ACI VMM統合のトラブルシューティング

内容

はじめに

背景説明

Virtual Machine Managerの概要

vCenter接続

- ロールベースアクセスコントロール(RBAC)
- RBAC関連の問題のトラブルシューティング
  - RBAC関連の問題のソリューション
- 接続のトラブルシューティング

VMwareインベントリ

- APICで管理されるVMware VDSパラメータ
- APICによって管理されるVMWare VDSポートグループのパラメータ
- VMwareインベントリのトラブルシューティング
- VMware DVSバージョン

ホストの動的検出

- ホスト/VMの検出プロセス
- ファブリックLooseNode/中間スイッチ – 使用例
- 解決の緊急性
- 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
  - APICプッシュDVSに接続されたvCenter/ESXi管理VMK
  - LooseNodeの背後で検出されないホスト隣接関係
  - F606391 – ホスト上の物理アダプタの隣接関係の欠落

ハイパーバイザアップリンクロードバランシング

- ラックサーバ
- チーミングおよびACI vSwitchポリシー
- Cisco UCS Bシリーズ使用例

はじめに

このドキュメントでは、ACI Virtual Machine Manager(VM)統合(VMM)を理解し、トラブルシューティングする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』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』の章から抽出されています。

Virtual Machine Managerの概要

ACIコントローラには、サードパーティの仮想マシンマネージャ(VMM)と統合する機能があります。

これは、ファブリックのエンドツーエンドネットワーキング設定と、ファブリックに接続するワークロードの操作を簡素化および自動化する、ACIの重要な機能の1つです。ACIは、複数のワークロードタイプ（仮想マシン、ベアメタルサーバ、コンテナ）に拡張可能な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の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。

読者は次の項目について説明します。

- vCenter通信の障害に関する調査
- 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 Controller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アカウントによって異なります。APICがvCenter上で操作を正常に実行できるようにするための、VMMドメインに関連付けられたvCenterユーザの固有の要件の概要を説明します。この要件は、インベントリと設定のプッシュと取得、または管理対象インベントリ関連イベントのモニタリングとリスニングのいずれでも同じです。

このような要件に関する懸念を解消する最も簡単な方法は、フルアクセス権を持つ管理者vCenterアカウントを使用することです。ただし、この種の自由はACI管理者が常に利用できるとは限りません。

ACIバージョン4.2における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用で、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

    - さらに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。
    - ホスト。構成。詳細設定
    - Host.Local operations.Reconfigure virtual machine（仮想マシンの再構成）
    - Host.Configuration.Network設定
    - これは、AVSと、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では、APICが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
    - サービスグラフを使用している場合は、仮想アプライアンスに対する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頻繁に発生しますが、初期セットアップの実行後に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。

症状は次のように現れます。

- 新しいサービスを展開できない部分または完全な機能（DVSの作成、ポートグループの作成、一部のオブジェクトが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ない。
- サポートされていないvCenter操作またはいずれかのシナリオ（ポートグループの展開の失敗など）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に関連する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

VMMドメインで設定されているvCenterユーザにすべての権限が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されたも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を含む）を試行する方法です。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、正しい権限がユーザに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

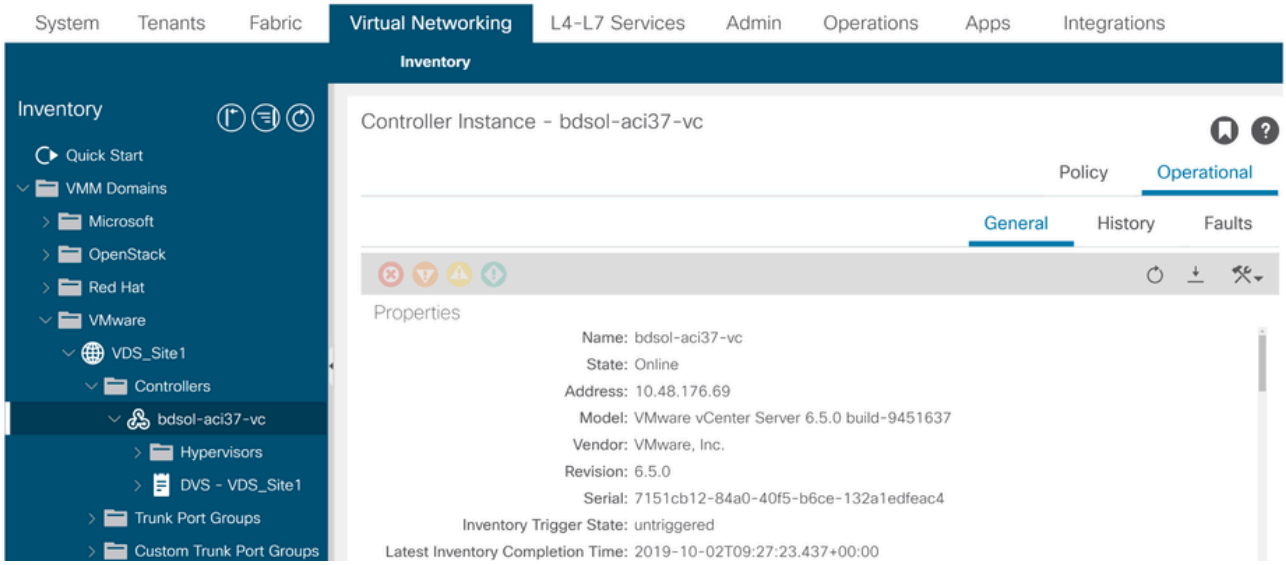
VMMの接続関連の問題をトラブルシューティングする際は、ACIがvCenterと通信する方法の基本的な動作の一部に注意することが重要です。

1つ目の最も関連性の高い動作は、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ドメインのシャードリーダーと呼ばれ

ます。ただし、複数のAPIC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把握するために、vCenterイベントをリッスンしています。APICの同じ分散アーキテクチャに従って、特定のVMMドメインに、プライマリデータと機能を処理する1つのAPIC（この場合はシャードリーダー）、および2つのレプリカ(VMMの場合はフォロワー)があります。APIC全体にVMMの通信と機能の処理を分散させるには、任意の2つのVMMドメインに同じシャードリーダーまたは異なるシャードリーダーを設定します。

vCenterの接続状態は、GUIで対象のVMMコントローラに移動するか、次に示すCLIコマンドを使用して確認できます。

VMWare VMMドメイン – vCenterの接続状態



<#root>

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: dom
```

これらの手順は、VCとAPIC間の接続の問題をトラブルシューティングするために使用できます。

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ための最初の手順は、特定のVMMドメインのシャードリーダーである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でコマンドshow vmware domain name <domain>を実行することです。

<#root>

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を特定したら、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。

<#root>

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します

APICルーティングテーブルを確認して、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。

<#root>

apic1#

bash

admin@apic1:~>

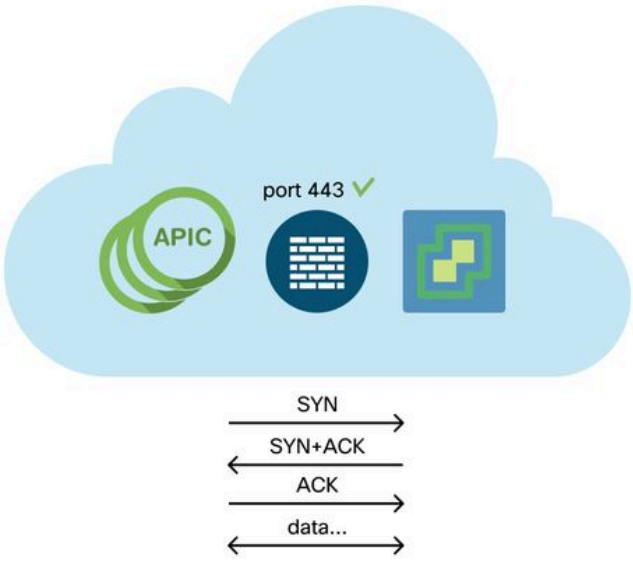
route

```
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の間でポート443が許可されていることを確認します。これには、通信経路にあるファイアウォールも含まれます。

