

地址ACI故障代碼：F606347、F606350F606391

目錄

[簡介](#)

[背景資訊](#)

[故障F606347:VM控制器上的埠組新增或刪除失敗](#)

[說明](#)

[建議的操作](#)

[第1步 — 檢驗APIC到vCenter的連線](#)

[第2步 — 驗證vCenter憑據和許可權](#)

[第3步 — 驗證ACI和vCenter版本的相容性](#)

[第4步 — 檢查VMM控制器操作狀態和事件日誌](#)

[第5步 — 檢視受影響的EPG和VMM域關聯](#)

[步驟6 — 收集診斷資訊，並在故障持續時聯絡TAC](#)

[其他詳細資訊](#)

[故障F606350:DVS的LACP Lag策略更新失敗](#)

[說明](#)

[建議的操作](#)

[其他詳細資訊](#)

[故障F606391:未找到物理介面卡的LLDP/CDP鄰接關係](#)

[說明](#)

[建議的操作](#)

[第1步 — 驗證DVS上的LLDP/CDP配置](#)

[第2步 — 在物理枝葉交換機上驗證LLDP/CDP](#)

[第3步 — 在連線到主機物理交換機上驗證LLDP/CDP](#)

[第4步 — 更改後驗證APIC鄰接狀態](#)

[其他詳細資訊](#)

[未來預防](#)

簡介

本文檔介紹以下思科以應用為中心的基礎設施(ACI)VMware Virtual Machine Manager(VMM)整合故障的修復後續步驟：故障F606347 (VM控制器上的埠組新增或刪除失敗)、故障F606350 (分散式虛擬交換機上的LACP Lag策略更新失敗) 和故障F606391 (在主機上找不到物理介面卡的鏈路層發現協定/思科發現協定鄰接資訊)。

背景資訊

在使用ACI VMM域與VMware vCenter和分散式虛擬交換機(DVS)整合的交換矩陣中會出現這些故障

。ACI通過vCenter API連續同步策略(包括埠組生命週期、鏈路聚合控制協定(LACP)延遲策略和物理上行鏈路拓撲)與DVS。當同步失敗或缺少先決條件發現資訊時，ACI會引發這些錯誤，以暴露條件供操作員檢查。

故障F606347:VM控制器上的埠組新增或刪除失敗

說明

當ACI在EPG到VMM域策略同步過程中未能新增或刪除VM控制器 (例如VMware vCenter) 上的埠組時，將引發此故障。當EPG與VMM域關聯或解除關聯時，APIC會指示VM控制器在分散式虛擬交換機(DVS)上建立或刪除相應的埠組。如果管理此操作的有限狀態機(FSM)未成功完成，ACI將在受影響的VMM域控制器對象上引發故障F606347。

```
"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"
```

建議的操作

此故障通常由ACI版本和VM控制器版本之間的通訊或相容性問題引起。聯絡思科技術協助中心(TAC)之前，請完成以下步驟。

第1步 — 檢驗APIC到vCenter的連線

埠組操作通過vCenter API執行。如果APIC無法訪問VM控制器，FSM將超時並引發故障。

1. 在APIC GUI中，導航至VM Networking > VMware > [DVS Domain] > Controllers > [vCenter Controller]，確認運行狀態為在線。
2. 確定作為域的VMM領導者的APIC，並驗證基本網路可達性。從該APIC ping並嘗試與vCenter的HTTPS連線：

```
<#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
```

成功的HTTPS響應確認APIC可以向vCenter進行身份驗證。連線失敗或身份驗證錯誤表示在埠組操作成功之前必須解決網路或憑證問題。

第2步 — 驗證vCenter憑據和許可權

在VMM域中配置的vCenter帳戶必須有效並且必須具有足夠的許可權才能在DVS上建立並刪除埠組。

1. 在APIC GUI中，導航至VM Networking > VMware > [DVS Domain] > vCenter Credentials，確認使用者名稱和密碼為最新密碼。
2. 確認vCenter使用者帳戶對DVS至少具有以下許可權：
 - DVS:建立、刪除和修改埠組。
 - 網路：將網路策略分配給埠組。有關所需的vCenter許可權的完整清單，請參閱[ACI VMM故障排除指南](#)。

