

Fehlerbehebung bei ACI VMM-Integration

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Virtual Machine Manager - Überblick](#)

[vCenter-Anbindung](#)

[Rollenbasierte Zugriffskontrolle](#)

[Fehlerbehebung bei RBAC-Problemen](#)

[Lösung für Probleme im Zusammenhang mit RBAC](#)

[Verbindungsproblembehandlung](#)

[1. Identifizierung des Anführers](#)

[2. Überprüfen der Verbindung mit vCenter](#)

[3. Überprüfen Sie, ob OOB oder INB verwendet wird.](#)

[4. Stellen Sie sicher, dass Port 443 zwischen allen APICs und vCenter zulässig ist, einschließlich aller Firewalls im Kommunikationspfad.](#)

[5. Paketerfassung durchführen](#)

[VMware-Bestand](#)

[Von APIC verwaltete VMware VDS-Parameter](#)

[Von APIC verwaltete VMWare VDS-Portgruppenparameter](#)

[VMware-Bestands-Fehlerbehebung](#)

[Szenario 1 - Virtuelles System mit ungültiger Sicherung:](#)

[Szenario 2 - vCenter-Administrator hat ein verwaltetes VMM-Objekt in vCenter geändert:](#)

[VMware DVS-Version](#)

[Dynamische Host-Erkennung](#)

[Host-/VM-Erkennungsprozess](#)

[Fabric LooseNode/Intermediate Switch - Anwendungsfall](#)

[Behebungssofortigkeit](#)

[Fehlerbehebungsszenarien](#)

[VM kann ARP für das Standard-Gateway nicht auflösen](#)

[vCenter/ESXi-Management VMK verbunden mit APIC-gestütztem DVS](#)

[Unbekannte Host-Adjacencies hinter LooseNode](#)

[F606391 - Fehlende Adjacencies für den physischen Adapter auf dem Host](#)

[Hypervisor-Uplink-Lastenausgleich](#)

[Rack-Server](#)

[Teaming- und ACI vSwitch-Richtlinie](#)

[Anwendungsfall der Cisco UCS B-Serie](#)

Einleitung

In diesem Dokument werden die Schritte zum Verständnis und zur Fehlerbehebung bei der ACI Virtual Machine Manager Integration (VMM) beschrieben.

Hintergrundinformationen

Das Material aus diesem Dokument wurde aus dem Buch [Troubleshooting Cisco Application Centric Infrastructure, Second Edition](#), extrahiert. Dies betrifft insbesondere die Kapitel **VMM Integration - Overview**, **VMM Integration - vCenter Connectivity**, **VMM Integration - Host Dynamic Discovery** und **VMM Integration - Hypervisor Uplink Load Balancing**.

Virtual Machine Manager - Überblick

ACI-Controller können in Virtual Machine Manager (VMMs) von Drittanbietern integriert werden.

Dies ist eine der Hauptfunktionen der ACI, da sie die Vorgänge für die End-to-End-Netzwerkconfiguration der Fabric und der damit verbundenen Workloads vereinfacht und automatisiert. Die ACI bietet ein Modell mit einer einzigen Overlay-Richtlinie, das auf verschiedene Workload-Typen erweitert werden kann, z. B. virtuelle Systeme, Bare-Metal-Server und Container.

In diesem Kapitel werden einige typische Fehlerbehebungsszenarien im Zusammenhang mit der VMware vCenter VMM-Integration behandelt.

Folgende Themen werden behandelt:

- Untersuchung von vCenter-Kommunikationsfehlern
- Dynamische Erkennungsprozesse und Fehlerszenarien für Host und VM.
- Hypervisor-Lastenausgleichsalgorithmen.

vCenter-Anbindung

Rollenbasierte Zugriffskontrolle

Die Mechanismen, über die der APIC mit dem vCenter-Controller kommunizieren kann, hängen von dem Benutzerkonto ab, das einer VMM-Domäne zugeordnet ist. Spezifische Anforderungen sind für den vCenter-Benutzer in Verbindung mit der VMM-Domäne festgelegt, um sicherzustellen, dass der APIC Vorgänge in vCenter erfolgreich durchführen kann, unabhängig davon, ob er Bestände und Konfigurationen weiterleitet und abrufen oder ob er Ereignisse überwacht, die mit dem verwalteten Bestand zusammenhängen.

Die einfachste Möglichkeit, Bedenken hinsichtlich dieser Anforderungen auszuräumen, besteht darin, das vCenter-Administratorkonto mit uneingeschränktem Zugriff zu verwenden. Diese Freiheit steht dem ACI-Administrator jedoch nicht immer zur Verfügung.

Die Mindestberechtigungen für ein benutzerdefiniertes Konto sind ab ACI Version 4.2 die folgenden:

- **Alarmer** Der APIC erstellt zwei Alarmer für den Ordner. Einer für DVS und einer für die Portgruppe. Wenn die EPG- oder VMM-Domänenrichtlinie auf dem APIC gelöscht wird, wird ein Alarm ausgelöst. vCenter kann jedoch die entsprechende Port-Gruppe oder den DVS nicht löschen, da VMs daran angeschlossen sind.
- **Verteilter Switch**
- **dvPort-Gruppe**

- **Ordner**
- **Netzwerk** Der APIC verwaltet die Netzwerkeinstellungen wie Hinzufügen oder Löschen von Portgruppen, Festlegen von Host-/DVS-MTU, LLDP/CDP, LACP usw.
- **Host** Wenn AVS zusätzlich zu den oben genannten verwendet wird, benötigt der Benutzer die Host-Berechtigung für das Rechenzentrum, in dem der APIC DVS erstellt.**Host.Configuration.Advanced-Einstellungen****Host.Lokale Vorgänge.Virtuelle Maschine neu konfigurieren****Host.Configuration.Network-Konfiguration**Dies ist für AVS und die Funktion zur automatischen Platzierung für virtuelle Layer-4- bis Layer-7-Service-VMs erforderlich. Für AVS erstellt der APIC eine VMK-Schnittstelle und platziert diese in einer VTEP-Portgruppe, die für OpFlex verwendet wird.
- **Virtuelles System** Wenn Servicediagramme verwendet werden, ist auch die Berechtigung für virtuelle Systeme für die virtuellen Appliances erforderlich.**Virtuelle Maschine.Konfiguration.Geräteeinstellungen ändern****Virtuelle Maschine.Konfiguration.Einstellungen**

Fehlerbehebung bei RBAC-Problemen

RBAC-Probleme treten meist während der Ersteinrichtung einer VMM-Domäne auf, können aber auftreten, wenn ein vCenter-Administrator die Berechtigungen des Benutzerkontos, das mit der VMM-Domäne verknüpft ist, ändert, nachdem die Ersteinrichtung bereits erfolgt ist.