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。

<#root>

```
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)
...
```

シャードリーダーのポート443でnetstatコマンドを使用し、TCP接続が確立されていることを確認します。

<#root>

```
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、シャードリーダーとvCenterの間のパスに沿ってパケットキャプチャを実行し、トラフィックがどちらのデバイスでも送受信されているかどうかを確認します。

VMwareインベントリ

次の表に、VMWare VDSパラメータのリストを示し、APICでこれらを設定できるかどうかを指定します。

APICで管理されるVMware VDSパラメータ

VMware VDS	デフォルト値	Cisco APICポリシー
[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』	いいえ
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による最高のサポート	Yes
検出プロトコル	LLDP	Yes
アップリンクポートとアップリンク名	8	対応(Cisco APICリリース 4.2(1)以降)
アップリンク名プレフィックス	アップリンク	対応(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

VMware VDS	デフォルト値	Cisco APICポリシー
アラーム	フォルダレベルで2つのアラームが追加されました。	いいえ

次の表に、VMWare VDSポートグループのパラメータのリストを示し、APICでこれらが設定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ポートグループのパラメータ

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から取得）
ポートバインド	静的バインド	いいえ
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のポートチャネルポリシーに基づいて取得	Yes
無差別モード	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	いいえ

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の間で発生するインベントリ同期イベントには、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の2種類がありま

す。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、これらのホストが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、オンデマンド展開の即時性のシナリオでは、ソースリーフのEPGをプログラミング解除して、宛先リーフのEPGをプログラミングします。

VMMドメインに関連付けられたEPGの展開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、エラーの原因となったオブジェクトを示すエラーが常に発生します。

シナリオ1 – 無効なバッキングを持つ仮想マシン：

仮想マシンが1つのvCenterから別のvCenterに移動された場合、または仮想マシンのバッキングが無効であると判断された場合（たとえば、古い/削除されたDVSにポートグループが接続された場合）、vNICに動作上の問題があることが報告されます。

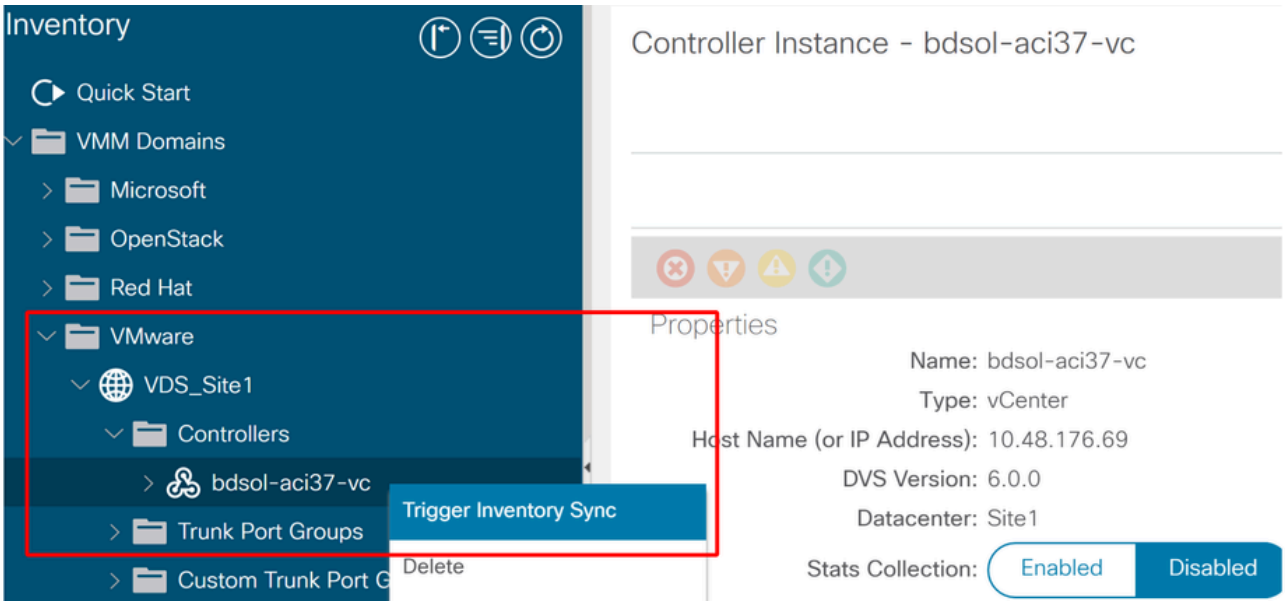
```
Fault fltCompVNicOperationalIssues
Rule ID:2842
Explanation:
This fault is raised when ACI controller failed to update the properties of a VNIC (for instance, it ca
Code: F2842
Message: Operational issues detected for VNic name on VM name in VMM controller: hostOrIp with name nam
Resolution:
Remediate the virtual machines indicated in the fault by assigning a valid port group on the affected v
```

シナリオ2:vCenter管理者がvCenter上のVMM管理対象オブジェクトを変更した。

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。このエラーは、サポートされていない操作がvCenterで実行された場合に発生します。

