주소 ACI 결함 코드: F606347, F606350 F606391

목차

소개

배경 정보

결함 F606347: VM 컨트롤러에서 포트 그룹 추가 또는 삭제 실패

- 설명
- 권장 조치
  - 1단계 — APIC-vCenter 연결 확인
  - 2단계 — vCenter 자격 증명 및 권한 확인
  - 3단계 — ACI 및 vCenter 버전 호환성 확인
  - 4단계 — VMM 컨트롤러 작동 상태 및 이벤트 로그 확인
  - 5단계 — 영향을 받는 EPG 및 VMM 도메인 연결 검토
  - 6단계 — 진단 정보를 수집하고 결함이 지속되면 TAC에 문의하십시오.
- 추가 세부 정보

결함 F606350: DVS에서 LACP 지연 정책 업데이트 실패

- 설명
- 권장 조치
- 추가 세부 정보

결함 F606391: 물리적 어댑터에 대한 LLDP/CDP 인접성을 찾을 수 없음

- 설명
- 권장 조치
  - 1단계 — DVS에서 LLDP/CDP 구성 검증
  - 2단계 — 물리적 리프 스위치에서 LLDP/CDP 검증
  - 3단계 — 호스트에 연결된 물리적 스위치에서 LLDP/CDP 검증
  - 4단계 — 변경 후 APIC 인접성 상태 확인
- 추가 세부 정보
- 향후 차단

소개

이 문서에서는 다음 Cisco ACI(Application Centric Infrastructure) VMware VMM(Virtual Machine Manager) 통합 결함을 해결하기 위한 다음 단계에 대해 설명합니다. fault F606347(VM 컨트롤러에서 포트 그룹 추가 또는 삭제 실패), fault F606350(분산된 가상 스위치에서 LACP 지연 정책 업데이트 실패), fault F606391(호스트의 물리적 어댑터에 대한 Link Layer Discovery Protocol/Cisco Discovery Protocol 인접성 정보를 찾을 수 없음)

배경 정보

이러한 결함은 ACI VMM 도메인을 VMware vCenter 및 DVS(Distributed Virtual Switch)와 통합하는 패브릭에서 발생합니다. ACI는 vCenter API를 통해 포트 그룹 라이프사이클, LACP(Link Aggregation Control Protocol) 지연 정책, 물리적 업링크 토폴로지 등의 정책을 DVS와 지속적으로 동기화합니다. 해당 동기화가 실패하거나 필수 구성 요소 검색 정보가 누락된 경우 ACI는 이러한 오류를 발생시켜 운영자 검토 조건을 표시합니다.

결함 F606347: VM 컨트롤러에서 포트 그룹 추가 또는 삭제 실패

설명

이 결함은 ACI가 EPG-VMM 도메인 정책 동기화의 일부로 VM 컨트롤러(예: VMware vCenter)에 포트 그룹을 추가하거나 삭제하지 못할 때 제기됩니다. EPG가 VMM 도메인과 연결되거나 VMM 도메인에서 분리된 경우, APIC는 VM 컨트롤러에 DVS(Distributed Virtual Switch)에서 해당 포트 그룹을 생성하거나 제거하도록 지시합니다. 이 작업을 관리하는 FSM(Finite State Machine)이 성공적으로 완료되지 않으면 ACI는 영향을 받는 VMM 도메인 컨트롤러 개체에서 결함 F606347을 발생시킵니다.

```
"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"
```

권장 조치

이 결함은 ACI 버전과 VM 컨트롤러 버전 간의 통신 또는 호환성 문제로 인해 발생하는 경우가 가장 많습니다. Cisco TAC(Technical Assistance Center)에 문의하기 전에 다음 단계를 수행하십시오.

1단계 — APIC-vCenter 연결 확인

포트 그룹 작업은 vCenter API를 통해 실행됩니다. APIC에서 VM 컨트롤러에 연결할 수 없는 경우 FSM이 시간 초과되고 결함이 제기됩니다.