Das Symptom kann sich wie folgt präsentieren:

- Teilweise oder vollständige Unfähigkeit, neue Dienste bereitzustellen (DVS-Erstellung, Port-Gruppenerstellung, einige Objekte wurden erfolgreich bereitgestellt, aber nicht alle).
- Der betriebliche Bestand ist unvollständig oder fehlt in den ACI-Administratoransichten.
- Fehler, die bei einem nicht unterstützten vCenter-Betrieb oder in einem der oben genannten Szenarien auftreten (z. B. Fehler bei der Port-Gruppen-Bereitstellung).
- Der vCenter-Controller wird als offline gemeldet, und Fehler weisen auf Verbindungs- oder Anmeldeprobleme hin.

Lösung für Probleme im Zusammenhang mit RBAC

Vergewissern Sie sich, dass alle oben genannten Berechtigungen dem vCenter-Benutzer gewährt wurden, der in der VMM-Domäne konfiguriert ist.

Eine weitere Methode besteht darin, sich mit denselben Anmeldeinformationen wie in der VMM-Domänenkonfiguration direkt beim vCenter anzumelden und ähnliche Vorgänge (Erstellung von Portgruppen usw.) auszuführen. Wenn der Benutzer nicht in der Lage ist, diese Vorgänge auszuführen, während er direkt beim vCenter angemeldet ist, werden dem Benutzer eindeutig nicht die richtigen Berechtigungen erteilt.

Verbindungsproblembehandlung

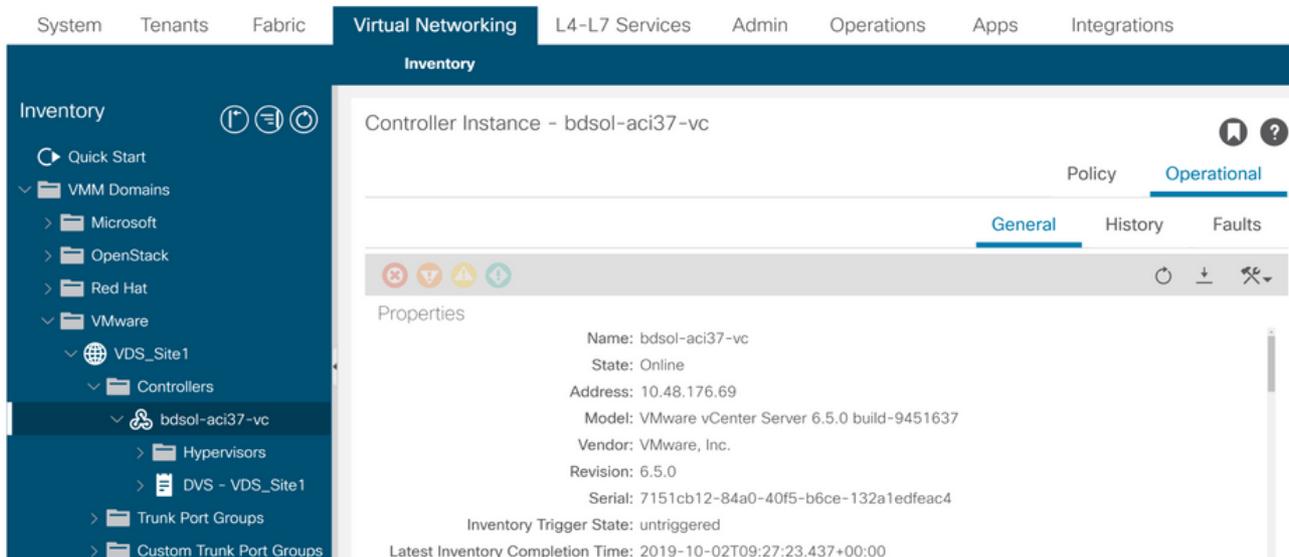
Bei der Behebung eines Problems im Zusammenhang mit der VMM-Konnektivität müssen einige der grundlegenden Verhaltensweisen der ACI bei der Kommunikation mit vCenter beachtet werden.

Das erste und relevanteste Verhalten besteht darin, dass nur ein APIC im Cluster die

Konfiguration sendet und den Bestand an einem bestimmten Punkt erfasst. Dieser APIC wird als **gemeinsamer Marktführer** für diese VMM-Domäne bezeichnet. Allerdings überwachen mehrere APICs **vCenter-Ereignisse**, um ein Szenario zu berücksichtigen, in dem der Leiter der Shared Switches ein Ereignis aus irgendeinem Grund verpasst hat. Entsprechend derselben verteilten Architektur von APICs verfügt eine bestimmte VMM-Domäne über einen APIC, der primäre Daten und Funktionen (in diesem Fall den Shared Leader) verarbeitet, sowie über zwei Replikate (im Fall von VMM werden sie als **Follower** bezeichnet). Um die Handhabung der VMM-Kommunikation und -Funktionen auf die APICs zu verteilen, können zwei beliebige VMM-Domänen entweder die gleichen oder unterschiedliche gemeinsame Führungskräfte haben.

Der vCenter-Verbindungsstatus kann über den VMM-Controller in der GUI oder den CLI-Befehl unten ermittelt werden.

VMWare VMM-Domäne - vCenter-Verbindungsstatus



```
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

Wenn ein VMM-Controller als offline angezeigt wird, wird ein Fehler ausgelöst, ähnlich wie unten:

```
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: domName is failing repeatedly with error: [remoteErrMsg]. Please verify network connectivity of VMM controller hostOrIp and check VMM controller user credentials are valid.

Mit den folgenden Schritten können Sie Verbindungsprobleme zwischen VC und den APICs beheben.

1. Identifizierung des Anführers

Der erste Schritt bei der Behebung eines Verbindungsproblems zwischen dem APIC und vCenter besteht darin, zu ermitteln, welcher APIC für die jeweilige VMM-Domäne der gemeinsame Marktführer ist. Der einfachste Weg, diese Informationen zu ermitteln, besteht darin, den Befehl "show vmware domain name <domain>" auf einem beliebigen APIC auszuführen.

```
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. Überprüfen der Verbindung mit vCenter

Nachdem der APIC identifiziert wurde, der aktiv mit dem vCenter kommuniziert, überprüfen Sie die IP-Verbindung mit Tools wie Ping.

