地址ACI故障代码：F606347、F606350F606391

目录

简介

本文档介绍修复以下思科以应用为中心的基础设施(ACI)VMware Virtual Machine Manager(VMM)集成故障的后续步骤：故障F606347（VM控制器上的端口组添加或删除失败）、故障F606350（分布式虚拟交换机上的LACP Lag策略更新失败）和故障F606391（在主机上找不到物理适配器的链路层发现协议/思科发现协议邻接信息）。

背景信息

在使用ACI VMM域与VMware vCenter和分布式虚拟交换机(DVS)集成的交换矩阵中会出现这些故障

。ACI通过vCenter API持续将策略(包括端口组生命周期、链路汇聚控制协议(LACP)延迟策略和物理上行链路拓扑)与DVS同步。当同步失败或缺少先决条件发现信息时，ACI会引发这些故障，以显现条件供操作员检查。

故障F606347:VM控制器上的端口组添加或删除失败

描述

当ACI无法作为EPG到VMM域策略同步的一部分在VM控制器（例如VMware vCenter）上添加或删除端口组时，会引发此故障。当EPG与VMM域关联或从VMM域取消关联时，APIC会指示VM控制器在分布式虚拟交换机(DVS)上创建或删除相应的端口组。 如果管理此操作的有限状态机(FSM)未成功完成，ACI将在受影响的VMM域控制器对象上引发故障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"
```

建议操作

此故障通常由ACI版本和VM控制器版本之间的通信或兼容性问题引起。联系思科技术支持中心(TAC)之前，请完成以下步骤。

第1步 — 检验APIC到vCenter的连接

端口组操作通过vCenter API执行。如果APIC无法到达VM控制器，FSM将超时并引发故障。

1. 在APIC GUI中，导航到VM Networking > VMware > [DVS Domain] > Controllers > [vCenter Controller]，并确认运行状态为在线。
2. 确定作为域的VMM领导者的APIC，并验证基本网络可达性。从该APIC ping并尝试与vCenter建立HTTPS连接：
   <#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响应确认APIC可以向vCenter进行身份验证。连接失败或身份验证错误表示在端口组操作成功之前必须解决网络或凭证问题。

第2步 — 验证vCenter凭证和权限

在VMM域中配置的vCenter帐户必须有效，并且必须具有在DVS上创建和删除端口组的足够权限。

1. 在APIC GUI中，导航到VM Networking > VMware > [DVS Domain] > vCenter Credentials，并确认用户名和密码为最新密码。
2. 确认vCenter用户帐户在DVS上至少具有以下权限：
   - DVS:创建、删除和修改端口组。
   - 网络:将网络策略分配给端口组。

   有关所需vCenter权限的完整列表，请参阅ACI VMM故障排除指南。

第3步 — 验证ACI和vCenter版本兼容性

ACI软件版本和VM控制器版本之间的不兼容可能导致端口组API调用以静默方式失败，或返回APIC FSM无法从中恢复的意外错误。

1. 确认当前在交换矩阵中运行的ACI版本已列出为受支持的vCenter版本。请参阅Cisco.com上的ACI兼容性表。
2. 如果最近的ACI或vCenter升级发生此故障之前，请参阅升级版本的ACI版本说明，以确定已知的VMM集成问题或所需的最低vCenter版本。
3. 如果vCenter版本不兼容，请将vCenter（或ACI）升级到支持的组合。有关版本特定的已知问题，请参阅ACI VMM故障排除指南。

第4步 — 检查VMM控制器运行状态和事件日志

1. 在APIC GUI中，导航到VM Networking > VMware > [DVS Domain] > Controllers > [vCenter Controller]，然后打开Operational选项卡。查看Events和Faults子选项卡以了解并发VMM连接故障(例如，F606225或F606327)。 如果存在更广泛的连接故障，请先解决它们。
2. 您还可以通过APIC REST API直接查询故障，以便从FSM查看完整的故障说明和特定的错误文本：
   <#root>

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

   输出中的description字段包含FSM错误详细信息，包括VM控制器名称、VM域、VM提供程序以及触发操作的EPG。使用此信息将调查范围缩小到所涉及的特定EPG和VMM域。

第5步 — 查看受影响的EPG和VMM域关联

1. 确定故障说明(uni/tn-<TENANT>/ap-<APP-PROFILE>/epg-<EPG>)中指定的EPG。
2. 在APIC GUI中，导航到租户> [租户] >应用配置文件> [应用配置文件] >应用EPG > [EPG] >域，并确认VMM域关联存在且处于正确的状态。
3. 如果端口组操作由意外配置更改触发，请验证EPG到VMM域关联是否应该存在。删除并重新添加关联可以重置FSM，并在基本基础设施问题得到解决后清除故障。

第6步 — 收集诊断信息并在故障持续时联系TAC

如果完成上述步骤后故障仍未清除，请收集以下信息并向Cisco TAC提交案例：

- APIC技术支持捆绑包：在APIC GUI中导航到System > Troubleshooting > Tech Support以生成和下载捆绑包。
- 第4步中`moquery`输出的完整故障DN和说明文本。
- ACI软件版本(从System > Controllers > [APIC] > Summary)和vCenter版本。
- 首次发生的时间表以及升级或配置更改后是否出现故障。

其他详细信息

当EPG与VMM域关联时，ACI会通过vCenter API对DVS上的相应端口组进行编程。有限状态机(FSM)任务`CompEpPDAddorDelExtPol`管理此生命周期操作。FSM尝试添加或删除端口组，并转换到一组状态。如果任何状态转换失败（例如，由于vCenter返回的API错误、超时或身份验证失败），则FSM标记为FAILED，并且在受影响的VM控制器的`vmmCtrlr`对象上引发故障F606347。

常见的故障场景包括：

- ACI到vCenter版本不兼容— ACI或vCenter升级会导致API行为更改，从而导致端口组操作失败。这是最常见的根本原因之一，通过将两种产品与兼容的版本组合对齐即可解决。有关详细信息，请参阅ACI虚拟化表。
- vCenter API超时或暂时性错误 — 过载或暂时不可用的vCenter返回错误或在FSM超时内没有响应。不会在所有代码路径中自动重试该操作；手动删除并重新添加EPG到VMM域关联会触发新的FSM运行。
- vCenter权限不足 — vCenter服务帐户没有创建或删除端口组的权限，导致API调用返回授权错误。
- 端口组命名冲突 — 手动创建的端口组，其名称与ACI尝试创建的端口组名称相同，已存在于DVS上，导致操作失败。在重新尝试关联之前，请删除冲突端口组或对其重命名。

注意：由于FSM状态会一直保留，直到关联被删除或新的触发器到达，因此即使在底层网络或凭证问题解决之后，故障也可能会持续。如果在修复根本原因后故障仍然存在，请删除并重新添加EPG到VMM域的关联以强制执行新的FSM。

故障F606350:DVS的LACP Lag策略更新失败

描述

当ACI尝试通过vCenter API在DVS上更新LACP延迟策略且操作失败时，会引发此故障。ACI将LACP配置作为VMM域策略同步的一部分推送到DVS，尤其是当LACP策略与连接到DVS的VMM域相关联时。当无法应用更新时，ACI在受影响的枝叶节点上引发故障F606350。

