Probleemoplossing voor ACI VMM-integratie

Inhoud

Inleiding

Dit document beschrijft stappen om ACI Virtual Machine Manager Integration (VMM) te begrijpen en problemen op te lossen.

Achtergrondinformatie

Het materiaal van dit document is afgeleid uit het boek Cisco Application Centric Infrastructure, Second Edition, met name de VMM Integration - Overview, VMM Integration - vCenter Connectivity, VMM Integration - Host Dynamic Discovery en VMM Integration - Hypervisor Uplink Taakverdeling hoofdstukken.

Overzicht van Virtual Machine Manager

ACI-controllers kunnen integreren met virtuele-machinemanagers (VMM's) van derden.

Dit is een van de belangrijkste functies van ACI omdat het de bewerkingen voor end-to-end netwerkconfiguratie van de stof en de werkbelastingen die er verbinding mee maken, vereenvoudigt en automatiseert. ACI biedt één enkel beleidsmodel voor overlay dat over meerdere werklasttypen kan worden uitgebreid, d.w.z. virtuele machines, bare metal servers en containers.

In dit hoofdstuk wordt specifiek aandacht besteed aan een aantal typische probleemoplossingsscenario's met betrekking tot de VMware vCenter VMM-integratie.

De lezer zal er doorheen lopen:

- Onderzoek naar vCenter-communicatiestoringen.
- Dynamische detectie van host en VM en storingsscenario's.
- Hypervisor-algoritmen voor taakverdeling.

vCenter-connectiviteit

Op rollen gebaseerde toegangscontrole (RBAC)

De mechanismen waarmee APIC kan communiceren met de vCenter-controller zijn afhankelijk van de gebruikersaccount die aan een bepaald VMM-domein is gekoppeld. Er worden specifieke vereisten geschetst voor de vCenter-gebruiker die bij het VMM-domein is aangesloten om ervoor te zorgen dat de APIC met succes bewerkingen op het vCenter kan uitvoeren, of het nu gaat om het doorsturen en ophalen van inventarislijsten en configuraties of het controleren en luisteren naar gebeurtenissen die verband houden met beheerde inventarissen.

De gemakkelijkste manier om zorg over dergelijke vereisten te verwijderen is het gebruik van de administrateur vCenter-account die volledige toegang heeft; dit soort vrijheid is echter niet altijd beschikbaar voor de ACI-beheerder.

De minimumrechten voor een aangepaste gebruikersaccount, vanaf ACI versie 4.2, zijn als volgt:

- Alarmen
    - APIC maakt twee alarmen op de map aan. Een voor DVS en een ander voor poortgroep. Er wordt een alarm afgegeven wanneer het EPG- of VMM-domeinbeleid

op de APIC wordt verwijderd, maar vCenter kan de corresponderende poortgroep of DVS niet verwijderen omdat er VM's op zijn aangesloten.

- Gedistribueerde Switch
- DVpoortgroep
- Map
- Netwerk
  - APIC beheert de netwerkinstellingen zoals poortgroepen toevoegen of verwijderen, host/DVS MTU, LLDP/CDP, LACP instellen, etc.
- Host
  - Als u AVS naast bovenstaande gebruikt, heeft de gebruiker de hostrechten nodig op het datacenter waar APIC DVS zal maken.
  - Host.Configuration.Geavanceerde instellingen
  - Host.Local Operations.Reconfigureren virtuele machine
  - Host.Configuration.Netwerkconfiguratie
  - Dit is nodig voor AVS en de automatische plaatsingsfunctie voor virtuele Layer 4 tot Layer 7 Service-VM's. Voor AVS maakt APIC VMK-interface en plaatst het in VTEP-poortgroep die wordt gebruikt voor OpFlex.
- Virtuele machine
  - Als er servicegrafieken worden gebruikt, is ook de virtuele machineprioriteit voor de virtuele apparaten vereist.
  - Virtual machine.Configuration.Wijzig apparaatinstellingen
  - Virtuele machine.Configuration.Settings

Problemen met RBC oplossen

RBAC-problemen worden het meest aangetroffen tijdens de eerste configuratie van een VMM-domein, maar kunnen worden ondervonden als een vCenter-beheerder de rechten van de gebruikersaccount die aan het VMM-domein is gekoppeld, zou moeten wijzigen nadat de eerste configuratie al heeft plaatsgevonden.

Het symptoom kan zich op de volgende manieren voordoen:

- Gedeeltelijk of volledig onvermogen om nieuwe services te implementeren (DVS-creatie, poortgroepscreatie, sommige objecten worden met succes geïmplementeerd, maar niet allemaal).
- De operationele inventaris is onvolledig of ontbreekt in de standpunten van de ACI-beheerder.
- Gewichten voor niet-ondersteunde vCenter-werking of voor een van de bovenstaande scenario's (bijv. poortgroepimplementatiefout).
- vCenter-controller wordt als offline gerapporteerd en fouten duiden erop dat er problemen zijn met connectiviteit of referenties.

Oplossing voor met RBAC verband houdende problemen

Controleer of alle bovenstaande rechten zijn verleend aan de vCenter-gebruiker die is geconfigureerd in het VMM-domein.

Een andere methode is om rechtstreeks aan te melden bij vCenter met dezelfde referenties als gedefinieerd in de VMM Domain-configuratie en soortgelijke bewerkingen te proberen (poortgroep maken, enzovoort). Als de gebruiker niet in staat is dezelfde bewerkingen uit te voeren terwijl hij rechtstreeks is aangemeld bij het vCenter, is het duidelijk dat de juiste rechten niet aan de gebruiker worden verleend.

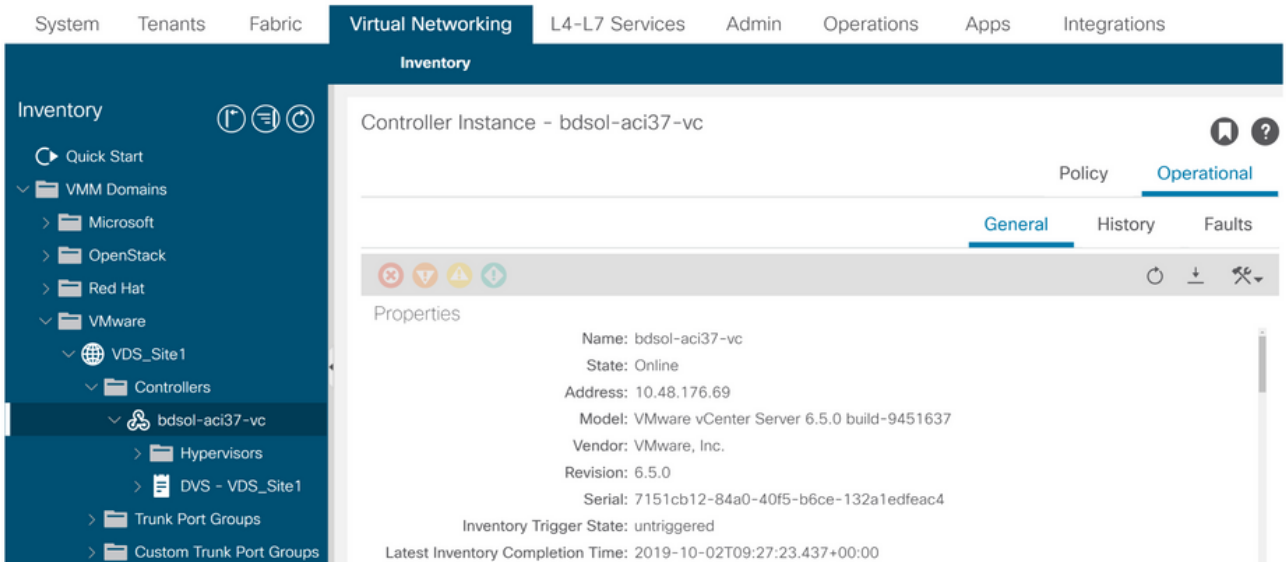
Probleemoplossing voor verbindingen

Bij het oplossen van problemen met een probleem dat te maken heeft met VMM-connectiviteit, is het belangrijk rekening te houden met een aantal van de fundamentele gedragingen van de manier waarop ACI met vCenter communiceert.

Het eerste en meest relevante gedrag is dat slechts één APIC in het cluster configuratie en inventarisatie op elk gegeven punt verzendt. Dit APIC wordt de gedeelde leider genoemd voor dit VMM-domein. Echter, meerdere APIC's luisteren naar vCenter Events om rekening te houden met een scenario waarbij de gedeelde leider een gebeurtenis om welke reden dan ook miste. Volgens dezelfde gedistribueerde architectuur van APIC's zal een bepaald VMM-domein één APIC hebben dat primaire gegevens en functionaliteit verwerkt (in dit geval de gedeelde leider), en twee replica's (in het geval van VMM worden ze aangeduid als volgers). Om de verwerking van VMM communicatie en functionaliteit over APICs te verdelen, kunnen om het even welke twee VMM Domeinen of het zelfde of een verschillende gedeelde leiders hebben.

De staat van de vCenter-verbinding kan worden gevonden door naar de VMM-controller van belang in de GUI te navigeren of door de CLI-opdracht te gebruiken die hieronder wordt vermeld.

VMWare VMM Domain - status van vCenter-connectiviteit



<#root>

```
apic2#
```

`show vmware domain name VDS_Site1 vcenter 10.48.176.69`

```
Name                          : bdsol-aci37-vc
```

```
Type                         : vCenter
Hostname or IP               : 10.48.176.69
Datacenter                   : Site1
DVS Version                  : 6.0
Status                       : online
Last Inventory Sync          : 2019-10-02 09:27:23
Last Event Seen              : 1970-01-01 00:00:00
Username                     : administrator@vsphere.local
Number of ESX Servers        : 2
Number of VMs                : 2
Faults by Severity           : 0, 0, 0, 0
Leader                       : bdsol-aci37-apic1

Managed Hosts:
ESX              VMs       Adjacency   Interfaces
---------------  --------  ----------  ------------------------------------------------
10.48.176.66     1         Direct      leaf-101 eth1/11, leaf-102 eth1/11
10.48.176.67     1         Direct      leaf-301 eth1/11, leaf-302 eth1/11
```

Als een VMM-controller offline is, wordt een fout als hieronder weergegeven:

```
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: do
```

De onderstaande stappen kunnen worden gebruikt om problemen met de connectiviteit tussen VC en APIC's op te lossen.

1. Identificatie van de gedeelde leider

De eerste stap in het oplossen van een connectiviteitsprobleem tussen APIC en vCenter is het begrijpen van welke APIC de gedeelde leider is voor het gegeven VMM-domein. De gemakkelijkste manier om deze informatie te bepalen is door de opdracht 'toon vmware domeinnaam <domain>' op een APIC uit te voeren.