```
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

Wenn vCenter mit FQDN anstelle von IP-Adresse konfiguriert wurde, kann der Befehl nslookup verwendet werden, um die Namensauflösung zu überprüfen.

```
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. Überprüfen Sie, ob OOB oder INB verwendet wird.

Prüfen Sie in der APIC-Routing-Tabelle, ob Out-of-Band oder In-Band für die Verbindung bevorzugt wird und welches Gateway verwendet wird:

```
apic1# bash
```

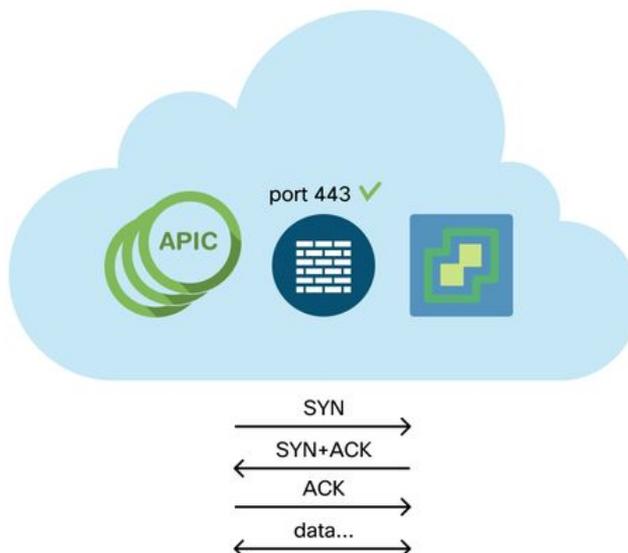
```
admin@apic1:~> route
```

```
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. Stellen Sie sicher, dass Port 443 zwischen allen APICs und vCenter zulässig ist, einschließlich aller Firewalls im Kommunikationspfad.

vCenter <-> APIC - HTTPS (TCP-Port 443) - Kommunikation



Die allgemeine HTTPS-Erreichbarkeit vom APIC zum vCenter kann mit einer Kurve getestet werden:

```
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)
```

...

Überprüfen Sie mithilfe des Befehls netstat, ob die gemeinsame Leitung über eine hergestellte TCP-Verbindung an Port 443 verfügt.

```
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. Paketerfassung durchführen

Führen Sie nach Möglichkeit eine Paketerfassung entlang des Pfades zwischen dem gemeinsam genutzten Leader und vCenter durch, um festzustellen, ob Datenverkehr von einem der Geräte gesendet und empfangen wird.

VMware-Bestand

Die nachfolgende Tabelle enthält eine Liste der VMWare VDS-Parameter und gibt an, ob diese vom APIC konfiguriert werden können.

Von APIC verwaltete VMware VDS-Parameter

VMware VDS	Standardwert	Über die Cisco APIC-Richtlinie konfigurierbar?
Name	VMM-Domänenname	Ja (von Domäne abgeleitet)
Beschreibung	Virtueller APIC-Switch	Nein
Ordnername	VMM-Domänenname	Ja (von Domäne abgeleitet)
Version	Höchste Unterstützung durch vCenter	Ja
Discovery-Protokoll	LLDP	Ja
Uplink-Ports und Uplink-Namen	8	Ja (von Cisco APIC Version 4.2(1))
Uplink-Namenspräfix	Aufwärtsstrecke	Ja (von Cisco APIC Version 4.2(1))
Maximale MTU	9000	Ja
LACP-Richtlinie	disabled	Ja
Port-Spiegelung	0 Sitzungen	Ja
Alarmer	2 Alarmer auf Ordnernebene hinzugefügt	Nein

Die nachfolgende Tabelle enthält eine Liste der VMWare VDS-Portgruppenparameter und gibt an, ob diese vom APIC konfiguriert werden können.

Von APIC verwaltete VMWare VDS-Portgruppenparameter

VMware VDS-Portgruppe	Standardwert	Konfigurierbar mit APIC-Richtlinie
Name	Tenant-Name Name des Anwendungsprofils EPG-Name	Ja (von EPG abgeleitet)
Portbindung	Statische Bindung	Nein
VLAN	Aus VLAN-Pool ausgewählt	Ja

Lastenausgleichsalgorithmus	Abgeleitet von Port-Channel-Richtlinie auf dem APIC	Ja
Promiscuous-Modus	Deaktiviert	Ja
Gefälschte Übertragung	Deaktiviert	Ja
MAC-Änderung	Deaktiviert	Ja
Alle Ports sperren	FALSCH	Nein

VMware-Bestands-Fehlerbehebung

Synchronisierungsereignisse im Bestand stellen sicher, dass der APIC vCenter-Ereignisse erkennt, die eine dynamische Aktualisierung der Richtlinie durch den APIC erfordern. Es gibt zwei Arten von Bestandssynchronisierungsereignissen, die zwischen vCenter und dem APIC auftreten können: eine vollständige Bestandssynchronisierung und eine ereignisbasierte Bestandssynchronisierung. Der Standardzeitplan für eine vollständige Bestandssynchronisierung zwischen dem APIC und vCenter beträgt 24 Stunden, kann jedoch auch manuell ausgelöst werden. Ereignisbasierte Bestandssynchronisierungen sind in der Regel mit ausgelösten Aufgaben wie vMotion verknüpft. Wenn in diesem Szenario ein virtuelles System von einem Host zu einem anderen verschoben wird und diese Hosts mit zwei verschiedenen Leaf-Switches verbunden sind, sucht der APIC nach dem VM-Migrationsereignis und entprogrammiert die EPG im Szenario einer sofortigen On-Demand-Bereitstellung auf dem Quell-Leaf und programmiert die EPG auf dem Ziel-Leaf.

Je nachdem, wie schnell EPGs bereitgestellt werden, die einer VMM-Domäne zugeordnet sind, kann ein fehlendes Abrufen des Bestands aus vCenter unerwünschte Folgen haben. Bei einem fehlgeschlagenen oder teilweisen Bestand wird immer ein Fehler ausgelöst, der das Objekt oder die Objekte angibt, die den Fehler verursacht haben.

Szenario 1 - Virtuelles System mit ungültiger Sicherung:

Wenn ein virtuelles System von einem vCenter in ein anderes verschoben wird oder festgestellt wird, dass das virtuelle System eine ungültige Sicherung aufweist (z. B. eine Portgruppenanbindung an einen alten/gelöschten DVS), wird gemeldet, dass der vNIC Probleme beim Betrieb hat.