```
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
Resolution:
If this scenario is encountered, try to undo the unsupported change in vCenter and then trigger an 'inv
```

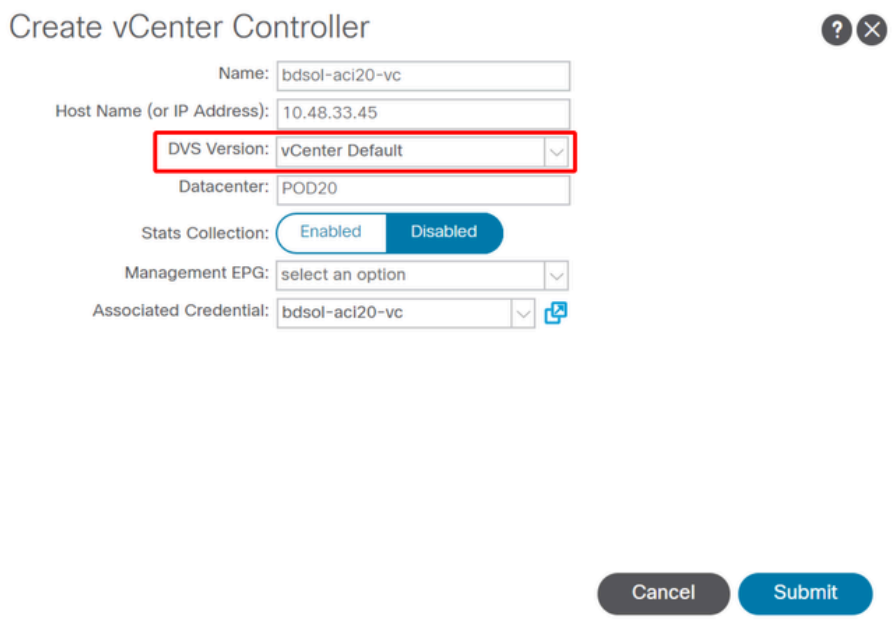
VMWare VMMドメイン – vCenterコントローラ – インベントリ同期のトリガー



VMware DVSバージョン

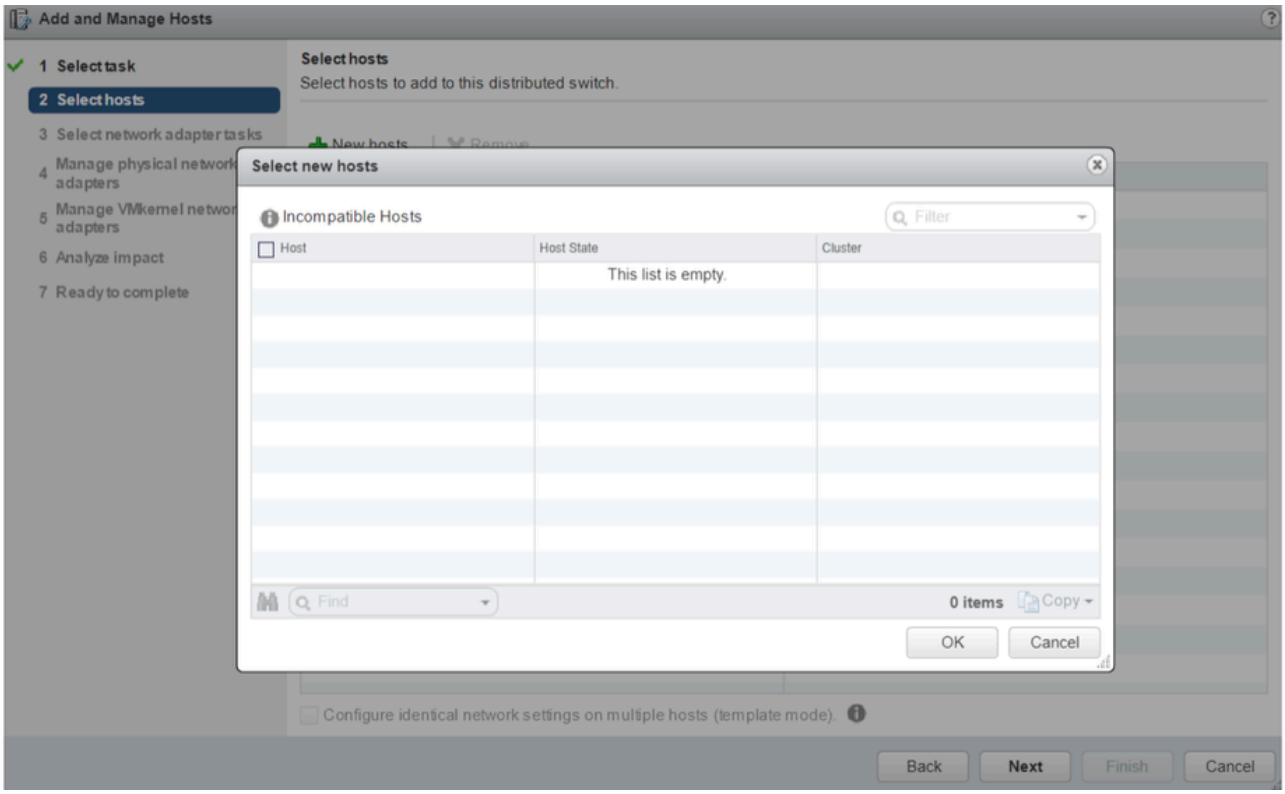
VMMドメインの一部として新しいvCenterコントローラを作成する場合、DVSバージョンのデフォルト設定は「vCenterデフォルト」を使用します。 これを選択すると、DVSバージョンがvCenterのバージョンで作成されます。

VMWare VMMドメイン – vCenterコントローラの作成

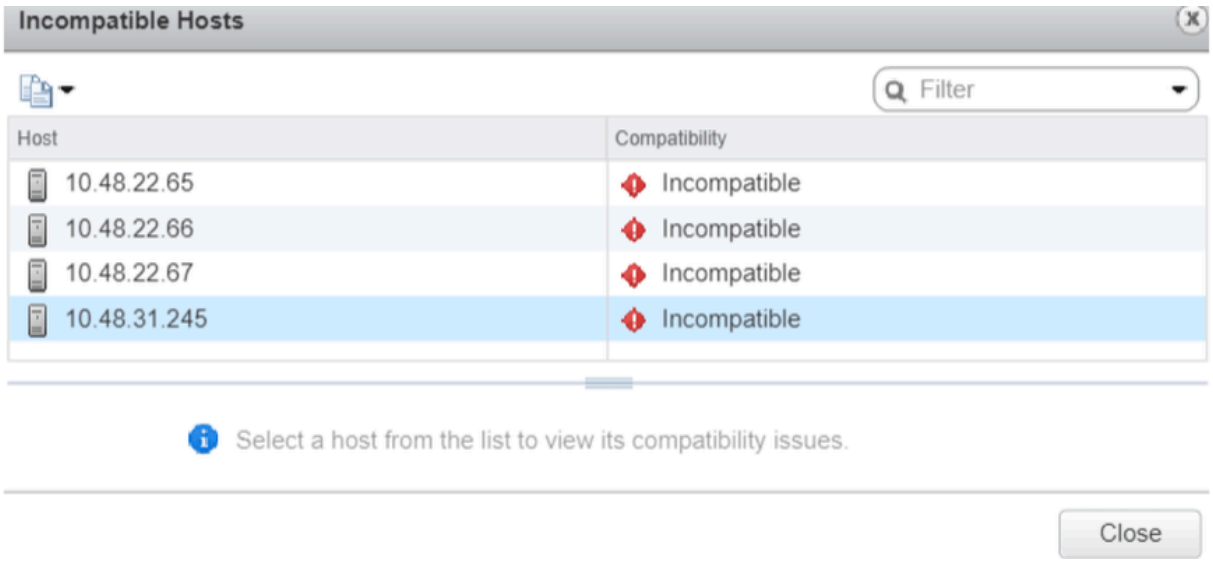


つまり、6.5を実行するvCenterと6.0を実行するESXiサーバの例では、APICがバージョン6.5のDVSを作成するため、vCenter管理者は6.0を実行するESXiサーバをACI DVSに追加できません。

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際には、必要なESXiサーバをDVSに追加できるように、正しい「DVSバージョン」を選択してください。

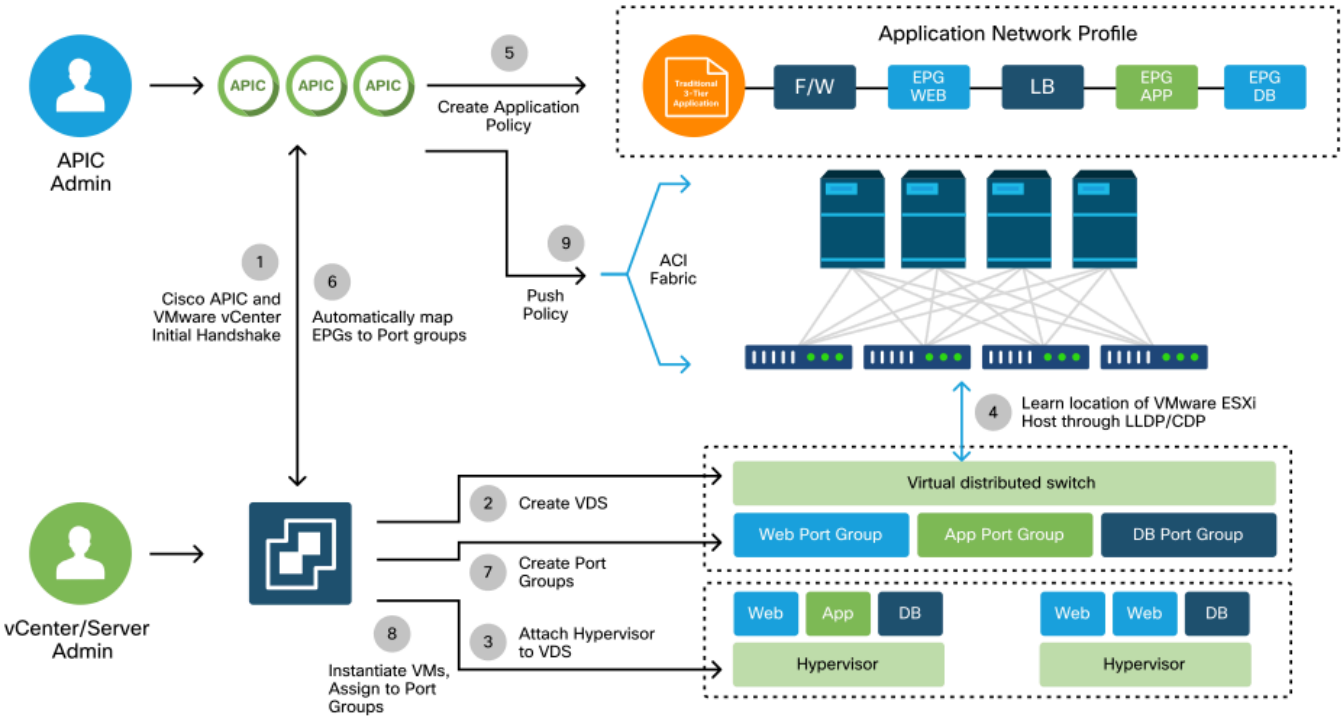
ホストの動的検出

ホスト/VMの検出プロセス

ACIでのVMM統合は、手動プロビジョニングとは異なり、ファブリックがホストと該当する仮想マシンの接続先を動的に検出して、ポリシーを効率的に展開できます。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上に展開される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るのは、ポリシーを必要とするエンドポイントが接続されて

いる場合だけです。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が接続されるVLAN/ポリシーがACIによって自動的にプロビジョニングされることです。ポリシーをどこに展開する必要があるかを決定するために、APICは複数のソースからの情報を使用します。この図は、DVSベースのVMMドメインを使用する際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 – 展開ワークフロー



要するに、これらの重要なステップは次の場合に発生します。

- LLDPまたはCDPは、ハイパーバイザスイッチとリーフスイッチ間で交換されます。
- ホストはvCenterに隣接関係の情報を報告します。
- vCenterがAPICにアジャセンシー関係情報を通知：
  - APICはインベントリ同期によってホストを認識します。
- APICがリーフポートにポリシーをプッシュ：
  - これらの条件の詳細については、「解決の緊急度」のサブセクションを参照してください。
- vCenter隣接関係情報が失われた場合、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。