第3步 — 驗證ACI和vCenter版本的相容性

ACI軟體版本和VM控制器版本之間的不相容會導致埠組API呼叫靜默失敗，或返回APIC FSM無法從恢復中恢復的意外錯誤。

1. 確認當前在交換矩陣中運行的ACI版本已列為受支援的vCenter版本。請參閱Cisco.com上的[ACI相容性矩陣](#)。
2. 如果在出現此故障之前對ACI或vCenter進行了最新升級，請查閱升級版本的ACI發行說明，以確定已知的VMM整合問題或所需的最低vCenter版本。
3. 如果vCenter版本不相容，請將vCenter（或ACI）升級到受支援的組合。有關版本特定的已知問題，請參閱[ACI VMM故障排除指南](#)。

第4步 — 檢查VMM控制器操作狀態和事件日誌

1. 在APIC GUI中，導航到VM Networking > VMware > [DVS Domain] > Controllers > [vCenter Controller]，然後開啟Operational頁籤。檢視Events和Faults子頁籤以瞭解併發VMM連線故障（例如F606225或F606327）。如果存在更廣泛的連線故障，請先解決它們。
2. 您還可以通過APIC REST API直接查詢故障，以檢視FSM的完整故障說明和特定錯誤文本：

```
<#root>
```

```
apic#
```

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

輸出中的description欄位包含FSM錯誤詳細資訊，包括VM控制器名稱、VM域、VM提供程式以及觸發操作的EPG。使用此資訊將調查範圍縮小到所涉及的特定EPG和VMM域。

第5步 — 檢視受影響的EPG和VMM域關聯

1. 確定故障描述中命名的EPG(uni/tn-<TENANT>/ap-<APP-PROFILE>/epg-<EPG>)。
2. 在APIC GUI中，導航到租戶> [租戶]>應用配置檔案> [應用配置檔案]>應用EPG > [EPG] >域，並確認VMM域關聯存在且處於正確的狀態。
3. 如果意外配置更改觸發了埠組操作，請驗證EPG到VMM域關聯是否應該存在。刪除並重新新增關聯可以重置FSM，並在底層基礎設施問題得到解決後清除故障。

步驟6 — 收集診斷資訊，並在故障持續時聯絡TAC

如果完成上述步驟後故障未清除，請收集以下資訊並使用Cisco TAC建立案例：


- APIC技術支援捆綁包：在APIC GUI中導航至System > Troubleshooting > Tech Support，以生成和下載捆綁包。
- 步驟4中`moquery`輸出的完整故障DN和說明文本。
- ACI軟體版本(來自System > Controllers > [APIC] > Summary)和vCenter版本。
- 首次發生的時間範圍以及升級或配置更改後是否出現故障。

其他詳細資訊

當EPG與VMM域關聯時，ACI會通過vCenter API對DVS上的相應埠組進程式設計。有限狀態機(FSM)任務`CompEppDAddorDelExtPol`管理此生命週期操作。FSM會嘗試埠組新增或刪除並通過一組狀態轉換。如果任何狀態轉換失敗(例如，由於vCenter返回的API錯誤、超時或身份驗證失敗)，FSM將標籤為FAILED，並在受影響的VM控制器的`vmmCtrlr`對象上引發故障F606347。