```
"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
```

建议操作

ACI将自动重试此任务。APIC和vCenter之间的瞬时vCenter API延迟或瞬时连接中断可能导致此故障的单个实例。在许多情况下，重试成功，故障自行清除。

如果您观察到反复或持续的故障，请在联系思科技术支持中心(TAC)之前采取以下步骤：

1. 验证APIC可以通过网络到达vCenter服务器。在应用策略基础设施控制器(APIC)GUI中导航到VM Networking > VMware > [DVS Domain] > Controllers > [DVS Controller]，并确认运行状态为online。
2. 确认VMM域中配置的vCenter凭证有效且未过期。导航到VM Networking > VMware > [DVS Domain] > vCenter Credentials，验证用户名和密码是否正确。
3. 确认与VMM域关联的vCenter用户帐户具有所需的权限。至少该帐户必须具有DVS配置和主机网络管理权限。有关所需vCenter权限的完整列表，请参阅《思科ACI VMware vSphere集成指南》(在Cisco.com上提供)或《ACI VMM故障排除指南》。
4. 查看APIC系统故障和事件日志以了解并发VMM连接故障(例如，F606225或F606327)，这些故障表明存在更广泛的vCenter API通信问题。如果存在此类故障，请先解决连接问题。
    1. 您可以使用以下命令确认apic Leader，并在必要时通过nslookup、ping和HTTPS测试连接。