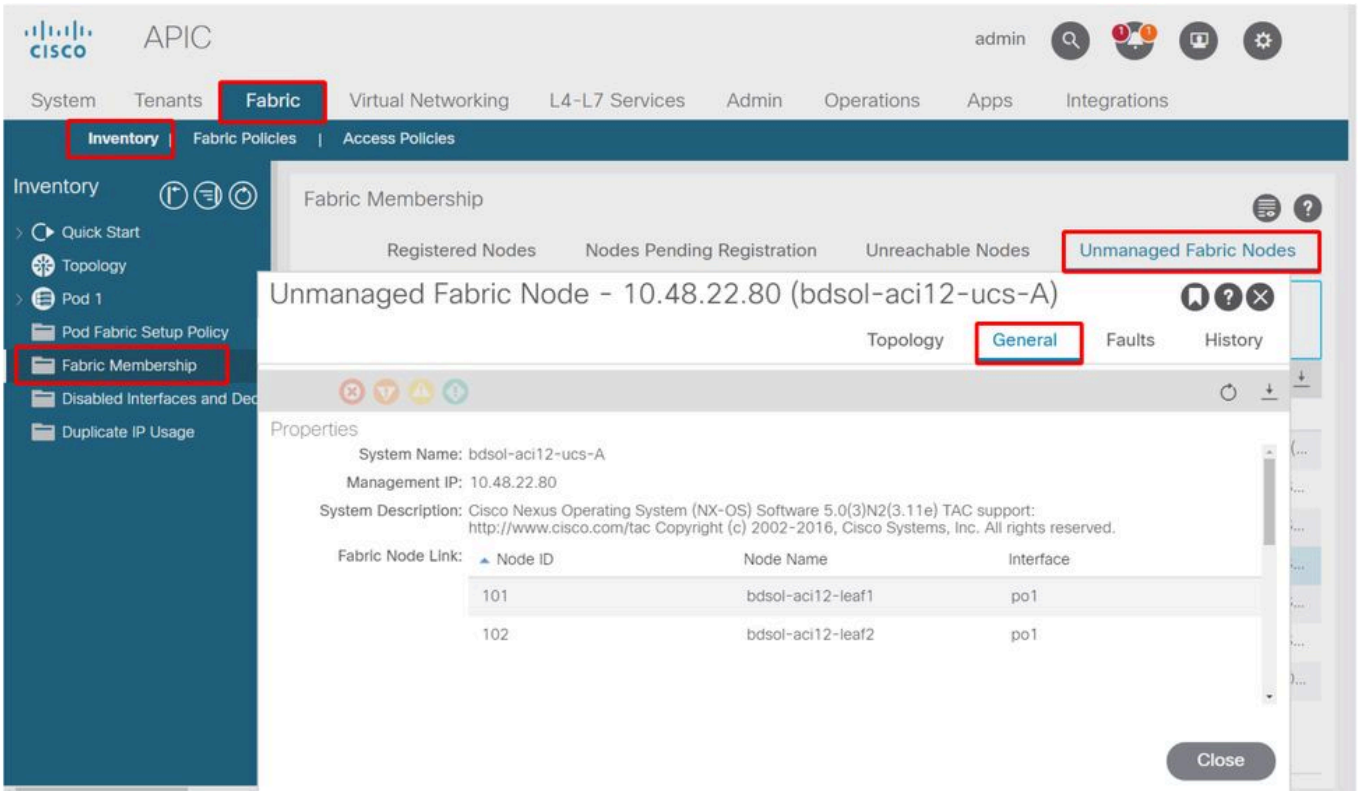
ファブリックLooseNode/中間スイッチ – 使用例

ブレードシャーシを使用し、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配置する導入では、APICはアジャセンシー関係を「縫い合わせる」必要があります。このシナリオでは、中間スイッチのプロトコル要件がホストとは異なるため、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（つまり、ブレードシャーシスイッチ）を使用した設定では、

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できます。ACIでは、中継スイッチはLooseNodeまたは「アンマネージドファブリックノード」と呼ばれます。検出されたLooseNodeは、Fabric > Inventory > Fabric Membership > Unmanaged Fabric Nodesの順に選択することで確認できます。GUIでこれらのタイプのサーバのいずれかに移動することで、ユーザはリーフから中間スイッチを経由するホストへのパスを表示できます。

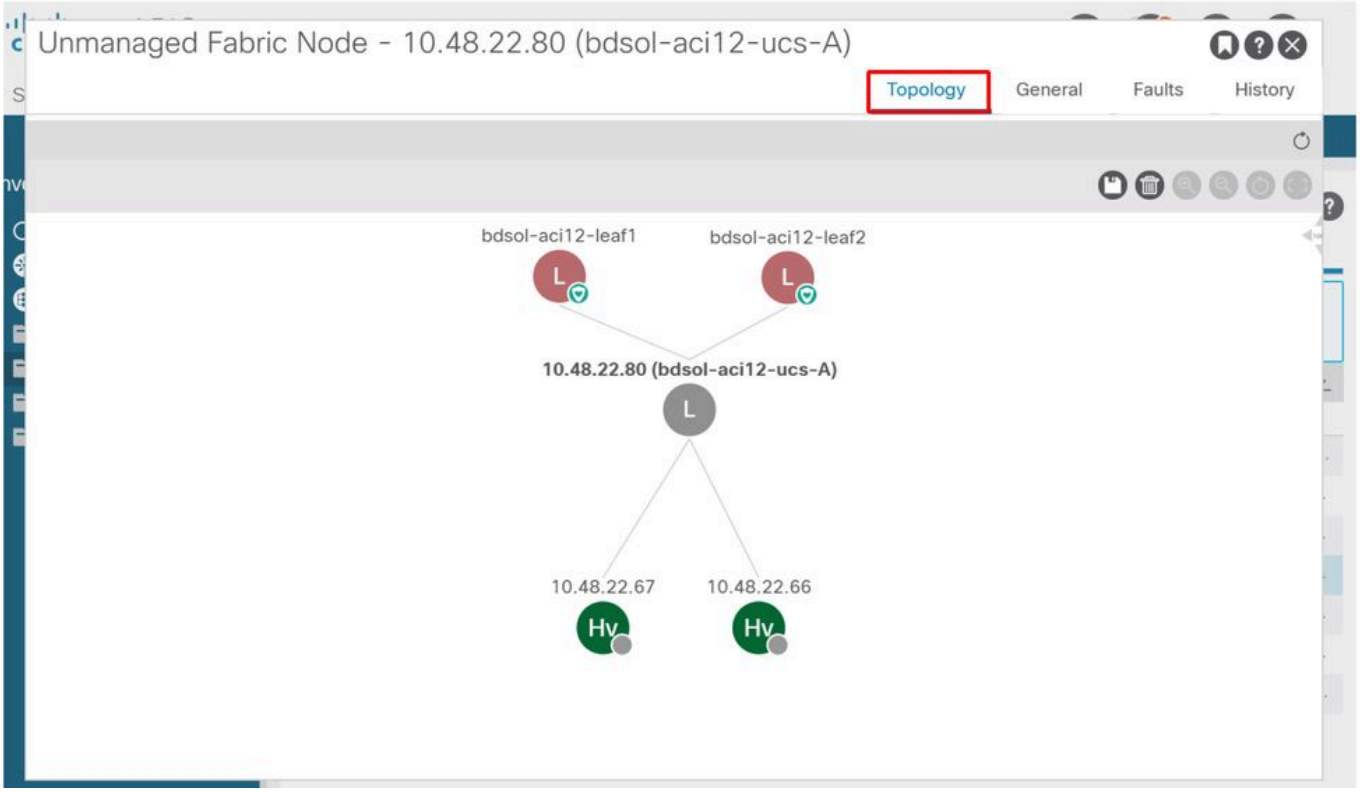
APIC UI：アンマネージドファブリックノード(LooseNodes)



LLDPまたはCDP検出を実行すると、中間スイッチのハイパーバイザダウンストリームがVMM統合によって管理され、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っていることを前提として、ACIはこのようなLooseNodeのトポロジを決定できます。

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

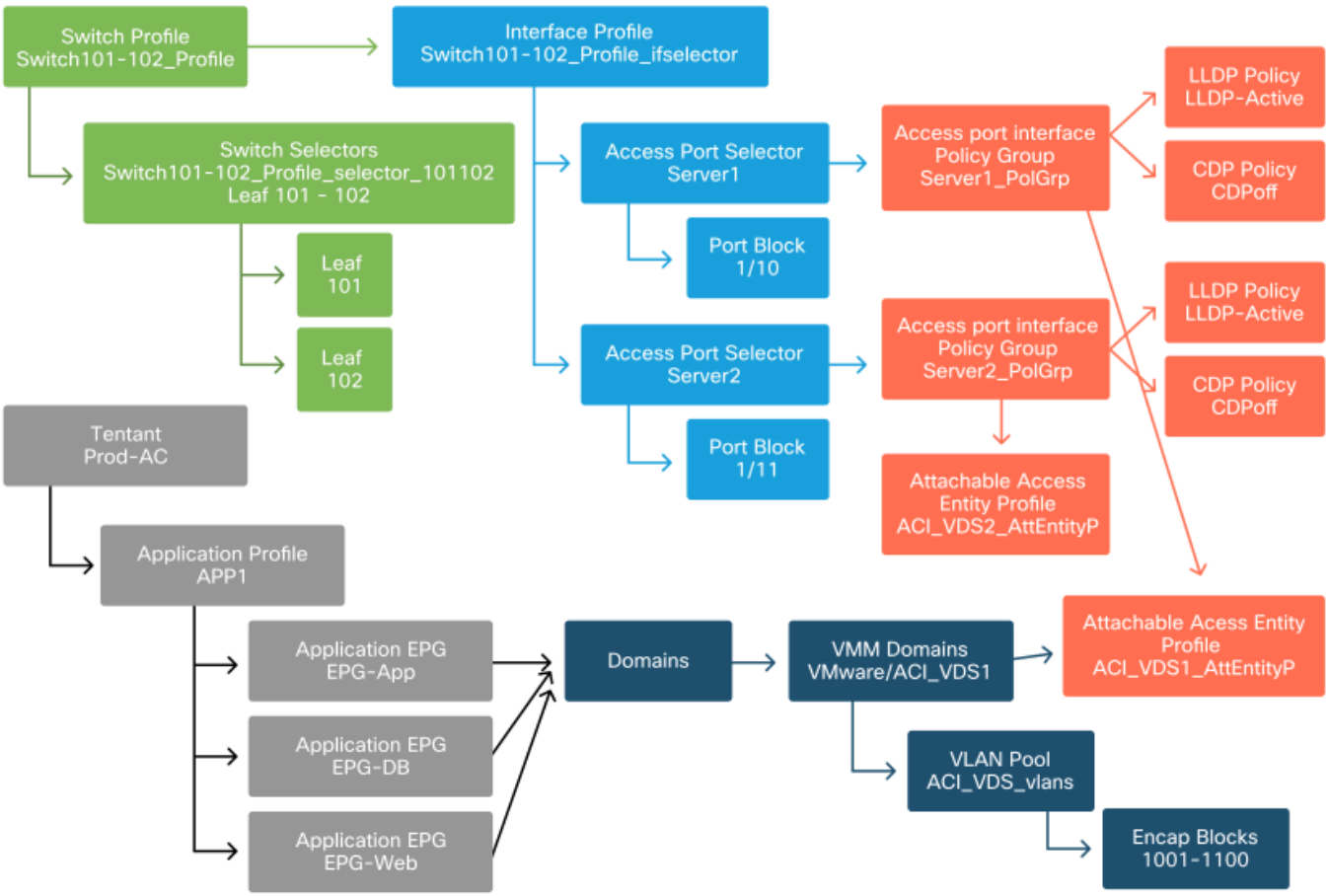


解決の緊急性

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、事前プロビジョニング解決の即時性を使用することが賢明です。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がホストに面する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、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常に展開されます。これにより、検出プロトコル関連の隣接関係イベントが原因で、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。

次のダイヤグラム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要約するには、次の手順に従います。

- オンデマンド：ポリシーは、リーフ/ホストと、ポートグループに接続されたVMとの間に隣接関係が確立されたときに展開されます。
- Immediate：リーフとホストの間に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のネットワーク接続を確立するには、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かどうかをチェックできます。

<#root>