<#root>

```
apic1#
```

show vmware domain name VDS_Site1

```
Domain Name                      : VDS_Site1
Virtual Switch Mode              : VMware Distributed Switch
Vlan Domain                      : VDS_Site1 (1001-1100)
Physical Interfaces              : leaf-102 eth1/11, leaf-301 eth1/11, leaf-302 eth1/11,
                                   leaf-101 eth1/11
Number of EPGs                   : 2
Faults by Severity               : 0, 0, 0, 0
```

```
LLDP override                       : RX: enabled, TX: enabled
CDP override                        : no
Channel Mode override               : mac-pinning
NetFlow Exporter Policy             : no
Health Monitoring                   : no

vCenters:
Faults: Grouped by severity (Critical, Major, Minor, Warning)
vCenter               Type      Datacenter            Status    ESXs   VMs    Faults
--------------------  --------  --------------------  --------  -----  -----  ---------------
10.48.176.69          vCenter   Site1                 online    2      2      0,0,0,0

APIC Owner:
Controller    APIC      Ownership
------------  --------  ---------------
bdsol-        apic1     Leader
aci37-vc
bdsol-        apic2     NonLeader
aci37-vc
bdsol-        apic3     NonLeader
aci37-vc
```

2. Connectiviteit met vCenter verifiëren

Na het identificeren van de APIC die actief communiceert met vCenter, verifieert IP connectiviteit met hulpmiddelen zoals pingelen.

```
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
```

Als vCenter is geconfigureerd met FQDN in plaats van IP-adres, kan de opdracht nslookup worden gebruikt om de naamresolutie te verifiëren.

<#root>

```
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
```

```
Address: 10.48.176.69
```

3. Controleer of OOB of INB wordt gebruikt

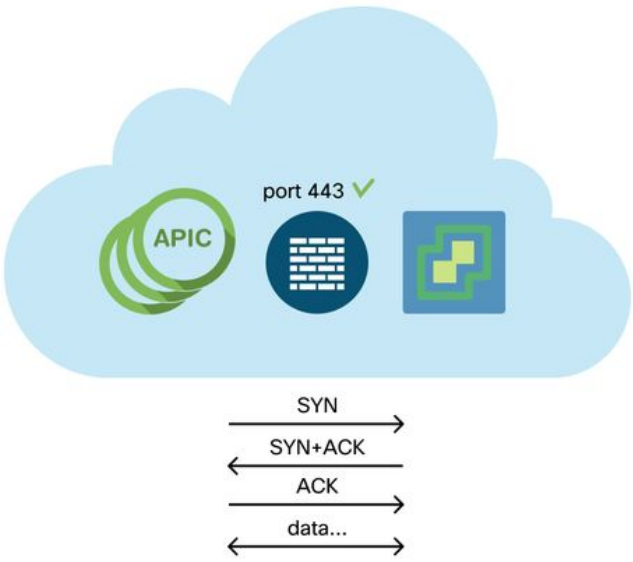
Controleer de APIC-routeringstabel om te controleren of out-of-band of in-band de voorkeur heeft voor connectiviteit en welke gateway wordt gebruikt:

<#root>

```
apic1#
bash

admin@apic1:~>
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. Zorg ervoor dat poort 443 is toegestaan tussen alle APIC's en het vCenter, inclusief firewalls op het communicatiepad.

vCenter <-> APIC - HTTPS (TCP-poort 443) - communicatie



De algemene bereikbaarheid van HTTPS van APICs aan vCenter kan met een krul worden getest:

<#root>

```
apic2#
curl -v -k https://10.48.176.69

* Rebuilt URL to: https://10.48.176.69/*   Trying 10.48.176.69...
* TCP_NODELAY set
* Connected to 10.48.176.69 (10.48.176.69) port 443 (#0)
...
```

Controleer of de gedeelde leider een vaste TCP-verbinding heeft op poort 443 met behulp van de netstat opdracht.

```
<#root>
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. Voer een pakketvastlegging uit

Indien mogelijk moet u een pakketopname langs het pad uitvoeren tussen de gedeelde leider en vCenter om na te gaan of er verkeer wordt verzonden en ontvangen door een van beide apparaten.

VMware-inventaris

De volgende tabel toont een lijst van VMWare VDS-parameters en specificeert of deze door de APIC kunnen worden geconfigureerd.

VMware VDS-parameters beheerd door APIC

VMware VDS	Standaardwaarde	Configureerbaar met Cisco APIC-beleid?
Naam	VMM Domain Name	Ja (afgeleid van domein)
Beschrijving	APIC virtuele Switch	Nee
Mapnaam	VMM Domain Name	Ja (afgeleid van domein)

VMware VDS	Standaardwaarde	Configureerbaar met Cisco APIC-beleid?
Versie	Hoogst ondersteund door vCenter	Ja
Detectieprotocol	LLDP	Ja
Uplink-poorten en uplinknamen	8	Ja (van Cisco APIC release 4.2(1))
Naamprefix voor uplink	opstraalverbinding	Ja (van Cisco APIC release 4.2(1))
Maximaal MTU	9000	Ja
LACS-beleid	uitgeschakeld	Ja
Poortmirroring	0 sessies	Ja
Alarmen	2 alarmen toegevoegd op mapniveau	Nee

De volgende tabel toont een lijst van VMWare VDS-poortgroepparameters en specificeert of deze door de APIC kunnen worden geconfigureerd.

VMWare VDS-poortgroepparameters beheerd door APIC

VMware VDS-poortgroep	Standaardwaarde	Configureerbaar met APIC-beleid
Naam	Naam huurder | Naam van toepassingsprofiel | EPG-naam	Ja (afgeleid van EPG)
Poortbinding	Statische binding	Nee

VMware VDS-poortgroep	Standaardwaarde	Configureerbaar met APIC-beleid
VLAN	Geselecteerd uit VLAN-pool	Ja
Algoritme voor taakverdeling	Afgeleid op basis van poortkanaalbeleid inzake APIC	Ja
Beloftevolle modus	Uitgeschakeld	Ja
Vervalste verzending	Uitgeschakeld	Ja
MAC-wijziging	Uitgeschakeld	Ja
Alle poorten blokkeren	ONJUIST	Nee

Probleemoplossing voor VMware-inventaris

Er vinden inventarissynchronisatiegebeurtenissen plaats om ervoor te zorgen dat de APIC zich bewust is van vCenter-gebeurtenissen die wellicht vereisen dat de APIC het beleid dynamisch bijwerkt. Er zijn twee typen inventarissynchronisatiegebeurtenissen die kunnen optreden tussen vCenter en APIC; een volledige inventarissynchronisatie en een gebeurtenisgebaseerde inventarissynchronisatie. Het standaardschema van een volledige inventarissynchronisatie tussen de APIC en vCenter is om de 24 uur, maar deze kunnen ook handmatig worden geactiveerd. Op gebeurtenissen gebaseerde inventarissyncs zijn doorgaans gekoppeld aan geactiveerde taken, zoals een vMotion. In dit geval, als een virtuele machine van de ene host naar de andere verplaatst en die hosts zijn verbonden met twee verschillende switches, zal de APIC luisteren naar de VM-migratiegebeurtenis en, in het geval van on-demand implementatiedemping, de EPG op het bronblad deprogrammeren en de EPG op het doelblad programmeren.

Afhankelijk van de implementatiedruk van EPG's die gekoppeld zijn aan een VMM-domein, kan het niet ophalen van inventaris uit het vCenter ongewenste gevolgen hebben. In het scenario dat de inventarisatie niet is voltooid of gedeeltelijk is, zal er altijd een fout worden gemaakt die het object of de objecten die de storing hebben veroorzaakt, aangeeft.

Scenario 1 - Virtuele machine met ongeldige ondersteuning:

Als een virtuele machine van het ene vCenter naar het andere wordt verplaatst, of als wordt vastgesteld dat de virtuele machine een ongeldige back-up heeft (bijv. een poortgroepsbijlage bij

een oude/verwijderde DVS), wordt de vNIC weergegeven als operationeel probleem.

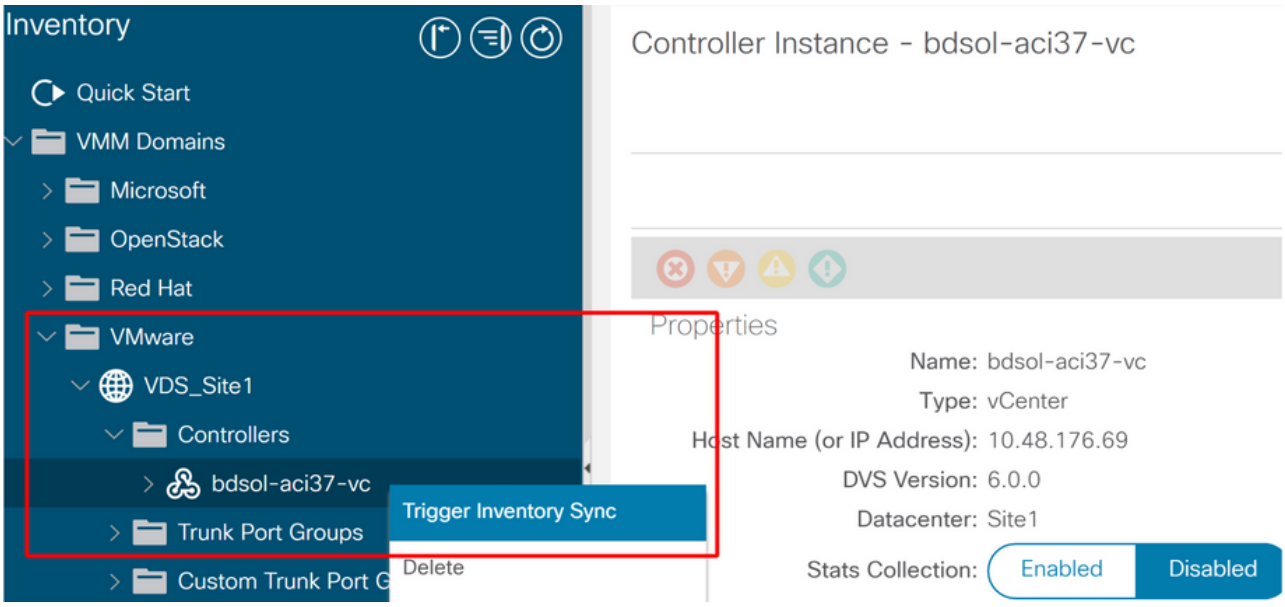
```
Fault fltCompVNicOperationalIssues
Rule ID:2842
Explanation:
This fault is raised when ACI controller failed to update the properties of a VNIC (e.g., it can not fi
Code: F2842
Message: Operational issues detected for VNic name on VM name in VMM controller: hostOrIp with name nam
Resolution:
Remediate the virtual machines indicated in the fault by assigning a valid port group on the affected v
```

Scenario 2 — vCenter-beheerder heeft een VMM-beheerd object op vCenter gewijzigd:

Het wijzigen van objecten die worden beheerd met APIC vanuit vCenter is geen ondersteunde bewerking. De volgende fout wordt weergegeven als een niet-ondersteunde bewerking op vCenter wordt uitgevoerd.

```
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
Resolution:
If this scenario is encountered, try to undo the unsupported change in vCenter and then trigger an 'inv
```