常見的故障情形包括：

- ACI到vCenter版本不相容— ACI或vCenter升級會導致API行為更改，從而導致埠組操作失敗。這是最常見的根本原因之一，通過將兩種產品關聯到相容的版本組合來解決該問題。有關詳細資訊，請參閱[ACI虛擬化表](#)。
- vCenter API超時或暫時性錯誤 — 過載或暫時不可用的vCenter將返回錯誤或在FSM超時內沒有響應。此操作不會在所有代碼路徑中自動重試；手動刪除並重新新增EPG到VMM域關聯會觸發新的FSM運行。
- vCenter許可權不足 — vCenter服務帳戶沒有建立或刪除埠組的許可權，導致API呼叫返回授權錯誤。
- 埠組命名衝突 — 手動建立的埠組(名稱與ACI嘗試建立的埠組名稱相同)已存在於DVS上，從而導致操作失敗。在重新嘗試關聯之前，請刪除衝突的埠組或重新命名該埠組。

 附註：因為FSM狀態會一直保留，直到關聯被刪除或新的觸發器到達，所以即使在底層網路或憑證問題解決之後，故障也可能會持續。如果在修復根本原因後仍存在故障，請刪除並重新新增EPG到VMM域的關聯以強制執行新的FSM。

故障F606350:DVS的LACP Lag策略更新失敗

說明

當ACI嘗試通過vCenter API更新DVS上的LACP延遲策略並且操作失敗時，將引發此故障。ACI將LACP配置作為VMM域策略同步的一部分推送到DVS，尤其是當LACP策略與連線到DVS的VMM域關聯時。當無法應用更新時，ACI在受影響的枝葉節點上引發故障F606350。

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

建議的操作

ACI將自動重試此任務。APIC和vCenter之間的瞬時vCenter API延遲或瞬時連線中斷可能導致此故障的單個例項。在許多情況下，重試會成功，故障會自行清除。

