アドレスACI障害コード：F606347、F606350 F606391

内容

はじめに

このドキュメントでは、Cisco Application Centric Infrastructure(ACI)VMware Virtual Machine Manager(VMM)統合の障害である障害F606347（VMコントローラでのポートグループの追加または削除の障害）、障害F606350（分散仮想スイッチでのLACP Lagポリシーの更新障害）、および障害F606391（ホスト上の物理アダプタにリンク層検出プロトコル/Cisco Discovery Protocol隣接関係情報が見つからない）を修復するためののの次のの手順について説明します。

バックグラウンド情報

これらの障害は、ACI VMMドメインとVMware vCenterおよび分散仮想スイッチ(DVS)との統合を使用するファブリックで発生します。 ACIは、vCenter APIを介して、ポートグループライフサイクル、Link Aggregation Control Protocol(LACP)lagポリシー、物理アップリンクトポロジなどのポリシーをDVSと継続的に同期します。その同期が失敗するか、または前提条件となる検出情報が欠落している場合、ACIはこれらのエラーを発生させ、オペレータのレビューの条件を提示します。

障害F606347:VMコントローラでのポートグループの追加または削除が失敗する

説明

このエラーは、EPGとVMMドメインポリシーの同期の一部として、ACIがVMコントローラ（VMware vCenterなど）でポートグループの追加または削除に失敗すると発生します。EPGがVMMドメインに関連付けられている、または関連付けられていない場合、APICは、分散仮想スイッチ(DVS)で対応するポートグループを作成または削除するようにVMコントローラに指示します。 この操作を管理する有限状態マシン(FSM)が正常に完了しない場合、ACIは影響を受けるVMMドメインコントローラーオブジェクトでエラーF606347を発生させます。

```
"Code" : "F606347",
"Description" : "[FSM:FAILED]: Addition or Deletion of Port Group for: (uni/tn-<TENANT>/ap-<APP-PROFILE>
"Dn" : "uni/vmmp-<VM-Provider>/dom-<VMM-NAME>/ctrlr-[<VMC>]/fault-F606347"
```

推奨アクション

この障害は、通常、ACIバージョンとVMコントローラのバージョン間の通信または互換性の問題が原因で発生します。Cisco Technical Assistance Center(TAC)に問い合わせる前に、次の手順に従ってください。

手順1:APICからvCenterへの接続の確認

ポートグループ操作は、vCenter APIを介して実行されます。APICがVMコントローラに到達できない場合、FSMはタイムアウトし、障害が発生します。

1. APIC GUIで、VM Networking > VMware > [DVS Domain] > Controllers > [vCenter

Controller]の順に移動し、動作状態がonlineであることを確認します。

2. ドメインのVMMリーダーであるAPICを特定し、基本的なネットワークの到達可能性を確認します。そのAPICからpingを実行し、vCenterへのHTTPS接続を試行します。
<#root>

```
apic1#

show vmware domain name




        | grep " Leader"



 <VMM-NAME>     apic2   Leader

apic2#

ping




PING <VC-IP> (<VC-IP>) 56(84) bytes of data.
64 bytes from <VC-IP>: icmp_seq=1 ttl=63 time=0.312 ms
^C

apic2#

curl -k -X POST -H 'Accept: application/json' --basic \
  -u




       @vsphere.local:




         \
  https://




         /rest/com/vmware/cis/session
```

正常なHTTPS応答は、APICがvCenterに対して認証できることを確認します。接続エラーまたは認証エラーは、ネットワークまたは資格情報の問題を示します。ポートグループの操作が成功するには、この問題を解決する必要があります。

手順2:vCenterのクレデンシャルと権限の確認

VMMドメインで構成されたvCenterアカウントが有効であり、DVSでポートグループを作成および削除するための十分な権限を持っている必要があります。

1. APIC GUIで、VM Networking > VMware > [DVS Domain] > vCenter Credentialsの順に移動し、ユーザ名とパスワードが現在のものであることを確認します。
2. vCenterユーザアカウントに、少なくともDVS上で次の権限があることを確認します。
   - DVS：ポートグループを作成、削除、および変更します。
   - ネットワーク：ネットワークポリシーをポートグループに割り当てます。