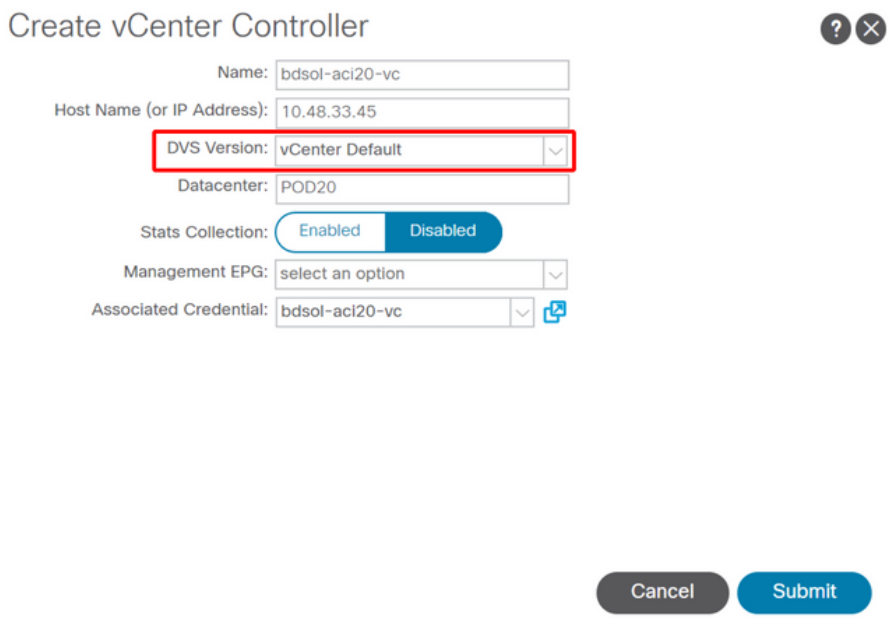
VMWare VMM Domain - vCenter-controller - inventarissynchronisatie activeren



VMware DVS-versie

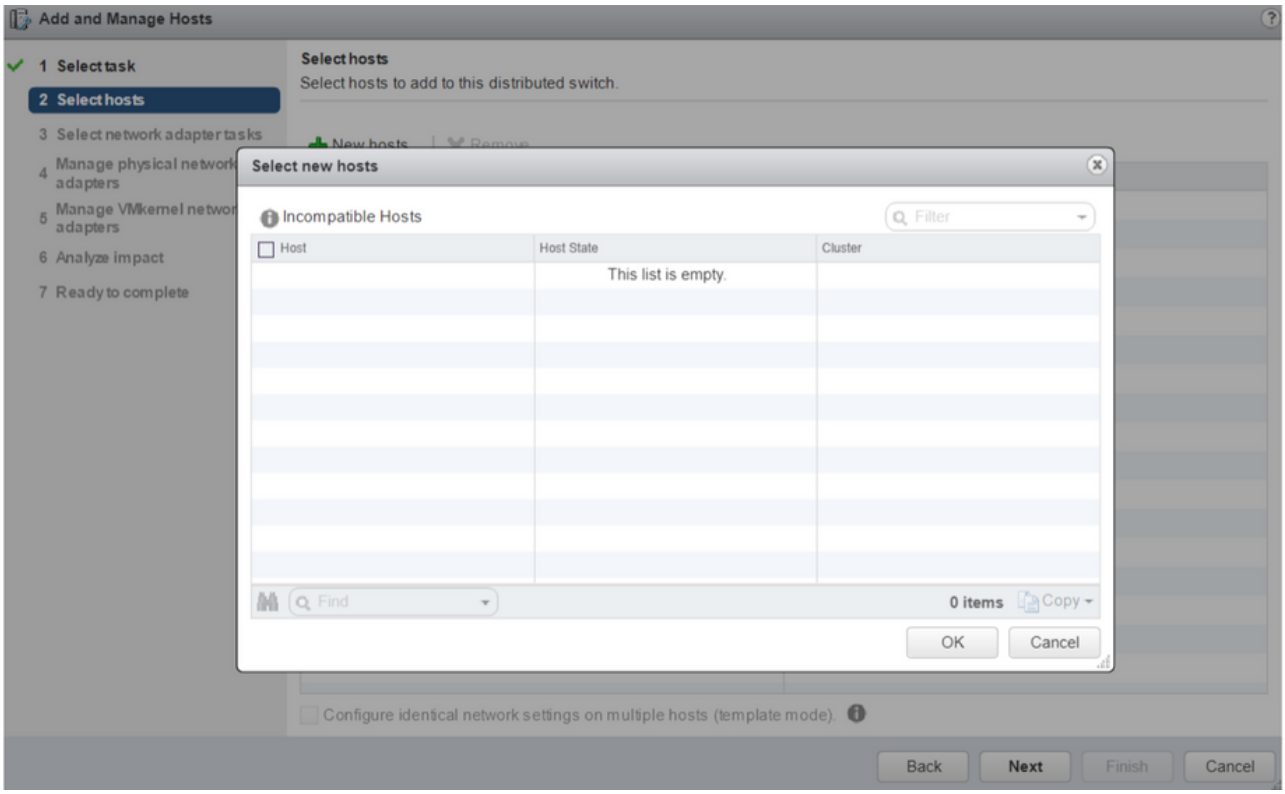
Wanneer u een nieuwe vCenter-controller maakt als onderdeel van een VMM-domein, wordt de standaardinstelling voor de DVS-versie bepaald door het 'vCenter Default' te gebruiken. Bij het selecteren van dit, zal de versie DVS worden gemaakt met de versie van vCenter.

VMWare VMM Domain - vCenter-controller maken

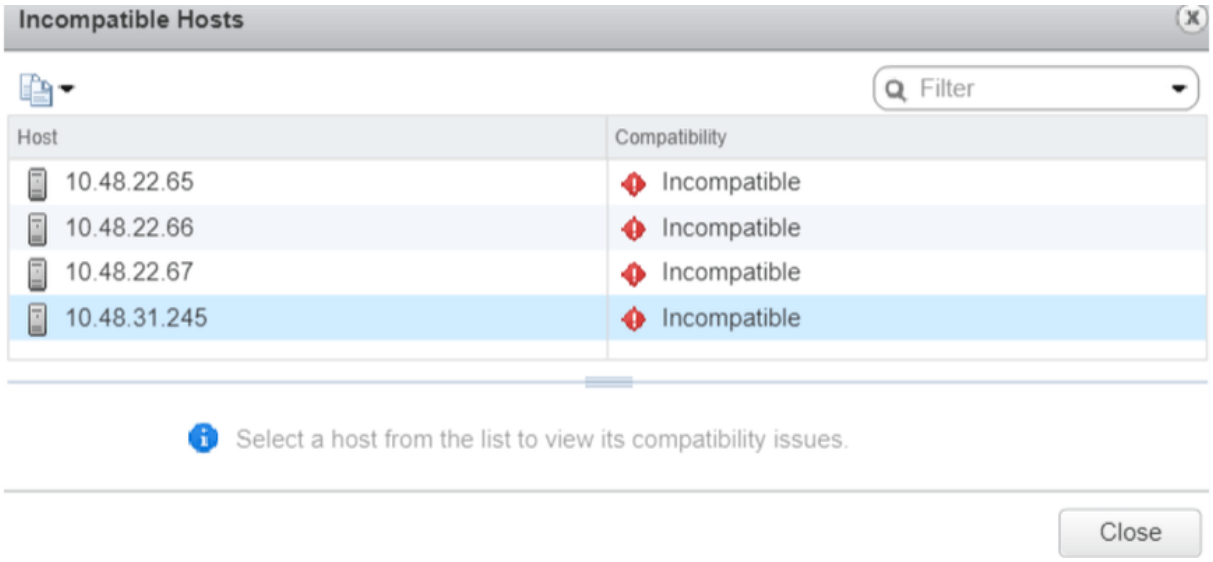


Dit betekent dat in het voorbeeld van een vCenter met 6.5 en ESXi-servers met 6.0, de APIC een DVS met versie 6.5 zal maken en dat de vCenter-beheerder de ESXi-servers met 6.0 niet kan toevoegen aan de ACI DVS.

APIC beheerde DVS - vCenter-hosttoevoeging - lege lijst



APIC beheerde DVS - vCenter-hosttoevoeging - incompatibele hosts



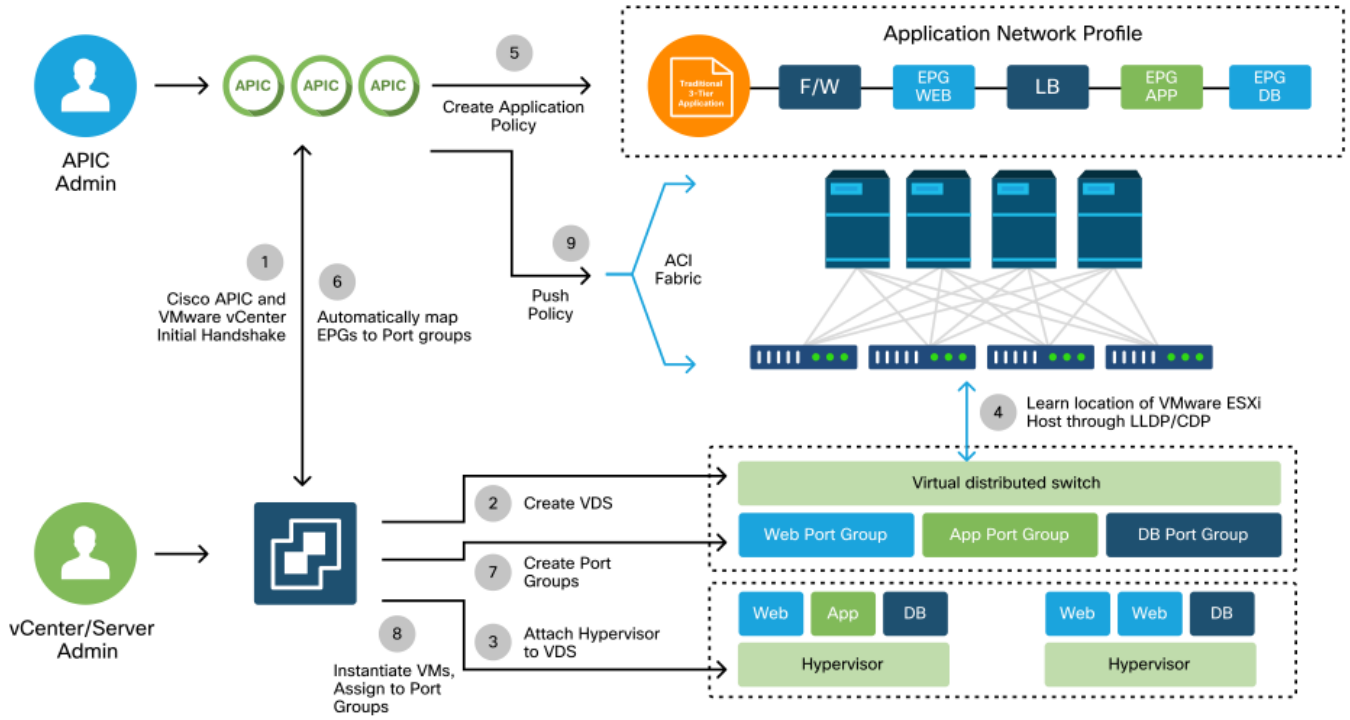
Zorg er dus bij het maken van een VMM-domein voor dat u de juiste 'DVS-versie' selecteert, zodat de benodigde ESXi-servers aan de DVS kunnen worden toegevoegd.