1. APIC GUI에서 VM Networking(VM 네트워킹) > VMware > [DVS Domain] > Controllers(컨트롤러) > [vCenter Controller](vCenter 컨트롤러)로 이동하고 운영 상태가 온라인 상태인지 확인합니다.
2. 도메인의 VMM 리더인 APIC를 식별하고 기본 네트워크 연결성을 확인합니다. 해당 APIC에서 vCenter에 대한 HTTPS 연결을 ping하고 시도합니다.
   <#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
```

HTTPS 응답에 성공하면 APIC에서 vCenter에 인증할 수 있음을 확인합니다. 연결 실패 또는 인증 오류는 포트 그룹 작업이 성공하기 전에 네트워크 또는 자격 증명 문제를 해결해야 함을 나타냅니다.

2단계 — vCenter 자격 증명 및 권한 확인

VMM 도메인에 구성된 vCenter 계정은 유효해야 하며 DVS에서 포트 그룹을 만들고 삭제할 수 있는 충분한 권한이 있어야 합니다.

1. APIC GUI에서 VM Networking(VM 네트워킹) > VMware > [DVS Domain] > vCenter Credentials(vCenter 자격 증명)로 이동하고 사용자 이름과 비밀번호가 최신 상태인지 확인합니다.
2. vCenter 사용자 계정에 DVS에 대해 최소한 다음 권한이 있는지 확인합니다.
   - DVS: 포트 그룹을 생성, 삭제 및 수정합니다.
   - 네트워크: 네트워크 정책을 포트 그룹에 할당합니다.

   필요한 vCenter 권한의 전체 목록은 ACI VMM 트러블슈팅 가이드를 참조하십시오.

3단계 — ACI 및 vCenter 버전 호환성 확인

ACI 소프트웨어 버전과 VM 컨트롤러 버전 간의 비호환성으로 인해 포트 그룹 API 호출이 자동으로 실패하거나 APIC FSM에서 복구할 수 없는 예기치 않은 오류가 반환될 수 있습니다.

1. vCenter 버전이 패브릭에서 현재 실행 중인 ACI 릴리스에 대해 지원되는 것으로 나열되는지 확인합니다. Cisco.com에서 ACI Compatibility Matrix를 참조하십시오.
2. ACI 또는 vCenter의 최근 업그레이드가 먼저 이 결함이 발생한 경우, ACI 릴리스 정보에서 업그레이드된 버전을 참조하여 알려진 VMM 통합 문제 또는 필요한 최소 vCenter 버전을 확인하십시오.
3. vCenter 버전이 호환되지 않을 경우 vCenter(또는 ACI)를 지원되는 조합으로 업그레이드합니다. 버전별 알려진 문제는 ACI VMM 트러블슈팅 가이드를 참조하십시오.

4단계 — VMM 컨트롤러 작동 상태 및 이벤트 로그 확인

1. APIC GUI에서 VM Networking(VM 네트워킹) > VMware > [DVS Domain] > Controllers(컨트롤러) > [vCenter Controller](vCenter 컨트롤러)로 이동하고 Operational(운영) 탭을 엽니다. 동시 VMM 연결 결함(예: F606225 또는 F606327)에 대한 Events and Faults 하위 탭을 검토합니다. 더 광범위한 연결 장애가 있는 경우 먼저 해결하십시오.
2. APIC REST API를 통해 직접 결함을 쿼리하여 전체 결함 설명과 FSM의 특정 오류 텍스트를 검토할 수도 있습니다.
   <#root>

   ```
   apic#

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

   출력의 description 필드에는 VM 컨트롤러 이름, VM 도메인, VM 제공자 및 작업을 트리거한 EPG를 비롯한 FSM 오류 세부사항이 포함됩니다. 이 정보를 사용하여 관련된 특정 EPG 및

VMM 도메인으로 조사의 범위를 좁힐 수 있습니다.