```
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>

```
[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

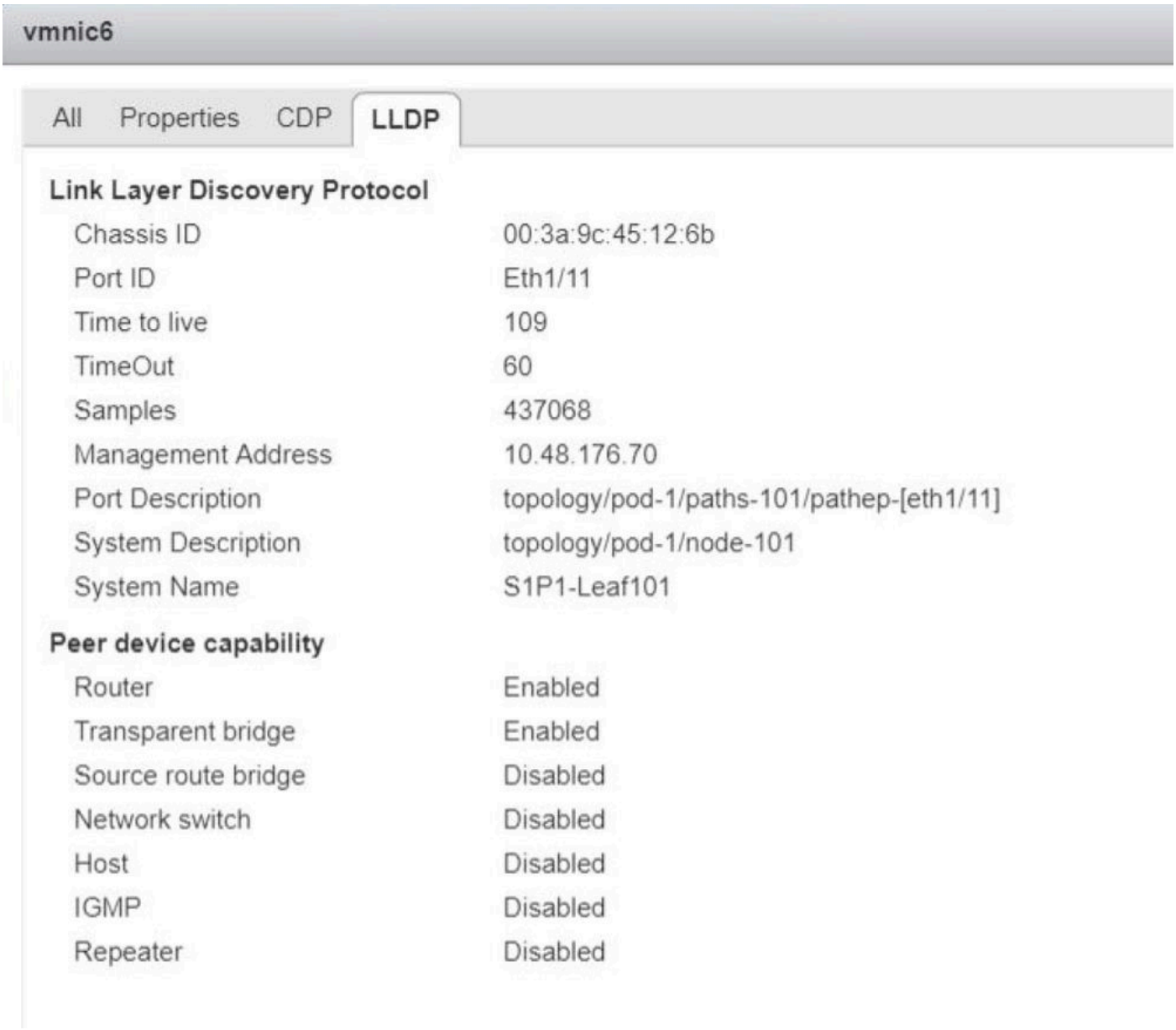
```
Name    PCI          Driver      Link Speed     Duplex MAC Address       MTU    Description
vmnic6  0000:09:00.0 enic        Up   10000Mbps Full   4c:77:6d:49:cf:30 9000   Cisco Systems Inc Cisco
vmnic7  0000:0a:00.0 enic        Up   10000Mbps Full   4c:77:6d:49:cf:31 9000   Cisco Systems Inc Cisco
```