Dynamische detectie van host

Host/VM-detectieproces

De integratie van VMM in ACI onderscheidt zich van handmatige levering in die zin dat de stof dynamisch kan ontdekken waar de gastheren en de toepasselijke virtuele machines worden verbonden om beleid efficiënt te implementeren. Door dit dynamische proces kan ACI het gebruik van hardwareresources op de switches optimaliseren, aangezien VLAN's, SVI's, zoningregels, enz. alleen op knooppunten worden ingezet wanneer er een verbonden eindpunt is dat het beleid vereist. Vanuit het oogpunt van gebruiksgemak is het voordeel voor de netwerkbeheerder dat ACI VLAN/beleid zal provisioneren waar VM's op geautomatiseerde wijze verbinding maken. Om te bepalen waar het beleid moet worden ingezet, zal de APIC informatie uit meerdere bronnen gebruiken. In het volgende diagram worden de basisstappen van het hostdetectieproces beschreven bij gebruik van een op DVS gebaseerd VMM-domein.

VMWare VMM-domein — implementatieworkflow



In het kort zijn de volgende belangrijke stappen gaande wanneer:

- SWITCH LLDP of CDP wordt uitgewisseld tussen hypervisor- en bladmodules.
- Hosts rapporteren nabijheidsinformatie aan vCenter.
- vCenter informeert APIC over nabijheidsinformatie:
  - APIC weet van host via inventarissynchronisatie.
- APIC dwingt beleid naar de bladpoort:
  - raadpleeg de subsectie "Problemen met onmiddellijke oplossing" in deze sectie om deze voorwaarden nader te begrijpen.
- Als vCenter nabijheidsinformatie verloren gaat, kan APIC beleid verwijderen.

Zoals kan worden gezien, speelt CDP/LLDP een belangrijke rol in het ontdekkingsproces en het is belangrijk om ervoor te zorgen dat dit goed is geconfigureerd en beide kanten hetzelfde protocol gebruiken.

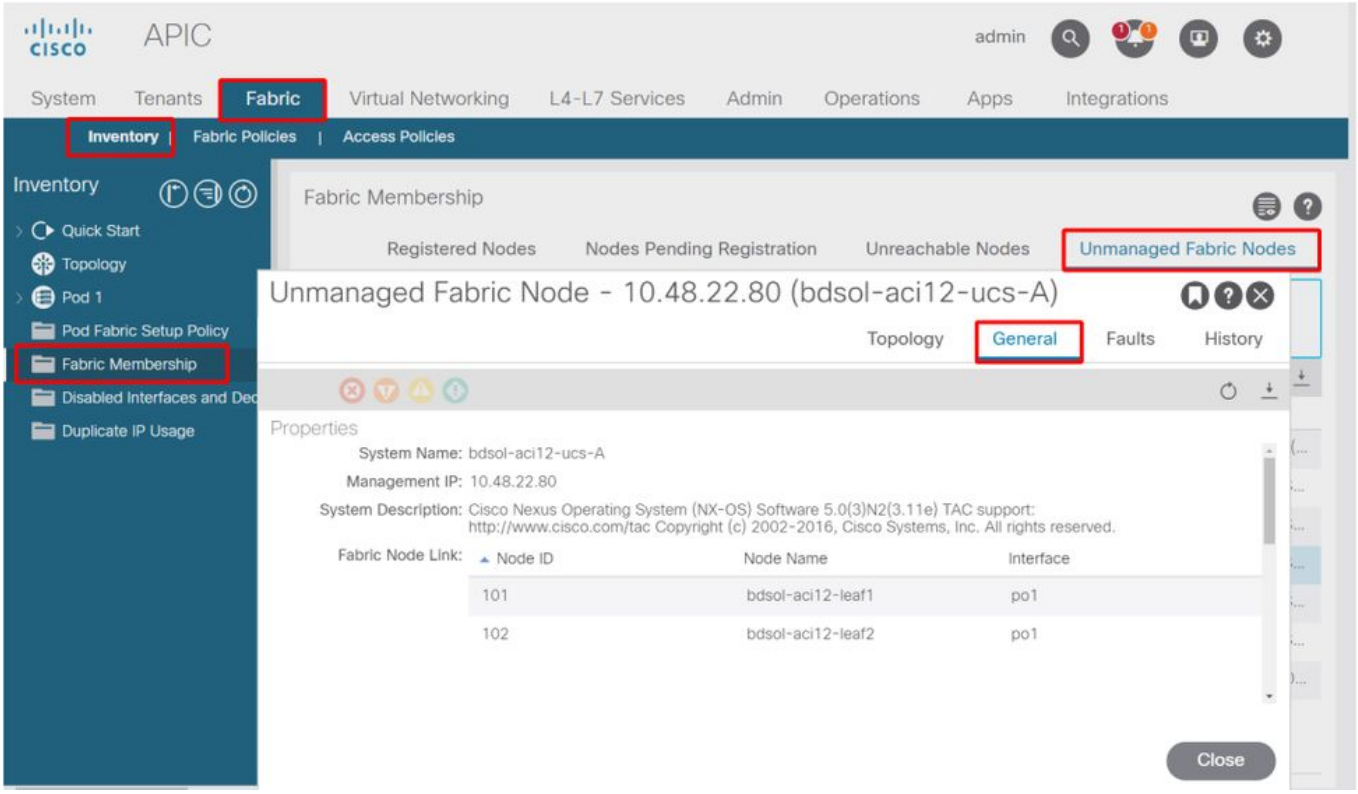
Fabric Losse Knooppunt / Tussenfase switch - use case

In een inzet met een bladechassis met een tussenliggende switch tussen de switches en de hypervisor, moet de APIC de nabijheid 'naaien'. In dit scenario zouden meerdere detectieprotocollen kunnen worden gebruikt omdat de intermediaire switch mogelijk andere protocolvereisten heeft dan de host.

In een installatie met een bladeserver en een tussenliggende switch (d.w.z. bladechassis-switch) moet ACI de tussenliggende switch detecteren en de hypervisors erachter in kaart brengen. De intermediaire switch wordt in ACI een Losse Knooppunt of een 'Unmanaged Fabric Node' genoemd. De gedetecteerde losse knooppunten kunnen worden bekeken onder 'Fabric > Inventaris > Fabric Membership > Unmanaged Fabric Nodes'. Door naar een van deze typen servers in de GUI te navigeren, kan de gebruiker het pad van blad naar intermediaire switch naar

host bekijken.

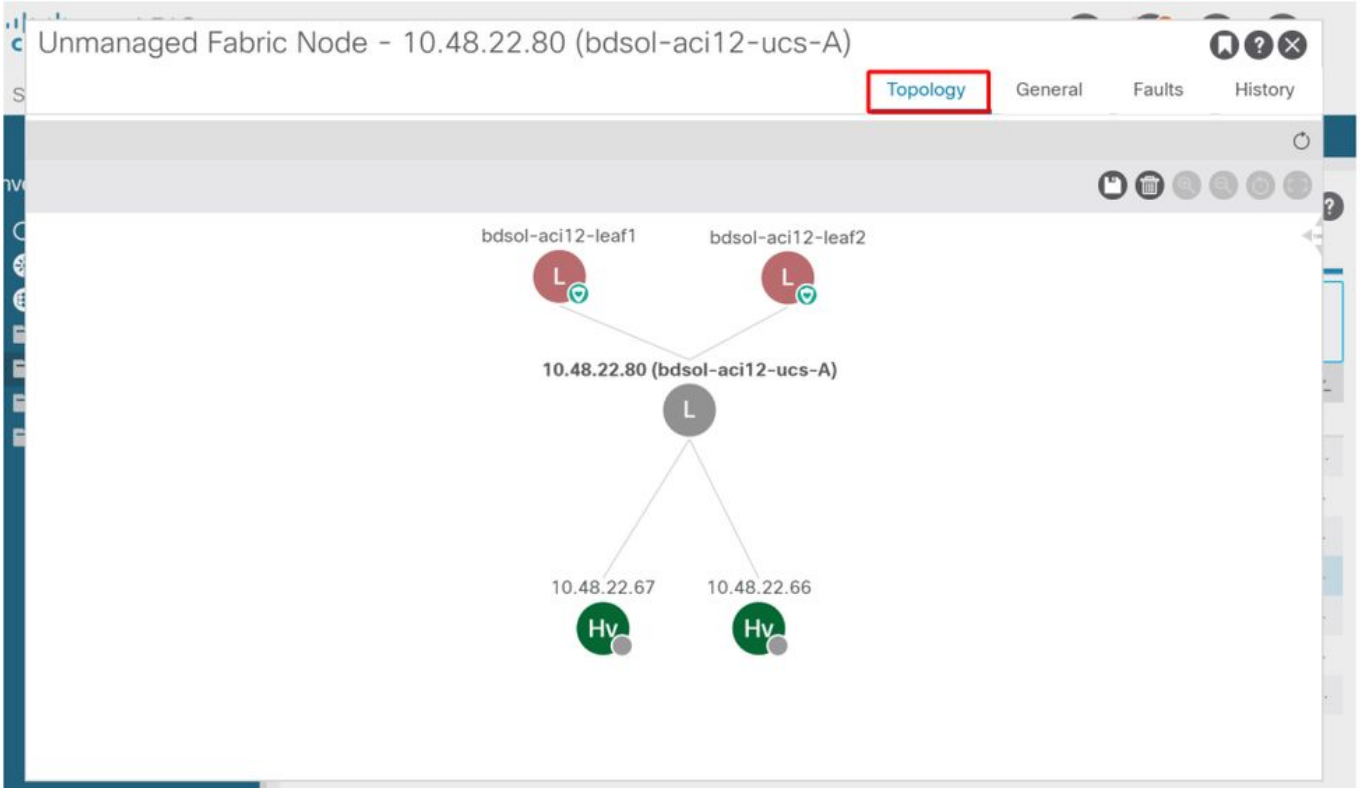
APIC UI — onbeheerde fabricknooppunten (losse knooppunten)



Met LLDP- of CDP-detectie kan ACI de topologie voor dergelijke losse knooppunten bepalen, omdat de hypervisor downstream van de tussenliggende switch wordt beheerd via VMM-integratie en het blad zelf een nabijheid heeft van de tussenliggende switch downstream.