5단계 — 영향을 받는 EPG 및 VMM 도메인 연결 검토

1. 결함 설명에 이름이 지정된 EPG를 식별합니다(uni/tn-<TENANT>/ap-<APP-PROFILE>/epg-<EPG>).
2. APIC GUI에서 Tenants(테넌트) > [Tenant(테넌트)] > Application Profiles(애플리케이션 프로파일) > [App Profile] > Application EPGs(애플리케이션 EPG) > [EPG] > Domains(도메인)로 이동하고 VMM 도메인 연결이 있으며 올바른 상태인지 확인합니다.
3. 포트 그룹 작업이 우발적인 컨피그레이션 변경으로 트리거된 경우, EPG와 VMM 도메인 간의 연결이 있어야 하는지 확인하십시오. 연결을 제거하고 다시 추가하면 기본 인프라 문제가 해결된 경우 FSM을 재설정하고 오류를 해결할 수 있습니다.

6단계 — 진단 정보를 수집하고 결함이 지속되면 TAC에 문의하십시오.

위의 단계를 완료해도 결함이 제거되지 않을 경우, 다음 정보를 수집하여 Cisco TAC에 케이스를 여십시오.

- APIC 기술 지원 번들: APIC GUI에서 System(시스템) > Troubleshooting(문제 해결) > Tech Support(기술 지원)로 이동하여 번들을 생성하고 다운로드합니다.
- 4단계의 moquery 출력에서 제공되는 전체 결함 DN 및 설명 텍스트
- ACI 소프트웨어 버전(System > Controllers > [APIC] > Summary) 및 vCenter 버전.
- 첫 번째 발생의 기간 및 업그레이드 또는 컨피그레이션 변경 후 결함이 나타나는지 여부.

추가 세부 정보

EPG가 VMM 도메인과 연결된 경우 ACI는 vCenter API를 통해 DVS에 해당 포트 그룹을 프로그래밍합니다. FSM(Finite State Machine) 작업 CompEpPDAddorDelExtPol은 이 수명 주기 작업을 관리합니다. FSM은 포트 그룹 추가 또는 삭제를 시도하고 상태 집합을 통해 전환합니다. 상태 전환이 실패할 경우(예: vCenter에서 반환한 API 오류, 시간 초과 또는 인증 실패) FSM이 FAILED로 표시되고 F606347 오류가 발생한 VM 컨트롤러의 vmmCtrlr 개체에서 발생합니다.

일반적인 장애 시나리오는 다음과 같습니다.

- ACI-vCenter 버전 비호환성 — ACI 또는 vCenter 업그레이드에 따라 API 동작이 변경되어 포트 그룹 작업이 실패합니다. 이는 가장 일반적인 근본 원인 중 하나이며, 두 제품을 호환 가능한 버전 조합에 맞춰 조정함으로써 해결합니다. 자세한 내용은 ACI 가상화 매트릭스를 참조하십시오.
- vCenter API 시간 초과 또는 일시적인 오류 - 과부하 또는 일시적으로 사용할 수 없는 vCenter가 오류를 반환하거나 FSM 시간 초과 내에 응답하지 않습니다. 모든 코드 경로에서

작업이 자동으로 다시 시도되지는 않습니다. EPG와 VMM 도메인 간의 연결을 제거하고 다시 추가하면 새로운 FSM 실행이 수동으로 트리거됩니다.
- vCenter 권한 부족 - vCenter 서비스 계정에 포트 그룹을 만들거나 삭제할 권한이 없으므로 API 호출에서 권한 부여 오류를 반환합니다.
- 포트 그룹 명명 충돌 — 생성하려는 ACI와 동일한 이름을 사용하여 수동으로 생성한 포트 그룹이 DVS에 이미 있으므로 작업이 실패합니다. 연결을 다시 시도하기 전에 충돌하는 포트 그룹을 제거하거나 이름을 바꾸십시오.

✎ 참고: 연결이 제거되거나 새 트리거가 도착할 때까지 FSM 상태가 유지되므로, 기본 네트워크 또는 자격 증명 문제가 해결된 후에도 결함은 지속될 수 있습니다. 근본 원인을 해결한 후에도 결함이 남아 있으면 EPG-VMM 도메인 연결을 제거한 후 다시 추가하여 새 FSM 실행을 강제로 수행하십시오.