   必要なvCenter権限の完全なリストについては、『ACI VMM Troubleshooting Guide』を参照してください。

手順3:ACIとvCenterバージョンの互換性の確認

ACIソフトウェアバージョンとVMコントローラバージョンの間に互換性がないと、ポートグループAPIコールがサイレントに失敗したり、APIC FSMが回復できない予期しないエラーが返されたりする可能性があります。

1. ファブリックで現在実行されているACIリリースでサポートされるvCenterバージョンがリストされていることを確認します。Cisco.comの『ACI Compatibility Matrix』を参照してください。
2. ACIまたはvCenterの最新のアップグレードがこのエラーの発生より前に発生した場合、アップグレードされたバージョンのACIリリースノートを参照して、既知のVMM統合の問題または必要な最小vCenterバージョンを特定します。
3. vCenterのバージョンに互換性がない場合は、vCenter（またはACI）をサポートされている組み合わせにアップグレードします。バージョン固有の既知の問題については、『ACI VMMトラブルシューティングガイド』を参照してください。

手順4 — VMMコントローラーの操作状態とイベントログを確認します

1. APIC GUIで、VM Networking > VMware > [DVS Domain] > Controllers > [vCenter Controller]の順に移動し、Operationalタブを開きます。同時VMM接続障害(F606225やF606327など)の[イベント]サブタブと[障害]サブタブを確認します。 より広い範囲の接続障

害が存在する場合は、まずそれらを解決します。
2. また、APIC REST APIを使用して障害を直接照会し、障害の詳細な説明とFSMからの特定のエラーテキストを確認することもできます。
<#root>

```
apic#
moquery -c faultInst -x 'query-target-filter=eq(faultInst.code,"F606347")'
```

出力内のdescriptionフィールドには、VMコントローラ名、VMドメイン、VMプロバイダー、および操作をトリガーしたEPGを含むFSMエラーの詳細が含まれています。この情報を使用して、調査の範囲を、関連する特定のEPGおよびVMMドメインに絞り込みます。

手順5：影響を受けるEPGとVMMドメインの関連付けを確認します

1. 障害の説明(uni/tn-<TENANT>/ap-<APP-PROFILE>/epg-<EPG>)で指定されたEPGを特定します。
2. APIC GUIで、Tenants > [Tenant] > Application Profiles > [App Profile] > Application EPGs > [EPG] > Domainsの順に移動し、VMMドメインの関連付けが存在し、正しい状態になっていることを確認します。
3. ポートグループ操作が誤った構成変更によってトリガーされた場合は、EPGとVMMドメインの関連付けが存在するかどうかを確認します。関連付けの削除と再追加を行うと、FSMがリセットされ、基盤となるインフラストラクチャの問題が解決した場合は障害がクリアされます。

ステップ6：診断を収集し、障害が解消されない場合はTACに連絡する

上記の手順を実行しても障害が解決しない場合は、次の情報を収集し、Cisco TACでケースをオープンします。

- APICテクニカルサポートバンドル：APIC GUIでSystem > Troubleshooting > Tech Supportの順に選択し、バンドルを生成してダウンロードします。
- 完全な障害DNと、ステップ4の`moquery`出力の説明テキスト。
- ACIソフトウェアのバージョン(System > Controllers > [APIC] > Summaryから)とvCenterのバージョン
- 最初に発生した期間と、アップグレードまたは設定の変更後に障害が発生したかどうかを示します。

その他の詳細事項

EPGがVMMドメインに関連付けられると、ACIはvCenter APIを介してDVS上の対応するポートグループをプログラムします。有限状態マシン(FSM)タスクの`CompEpPDAddorDelExtPol`は、このライ

フサイクル操作を管理します。FSMは、ポートグループの追加または削除を試行し、一連の状態を遷移します。vCenterから返されたAPIエラー、タイムアウト、認証の失敗などが原因で状態遷移が失敗した場合、FSMはFAILEDとしてマークされ、障害F606347が、影響を受けたVMコントローラの`vmmCtrlr`オブジェクトで発生します。