Dit concept wordt geïllustreerd door de onderstaande afbeelding.

APIC UI — pad voor onbeheerd fabric-knooppunt

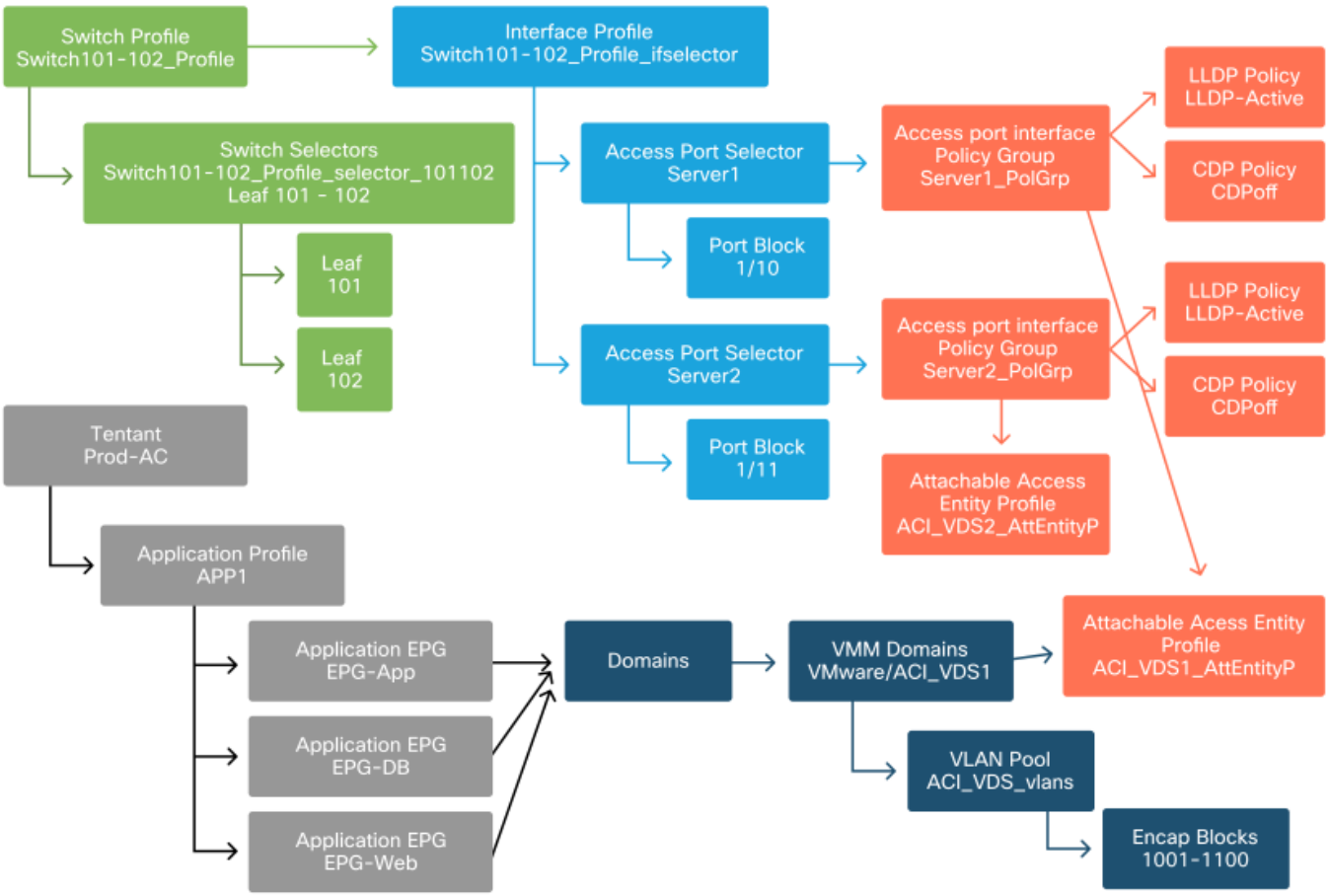


Onmiddellijkheid van oplossing

In scenario's waarin kritische services gebruik maken van de VMM-geïntegreerde DVS, zoals beheerconnectiviteit met vCenter/ESXi, is het verstandig om de Pre-Provision Resolution Immediacy te gebruiken. Met deze instelling wordt het mechanisme van dynamische hostdetectie verwijderd en worden in plaats daarvan beleid/VLAN's statisch geprogrammeerd op de host-omliggende interfaces. In deze configuratie zullen de VMM VLAN's altijd worden geïmplementeerd op alle interfaces die zijn gekoppeld aan de AEP waarnaar door het VMM-domein wordt verwezen. Dit verwijdert de mogelijkheid dat een kritisch VLAN (zoals beheer) wordt verwijderd uit een poort vanwege een gebeurtenis die te maken heeft met het detectieprotocol.

Raadpleeg het onderstaande schema:

Voorbeeld van implementatie vóór de provisioning



Als Pre-provisioning was ingesteld voor een EPG in het ACI_VDS1 VMM Domain, dan zouden VLAN's worden geïmplementeerd op koppelingen voor Server1 maar niet op Server2, omdat de AEP van Server2 het ACI_VDS1 VMM Domain niet bevat.

U kunt de instellingen voor de resolutie als volgt samenvatten:

- On-Demand - het beleid wordt geïmplementeerd wanneer de nabijheid is vastgesteld tussen blad en host en een VM is gekoppeld aan de poortgroep.
- Onmiddellijk - het beleid wordt opgesteld wanneer nabijheid tussen blad en gastheer duidelijk wordt gemaakt.
- Pre-provisioning - Het beleid wordt geïmplementeerd op alle poorten met behulp van een AEP met het VMM-domein ingesloten, er is geen nabijheid vereist.

Scenario's voor probleemoplossing

VM kan ARP niet oplossen voor zijn standaardgateway

In dit scenario is VMM-integratie geconfigureerd en is de DVS toegevoegd aan de hypervisor maar de VM kan ARP niet oplossen voor zijn gateway in ACI. Controleer of de nabijheid tot stand is gebracht en VLAN's worden geïmplementeerd om de VM netwerkconnectiviteit te bieden.

Ten eerste kan de gebruiker controleren of het blad de host heeft gedetecteerd met behulp van 'toon lldp buren' of 'toon cdp buren' op het blad afhankelijk van het geselecteerde protocol.

<#root>

```
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
bdsol-aci37-apic1     Eth1/1          120                    eth2-1
bdsol-aci37-apic2     Eth1/2          120                    eth2-1
bdsol-aci37-os1       Eth1/11         180        B           0050.565a.55a7
S1P1-Spine201         Eth1/49         120        BR          Eth1/1
S1P1-Spine202         Eth1/50         120        BR          Eth1/1
Total entries displayed: 5
```

Indien nodig vanuit het perspectief van probleemoplossing kan dit worden gevalideerd vanuit de ESXi-kant, zowel op de CLI als op de GUI:

<#root>

```
[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 -l

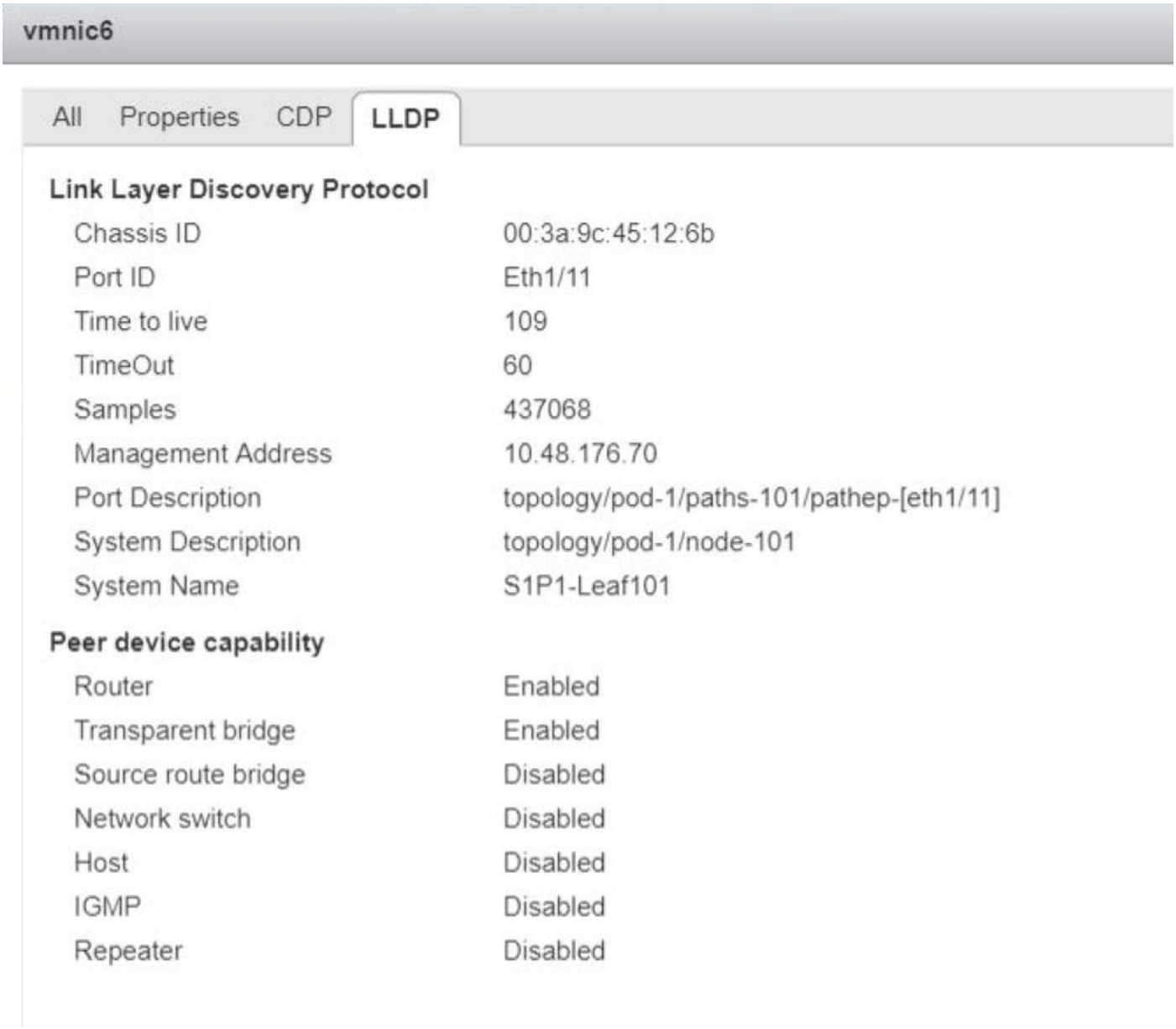
```
Name    PCI          Driver      Link Speed     Duplex MAC Address       MTU    Description
vmnic6  0000:09:00.0 enic        Up   10000Mbps Full   4c:77:6d:49:cf:30 9000   Cisco Systems Inc Cisco
vmnic7  0000:0a:00.0 enic        Up   10000Mbps Full   4c:77:6d:49:cf:31 9000   Cisco Systems Inc Cisco