```
[root@host:~]
```

vim-cmd hostsvc/net/query_networkhint --pnic-name=vmnic6 | grep -A2 "System Name"

```
               key = "System Name",
               value = "Leaf101"
            }
```

vCenter Webクライアント：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、多くの場合、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たことが原因です。ネットワークアダプタでLLDPが有効になっているかどうかと、すべてのLLDP情報が消費されているかどうかを確認します。この場合は、アダプタ自体でLLDPを無効にして、vSwitchポリシーによって制御されるようにします。

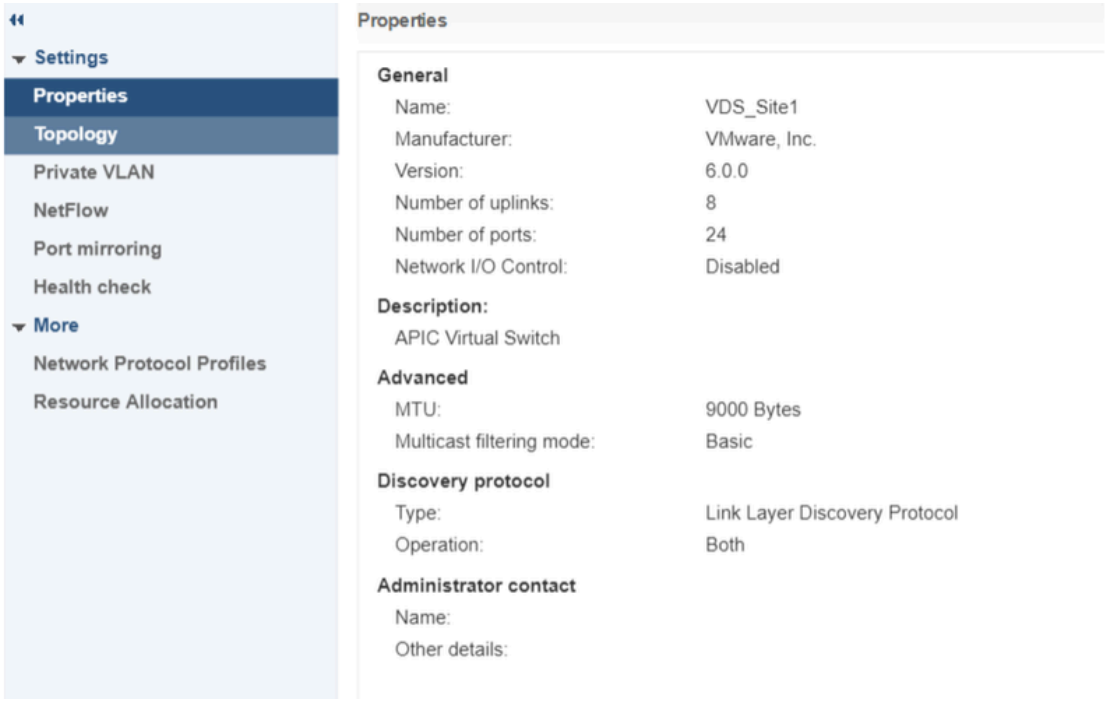
別の原因として、リーフとESXiハイパーバイザ間で使用される検出プロトコル間の不整合が考えられます。両端で同じディスカバリプロトコルを使用していることを確認します。

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の順に移動します。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、Networking > VDS > Configureの順に選択します。

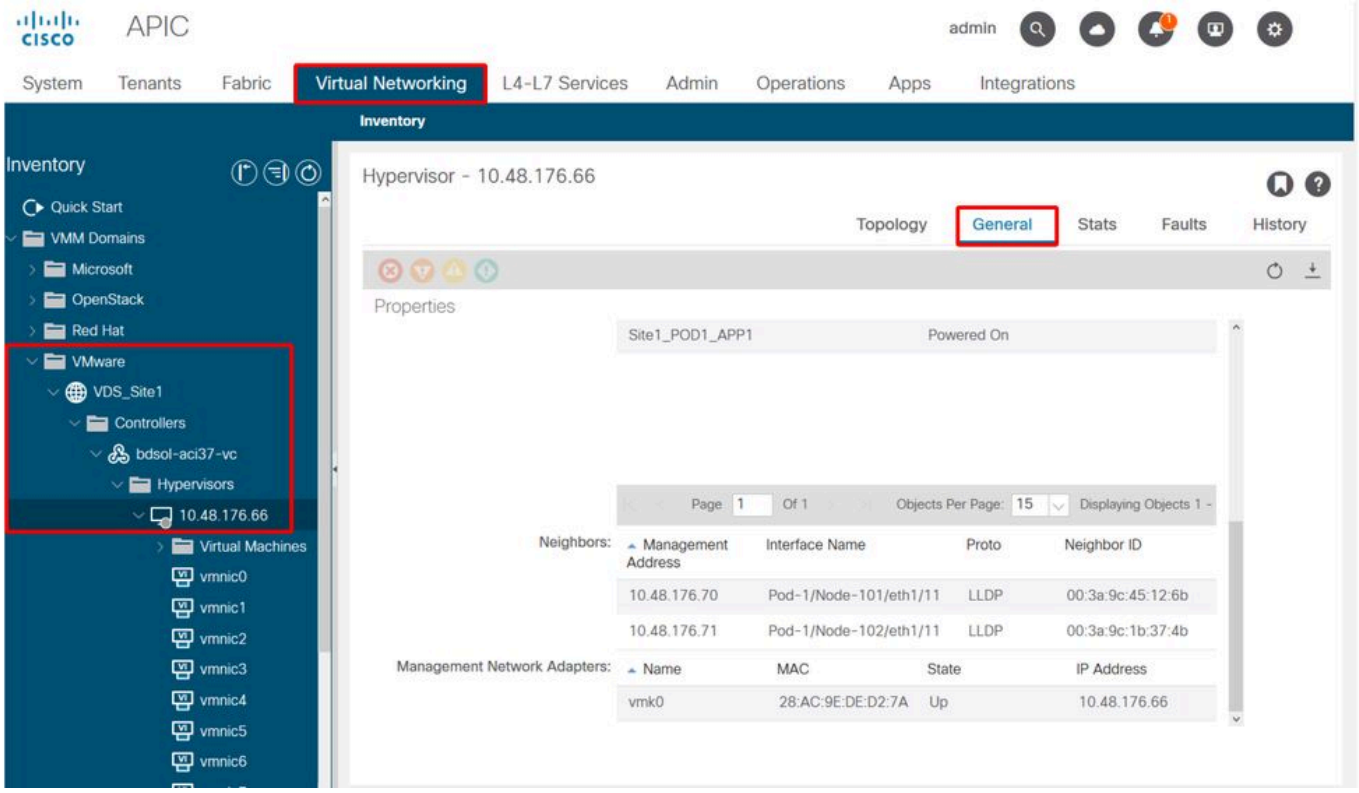
vCenter WebクライアントUI - VDSプロパティ



必要に応じてLLDP/CDP設定を修正します。

次に、APICが、UIの[Virtual Networking] > [VMM Domains] > [VMWare] > [Policy] > [Controller] > [Hypervisor] > [General]で、リーフスイッチに対するESXiホストのLLDP/CDPネイバーシップを監視してい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が存在することを検証できます。

<#root>

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、ダイナミックな隣接関係のアクティブ化と必要なVLANのアクティブ化に支障をきたさないように、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カプセル化VLANがリーフスイッチで常にプログラムされ、VMM統合が完全に設定される前に使用できるようにすることが重要です。VMM統合を設定した後でも、このEPGが常に使用可能であることを保証するために、このスタティックパスを保持することをお勧

めします。

ESXiハイパーバイザの場合は、Cisco.comの『Cisco ACI Virtualization Guide』に従い、vDSへの移行時に、VMKインターフェイスが接続されるEPGが展開され、解決緊急度が事前プロビジョニングに設定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上のネットワーク制御ポリシーを介して実行されます
- 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
  - インベントリの手動同期をトリガーして修正
- VMM VLANが中継スイッチに追加されていません
  - 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)
  - 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対して、VLANを設定して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の欠落

このエラーが表示された場合：