一般的な障害シナリオには次のものがあります。

- ACIとvCenter間のバージョンの非互換性:ACIまたはvCenterをアップグレードするとAPIの動作が変更され、ポートグループの動作に障害が発生します。これは最も一般的な根本原因の1つであり、両方の製品を互換性のあるバージョンの組み合わせに合わせることで対処します。詳細については、『ACI仮想化マトリックス』を参照してください。
- vCenter APIタイムアウトまたは一時的なエラー:vCenterが過負荷または一時的に使用できない場合に、エラーが返されるか、FSMタイムアウト内に応答がありません。操作はすべてのコードパスで自動的に再試行されるわけではありません。EPGとVMMドメインの関連付けを手動で削除して再度追加すると、新しいFSMの実行がトリガーされます。
- vCenter権限が不十分:vCenterサービスアカウントにポートグループを作成または削除する権限がないため、APIコールが認証エラーを返す原因となります。
- ポートグループ名の競合:ACIが作成しようとしているポートグループと同じ名前で手動で作成されたポートグループがDVSにすでに存在しており、操作が失敗する原因になっています。関連付けを再試行する前に、競合するポートグループを削除するか、名前を変更してください。

注:FSMの状態は関連付けが削除されるか新しいトリガーが到着するまで保持されるため、障害は基盤となるネットワークまたはクレデンシャルの問題が解決された後でも続く可能性があります。根本原因を修正した後もエラーが解決しない場合は、EPGとVMMドメインの関連付けを削除して再度追加し、新しいFSMの実行を強制します。

障害F606350:DVSでのLACP Lagポリシーの更新が失敗する

説明

このエラーは、ACIがvCenter APIを介してDVS上のLACP lagポリシーを更新しようとして操作が失敗すると発生します。ACIは、特にLACPポリシーがDVSに接続されたVMMドメインに関連付けられている場合、VMMドメインポリシー同期の一部としてLACP設定をDVSにプッシュします。アップデートを適用できない場合、ACIは影響を受けるリーフノードでエラーF606350を発生させます。

```
"Code" : "F606350",
"Description" : "Updating LACP Lag Policy at DVS failed.",
"Dn" : "topology/pod-<podId>/node-<leafNodeId>/local/svc-policyelem-id-0/uni/epp/fv-[uni/vmmp-VMware/do
```

推奨アクション

このタスクはACIによって自動的に再試行されます。一時的なvCenter APIの遅延、またはAPICとvCenter間の一時的な接続中断により、この障害の単一インスタンスが発生する可能性があります。多くの場合、再試行は成功し、障害は自動的にクリアされます。

繰り返される障害または持続的な障害が発生する場合は、Cisco Technical Assistance Center(TAC)に問い合わせる前に、次の手順に従ってください。

1. APICがネットワーク経由でvCenterサーバに到達できることを確認します。Application Policy Infrastructure Controller(APIC)GUIでVM Networking > VMware > [DVS Domain] > Controllers > [DVS Controller]の順に選択して、動作状態がonlineであることを確認します。
2. VMMドメインで構成されたvCenter資格情報が有効であり、有効期限が切れていないことを確認してください。VM Networking > VMware > [DVS Domain] > vCenter Credentialsの順に移動し、ユーザ名とパスワードが正しいことを確認します。
3. VMMドメインに関連付けられたvCenterユーザーアカウントに必要な特権があることを確認します。少なくとも、アカウントにはDVS構成とホストネットワーク管理のアクセス許可が必要です。必要なvCenter権限の完全なリストについては、『Cisco ACI VMware vSphere Integration Guide』(Cisco.comで入手可能)または『ACI VMM Troubleshooting Guide』を参照してください。
4. APICシステムの障害とイベントログを確認し、より広範なvCenter API通信の問題を示す同時VMM接続障害(F606225やF606327など)を探します。このような障害が存在する場合は、まず接続の問題を解決します。
    1. 次のコマンドを使用してapicリーダーを確認し、必要に応じてnslookupで接続をテストします。pingとHTTPS(IPsec Security Protocol)を使用します。

```
apic1# show vmware domain name shared-dvs | grep " Leader"
 shared-vc     apic2   Leader
apic2# nslookup




apic2# ping



PING


            (


            ) 56(84) bytes of data.
64 bytes from
```

```
             : icmp_seq=1 ttl=63 time=0.237 ms
64 bytes from



              : icmp_seq=2 ttl=63 time=0.406 ms
^C
---



                ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.237/0.321/0.406/0.084 ms

apic2# curl -k -X POST -H 'Accept: application/json' --basic -u



                @vsphere.local:



                  https://



                  /rest/com/vmware/cis/session > cookie.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
100   408    0   408    0     0   1393      0 --:--:-- --:--:-- --:--:--  1397
```