[root@host:~]
```

vim-cmd hostsvc/net/query_networkhint --pnic-name=vmnic6 | grep -A2 "System Name"

```
               key = "System Name",
```

```
        value = "Leaf101"
    }
```

vCenter Web Client - host - vmnic LLDP/CDP-nabijheidsgegevens



Als de LLDP-nabijheid van het blad niet vanaf de ESXi-host kan worden gezien, wordt dit vaak veroorzaakt door het gebruik van een netwerkadapter die is geconfigureerd om LLDPDU's te genereren in plaats van het ESXi-besturingssysteem. Controleer of de netwerkadapter LLDP heeft ingeschakeld en dus alle LLDP-informatie verbruikt. Als dit probleem zich voordoet, moet u LLDP uitschakelen op de adapter zelf, zodat deze wordt bestuurd via het vSwitch-beleid.

Een andere oorzaak zou kunnen zijn dat er een verkeerde uitlijning tussen de ontdekkingsprotocollen is die tussen blad en ESXi Hypervisor worden gebruikt. Zorg ervoor dat u aan beide uiteinden hetzelfde detectieprotocol gebruikt.

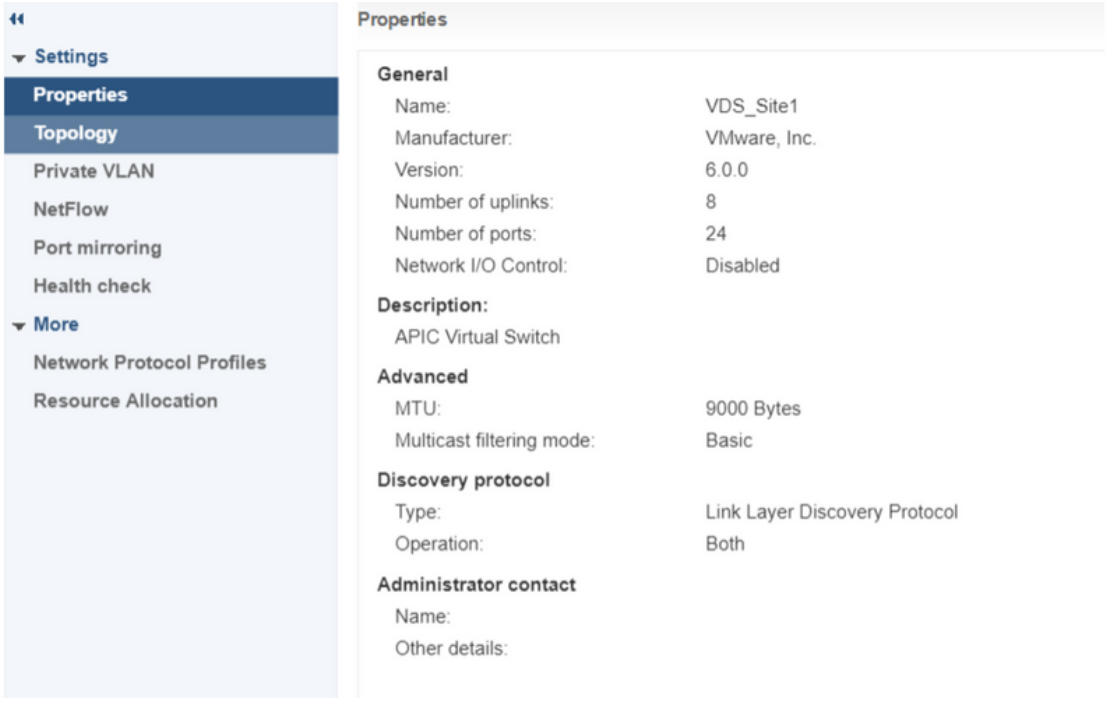
Om te controleren of de CDP/LLDP-instellingen zijn uitgelijnd tussen ACI en de DVS in de APIC UI, navigeer je naar 'Virtual Networking > VMM Domains > VMWare > Policy > vSwitch Policy'.

Zorg ervoor dat u alleen LLDP- of CDP-beleid inschakelt, aangezien deze elkaar uitsluiten.

APIC UI - VMWare VMM-domein - vSwitch-beleid

Ga in vCenter naar: 'Netwerken > VDS > Configureren'.

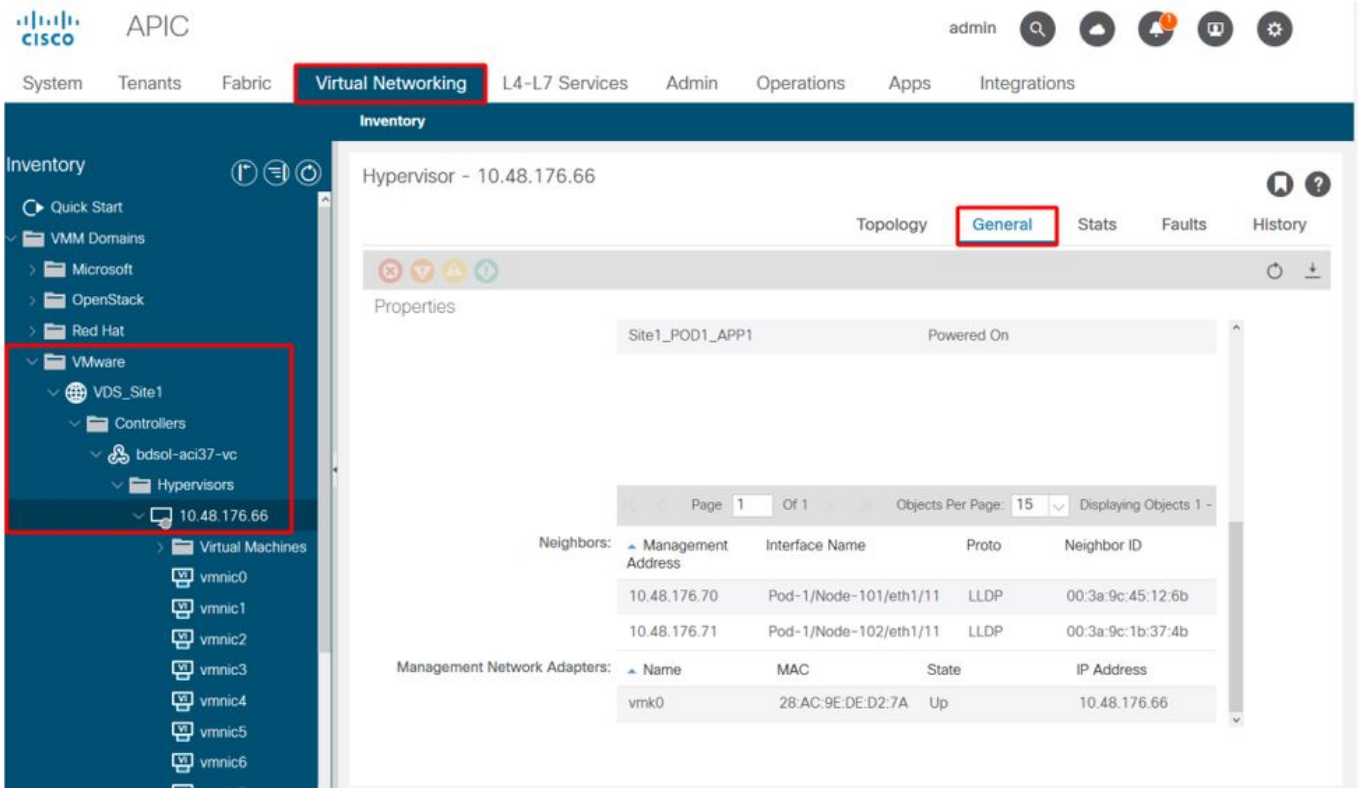
vCenter Web Client UI - VDS-eigenschappen



Corrigeer de LLDP/CDP-instellingen indien nodig.

Vervolgens valideren van de APIC observeert de LLDP/CDP-buurt van de ESXi-host tegen de switch in de UI onder 'Virtual Networking > VMM Domains > VMWare > Policy > Controller > Hypervisor > General'.

APIC UI - VMWare VMM-domein - Hypervisor details



Als dit verwachte waarden toont, dan kan de gebruiker bevestigen dat VLAN op de haven naar de gastheer aanwezig is.

<#root>

S1P1-Leaf101#

show vlan encap-id 1035

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
12   Ecommerce:Electronics:APP         active    Eth1/11

VLAN Type  Vlan-mode
---- ----- ----------
12   enet  CE
```

vCenter/ESXi-beheer VMK aangesloten op APIC-gedrukte DVS

In een scenario waarin vCenter- of ESXi-beheerverkeer gebruik moet maken van de geïntegreerde VMM-DVS, is het belangrijk om wat extra zorg te besteden aan het voorkomen van een patstelling in het activeren van de dynamische nabijheid en het activeren van de vereiste VLAN's.

Voor vCenter, dat doorgaans wordt gebouwd voordat VMM-integratie is geconfigureerd, is het belangrijk om een fysiek domein en statisch pad te gebruiken om er zeker van te zijn dat de encap VLAN van vCenter VM's altijd op de switches van het blad is geprogrammeerd, zodat deze kan

worden gebruikt voordat de VMM-integratie volledig is ingesteld. Zelfs na het opzetten van de VMM integratie, is het raadzaam om dit statische pad te laten om altijd de beschikbaarheid van deze EPG te verzekeren.

Voor de ESXi-hypervisors is het volgens de "Cisco ACI Virtualization Guide" op Cisco.com belangrijk dat u er bij de migratie naar de vDS voor zorgt dat de EPG waar de VMK-interface wordt aangesloten, wordt geïmplementeerd met de resolutie directheid ingesteld op Pre-provisioning. Dit zorgt ervoor dat het VLAN altijd op de switches van het blad geprogrammeerd is zonder te vertrouwen op LLDP/CDP-detectie van de ESXi-hosts.

Host nabijheid niet ontdekt achter LooseNode

De typische oorzaken van LosseNode ontdekkingskwesties zijn:

- CDP/LLDP is niet ingeschakeld
  - CDP/LLDP moet worden uitgewisseld tussen de intermediaire switch, de switches en ESXi-hosts
  - Voor Cisco UCS gebeurt dit via een netwerkbeheerbeleid op de vNIC
- Een wijziging in het IP-beheer van de LLDP/CDP-buur breekt de connectiviteit
  - Het vCenter zal het nieuwe IP-beheer zien in de nabijheid van LLDP/CDP, maar zal APIC niet bijwerken
  - Een handmatige inventarissynchronisatie starten om te repareren
- VMM VLAN’s worden niet toegevoegd aan de tussenliggende switch
  - De APIC programmeert geen blade/tussenliggende switches van derden.
  - Cisco UCS M-integratieapp (ExternalSwitch) beschikbaar in release 4.1(1).
  - VLAN’s moeten worden geconfigureerd en trunked naar uplinks die zijn aangesloten op ACI-bladknooppunten en downlinks die zijn aangesloten op hosts

F606391 - Ontbrekende nabijheid voor de fysieke adapter op de host

Bij onderstaande foutmelding:

```
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:
```

Gelieve de workflow in de sectie "VM kan ARP niet oplossen voor zijn standaardgateway" te herzien, aangezien dit betekent dat er ontbrekende CDP/LLDP-nabijheid zijn. Deze nabijheid moet van begin tot eind worden geverifieerd.