```
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 find the EPG that the VNIC attached to).
```

```
Code: F2842
```

```
Message: Operational issues detected for VNic name on VM name in VMM controller: hostOrIp with name name in datacenter rootContName in domain: domName due to error: issues.
```

```
Resolution:
```

```
Remediate the virtual machines indicated in the fault by assigning a valid port group on the affected vNIC of the VM.
```

Szenario 2 - vCenter-Administrator hat ein verwaltetes VMM-Objekt in vCenter geändert:

Das Ändern von Objekten, die vom APIC über vCenter verwaltet werden, wird nicht unterstützt. Der folgende Fehler tritt auf, wenn ein nicht unterstützter Vorgang in vCenter ausgeführt wird.

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 in domain domName detected, error: [deployIssues]

Resolution:

If this scenario is encountered, try to undo the unsupported change in vCenter and then trigger an 'inventory sync' manually.

VMWare VMM-Domäne - vCenter-Controller - Auslösung der Bestandssynchronisierung

The screenshot shows the VMware VMM interface. On the left, the 'Inventory' pane is expanded to show the 'VMware' folder, which contains 'VDS_Site1' and 'Controllers'. The 'Controllers' folder is further expanded to show 'bdsol-aci37-vc'. A red box highlights this area, and a blue button labeled 'Trigger Inventory Sync' is overlaid on the 'bdsol-aci37-vc' entry. On the right, the 'Controller Instance - bdsol-aci37-vc' properties are displayed, including Name, Type, Host Name, DVS Version, and Datacenter. The 'Stats Collection' is set to 'Enabled'.

VMware DVS-Version

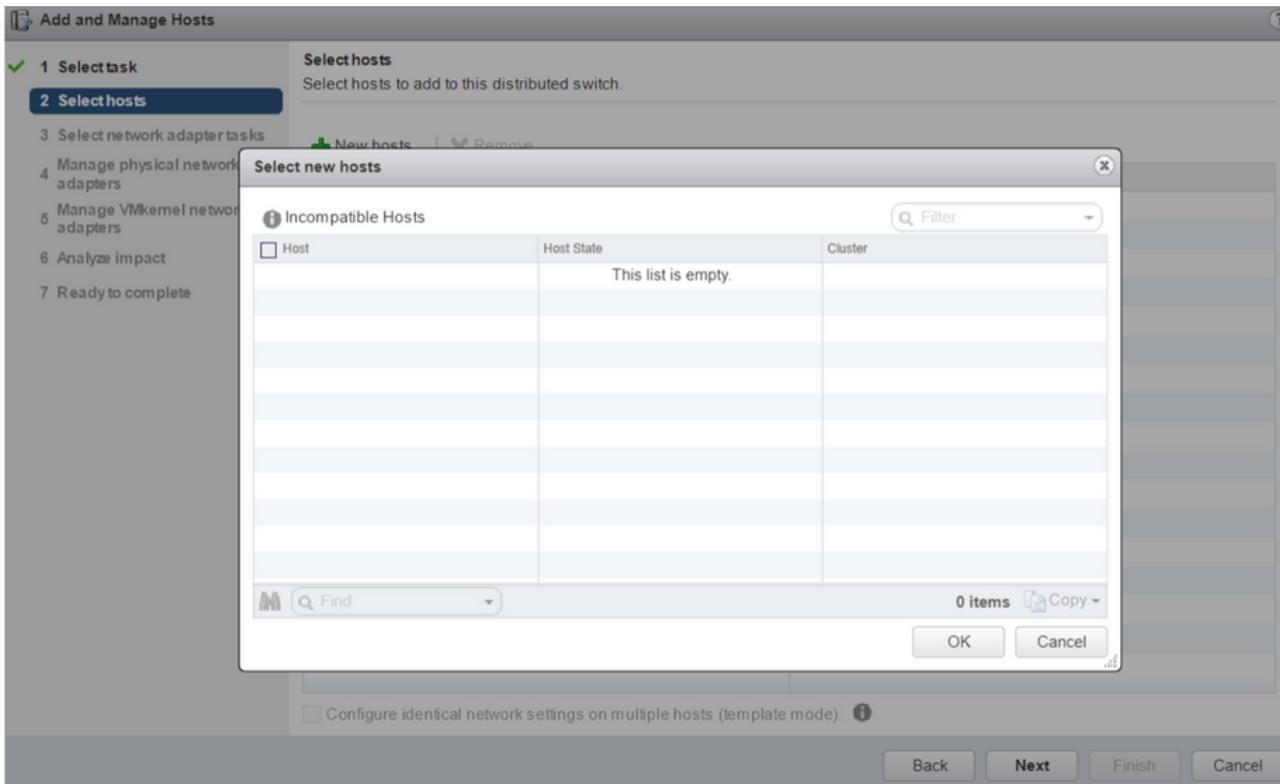
Wenn Sie einen neuen vCenter-Controller als Teil einer VMM-Domäne erstellen, lautet die Standardeinstellung für die DVS-Version "vCenter-Standard". Wenn Sie diese Option auswählen, wird die DVS-Version mit der Version von vCenter erstellt.

VMWare VMM-Domäne - Erstellung des vCenter-Controllers

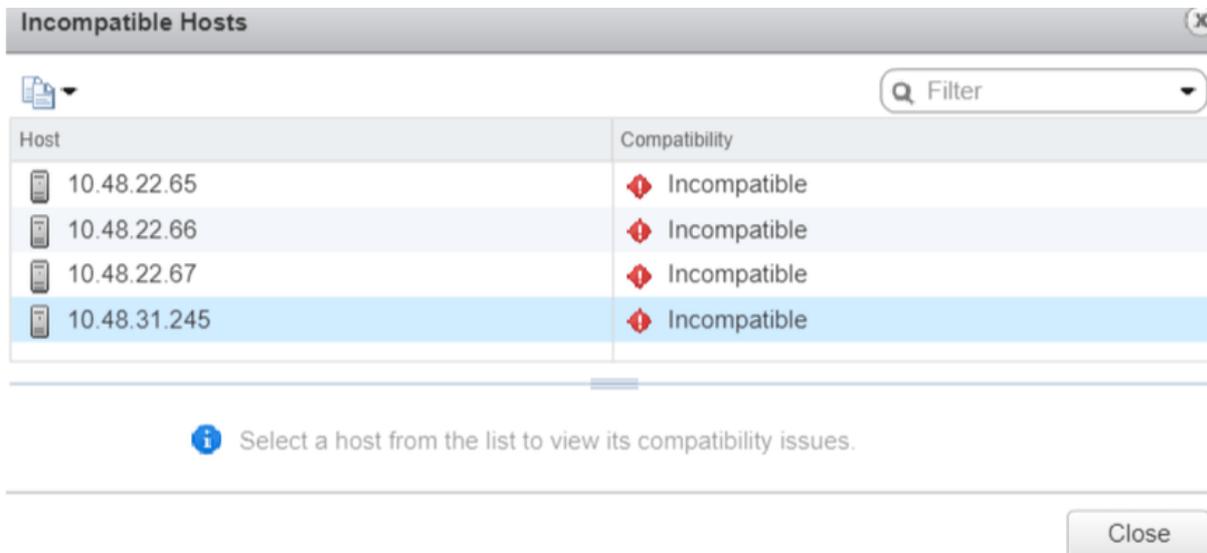