결함 F606350: DVS에서 LACP 지연 정책 업데이트 실패

설명

이 결함은 ACI가 vCenter API를 통해 DVS에서 LACP 지연 정책을 업데이트하려고 시도했지만 작업이 실패했을 때 제기됩니다. ACI는 VMM 도메인 정책 동기화의 일부로 LACP 컨피그레이션을 DVS에 푸시하며, 특히 LACP 정책이 DVS에 연결된 VMM 도메인과 연결된 경우 이러한 기능을 수행합니다. 업데이트를 적용할 수 없는 경우 ACI는 영향을 받는 리프 노드에 대해 결함 F606350을 제기합니다.

```
"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
```

권장 조치

이 작업은 ACI에 의해 자동으로 재시도됩니다. APIC과 vCenter 간의 일시적인 vCenter API 지연 또는 일시적인 연결 중단으로 인해 이 결함의 단일 인스턴스가 발생할 수 있습니다. 대부분의 경우 재시도가 성공하고 결함은 자체적으로 지워집니다.

반복적으로 또는 지속적으로 장애가 발생하는 경우 Cisco TAC(Technical Assistance Center)에 문의하기 전에 다음 단계를 수행하십시오.

1. APIC가 네트워크를 통해 vCenter 서버에 연결할 수 있는지 확인합니다. APIC(Application Policy Infrastructure Controller) GUI에서 VM Networking(VM 네트워킹) > VMware > [DVS

Domain] > Controllers(컨트롤러) > [DVS Controller]로 이동하고 운영 상태가 온라인 상태인지 확인합니다.

2. VMM 도메인에 구성된 vCenter 자격 증명이 유효하며 만료되지 않았는지 확인합니다. VM Networking(VM 네트워킹) > VMware > [DVS Domain] > vCenter Credentials(vCenter 자격 증명)로 이동하고 사용자 이름과 암호가 올바른지 확인합니다.
3. VMM 도메인과 연결된 vCenter 사용자 계정에 필요한 권한이 있는지 확인합니다. 적어도 어카운트에는 DVS 구성 및 호스트 네트워크 관리 권한이 있어야 합니다. 필요한 vCenter 권한의 전체 목록은 Cisco ACI VMware vSphere Integration Guide(Cisco.com)나 ACI VMM Troubleshooting Guide(ACI VMware vSphere 통합 설명서)를 참조하십시오.
4. APIC 시스템 결함 및 이벤트 로그에서 더 광범위한 vCenter API 통신 문제를 나타내는 동시 VMM 연결 결함(예: F606225 또는 F606327)을 검토합니다. 그러한 결함이 있을 경우, 먼저 연결 문제를 해결하십시오.
    1. 다음 명령을 사용하여 필요한 경우 nslookup, ping 및 HTTPS를 통해 apic Leader를 확인하고 그로부터 연결을 테스트할 수 있습니다.

```