Hypervisor uplink-taakverdeling

Wanneer u hypervisors zoals ESXi aansluit op een ACI-fabric, zullen deze hypervisors meestal worden aangesloten met meerdere uplinks. Sterker nog, het is aan te raden om een ESXi-host aan te sluiten op ten minste twee switches. Dit zal de impact van storingsscenario's of upgrades

minimaliseren.

Om te optimaliseren hoe uplinks worden gebruikt door de werkbelastingen die op een hypervisor worden uitgevoerd, kunnen met VMware vCenter-configuraties meerdere taakverdelingsalgoritmen voor VM-gegenereerd verkeer naar de uplinks van de hypervisor worden geconfigureerd.

Het is van cruciaal belang dat alle hypervisors en de ACI-fabric zijn uitgelijnd met dezelfde configuratie van taakverdelingsalgoritme om ervoor te zorgen dat de juiste connectiviteit beschikbaar is. Als u dit niet doet, kan dit leiden tot intermitterende verkeersstroomdalingen en endpointbewegingen in het ACI-weefsel.

Dit kan worden gezien in een ACI-structuur door overmatige waarschuwingen zoals:

```
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
```

Dit hoofdstuk zal VMWare ESXi-hostconnectiviteit naar ACI dekken, maar is van toepassing voor de meeste hypervisors.

Rackserver

Als we kijken naar de verschillende manieren waarop een ESXi-host verbinding kan maken met een ACI-fabric, zijn ze verdeeld in 2 groepen, switch-afhankelijke en switch-onafhankelijke taakverdelingsalgoritmen.

Switch onafhankelijke load balancing algoritmen zijn manieren om verbinding te maken waar geen specifieke switch configuratie nodig is. Voor switch-afhankelijke taakverdeling zijn switch-specifieke configuraties vereist.

Controleer of het vSwitch-beleid in overeenstemming is met de vereisten van de ACI-toegangsbeleidsgroep in de onderstaande tabel.

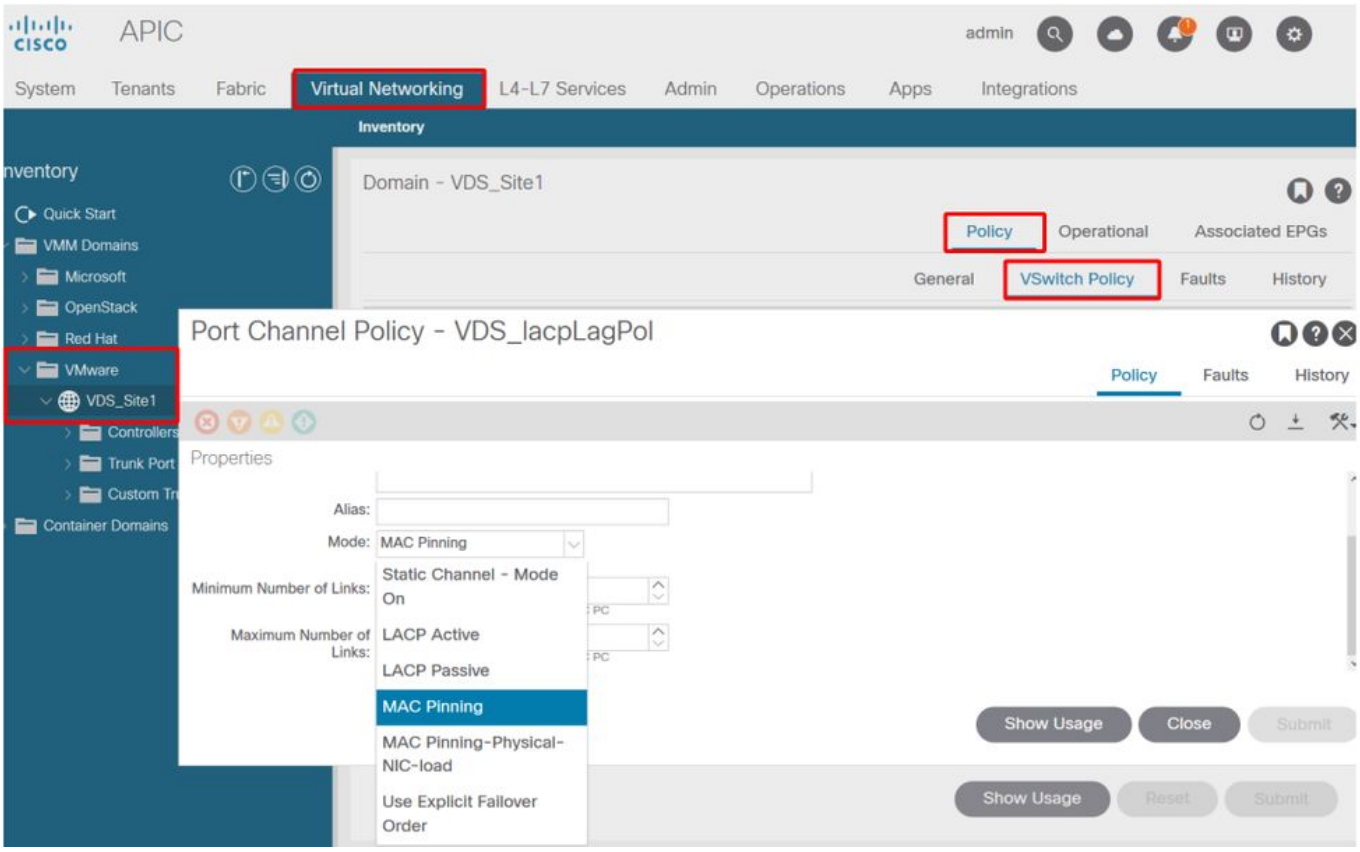
Teaming- en ACI vSwitch-beleid

VMware-teams en failover-modus	ACI vSwitch-beleid	Beschrijving	ACI Access Policy Group - poortkanaal vereist
Route op basis van de oorspronkelijke virtuele poort	MAC Pinning	Selecteer een uplink op basis van de virtuele poort-ID's op de switch. Nadat de virtuele switch een uplink voor een virtuele machine of een VMKernel adapter selecteert, wordt het verkeer altijd door dezelfde uplink voor deze virtuele machine of VMKernel adapter doorgestuurd.	Nee
Route op basis van MAC-hash	NA	Selecteer een uplink op basis van een hash van het bron MAC-adres	NA
Expliciete failover-volgorde	Expliciete failover-modus gebruiken	Gebruik in de lijst met actieve adapters altijd de hoogste ordeuplink die voldoet aan de criteria voor failover-detectie. Bij deze optie wordt geen werkelijke taakverdeling uitgevoerd.	Nee
Link Aggregation (LAG) - op basis van IP-hash	Statisch kanaal - Modus aan	Selecteer een uplink op basis van een hash van de bron- en doelIP-adressen van elk pakket. Voor niet-IP-pakketten gebruikt de switch de gegevens in die velden om de hash te berekenen. IP-gebaseerde teaming vereist dat aan de ACI-kant een poortkanaal / VPC is geconfigureerd met 'mode on'.	Ja (kanaalmodus ingesteld op 'aan')
Link Aggregation (LAG) - LACP	LACP actief/passief	Selecteer een uplink op basis van een geselecteerde hash (20 verschillende hashopties beschikbaar). LACP-gebaseerde teaming vereist dat aan de ACI-kant een poortkanaal / VPC is geconfigureerd met LACP ingeschakeld. Zorg ervoor dat u een uitgebreid logbeleid in ACI maakt en dit op het VS-switchbeleid toepast.	Ja (kanaalmodus ingesteld op 'LACP Active/Passive')

VMware-teams en failover-modus	ACI vSwitch-beleid	Beschrijving	ACI Access Policy Group - poortkanaal vereist
Route op basis van fysieke NIC-lading (LBT)	MAC Pinning - Physical-NIC-load	Beschikbaar voor gedistribueerde poortgroepen of gedistribueerde poorten. Selecteer een uplink op basis van de huidige lading van de fysieke netwerkadapters die zijn aangesloten op de poortgroep of poort. Als een uplink 30 seconden lang 75% of hoger bezet blijft, verplaatst vSwitch van de host een deel van het verkeer van de virtuele machine naar een fysieke adapter met vrije capaciteit.	Nee

Zie de schermafbeelding hieronder hoe u het poortkanaalbeleid kunt valideren als onderdeel van het vSwitch-beleid.

ACI vSwitch-beleid — Beleid voor poortkanaal



N.B.: Raadpleeg vSphere Networking op https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.networking.doc/GUID-D34B1ADD-B8A7-43CD-AA7E-

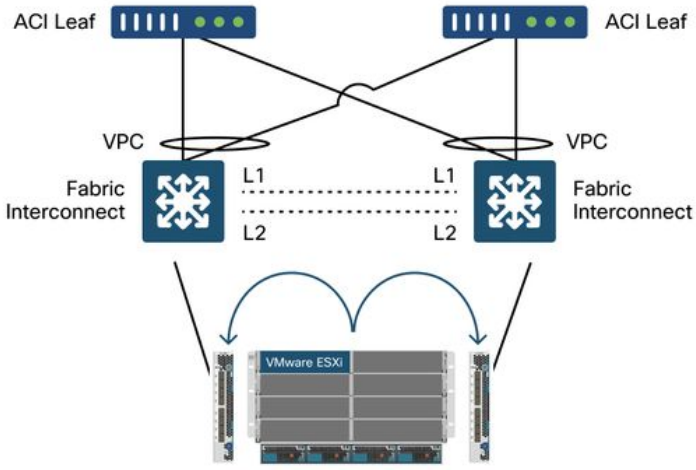
2832A0F7EE76.html voor een diepgaande beschrijving van de VMware-netwerkfuncties

Cisco UCS B-Series gebruikscase

Wanneer u Cisco UCS B-Series servers gebruikt, is het belangrijk om te onthouden dat deze binnen hun chassis verbinding maken met UCS Fabric Interconnects (FI's) die geen uniform dataplane hebben. Dit gebruiksgeval is ook van toepassing op andere leveranciers die een vergelijkbare topologie gebruiken. Hierdoor kan er een verschil zijn tussen de werklastverdelingsmethode die wordt gebruikt aan de kant van een ACI-switch en de kant van de vSwitch.