如果您觀察到重複或持續故障，請在聯絡思科技術協助中心(TAC)之前採取以下步驟：

1. 驗證APIC是否可以通過網路訪問vCenter伺服器。在Application Policy Infrastructure Controller(APIC)GUI中，導航到VM Networking > VMware > [DVS Domain] > Controllers > [DVS Controller]，並確認運行狀態是online。
2. 確認在VMM域中配置的vCenter憑據有效且未過期。導航到VM Networking > VMware > [DVS Domain] > vCenter Credentials，然後驗證使用者名稱和密碼是否正確。
3. 確認與VMM域關聯的vCenter使用者帳戶具有所需的許可權。至少該帳戶必須具有DVS配置和主機網路管理許可權。有關所需的vCenter許可權的完整清單，請參閱《思科ACI VMware vSphere整合指南》(在Cisco.com上提供)或《[ACI VMM故障排除指南](#)》。
4. 檢視APIC系統故障和事件日誌，瞭解併發VMM連線故障(例如F606225或F606327)，這些故障表明存在更廣泛的vCenter API通訊問題。如果存在此類故障，請先解決連線問題。
 1. 您可以使用以下命令確認apic Leader，並在必要時通過nslookup、ping和HTTPS測試連線。

```
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. 檢查連線到VMM域介面策略組的LACP策略。導航到Fabric > Access Policies > Interface >


Port Channel，確認LACP策略模式與vCenter中的DVS上行鏈路埠組配置相容，請參閱《[ACI VMM故障排除指南](#)》的「分組和ACI vSwitch策略」部分以檢視相容組合。

6. 如果在驗證以上所有內容後故障仍然存在，請收集APIC技術支援檔案並聯絡思科TAC。
 - 在APIC GUI中導覽至System > Troubleshooting > Tech Support，以便產生和下載技術支援套件。
 - 包括來自故障詳細資訊的故障DN和TAC案例中重複出現故障的時間範圍。

其他詳細資訊

ACI VMM整合使用vCenter API代表交換矩陣對DVS配置進程式設計。當LACP策略與VMM域介面策略組(infraAccPortGrp)關聯時，ACI會將該策略轉換為DVS LACP組配置，並將其推送到vCenter。推送操作失敗的原因可能有幾個：

- vCenter API超時 — 緩慢或超載的vCenter可能無法在APIC的超時視窗內響應。此操作將自動重試。
- 許可權不足 — 在VMM域中配置的vCenter服務帳戶沒有修改DVS上行埠組屬性所需的許可權。
- DVS版本不相容 — vCenter中的DVS版本不支援正在推送的LACP配置。ACI需要DVS 5.1版或更高版本才能支援LACP。
- LACP策略衝突 — DVS上行埠組上的現有手動LACP配置與ACI嘗試應用的策略衝突。

 附註：重試後清除的單個隔離F606350例項並不表示存在持續問題。僅在故障在較短視窗內重複出現或在幾分鐘內未清除時進行調查。

故障F606391:未找到物理介面卡的LLDP/CDP鄰接關係

說明

當ACI在VMM域管理的主機上找不到物理網路介面卡(vmnic)的鏈路層發現協定(LLDP)或思科發現協定(CDP)鄰接資訊時，將引發此故障。ACI使用LLDP或CDP來發現哪個枝葉交換機埠物理連線到主機上的每個vmnic。如果沒有此鄰接資訊，ACI無法正確將VM流量從DVS對映到相應的枝葉埠，這將影響該主機上虛擬機器的策略部署和終端學習。

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


建議的操作

此故障需要在路徑中的三個點手動驗證LLDP或CDP配置：vCenter中的DVS、ESXi主機和物理枝葉交換機。按順序完成以下步驟。

第1步 — 驗證DVS上的LLDP/CDP配置

DVS發現協定設定控制DVS是否通告和偵聽LLDP或CDP幀，這些協定是互斥的，如[ACI VMM故障排除指南中所述](#)。如果禁用此設定或設定為僅通告，則APIC無法從vCenter讀取鄰接資訊。

1. 登入到vSphere客戶端，然後導航到Home > Networking > [DVS Name] > Configure > Settings > Properties。
2. 找到Advanced部分並檢查Discovery Protocol欄位：
 - 型別 — 設定為鏈路層發現協定（建議用於ACI）或思科發現協議，具體取決於您的環境。
 - 操作 — 必須設定為Both或Listen。設定Advertise或Disabled會阻止DVS接收鄰居資訊，這意味著vCenter沒有要向APIC報告的鄰接資料。
3. 如果操作設定為Advertise或Disabled，請將其更改為Both並儲存設定。APIC需要幾分鐘時間重新查詢vCenter以獲取更新的鄰接資料。

 附註：更改DVS發現協定設定不會中斷VM流量。它只影響DVS和連線的交換機之間交換的控制平面發現資訊。

第2步 — 在物理枝葉交換機上驗證LLDP/CDP

連線到主機（或主機所連線的上游接入交換機）的枝葉交換機介面必須啟用LLDP或CDP。在ACI中，LLDP和CDP由應用於相關埠上使用的介面策略組的介面策略控制。

1. 確定連線到主機的枝葉埠。導航到Fabric > Inventory > [Pod] > [Leaf Node] > Interfaces > Physical Interfaces，然後找到承載主機vmnic流量的介面。
2. 導航到Fabric > Access Policies > Interfaces > Leaf Interfaces > Policy Groups，然後開啟應用於該埠的介面策略組。
3. 確認LLDP接口策略已連接到具有接收狀態的策略組：Enabled和Transmit State:已啟用。如果未附加LLDP策略，則使用預設策略，該策略同時啟用兩種狀態。
4. 如果您使用的是CDP，請確認CDP介面策略已連線為Admin State:已啟用。
5. 要確認枝葉在預期介面上接收LLDP鄰居，請通過SSH連線到枝葉並運行以下命令：

