ACI VMM統合のトラブルシューティング

内容

概要 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 1.シャード・リーダーの特定 2. vCenterへの接続の確認 3. OOBまたはINBが使用されているかどうかを確認する 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 <u>ていることを確認します。</u> 5.パケットキャプチャの実行 VMwareインベントリ APICによって管理されるVMware VDSパラメータ APICによって管理されるVMWare VDSポートグループパラメーター VMwareインベントリのトラブルシューティング シナリオ1-バッキングが無効な仮想マシン: 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。 VMware DVSバージョン ホストの動的検出 <u>ホスト/VMディスカバリプロセス</u> ファブリックLooseNode/中間スイッチ:使用例 解決の即時性 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がない 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シリーズユースケース

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、『<u>Troubleshooting Cisco Application Centric Infrastructure, Second</u> <u>Edition</u>』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

System	Tenants	Fabric	Virtual Networking	L4-L7 Services	Admin	Operations	Apps	Integ	gration	IS		
			Inventory									
Inventory	(Controller Instance	e - bdsol-aci37-vc							C	
C Quick S	Start							Delle		0		
VMM D	omains							Polic	y	Ope	ratio	onal
> 🚞 Micr	rosoft						General	ſ	History	/	Fa	ults
> 🚞 Ope	nStack							-				**
> 🚞 Red	Hat								(э.	+	***
~ 🖿 VMv	vare		Properties									
~ 🌐 \	/DS_Site1			Name: bdsol-aci3	7-vc							- 1
~ E	Controllers		•	Address: 10.48.176	69							- 1
		37-vc		Model: VMware v0	Center Server	r 6.5.0 build-9451637						
	> 🖿 Hypen	visors		Vendor: VMware, Ir	iC.							
	> 🗐 DVS -	VDS_Site1		Revision: 6.5.0								
	Trunk Port Gr			Serial: 7151cb12	-84a0-40f5-	b6ce-132a1edfeac4						
		Ded Groups	Inventory	Trigger State: untriggere	1	107.00.00						
	Custom Irun	k Port Groups	Latest Inventory Con	npletion Time: 2019-10-0	02109:27:23	.437+00:00						

apic2# show vmware	domain name	VDS_Site1	vcenter 10.48.176.69
Name	:	bdsol-aci3	37-vc
Туре	:	vCenter	
Hostname or IP	:	10.48.176	69
Datacenter	:	Sitel	
DVS Version	:	6.0	
Status	:	online	
Last Inventory Sync	:	2019-10-02	2 09:27:23
Last Event Seen	:	1970-01-01	L 00:00:00
Username	:	administra	ator@vsphere.local
Number of ESX Serve	ers :	2	
Number of VMs	:	2	
Faults by Severity	:	0, 0, 0, 0	
Leader	:	bdsol-aci	37-apic1
Managed Hosts:			
ESX VN	Adja Adja	icency Ir	nterfaces
10.48.176.66 1	Dire	ect le	eaf-101 eth1/11, leaf-102 eth1/11
10.48.176.67 1	Dire	ect le	eaf-301 eth1/11, leaf-302 eth1/11
VMMコントローラ	ーがオフライ	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 v	mware don	nain name '	VDS_Site1							
Domain Name			: VDS_Si	ite1						
Virtual Switch	h Mode		: VMware	: VMware Distributed Switch						
Vlan Domain	Vlan Domain			itel (1001-	1100)					
Physical Inter	rfaces		: leaf-1	102 eth1/11	, leaf-301	eth1/1	1, leaf	-302 eth1/11,		
			leaf-101	eth1/11						
Number of EPGs	S		: 2	: 2						
Faults by Severity			: 0, 0,	: 0, 0, 0, 0						
LLDP override			: RX: er	nabled, TX:	enabled					
CDP override			: no							
Channel Mode d	override		: mac-pi	inning						
NetFlow Export	ter Polio	су	: no							
Health Monitor	ring		: no							
vCenters: Faults: Groupe	ed by sev	verity (Cr.	itical, Majo	or, Minor,	Warning)					
vCenter		Туре	Datacenter		Status	ESXs	VMs	Faults		
10.48.176.69		vCenter	Site1		online	2	2	0,0,0,0		
APIC Owner:										
Controller	APIC	Ownersh	ip							
bdsol-	apic1	Leader								
aci37-vc										
bdsol-	apic2	NonLead	er							
aci37-vc										
bdsol-	apic3	NonLead	er							
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

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。

apicl# bash admin@apicl:~> 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 <u>https://10.48.176.69</u>
* Rebuilt URL to: <u>https://10.48.176.69/</u>* 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