5. VMMドメインインターフェイスポリシーグループに関連付けられているLACPポリシーを確認してください。Fabric > Access Policies > Policies > Interface > Port Channelの順に移動し、LACPポリシーモードがvCenterのDVSアップリンクポートグループ設定と互換性があることを確認します。互換性のある組み合わせについては、『ACI VMM Troubleshooting Guide』の「Teaming and ACI vSwitch Policy」の項を参照してください。

6. 上記のすべてを確認しても依然として障害が解決しない場合は、APICのtech-supportファイルを収集して、Cisco TACに連絡してください。
    - APIC GUIでSystem > Troubleshooting > Tech Supportの順に選択し、テクニカルサポートバンドルを生成してダウンロードします。
    - 障害の詳細からの障害DNと、TACケースで繰り返し発生する障害のタイムフレームを含めます。

その他の詳細事項

ACI VMMの統合では、vCenter APIを使用して、ファブリックに代わってDVS構成をプログラムします。LACPポリシーがVMMドメインインターフェイスポリシーグループ(**infraAccPortGrp**)に関連付けられると、ACIはポリシーをDVS LACPグループ設定に変換し、vCenterにプッシュします。プッシュ操作が失敗する理由はいくつかあります。

- vCenter APIタイムアウト：低速または過負荷のvCenterは、APICのタイムアウトウィンドウ内に応答しない場合があります。操作は自動的に再試行されます。
- 不十分な権限:VMMドメインに設定されているvCenterサービスアカウントに、DVSアップリンクポートグループのプロパティを変更するために必要な権限がありません。
- DVSバージョンの非互換性:vCenterのDVSバージョンでは、プッシュされるLACP設定がサポートされません。ACIでは、LACPをサポートするためにDVSバージョン5.1以降が必要です。
- LACPポリシー競合:DVSアップリンクポートグループ上の既存の手動LACP設定が、ACIが適用しようとしているポリシーと競合しています。

注：再試行後にクリアされるF606350の単一の分離インスタンスは、永続的な問題を示しません。短時間のうちに障害が繰り返し再発するか、数分以内に解消されない場合にのみ調査してください。

障害F606391：物理アダプタのLLDP/CDP隣接関係が見つかりません

説明

このエラーは、VMMドメインによって管理されているホスト上の物理ネットワークアダプター(vmnic)のリンク層検出プロトコル(LLDP)またはCisco Discovery Protocol (CDP)の隣接関係情報がACIで見つからない場合に発生します。ACIはLLDPまたはCDPを使用して、どのリーフスイッチポートがホストの各vmnicに物理的に接続されているかを検出します。この隣接関係情報がないと、ACIはDVSからのVMトラフィックを対応するリーフポートに正しくマッピングできません。これは、そのホストの仮想マシンのポリシー展開とエンドポイントラーニングに影響します。

```
"Code" : "F606391",
"Description" : "LLDP/CDP Adjacency information not found for physical adapters on the host.",
"Dn" : "topology/pod-<podId>/node-<leafNodeId>/local/svc-policyelem-id-0/uni/epp/fv-[uni/vmmp-VMware/do
```