The screenshot shows the 'Create vCenter Controller' dialog box. The fields are: Name: bdsol-aci20-vc, Host Name (or IP Address): 10.48.33.45, DVS Version: vCenter Default (highlighted with a red box), Datacenter: POD20, Stats Collection: Enabled, Management EPG: select an option, and Associated Credential: bdsol-aci20-vc. There are 'Cancel' and 'Submit' buttons at the bottom.

Im Beispiel eines vCenter mit 6.5 und eines ESXi-Servers mit 6.0 erstellt der APIC einen DVS mit Version 6.5. Daher kann der vCenter-Administrator die ESXi-Server mit 6.0 nicht zum ACI-DVS hinzufügen.

Vom APIC verwalteter DVS - Hinzufügen von vCenter-Hosts - leere Liste



APIC-verwalteter DVS - Hinzufügen von vCenter-Hosts - inkompatible Hosts



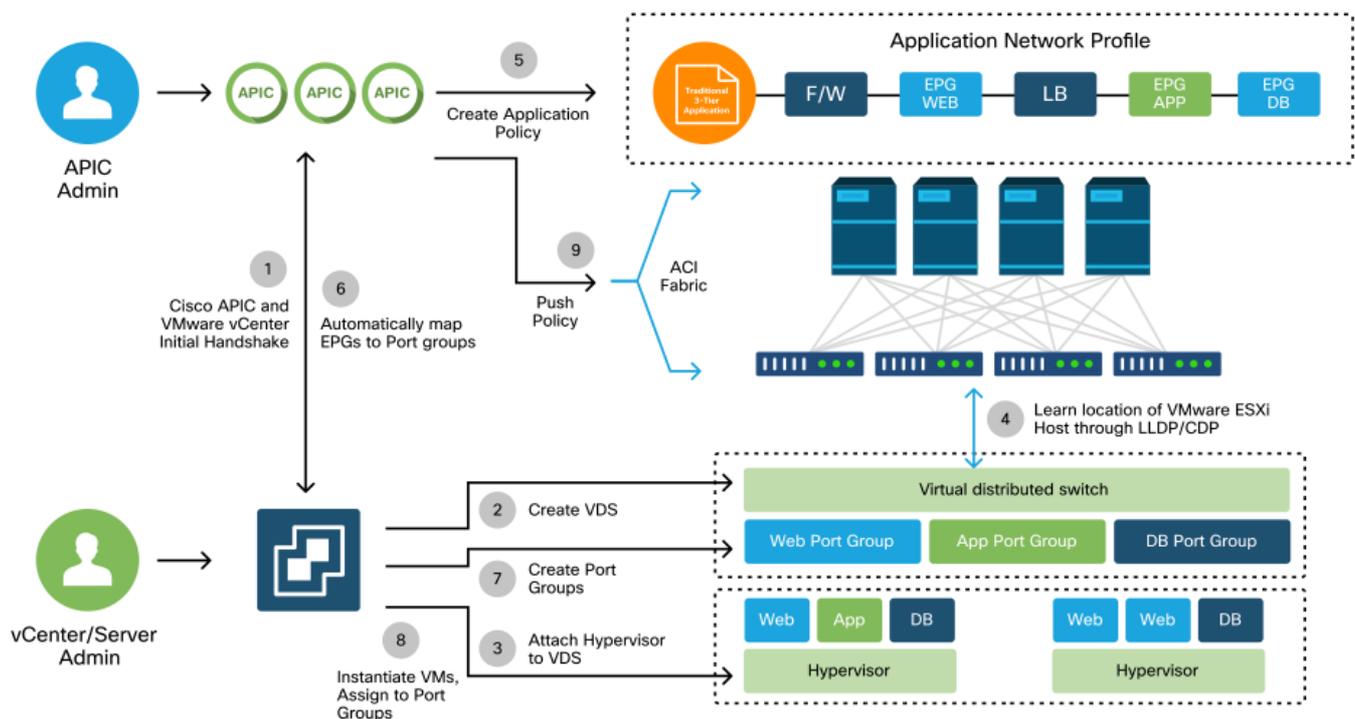
Wenn Sie also eine VMM-Domäne erstellen, stellen Sie sicher, dass Sie die richtige DVS-Version auswählen, sodass die erforderlichen ESXi-Server zum DVS hinzugefügt werden können.

Dynamische Host-Erkennung

Host-/VM-Erkennungsprozess

Die VMM-Integration in der ACI unterscheidet sich insofern von der manuellen Bereitstellung, als die Fabric dynamisch ermitteln kann, wo Hosts und entsprechende virtuelle Systeme verbunden sind, um Richtlinien effizient bereitzustellen. Durch diesen dynamischen Prozess kann die ACI die Auslastung der Hardwareressourcen auf den Leaf-Switches optimieren, da VLANs, SVIs, Zoning-Regeln usw. nur auf Knoten bereitgestellt werden, wenn ein Endpunkt angeschlossen ist, der die Richtlinie erfordert. Der Vorteil für den Netzwerkadministrator in Bezug auf die Benutzerfreundlichkeit besteht darin, dass die ACI VLAN/Richtlinien bereitstellt, über die VMs automatisch eine Verbindung herstellen. Um zu bestimmen, wo Richtlinien bereitgestellt werden müssen, verwendet der APIC Informationen aus mehreren Quellen. Im folgenden Diagramm werden die grundlegenden Schritte des Host-Erkennungsprozesses bei Verwendung einer DVS-basierten VMM-Domäne beschrieben.

VMWare VMM-Domäne - Bereitstellungs-Workflow



Kurz gesagt, die folgenden wichtigen Schritte werden ausgeführt, wenn:

- LLDP oder CDP wird zwischen Hypervisor- und Leaf-Switches ausgetauscht.
- Hosts melden Adjacency-Informationen an vCenter.
- vCenter informiert den APIC über Adjacency-Informationen: Der APIC erkennt den Host über eine Bestandssynchronisierung.