	ニフォリト店	Cisco APICポリシーを使用して
viviware vDS	テノオルト値	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 こう コート	vCenterによるサポート	No.
ハーション	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	0	あり(Cisco APICリリース
ップリンク名	0	4.2(1)以降)
アップリンク名プレフィ	マップリンク	あり(Cisco APICリリース
クス	アシアリンツ	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エラーが常に 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、次のエ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

Create vCenter Co	8 8	
Name:	bdsol-aci20-vc	
Host Name (or IP Address):	10.48.33.45	
DVS Version:	vCenter Default	
Datacenter	POD20	
Stats Collection:	Enabled Disabled	
Management EPG:	select an option \checkmark	
Associated Credential	bdsol-aci20-vc 🗸 🗸	

Cancel	Submit
Calicei	Submit

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

6	Add and Manage Hosts				6
~	1 Selecttask	Select hosts	add to this distributed switch.		
	2 Select hosts				
	3 Select network adapter tas	sks - New hosts	Remove		
	4 Manage physical network adapters	Select new hosts			(8)
	5 Manage VMkernel networ adapters	Incompatible Hos	ts	Q, Filter	*
	6 Analyze impact	Host	Host State	Cluster	
	7 Ready to complete		This list is emp	ty.	
	r ready to complete				
		M Q Find	· ·	0 iter	ns 🎦 Copy 🗝
				ОК	Cancel
		Configure id	entical network settings on multiple hosts	(template mode). 🕕	
				Back	Next Finish Cancel

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

Incompatible Hosts		×
	Q Filter	•
Host	Compatibility	
10.48.22.65	Incompatible	
10.48.22.66	Incompatible	
10.48.22.67	Incompatible	
10.48.31.245	Incompatible	

G Select a host from the list to view its compatibility issues.

Close

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)

cisco	APIC						admin	0 😲	• •)
System	Tenants	Fabric Virtua	I Networking	L4-L7 Services	Admin	Operations	Apps	Integrations		
Inve	ntory Fabric P	olicies Access	Policies							
Inventory	art () () () ()	Fabric Me	mbership	Nodos Dondia	a Pogistration	Lipropolak	la Nadas	Unmanage	G	0
Topology	У	Unmanag	ad Eabria N	lodo - 10.49	22.00 (bc			Onmanage		c3
> 😝 Pod 1	ric Setup Policy	Unmanage	eu rabric r	NOUE - 10.46.	.22.00 (bt	Topology	Genera) I Faults	History	
E Fabric M	Iembership	. 00							0 <u>+</u>	+
🔚 Duplicati	e IP Usage	Properties Syste	m Name: bdsol-ac	i12-ucs-A						(
		Manag	ement IP: 10.48.22	: 10.48.22.80						
		System De	Description: Cisco Nexus Operating System (NX-OS) Software 5.0(3)N2(3.11e) TAC support: http://www.cisco.com/tac Copyright (c) 2002-2016, Cisco Systems, Inc. All rights reserved.							k
		Fabric N	ode Link: 🔺 Node	D	Node Name		Interfa	ce		
			101		bdsol-aci12-leaf1		po1	51		
			102		bdsol-aci12	2-leaf2	po1			
)
								(Close	

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



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、Preprovision 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

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
                                 120
                                                       eth2-1
bdsol-aci37-apic1 Eth1/1
                                 120
bdsol-aci37-apic2
                  Eth1/2
                                                      eth2-1
bdsol-aci37-osl
                  Eth1/11
                                 180
                                          В
                                                      0050.565a.55a7
S1P1-Spine201
                  Eth1/49
                                 120
                                           BR
                                                      Eth1/1
                  Eth1/50
                                 120
S1P1-Spine202
                                           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 -1
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

vmnic6

Link Layer Discovery Protoc	ol
Chassis ID	00:3a:9c:45:12:6b
Port ID	Eth1/11
Time to live	109
TimeOut	60
Samples	437068
Management Address	10.48.176.70
Port Description	topology/pod-1/paths-101/pathep-[eth1/11]
System Description	topology/pod-1/node-101
System Name	S1P1-Leaf101
Peer device capability	
Router	Enabled
Transparent bridge	Enabled
Source route bridge	Disabled
Network switch	Disabled
Host	Disabled
IGMP	Disabled
Repeater	Disabled

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

Properties		
Port Channel Policy:	VDS_lacpLagPol	~ 🗗
LLDP Policy:	LLDP_enabled	~ 🗗
CDP Policy:	CDP_disabled	~ 🗗
NetFlow Exporter Policy:	select an option	\sim