```
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. 检查连接到VMM域接口策略组的LACP策略。导航到交换矩阵>访问策略>策略>接口>端口通

道，确认LACP策略模式与vCenter中的DVS上行链路端口组配置兼容，请参阅ACI VMM故障排除指南的“分组和ACI vSwitch策略”部分以查看兼容组合。

6. 如果在验证上述所有内容后故障仍然存在，请收集APIC技术支持文件并联系思科TAC。
    - 在APIC GUI中导航到System > Troubleshooting > Tech Support，以生成和下载技术支持捆绑包。
    - 包括故障详细信息中的故障DN和TAC案例中重复出现故障的时间段。

其他详细信息

ACI VMM集成使用vCenter API代表交换矩阵对DVS配置进行编程。当LACP策略与VMM域接口策略组(**infraAccPortGrp**)关联时，ACI会将该策略转换为DVS LACP组配置并将其推送到vCenter。推送操作可能会由于以下原因失败：

- vCenter API超时 — 缓慢或过载的vCenter可能无法在APIC的超时窗口内响应。操作将自动重试。
- 权限不足 — 在VMM域中配置的vCenter服务帐户没有修改DVS上行链路端口组属性所需的权限。
- DVS版本不兼容性 — vCenter中的DVS版本不支持推送的LACP配置。ACI需要DVS 5.1版或更高版本才能支持LACP。
- LACP策略冲突 — DVS上行链路端口组上的现有手动LACP配置与ACI尝试应用的策略冲突。

注意：重试后清除的单606350F1隔离实例并不表示存在持续问题。只有当故障在短时间内重复出现或几分钟内未清除时，才进行调查。

故障F606391:找不到物理适配器的LLDP/CDP邻接关系

描述

当ACI在VMM域管理的主机上找不到物理网络适配器(vmnic)的链路层发现协议(LLDP)或思科发现协议(CDP)邻接信息时，会引发此故障。ACI使用LLDP或CDP来发现哪个枝叶交换机端口物理连接到主机上的每个vmnic。如果没有此邻接信息，ACI无法将VM流量从DVS正确映射到对应的枝叶端口，这会影响该主机上虚拟机的策略部署和终端学习。

```
"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
```

建议操作

此故障需要在路径中的三个点手动验证LLDP或CDP配置：vCenter中的DVS、ESXi主机和物理枝叶交换机。请按顺序完成以下步骤。

第1步 — 在DVS上验证LLDP/CDP配置

DVS发现协议设置控制DVS是否通告和侦听LLDP或CDP帧，这些协议是互斥的，如ACI VMM故障排除指南中所述。如果禁用或设置为仅通告，则APIC无法从vCenter读取邻接信息。

1. 登录到vSphere客户端，然后导航到Home > Networking > [DVS Name] > Configure > Settings > Properties。
2. 找到Advanced部分并选中Discovery Protocol字段：
   - 类型 — 设置为链路层发现协议（建议用于ACI）或思科发现协议，具体取决于您的环境。
   - 操作 — 必须设置为Both或Listen。设置Advertise或Disabled会阻止DVS接收邻居信息，这意味着vCenter没有要向APIC报告的邻接数据。
3. 如果操作设置为Advertise或Disabled，请将其更改为Both并保存设置。几分钟后，APIC将重新查询vCenter以获取更新的邻接数据。

注意：更改DVS发现协议设置不会中断VM流量。它只影响DVS和连接的交换机之间交换的控制平面发现信息。

第2步 — 在物理枝叶交换机上验证LLDP/CDP

连接到主机（或主机所连接的上游接入交换机）的枝叶交换机接口必须启用LLDP或CDP。在ACI中，LLDP和CDP由应用于相关端口上使用的接口策略组的接口策略控制。