```
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:
```

「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および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できます。

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を使用して接続されます。実際には、ESXiホストを少なくとも2つ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によるアップリンクの使用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ファブリックで発生する可能性があります。

```
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方法を見ると、スイッチ依存とスイッチ非依存の2つ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。スイッチに依存する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適合し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

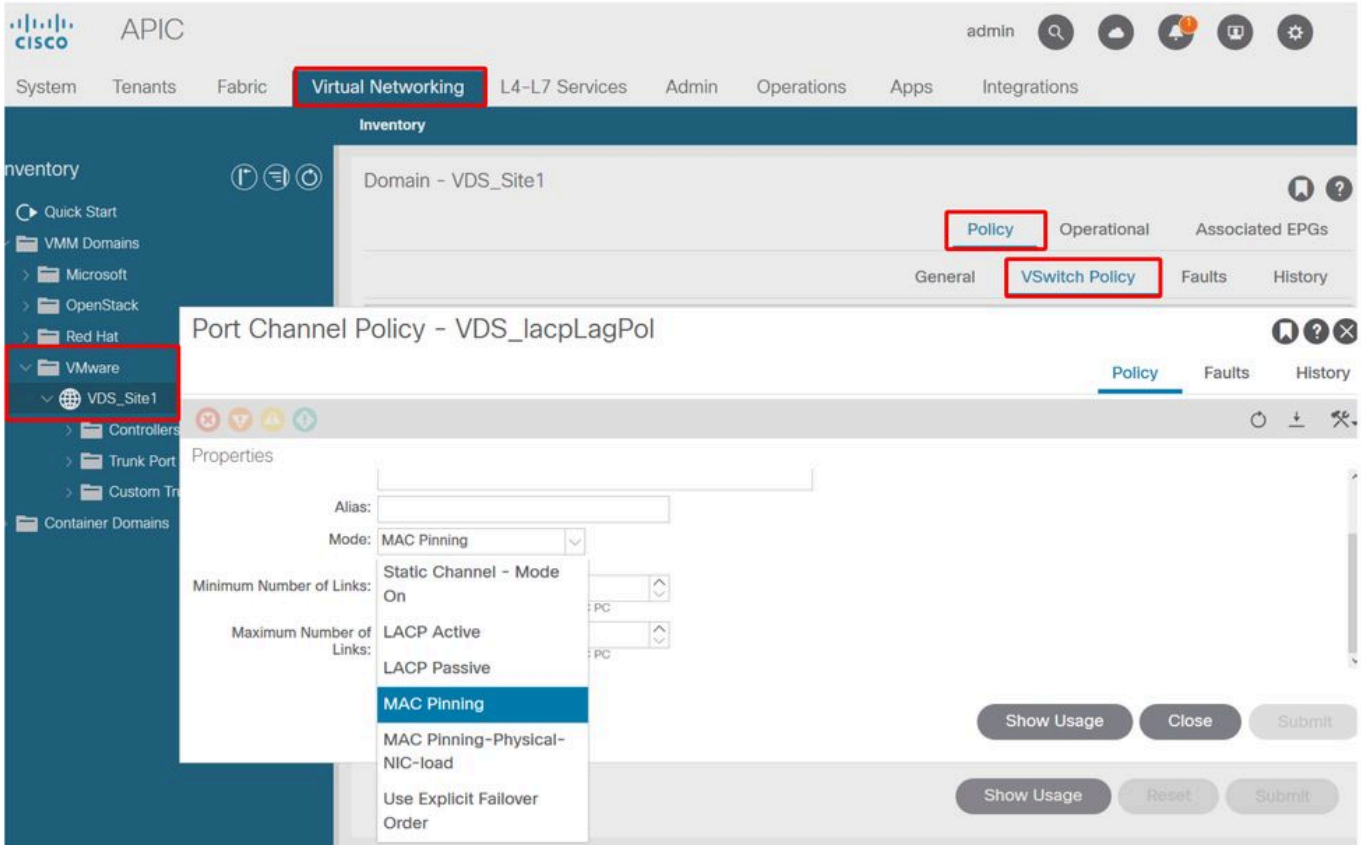
VMwareチーミングおよびフェイルオーバーモード	ACI vSwitchポリシー	説明	ACIアクセスポリシーグループ – ポートチャネルが必要
発信仮想ポートに基づくルート	MACピニング	スイッチの仮想ポートIDに基づいてアップリンクを選択します。仮想スイッチは、仮想マシンまたはVMKernelアダプタのアップリンクを選択すると、この仮想マシンまたはVMKernelアダプタの同じアップリンクを介してトラフィックを常	いいえ

VMwareチーミングおよびフェイルオーバーモード	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
		に転送します。	
送信元MACハッシュに基づくルーティング	適用外	発信元MACアドレスのハッシュに基づいてアップリンクを選択します	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。	いいえ
リンク集約(LAG):IPハッシュベース	静的チャネル – モードオン	各パケットの送信元IPアドレスと宛先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」で設定されている必要があります。	はい（チャネルモードを「オン」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種類の異なる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LACPを有効にしてポートチャネル/VPCを設定する必要があります。必ずACIで拡張Lagポリシーを作成し、それをVSwitchポリシーに適用してください。	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：物理NICロード	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	いいえ

VMwareチーミングおよびフェイルオーバーモード	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
		30秒間75 %以上のビジー状態が続くと、ホスト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。	

次のスクリーンショットは、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を示しています。

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 Networking(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。

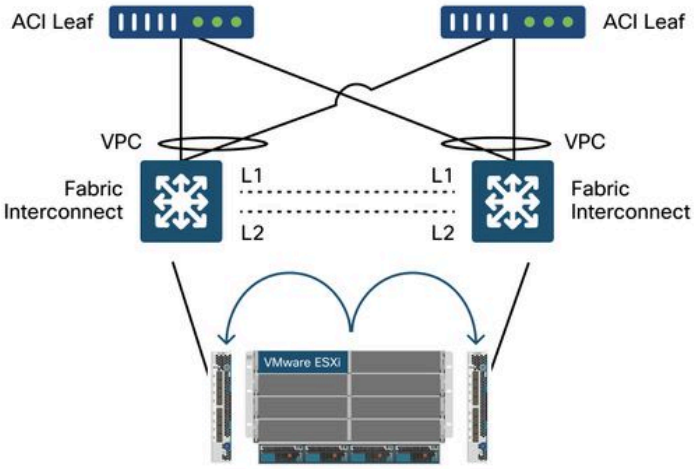
Cisco UCS Bシリーズ使用例

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することが重要です。この使用例は、同様のトポロジを採用してい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。

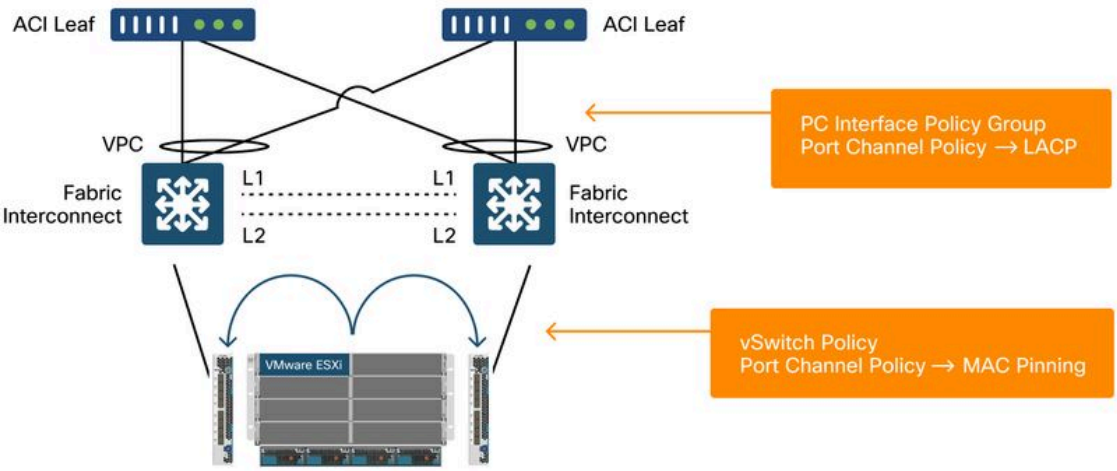
Cisco UCS FIとACIリーフスイッチ：トポロジ



注意すべき重要な事項：

- 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相互接続されます（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、いずれかのFIへのパスを使用します。
- ESXiホスト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。