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

44	Properties							
✓ Settings								
Properties	Name:	VDS Site1						
Тороlоду	Manufacturer:	VMware, Inc.						
Private VLAN	Version:	6.0.0						
NetFlow	Number of uplinks:	8						
Port mirroring	Number of ports:	24						
Health check	Network I/O Control:	Disabled						
Mare	Description:							
✓ More	APIC Virtual Switch							
Network Protocol Profiles	Advanced							
Resource Allocation	MTU:	9000 Bytes						
	Multicast filtering mode:	Basic						
	Discovery protocol							
	Туре:	Link Layer Discovery Protocol						
	Operation:	Both						
	Administrator contact							
	Name:							
	Other details:							
	Other details:							

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

cisco	APIC						admin	•	() 💿	٥
System	Tenants	Fabric	Virtual Networking	L4-L7 Service	s Admin	Operations Ap	ps Inte	egrations		
			Inventory	di-						
Inventory		()	Hypervisor - 1	0.48.176.66						0.0
C Quick	Start Domains		^			Topolo	gy Gen	eral Stats	Faults	History
> 🧮 Mic	rosoft		8000							0 ±
> 🚞 Ope	enStack		Properties							
> 🚞 Rec	d Hat				Site1_POD1_APP1		Powered Or	1		^
	ware									
~ 🐨 ~ F	Controllers									
	- 🖧 bdsol-aci	37-vc								
	V 🚞 Hyperv	visors	1							
	~ 🖵 10.	48.176.66			Page 1	Of 1 Ot	ojects Per Page	15 V Display	ng Objects 1 -	
		Virtual Machine	s	Neighbors:	 Management Address 	Interface Name	Proto	Neighbor	ID	
	e S	vmnic1			10.48.176.70	Pod-1/Node-101/eth	1/11 LLDP	00:3a:9c	:45:12:6b	
	E C	vmnic2			10.48.176.71	Pod-1/Node-102/eth	1/11 LLDP	00:3a:9c	1b:37:4b	
		vmnic3	Management	Network Adapters:	 Name 	MAC	State	IP Addr	ess	
	9	vmnic4			vmk0	28:AC:9E:DE:D2:7A	Up	10.48.	176.66	
	9	vmnic5								×.
	8	vmnic6								

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	Ecomme	erce:Electronics:APP	active	Eth1/11
VLAN	Туре	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

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/Passiv e」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

cisco	APIC							admin	Q	0	0	•	٢	
System	Tenants	Fabric Virtual I	Networking	L4-L7 Services	Admin	Operations	Apps	Integra	ations					
		In	ventory											
nventory			omain - VDS_	Site1									0	0
C Quick St	tart omains osoft nStack Hat	Port Channel Po	olicy - VDS	5_lacpLagPc	bl		Gene	Policy ral V	Ope Switch	erational Policy	Fau	ssociat	ed EPG Histor	s y
V 🖿 VMw	vare		,	_ 1 0						Polic	y	Faults	His	tory
~ ⊕ v	/DS_Site1	80000									_	Ċ	<u>+</u>	%.
> 🖬 > 🚰 Containe	Trunk Port Custom Tri er Domains	Properties Alias: Mode:	MAC Pinning Static Channel	- Mode										
		Minimum Number of Links: Maximum Number of Links:	On LACP Active LACP Passive	PC										
			MAC Pinning MAC Pinning-F NIC-load Use Explicit Fail Order	Physical-				Show	ow Usag Usage		Close			

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 (<u>https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.networking.doc/GUID-</u> <u>D34B1ADD-B8A7-43CD-AA7E-2832A0F7EE76.html</u>)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

cisco	APIC							admin Q	0	0	•	0
System	Tenants	Fabric	Virtual Networking	L4-L7 Services	Admin	Operations	Apps	Integrations	i .			
			Inventory									
Inventory		()	O Domain - VD	S_Site1								00
← Quick St ~ 🖿 VMM Do > 🖿 Micro	tart omains osoft		_				Gener	Policy O	perational	I As	sociate	ed EPGs History
> 🖬 Oper	Hat Vare	Port Cha	annel Policy - VI)S_lacpLagPo					Polic	y F	aults	History
	Controllers	804	0								Ó	± %-
> 🖬	Trunk Port	Properties Minimum Num Maximun	Name: VDS_lacpLagPc Description: Optional Alias: MAC Pinning Not Applicable for I Not Applicable for I n Number of 16 Links: Not Applicable for I	E IC PC EX PC/VPC and FC PC EX PC/VPC and FC PC								
								Show Us	age	Close		

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。