1. 确定连接到主机的枝叶端口。导航到Fabric > Inventory > [Pod] > [Leaf Node] > Interfaces > Physical Interfaces，然后找到传输主机vmnic流量的接口。
2. 导航到Fabric > Access Policies > Interfaces > Leaf Interfaces > Policy Groups，然后打开应用于该端口的接口策略组。
3. 确认LLDP接口策略已附加到具有接收状态的策略组：Enabled和Transmit State:启用.如果未附加LLDP策略，则使用默认策略，该策略同时启用两种状态。
4. 如果您正在使用CDP，请确认CDP接口策略连接了Admin State:启用.
5. 要确认枝叶在预期接口上接收LLDP邻居，请通过SSH连接到枝叶并运行以下命令：
   <#root>

   ```
   leaf101#

   show lldp neighbors
   ```

   输出列出了每个接口及其发现的邻居。主机的vmnic或上游接入交换机必须出现在预期接口的邻居表中。如果输出中缺少接口，则枝叶不会在该端口上接收LLDP帧，这表明LLDP在上游被

阻止或在连接的设备上被禁用。

6. 如果正在使用CDP，请运行以下命令以验证CDP邻居发现：
   <#root>

   ```
   leaf101#

   show cdp neighbors
   ```

   主机或上游交换机必须出现在预期接口的输出中。

第3步 — 在连接到主机的物理交换机上验证LLDP/CDP

如果主机vmnic连接到中间物理接入交换机（不直接连接到ACI枝叶），则必须通过交换机转发LLDP或CDP帧才能到达枝叶。在中间交换机上验证以下内容：

- 交换机上全局启用了LLDP或CDP。
- 在面向主机和ACI枝叶的接口上启用LLDP或CDP。
- 交换机未配置为过滤或阻止相关接口上的LLDP/CDP协议数据单元(PDU)（例如，通过服务策略或访问控制列表）。

注意：LLDP是一种本地链路协议。仅当交换机本身没有终止LLDP时，标准第2层交换机才能在同一VLAN中的端口之间透明地转发LLDP PDU。如果中间交换机终止LLDP，它将成为枝叶的LLDP邻居，而不是主机。在这种情况下，ACI将中间交换机视为邻居，这意味着它无法识别主机的vmnic。在中间交换机上启用LLDP直通，或直接将主机连接到ACI枝叶。

第4步 — 在更改后验证APIC邻接状态

更改配置后，验证APIC现在能够解析主机的物理上行链路拓扑。在APIC GUI中，导航到VM Networking > VMware > [DVS Domain] > [DVS Name] > Hosts > [Host Name] > Physical Interfaces，并确认Discovered字段显示每个vmnic的枝叶端口。如果邻接关系已正确解决，故障将自动清除。

您还可以查询APIC REST API以检查特定VMM域的邻接对象：

<#root>

```
apic#

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

该对**compHv**象表示VMM域内的虚拟机监控程序主机。相关**compNic**对象代表物理适配器。解析邻接关系时，**peerDn**对象的**compNic**属性会填充相应枝叶接口的DN。

如果在验证以上所有三个配置点后未清除故障，请收集APIC技术支持文件并联系思科TAC。

其他详细信息

ACI VMM集成使用vCenter API检索vCenter从DVS收集的LLDP和CDP邻居数据。APIC读取此数据，以构建主机vmnic连接到哪个枝叶端口的映射。此映射用于：

- 为离开给定主机的VM流量编程正确的枝叶接口策略。当将Resolution Immediacy配置为立即或按需时，如果主机和枝叶丢失LLDP/CDP邻居关系，则删除策略。
- 根据虚拟端点的物理连接点，对虚拟端点实施微分段和EPG成员资格。
- 支持ACI虚拟边缘(AVE)策略实施，需要准确了解主机的物理上行链路拓扑。

当缺少邻接信息时，ACI会引发故障F606391，表明它无法验证受影响主机的物理拓扑。虚拟机连接可能仍然可以在过渡期间正常工作（故障不会立即中断数据转发），但策略部署准确性和终端学习可靠性会降低。

未来防御

要防止故障F606391在解决后重新出现，请执行以下操作：

- 将DVS发现协议操作设置为Both，作为与ACI VMM域关联的所有DVS实例的标准生成要求。
- 将LLDP和CDP启用作为标准接口策略组模板的一部分，应用于连接到运行VMware ESXi的主机的所有枝叶端口。
- 如果在主机和ACI枝叶之间使用中间接入交换机，请在部署之前确认交换机供应商的LLDP转发行为与ACI VMM发现机制兼容。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。