推奨アクション

この障害では、パス内の3つのポイント（vCenter内のDVS、ESXiホスト、および物理リーフスイッチ）で、LLDPまたはCDP設定を手動で検証する必要があります。次の手順を順に実行します。

手順1:DVS上のLLDP/CDP設定を検証します

DVS Discovery Protocol設定は、DVSがLLDPフレームまたはCDPフレームをアドバタイズしてリッスンするかどうかを制御します。これらのプロトコルは、『ACI VMMトラブルシューティングガイド』で説明されているように相互に排他的です。この設定を無効にした場合、またはAdvertise Onlyに設定した場合、APICはvCenterから隣接情報を読み取ることができません。

1. vSphere Clientにログインし、Home > Networking > [DVS Name] > Configure > Settings > Propertiesの順に選択します。
2. Advancedセクションに移動し、Discovery Protocolのフィールドを確認します。
   - Type：環境に応じて、Link Layer Discovery Protocol(LLDP)（ACIに推奨）またはCisco Discovery Protocolに設定します。
   - Operation:BothまたはListenに設定する必要があります。AdvertiseまたはDisabledを設定すると、DVSはネイバー情報を受信できなくなります。これは、vCenterにはAPICに報告する隣接関係データがないことを意味します。
3. 操作がAdvertiseまたはDisabledに設定されている場合は、これをBothに変更して設定を保存します。APICがvCenterに対して更新された隣接関係データを再クエリするまで数分かかります。

注:DVS Discovery Protocolの設定を変更しても、VMトラフィックは中断されません。影響を受けるのは、DVSと接続されたスイッチの間で交換されるコントロールプレーン検出情報だけです。

手順2：物理リーフスイッチのLLDP/CDPを検証します

ホスト（またはホストが接続するアップストリームアクセススイッチ）に接続されているリーフスイッチインターフェイスでは、LLDPまたはCDPを有効にする必要があります。ACIでは、LLDPとCDPは、関連するポートで使用されるインターフェイスポリシーグループに適用されるインターフェイスポリシーによって制御されます。

1. ホストに接続されているリーフポートを特定します。Fabric > Inventory > [Pod] > [Leaf Node] > Interfaces > Physical Interfacesの順に移動し、ホストのvmnicトラフィックを搬送しているインターフェイスを見つけます。
2. Fabric > Access Policies > Interfaces > Leaf Interfaces > Policy Groupsの順に移動し、そのポートに適用されているインターフェイスポリシーグループを開きます。
3. 受信状態：有効および送信状態：有効のポリシーグループにLLDPインターフェイスポリシーが割り当てられていることを確認します。LLDPポリシーが適用されていない場合は、両方の状態が有効になっているデフォルトポリシーが使用されます。
4. CDPを使用している場合は、CDPインターフェイスポリシーがAdmin State: Enabledで接続されていることを確認します。
5. リーフが予想されるインターフェイスでLLDPネイバーを受信していることを確認するには、リーフにSSH接続して次のコマンドを実行します。
   <#root>

   ```
   leaf101#

   show lldp neighbors
   ```

   出力には、各インターフェイスと、そのインターフェイスで検出されたネイバーがリストされます。ホストのvmnicまたはアップストリームアクセススイッチは、想定されるインターフェイスのネイバーテーブルに表示される必要があります。出力にインターフェイスがない場合、リーフはそのポートでLLDPフレームを受信していません。これは、LLDPが接続デバイスのアップストリームでブロックされているか、無効になっていることを示しています。
6. CDPを使用している場合は、次のコマンドを実行してCDPネイバー探索を確認します。
   <#root>

   ```
   leaf101#

   show cdp neighbors
   ```

   予想されるインターフェイスの出力には、ホストまたはアップストリームスイッチが表示される必要があります。

手順3：ホストに接続されている物理スイッチ上のLLDP/CDPを検証します

ホストvmnicが中間の物理アクセススイッチ（ACIリーフに直接接続されていない）に接続されている場合、リーフに到達するには、LLDPまたはCDPフレームをそのスイッチ経由で転送する必要があります。中継スイッチで次の点を確認します。