```
<#root>
```

```
leaf101#
```

```
show lldp neighbors
```

輸出列出每個介面及其發現的鄰居。主機的vmnic或上游接入交換機必須出現在預期介面的鄰居表中。如果輸出中缺少介面，則枝葉不會在該埠上接收LLDP幀，這表示在上游阻止了

LLDP或在連線的裝置上禁用了LLDP。

6. 如果正在使用CDP，請運行以下命令以驗證CDP鄰居發現：


```
<#root>
leaf101#
show cdp neighbors
```

主機或上游交換機必須出現在預期介面的輸出中。

第3步 — 在連線到主機的物理交換機上驗證LLDP/CDP

如果主機vmnic連線到中間物理接入交換機（不直接連線到ACI枝葉），則必須通過交換機轉發LLDP或CDP幀才能到達枝葉。在中間交換機上驗證以下內容：

- 交換機上全域性啟用了LLDP或CDP。
- 在面向主機和ACI枝葉的介面上啟用LLDP或CDP。
- 交換機未配置為過濾或阻止相關介面上的LLDP/CDP協定資料單元(PDU)（例如，通過服務策略或訪問控制清單）。

 附註：LLDP是一種本地鏈路協定。只有在交換機本身沒有終止LLDP時，標準第2層交換機才能在同一VLAN中的埠之間透明地轉發LLDP PDU。如果中間交換機終止LLDP，它將成為枝葉的LLDP鄰居，而不是主機。在這種情況下，ACI將中間交換機視為鄰居，這意味著它無法識別主機的vmnic。在中間交換機上啟用LLDP直通，或直接將主機連線到ACI枝葉。

第4步 — 更改後驗證APIC鄰接狀態

更改配置後，驗證APIC現在是否可以解析主機的物理上行鏈路拓撲。在APIC GUI中，導航到VM Networking > VMware > [DVS Domain] > [DVS Name] > Hosts > [Host Name] > Physical Interfaces，並確認Discovered欄位顯示每個vmnic的枝葉埠。如果鄰接關係已正確解決，故障將自動清除。

您還可以查詢APIC REST API以檢查特定VMM域的鄰接對象：

```
<#root>
apic#
moquery -c compHv -x 'query-target-filter=eq(compHv.name,"hostname")'
```

該對compHv對象表示VMM域中的虛擬機器監控程式主機。相關compNic對象表示物理介面卡。解析鄰接時，用peerDn對應葉compNic介面的DN填充對象的屬性。

如果在驗證以上所有三個配置點後未清除故障，請收集APIC技術支援檔案並聯絡思科TAC。

其他詳細資訊

ACI VMM整合使用vCenter API檢索vCenter從DVS收集的LLDP和CDP鄰居資料。APIC讀取此資料，以構建哪個主機vmnic連線到哪個枝葉埠的對映。此對映用於：

- 為離開給定主機之VM流量程式設計正確的枝葉介面策略。當將「解決方案立即性」配置為立即或按需時，如果主機和枝葉丟失LLDP/CDP鄰居關係，則刪除策略。
- 基於虛擬端點的物理連線點實施虛擬端點的微分段和EPG成員資格。
- 支援ACI虛擬邊緣(AVE)策略實施，這要求準確瞭解主機的物理上行鏈路拓撲。

當缺少鄰接資訊時，ACI會引發故障F606391，表明它無法驗證受影響主機的物理拓撲。虛擬機器連線仍可能在過渡期間正常工作（故障不會立即中斷資料轉發），但策略部署準確性和端點學習可靠性會降低。

未來預防

要在解決故障F606391後防止其重複發生，請執行以下操作：

- 將DVS發現協定操作設定為Both，作為與ACI VMM域關聯的所有DVS例項的標準生成要求。
- 包括LLDP和CDP啟用，作為應用於連線到運行VMware ESXi的主機的所有枝葉埠的標準介面策略組模板的一部分。
- 如果在主機和ACI枝葉之間使用中間訪問交換機，請在部署之前確認交換機供應商的LLDP轉發行為與ACI VMM發現機制相容。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。