Hieronder is een topologie van UCS FI met ACI:

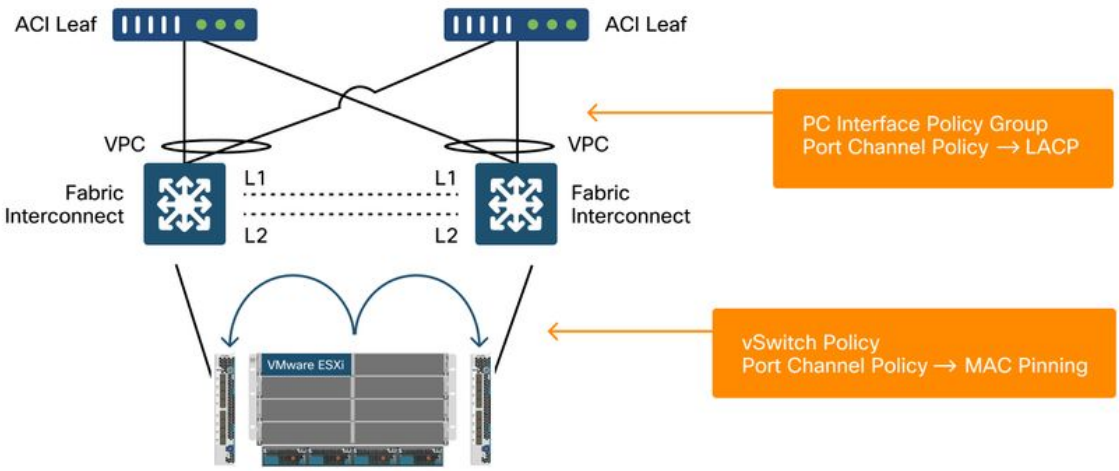
Cisco UCS FI met ACI-switches - topologie



Belangrijkste dingen om op te merken:

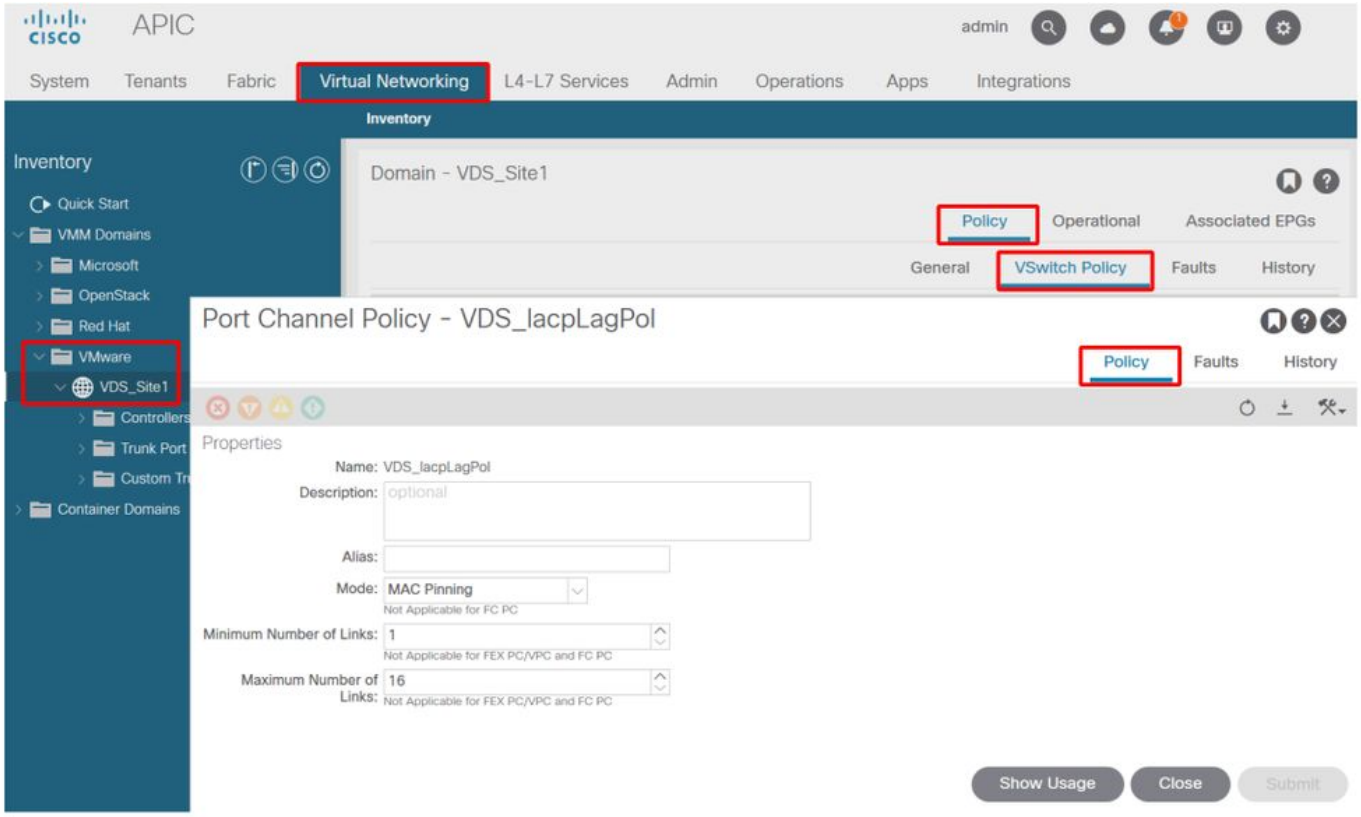
- Elke Cisco UCS FI heeft een poortkanaal naar de ACI-switches.
- De UCS FI's zijn alleen direct onderling verbonden voor hartslagdoeleinden (niet gebruikt voor dataplane).
- De vNIC van elke bladeserver is gekoppeld aan een specifieke UCS FI of maakt gebruik van een pad naar een van de FI's met behulp van UCS Fabric failover (Active-Standby).
- Het gebruik van IP-hash algoritmen op de vSwitch van de ESXi-host veroorzaakt MAC-flaps op de UCS FI's.

Voer de volgende handelingen uit om dit goed te configureren:



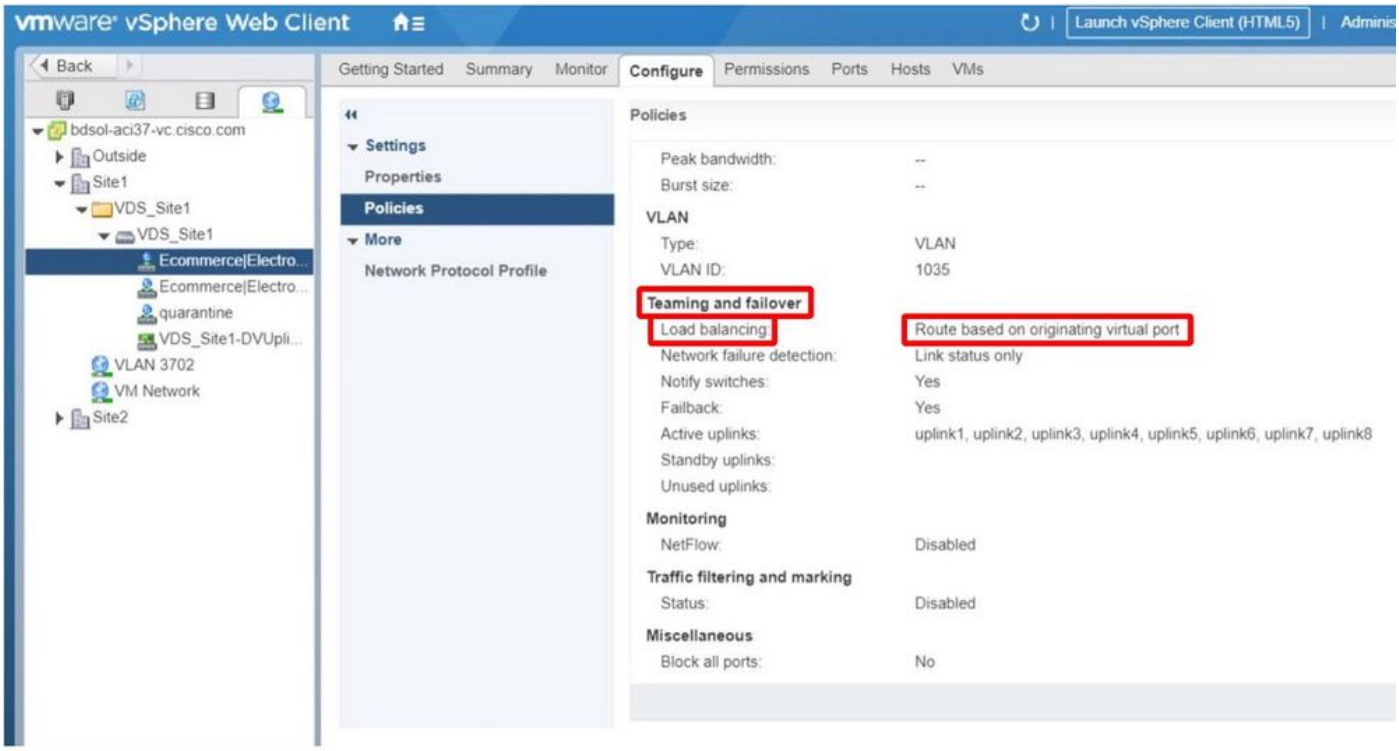
Wanneer MAC Pinning is ingesteld op het poortkanaalbeleid als onderdeel van het vSwitch-beleid in ACI, wordt dit weergegeven als 'Route gebaseerd op de oorspronkelijke virtuele poort' teamconfiguratie van de poortgroepen op de VDS.

ACI — Poortkanaalbeleid als onderdeel van vSwitch-beleid



Het poortkanaalbeleid dat in het bovenstaande voorbeeld wordt gebruikt, heeft de automatische naam van de wizard en wordt daarom "CDS_lacpLagPol" genoemd, hoewel we gebruik maken van Mode "MAC Pinning".

VMWare vCenter — ACI VDS — poortgroep — instelling voor taakverdeling


vmware vSphere Web Client
Launch vSphere Client (HTML5)
Back
bdsol-aci37-vc.cisco.com
Outside
Site1
VDS_Site1
VDS_Site1
Ecommerce|Electro...
Ecommerce|Electro...
quarantine
VDS_Site1-DVUpli...
VLAN 3702
VM Network
Site2
Getting Started
Summary
Monitor
Configure
Permissions
Ports
Hosts
VMs
Settings
Properties
Policies
More
Network Protocol Profile
Policies
Peak bandwidth: --
Burst size: --
VLAN
Type: VLAN
VLAN ID: 1035
Teaming and failover
Load balancing: Route based on originating virtual port
Network failure detection: Link status only
Notify switches: Yes
Failback: Yes
Active uplinks: uplink1, uplink2, uplink3, uplink4, uplink5, uplink6, uplink7, uplink8
Standby uplinks:
Unused uplinks:
Monitoring
NetFlow: Disabled
Traffic filtering and marking
Status: Disabled
Miscellaneous
Block all ports: No

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.