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 도메인 인터페이스 정책 그룹에 연결된 LACP 정책을 확인하십시오. Fabric(패브릭) > Access Policies(액세스 정책) > Policies(정책) > Interface(인터페이스) > Port Channel(포트 채널)로 이동하고 LACP 정책 모드가 vCenter의 DVS 업링크 포트 그룹 컨피그레이션과 호환되는지 확인합니다. 호환되는 조합을 보려면 ACI VMM 트러블슈팅 가이드의 "Teaming and ACI vSwitch Policy(티밍 및 ACI vSwitch 정책)" 섹션을 참조하십시오.
6. 위의 모든 사항을 확인한 후에도 결함이 지속될 경우, APIC 기술 지원 파일을 수집하고 Cisco TAC에 문의하십시오.
    - 기술 지원 번들을 생성하고 다운로드하려면 APIC GUI에서 System > Troubleshooting > Tech Support로 이동합니다.
    - 결함 세부사항의 결함 DN과 TAC 사례의 반복 실패 기간을 포함합니다.

추가 세부 정보

ACI VMM 통합에서는 vCenter API를 사용하여 패브릭을 대신하여 DVS 컨피그레이션을 프로그래밍합니다. LACP 정책이 VMM Domain Interface Policy Group(VMM Domain Interface Policy Group)**infraAccPortGrp**과 연결된 경우 ACI는 정책을 DVS LACP 그룹 컨피그레이션으로 변환하고

vCenter로 푸시합니다. 푸시 작업은 다음과 같은 몇 가지 이유로 실패할 수 있습니다.

- vCenter API 시간 초과 — 느리거나 과부하된 vCenter가 APIC의 시간 초과 기간 내에 응답하지 않을 수 있습니다. 작업이 자동으로 재시도됩니다.
- 권한 부족 — VMM 도메인에 구성된 vCenter 서비스 계정에 DVS 업링크 포트 그룹 속성을 수정하는 데 필요한 권한이 없습니다.
- DVS 버전 비호환성 — vCenter의 DVS 버전은 푸시되는 LACP 컨피그레이션을 지원하지 않습니다. ACI에서는 LACP 지원을 위해 DVS 버전 5.1 이상이 필요합니다.
- LACP 정책 충돌 - DVS 업링크 포트 그룹의 기존 수동 LACP 컨피그레이션이 ACI에서 적용하려는 정책과 충돌합니다.

✎ 참고: 재시도 후 지워지는 F606350의 단일 격리 인스턴스는 지속적인 문제를 나타내지 않습니다. 짧은 시간 내에 결함이 반복적으로 재발하거나 몇 분 내에 해결되지 않는 경우에만 조사합니다.

결함 F606391: 물리적 어댑터에 대한 LLDP/CDP 인접성을 찾을 수 없음

설명

이 결함은 ACI가 VMM 도메인에서 관리되는 호스트의 물리적 네트워크 어댑터(vmnic)에 대한 LLDP(Link Layer Discovery Protocol) 또는 CDP(Cisco Discovery Protocol) 인접성 정보를 찾을 수 없을 때 발생합니다. ACI는 LLDP 또는 CDP를 사용하여 어떤 leaf 스위치 포트가 호스트의 각 vmnic에 물리적으로 연결되어 있는지 확인합니다. 이 인접성 정보가 없으면 ACI는 DVS의 VM 트래픽을 해당 리프 포트에 올바르게 매핑할 수 없습니다. 이는 해당 호스트의 가상 머신에 대한 정책 구축 및 엔드포인트 학습에 영향을 줍니다.