- Der APIC überträgt die Richtlinie an den Leaf-Port: Lesen Sie den Unterabschnitt "Behebungssofortigkeit" in diesem Abschnitt, um diese Bedingungen besser zu verstehen.
- Wenn die vCenter-Adjacency-Informationen verloren gehen, kann der APIC die Richtlinie entfernen.

Wie Sie sehen, spielt CDP/LLDP eine Schlüsselrolle beim Erkennungsprozess, und es ist wichtig, sicherzustellen, dass dies ordnungsgemäß konfiguriert ist und beide Seiten dasselbe Protokoll verwenden.

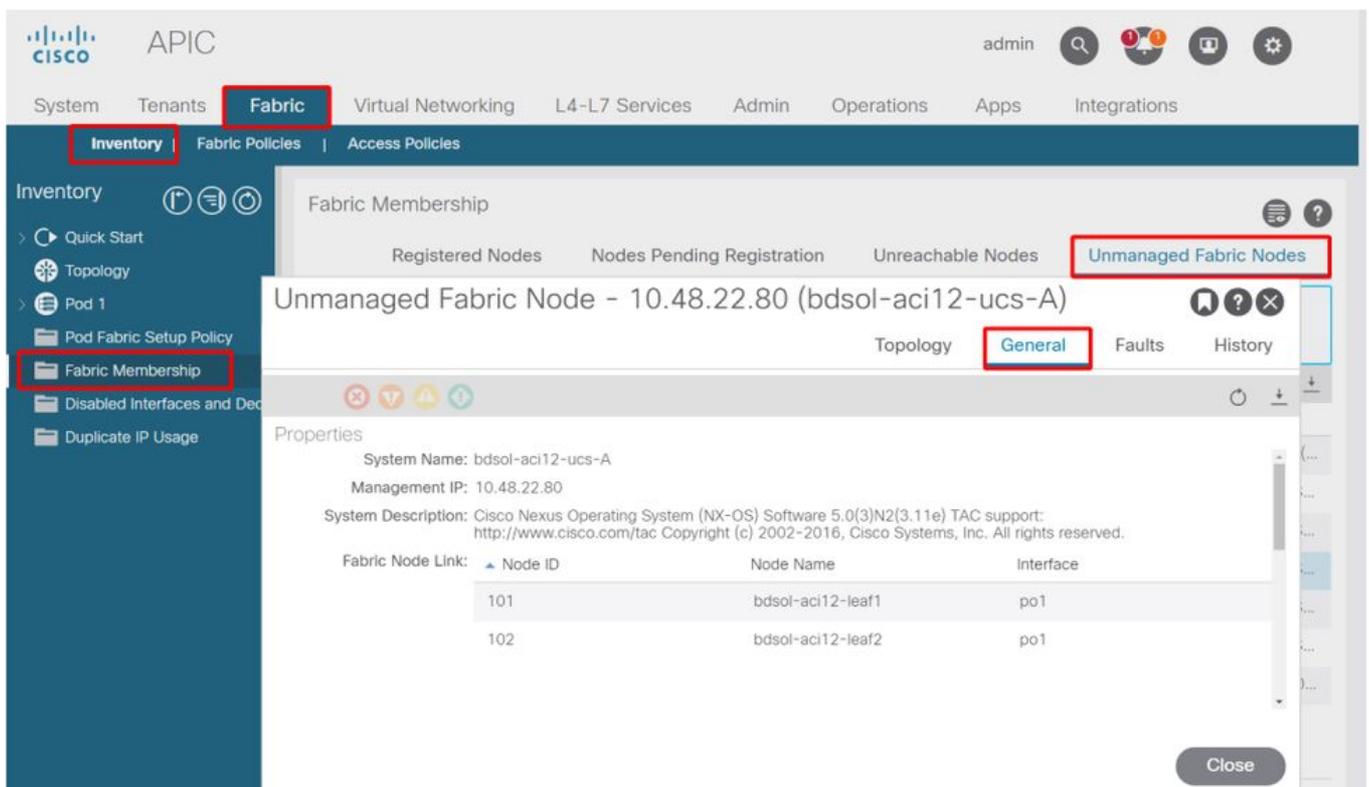
Fabric LooseNode/Intermediate Switch - Anwendungsfall

Bei einer Bereitstellung mit einem Blade-Chassis und einem dazwischen liegenden Switch

zwischen den Leaf-Switches und dem Hypervisor muss der APIC die Adjacency zusammenfügen. In diesem Szenario können mehrere Discovery-Protokolle verwendet werden, da der zwischengeschaltete Switch möglicherweise andere Protokollanforderungen als der Host hat.

In einer Konfiguration mit einem Blade-Server und einem Zwischen-Switch (d. h. Blade-Chassis-Switch) sollte die ACI den Zwischen-Switch erkennen und die dahinter liegenden Hypervisoren zuordnen. Der Zwischen-Switch wird in der ACI als LooseNode oder als "Unmanaged Fabric Node" bezeichnet. Die erkannten LooseNodes können unter "Fabric > Inventory > Fabric Membership > Unmanaged Fabric Nodes" (Fabric > Bestand > Fabric-Mitgliedschaft > Unmanaged Fabric Nodes) angezeigt werden. Wenn der Benutzer in der GUI zu einem dieser Servertypen navigiert, kann er den Pfad vom Leaf zu einem Zwischenswitch zum Host anzeigen.

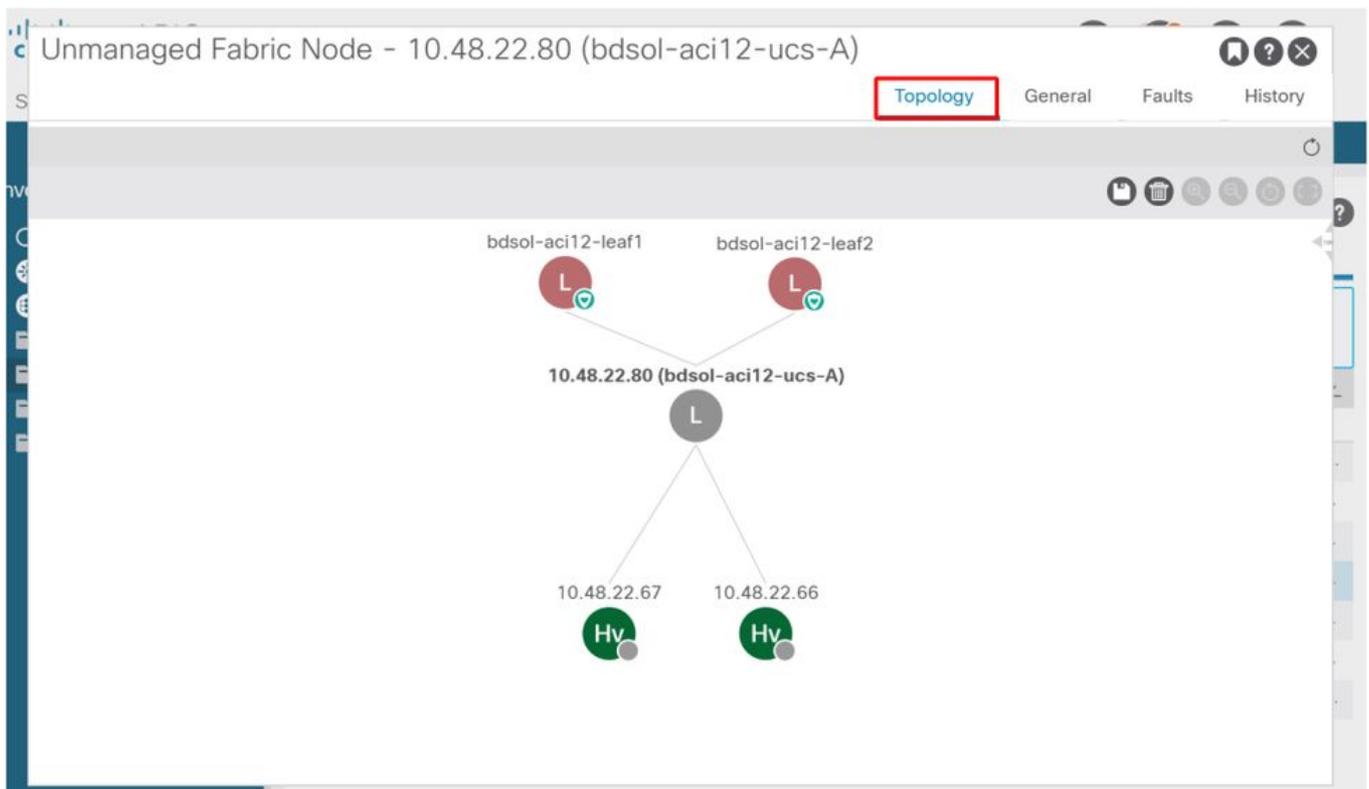
APIC-Benutzeroberfläche - Unmanaged Fabric Nodes (LooseNodes)



Mit der LLDP- oder CDP-Erkennung kann die ACI die Topologie für solche LooseNodes ermitteln, da der dem Zwischen-Switch nachgeschaltete Hypervisor durch VMM-Integration verwaltet wird und das Leaf selbst über eine Adjacency zum Zwischen-Switch vom Downstream verfügt.

Dieses Konzept wird in der folgenden Abbildung veranschaulicht.

APIC-Benutzeroberfläche - nicht verwalteter Fabric-Knotenpfad

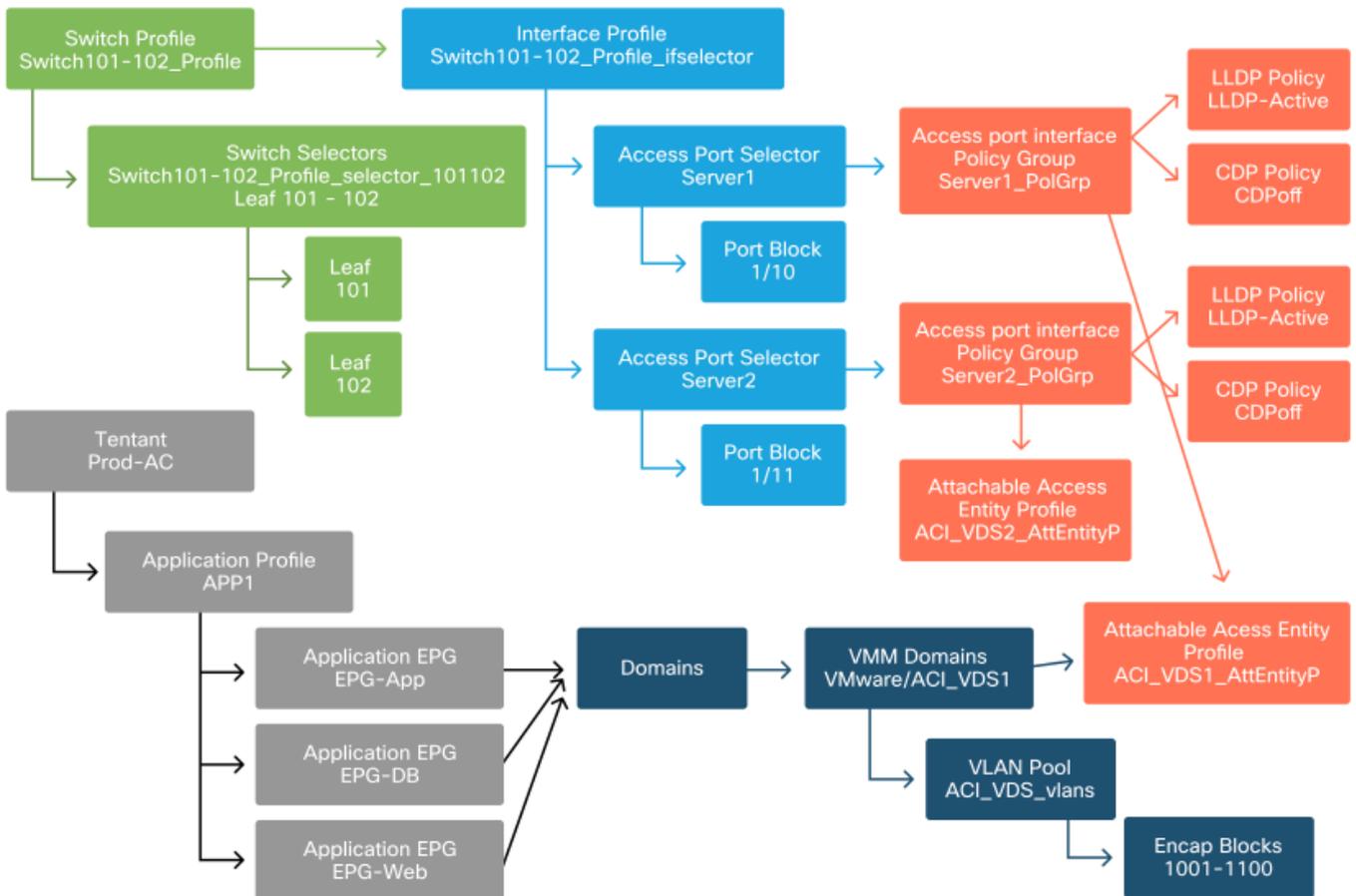


Behebungssofortigkeit