- LLDPまたはCDPがスイッチでグローバルに有効になっている。
- LLDPまたはCDPは、ホストとACIリーフの両方に面するインターフェイスで有効になっています。
- スイッチは、関連するインターフェイス上のLLDP/CDPプロトコルデータユニット(PDU)をフィルタリングまたはブロックするように設定されていません（たとえば、サービスポリシーまたはアクセスコントロールリストを使用して）。

注:LLDPはリンクローカルプロトコルです。標準レイヤ2スイッチは、LLDPがスイッチ自体で終端されていない場合にのみ、同じVLAN内のポート間でLLDP PDUを透過的に転送します。中間スイッチがLLDPを終端すると、ホストではなく、リーフのLLDPネイバーになります。この場合、ACIは中間スイッチをネイバーとして認識します。つまり、ホストのvmnicを識別できません。中間スイッチでLLDPパススルーを有効にするか、ホストをACIリーフに直接接続します。

手順4：変更後のAPIC隣接関係の状態の確認

設定を変更した後、APICがホストの物理アップリンクトポロジを解決できることを確認します。APIC GUIで、VM Networking > VMware > [DVS Domain] > [DVS Name] > Hosts > [Host Name] > Physical Interfacesの順に移動し、Discoveredフィールドに各vmnicのリーフポートが表示されていることを確認します。隣接関係が正しく解決されると、障害は自動的にクリアされます。

特定のVMMドメインの隣接オブジェクトを確認するために、APIC REST APIを照会することもできます。

<#root>

apic#

moquery -c compHv -x 'query-target-filter=eq(compHv.name,"*hostname*")'

compHvオブジェクトは、VMMドメイン内のハイパーバイザホストを表します。関連する**compNic**オブジェクトは物理アダプタを表します。隣接関係が解決されると、**compNic**オブジェクトの**peerDn**属性に、対応するリーフインターフェイスのDNが設定されます。

上記の3つの設定ポイントをすべて検証しても障害が解決しない場合は、APICテクニカルサポートファイルを収集して、Cisco TACにお問い合わせください。

その他の詳細事項

ACI VMM統合は、vCenter APIを使用して、vCenterがDVSから収集したLLDPおよびCDPネイバーデータを取得します。APICはこのデータを読み取って、どのホストvmnicがどのリーフポートに接続するかを示すマップを作成します。このマッピングは次の目的で使用されます。

- 特定のホストから送信されるVMトラフィックに対して正しいリーフインターフェイスポリシーをプログラムします。Resolution Immediacyが即時またはオンデマンドとして設定されている場合、ホストとリーフがLLDP/CDPネイバーシップを失うと、ポリシーは削除されま

す。
- 物理アタッチメントポイントに基づいて、仮想エンドポイントのマイクロセグメンテーションとEPGメンバーシップを適用します。
- ホストの物理アップリンクトポロジの正確な知識を必要とするACI仮想エッジ(AVE)ポリシー適用をサポートします。

隣接関係情報が欠落している場合、ACIは障害F606391を生成し、影響を受けるホストの物理トポロジを検証できないことを通知します。仮想マシンの接続は暫定期間中も機能する可能性があります。障害によってデータ転送がすぐに中断されるわけではありません。ただし、ポリシー導入の精度とエンドポイントの学習の信頼性は低下します。

将来の予防

障害F606391が解決された後に再発しないようにするには、次の手順を実行します。

- ACI VMMドメインに関連付けられたすべてのDVSインスタンスの標準構築要件として、DVS Discovery Protocol OperationをBothに設定します。
- VMware ESXiを実行するホストに接続するすべてのリーフポートに適用される標準のインターフェイスポリシーグループテンプレートの一部として、LLDPおよびCDPの有効化を含めます。
- ホストとACIリーフの間で中間アクセススイッチを使用する場合は、スイッチベンダーのLLDP転送動作がACI VMM検出メカニズムと互換性があることを展開前に確認してください。

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。