```
"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
```

권장 조치

이 결함은 경로의 세 지점에서 LLDP 또는 CDP 구성을 수동으로 검증해야 합니다. vCenter의 DVS, ESXi 호스트 및 물리적 리프 스위치 다음 단계를 순서대로 진행합니다.

1단계 — DVS에서 LLDP/CDP 구성 검증

DVS Discovery Protocol 설정은 DVS가 LLDP 또는 CDP 프레임을 광고하고 수신 대기할지 여부를 제어합니다. 이러한 프로토콜은 ACI VMM 문제 해결 가이드에 설명된 대로 상호 배타적입니다. 이 설정을 사용하지 않거나 Advertise Only로 설정하면 APIC에서 vCenter에서 인접성 정보를 읽을 수 없습니다.

1. vSphere Client에 로그인하고 Home(홈) > Networking(네트워킹) > [DVS Name] > Configure(구성) > Settings(설정) > Properties(속성)로 이동합니다.
2. Advanced(고급) 섹션을 찾아 Discovery Protocol(검색 프로토콜) 필드를 확인합니다.
   - 유형 — 환경에 따라 Link Layer Discovery Protocol(ACI에 권장) 또는 Cisco Discovery Protocol로 설정합니다.
   - 작업 — Both 또는 Listen으로 설정해야 합니다. Advertise 또는 Disabled를 설정하면 DVS에서 네이버 정보를 수신하지 못합니다. 즉, vCenter에 APIC에 보고할 인접성 데이터가 없습니다.
3. 작업이 Advertise 또는 Disabled로 설정된 경우 Both로 변경하고 설정을 저장합니다. APIC에서 vCenter에 업데이트된 인접성 데이터를 다시 쿼리할 수 있도록 몇 분 정도 기다립니다.

참고: DVS Discovery Protocol 설정을 변경하는 것은 VM 트래픽에 영향을 주지 않습니다. DVS와 연결된 스위치 간에 교환되는 컨트롤 플레인 검색 정보에만 영향을 미칩니다.

2단계 — 물리적 리프 스위치에서 LLDP/CDP 검증

호스트(또는 호스트가 연결하는 업스트림 액세스 스위치)에 연결된 리프 스위치 인터페이스에는 LLDP 또는 CDP가 활성화되어 있어야 합니다. ACI에서 LLDP 및 CDP는 관련 포트에서 사용되는 인터페이스 정책 그룹에 적용된 인터페이스 정책에 의해 제어됩니다.

1. 호스트에 연결된 leaf 포트를 식별합니다. Fabric(패브릭) > Inventory(인벤토리) > [Pod] > [Leaf Node] > Interfaces(인터페이스) > Physical Interfaces(물리적 인터페이스)로 이동하고 호스트의 vmnic 트래픽을 전달하는 인터페이스를 찾습니다.
2. Fabric(패브릭) > Access Policies(액세스 정책) > Interfaces(인터페이스) > Leaf Interfaces(리프 인터페이스) > Policy Groups(정책 그룹)로 이동하고 해당 포트에 적용된 인터페이스 정책 그룹을 엽니다.
3. LLDP 인터페이스 정책이 수신 상태의 정책 그룹에 연결되었는지 확인합니다. 사용 및 전송 상태: 활성화됨. 연결된 LLDP 정책이 없는 경우 기본 정책이 사용됩니다. 이 정책에는 두 가지 상태가 모두 활성화되어 있습니다.
4. CDP를 사용 중인 경우 CDP 인터페이스 정책이 Admin State(관리 상태)로 연결되어 있는지 확인합니다. 활성화됨.
5. Leaf가 예상 인터페이스에서 LLDP 네이버를 수신하는지 확인하려면 SSH를 leaf에 연결하고 다음 명령을 실행합니다.
   <#root>

   ```
   leaf101#