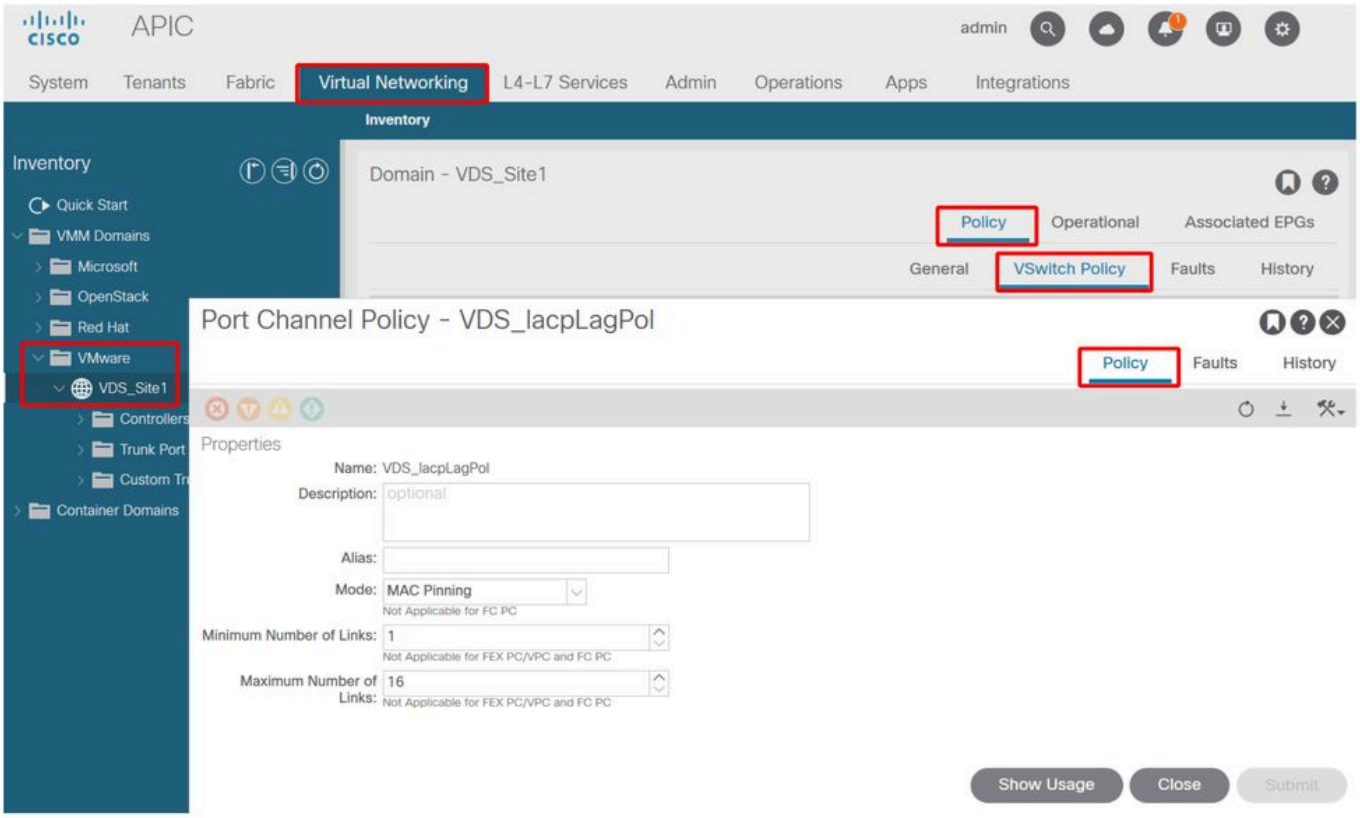
これを正しく設定するには、次の手順を実行します。



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

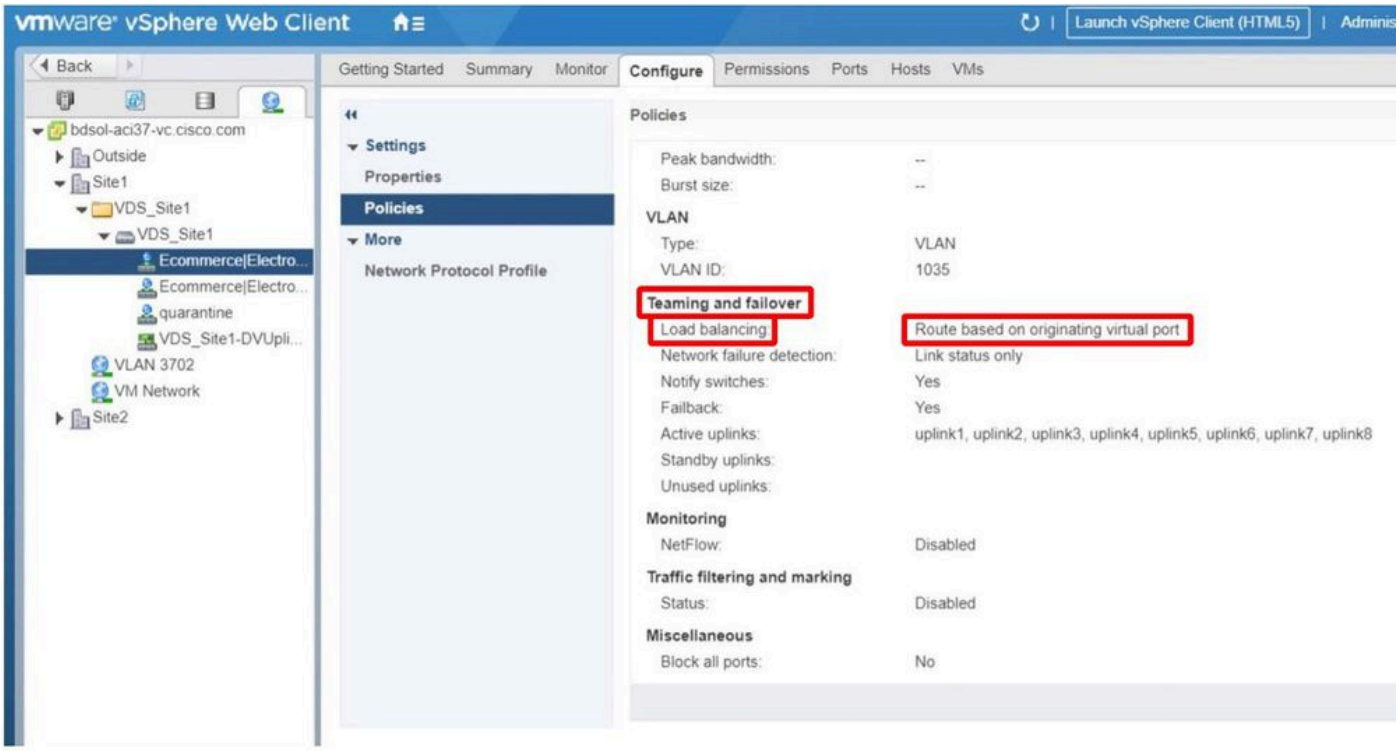
ます。

ACI:vSwitchポリシーの一部としてのポートチャネルポリシー



この例で使用されている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」を使用しても「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


vmware vSphere Web Client
Launch vSphere Client (HTML5)
Back
bdsol-aci37-vc.cisco.com
Outside
Site1
VDS_Site1
VDS_Site1
Ecommerce|Electro...
Ecommerce|Electro...
quarantine
VDS_Site1-DVUpli...
VLAN 3702
VM Network
Site2
Getting Started
Summary
Monitor
Configure
Permissions
Ports
Hosts
VMs
Settings
Properties
Policies
More
Network Protocol Profile
Policies
Peak bandwidth: --
Burst size: --
VLAN
Type: VLAN
VLAN ID: 1035
Teaming and failover
Load balancing: Route based on originating virtual port
Network failure detection: Link status only
Notify switches: Yes
Failback: Yes
Active uplinks: uplink1, uplink2, uplink3, uplink4, uplink5, uplink6, uplink7, uplink8
Standby uplinks:
Unused uplinks:
Monitoring
NetFlow: Disabled
Traffic filtering and marking
Status: Disabled
Miscellaneous
Block all ports: No

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。