In Szenarien, in denen kritische Services den in VMM integrierten DVS nutzen, z. B. für die Managementverbindung zu vCenter/ESXi, ist es ratsam, die Vorabentscheidungs-Lösungsinstanz zu verwenden. Bei dieser Einstellung wird der Mechanismus der dynamischen Hosterkennung entfernt, und stattdessen werden Richtlinien/VLANs statisch auf den Schnittstellen zum Host programmiert. In dieser Konfiguration werden die VMM-VLANs immer an allen Schnittstellen bereitgestellt, die mit dem AEP verbunden sind, auf den von der VMM-Domäne verwiesen wird. Dadurch wird die Möglichkeit ausgeschlossen, dass ein kritisches VLAN (z. B. die Verwaltung) aufgrund eines Adjacency-Ereignisses, das sich auf das Erkennungsprotokoll bezieht, von einem Port entfernt wird.

Siehe nachfolgendes Diagramm:

Bereitstellungsbeispiel vor der Bereitstellung



Wenn die Vorabbereitstellung für eine EPG in der ACI_VDS1 VMM-Domäne festgelegt wurde, würden VLANs auf den Verbindungen für Server1, aber nicht für Server2 bereitgestellt, da der AEP von Server2 die ACI_VDS1 VMM-Domäne nicht enthält.

So fassen Sie die Einstellungen für die Unmittelbarkeit der Auflösung zusammen:

- On-Demand - Die Richtlinie wird bereitgestellt, wenn eine Adjacency zwischen Leaf und Host und einem mit der Portgruppe verbundenen virtuellen System eingerichtet wird.
- Immediate (Sofort) - Die Richtlinie wird bereitgestellt, wenn eine Adjacency zwischen Leaf und Host hergestellt wird.
- Vorabbereitstellung - Die Richtlinie wird auf allen Ports bereitgestellt, die einen AEP mit enthaltener VMM-Domäne verwenden. Eine Adjacency ist nicht erforderlich.

Fehlerbehebungsszenarien

VM kann ARP für das Standard-Gateway nicht auflösen

In diesem Szenario wurde die VMM-Integration konfiguriert, und der DVS wurde dem Hypervisor hinzugefügt, aber das virtuelle System kann ARP für sein Gateway in der ACI nicht lösen. Damit das virtuelle System über Netzwerkverbindungen verfügt, müssen Sie sicherstellen, dass sich die Adjacency eingerichtet hat und VLANs bereitgestellt sind.

Zunächst kann der Benutzer überprüfen, ob das Leaf den Host erkannt hat, indem er je nach gewähltem Protokoll 'show lldp neighbors' oder 'show cdp neighbors' auf dem Leaf verwendet.