   show lldp neighbors
   ```

출력에는 각 인터페이스 및 검색된 인접 디바이스가 나열됩니다. 호스트의 vmnic 또는 업스트림 액세스 스위치는 예상 인터페이스의 네이버 테이블에 나타나야 합니다. 인터페이스가 출력에서 누락된 경우 leaf는 해당 포트에서 LLDP 프레임을 수신하지 않습니다. 이는 LLDP가 연결된 디바이스에서 업스트림으로 차단되거나 비활성화되었음을 나타냅니다.

6. CDP가 사용 중인 경우 다음 명령을 실행하여 CDP 네이버 검색을 확인합니다.
   <#root>

   ```
   leaf101#

   show cdp neighbors
   ```

   호스트 또는 업스트림 스위치가 예상 인터페이스의 출력에 표시되어야 합니다.

3단계 — 호스트에 연결된 물리적 스위치에서 LLDP/CDP 검증

호스트 vmnic가 중간 물리적 액세스 스위치(ACI leaf에 직접 연결되지 않음)에 연결되는 경우 leaf에 도달하려면 LLDP 또는 CDP 프레임이 해당 스위치를 통해 전달되어야 합니다. 중간 스위치에서 다음을 확인합니다.

- LLDP 또는 CDP는 스위치에서 전역적으로 활성화됩니다.
- LLDP 또는 CDP는 호스트 및 ACI leaf를 모두 접하는 인터페이스에서 활성화됩니다.
- 스위치는 관련 인터페이스(예: 서비스 정책 또는 액세스 제어 목록을 통해)에서 LLDP/CDP PDU(Protocol Data Unit)를 필터링하거나 차단하도록 구성되어 있지 않습니다.

참고: LLDP는 링크-로컬 프로토콜입니다. 표준 레이어 2 스위치는 스위치 자체에서 LLDP가 종료되지 않은 경우에만 동일한 VLAN의 포트 간에 LLDP PDU를 투명하게 전달합니다. 중간 스위치가 LLDP를 종료하면 호스트가 아니라 leaf에 대한 LLDP 인접 디바이스가 됩니다. 이 경우 ACI는 중간 스위치를 네이버로 인식하므로 호스트의 vmnic를 식별할 수 없습니다. 중간 스위치에서 LLDP pass-through를 활성화하거나 호스트를 ACI leaf에 직접 연결합니다.

4단계 — 변경 후 APIC 인접성 상태 확인

컨피그레이션을 변경한 후 APIC에서 호스트의 물리적 업링크 토폴로지를 확인할 수 있는지 확인합니다. APIC GUI에서 VM Networking(VM 네트워킹) > VMware > [DVS Domain] > [DVS Name] > Hosts(호스트) > [Host Name] > Physical Interfaces(물리적 인터페이스)로 이동하고 Discovered(검색된) 필드에 각 vmnic에 대한 leaf 포트가 표시되는지 확인합니다. 인접성이 올바르게 해결되면 결함은 자동으로 지워집니다.

특정 VMM 도메인에 대한 인접성 개체를 확인하기 위해 APIC REST API를 쿼리할 수도 있습니다.

<#root>

```
apic#

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

개체**compHv**는 VMM 도메인 내의 하이퍼바이저 호스트를 나타냅니다. 관련 **compNic** 객체는 물리적 어댑터를 나타냅니다. 인접성이 확인되면 객체**peerDn**의 속성이 **compNic** 해당 leaf 인터페이스의 DN으로 채워집니다.

위의 3가지 컨피그레이션 포인트를 모두 검증한 후에도 결함이 제거되지 않을 경우, APIC 기술 지원 파일을 수집하고 Cisco TAC에 문의하십시오.

추가 세부 정보

ACI VMM 통합에서는 vCenter API를 사용하여 vCenter가 DVS에서 수집하는 LLDP 및 CDP 네이버 데이터를 검색합니다. APIC는 호스트 vmnic가 어떤 리프 포트에 연결하는지에 대한 맵을 구축하기 위해 이 데이터를 읽습니다. 이 매핑을 사용하여 다음을 수행할 수 있습니다.

- 지정된 호스트를 떠나는 VM 트래픽에 대해 올바른 리프 인터페이스 정책을 프로그래밍합니다. Resolution Immediacy가 즉시 또는 온디맨드로 구성된 경우 호스트 및 leaf에서 LLDP/CDP 인접 관계가 손실되면 정책이 제거됩니다.
- 물리적 연결 지점을 기반으로 가상 엔드포인트에 대한 마이크로세그멘테이션 및 EPG 멤버십 적용
- ACI AVE(Virtual Edge) 정책 적용을 지원하므로 호스트의 물리적 업링크 토폴로지에 대한 정확한 지식이 필요합니다.

인접성 정보가 누락되면 ACI에서 결함 F606391을 발생시켜 영향을 받는 호스트에 대한 물리적 토폴로지를 검증할 수 없음을 알립니다. 가상 머신 연결이 중간에 계속 작동할 수 있습니다. 이 결함으로 인해 데이터 전달이 즉시 중단되지는 않지만 정책 구축 정확도와 엔드포인트 학습 신뢰도가 저하됩니다.

향후 차단

결함 F606391이 해결된 후 재발하지 않도록 하려면

- ACI VMM 도메인과 연결된 모든 DVS 인스턴스에 대한 표준 빌드 요구 사항으로 DVS 검색 프로토콜 작업을 Both로 설정합니다.
- LLDP 및 CDP 지원을 VMware ESXi를 실행하는 호스트에 연결하는 모든 리프 포트에 적용되는 표준 인터페이스 정책 그룹 템플릿의 일부로 포함합니다.
- 호스트와 ACI 리프 간에 중간 액세스 스위치를 사용하는 경우, 구축 전에 스위치 공급업체의 LLDP 포워딩 동작이 ACI VMM 검색 메커니즘과 호환되는지 확인하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.