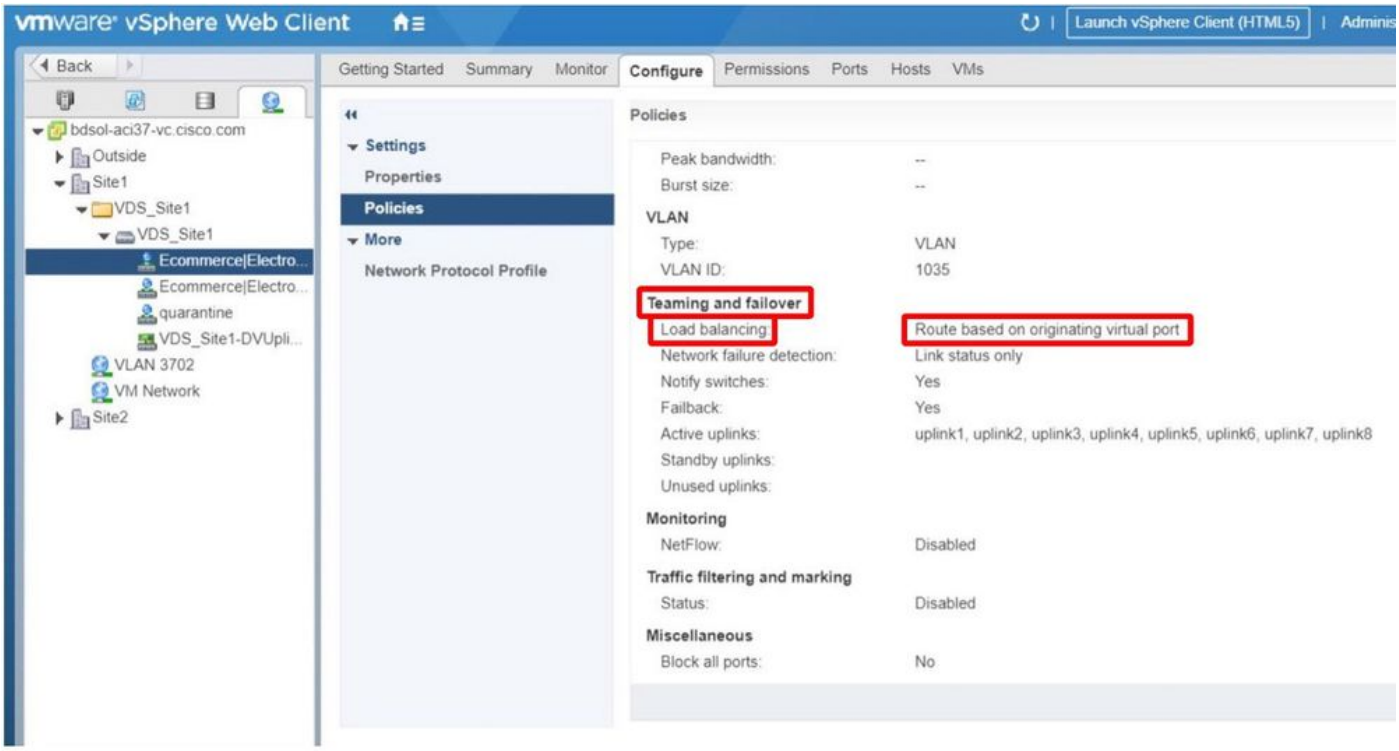
MACピニングがACIのvSwitchポリシーの一部としてポートチャネルポリシーで設定されている場合、これは「発信仮想ポートに基づくルート」としてVDSのポートグループのチーミング設定を示します。

ACI:vSwitchポリシーの一部としてのポートチャネルポリシー



上の例で使用したポートチャネルポリシーは、ウィザードによって自動的に名前が付けられるため、モード「MACピニング」を使用していますが、「CDS_lacpLagPol」と呼ばれます。

VMWare vCenter — ACI VDS – ポートグループ – ロードバランシング設定



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。