```
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
```

Falls dies aus Gründen der Fehlerbehebung erforderlich ist, kann dies von ESXi-Seite sowohl in der CLI als auch in der GUI validiert werden:

```
[root@host:~] esxcli network vswitch dvs vmware list
```

```
VDS_Sitel
```

```
Name: VDS_Sitel
```

```
...
```

```
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 VIC Ethernet NIC
vmnic7	0000:0a:00.0	enic	Up	10000Mbps	Full	4c:77:6d:49:cf:31	9000	Cisco Systems Inc Cisco VIC Ethernet NIC

```
[root@host:~] vim-cmd hostsvc/net/query_networkhint --pnuc-name=vmnic6 | grep -A2 "System Name"
```

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

```
value = "Leaf101"
```

```
}
```

vCenter-Web-Client - Host - vmnic LLDP/CDP-Adjacency-Details

All	Properties	CDP	LLDP
Link Layer Discovery Protocol			
Chassis ID			00:3a:9c:45:12:6b
Port ID			Eth1/11
Time to live			109
TimeOut			60
Samples			437068
Management Address			10.48.176.70
Port Description			topology/pod-1/paths-101/pathep-[eth1/11]
System Description			topology/pod-1/node-101
System Name			S1P1-Leaf101
Peer device capability			
Router			Enabled
Transparent bridge			Enabled
Source route bridge			Disabled
Network switch			Disabled
Host			Disabled
IGMP			Disabled
Repeater			Disabled

Wenn die Leaf-LLDP-Adjacency vom ESXi-Host nicht erkannt werden kann, wird dies häufig durch die Verwendung eines Netzwerkadapters verursacht, der so konfiguriert ist, dass er statt des ESXi-Betriebssystems LLDPDUs generiert. Überprüfen Sie, ob auf dem Netzwerkadapter LLDP aktiviert ist und daher alle LLDP-Informationen verwendet werden. Wenn dies der Fall ist, deaktivieren Sie LLDP auf dem Adapter selbst, sodass die Steuerung über die vSwitch-Richtlinie erfolgt.

Ein weiterer Grund kann darin bestehen, dass die Erkennungsprotokolle zwischen Leaf und ESXi-Hypervisor falsch ausgerichtet sind. Vergewissern Sie sich, dass Sie auf beiden Seiten dasselbe Erkennungsprotokoll verwenden.

Um zu überprüfen, ob die CDP-/LLDP-Einstellungen zwischen der ACI und dem DVS in der APIC-Benutzeroberfläche übereinstimmen, navigieren Sie zu Virtual Networking > VMM Domains > VMWare > Policy > vSwitch Policy. Aktivieren Sie nur die LLDP- oder CDP-Richtlinien, da diese sich gegenseitig ausschließen.

APIC-Benutzeroberfläche - VMWare VMM-Domäne - vSwitch-Richtlinie

Properties

Port Channel Policy:	VDS_lacpLagPol	▼	🔗
LLDP Policy:	LLDP_enabled	▼	🔗
CDP Policy:	CDP_disabled	▼	🔗
NetFlow Exporter Policy:	select an option	▼	

Gehen Sie in vCenter zu: "Networking > VDS > Configure" (Netzwerk > VDS > Konfigurieren).

vCenter-Webclient-Benutzeroberfläche - VDS-Eigenschaften

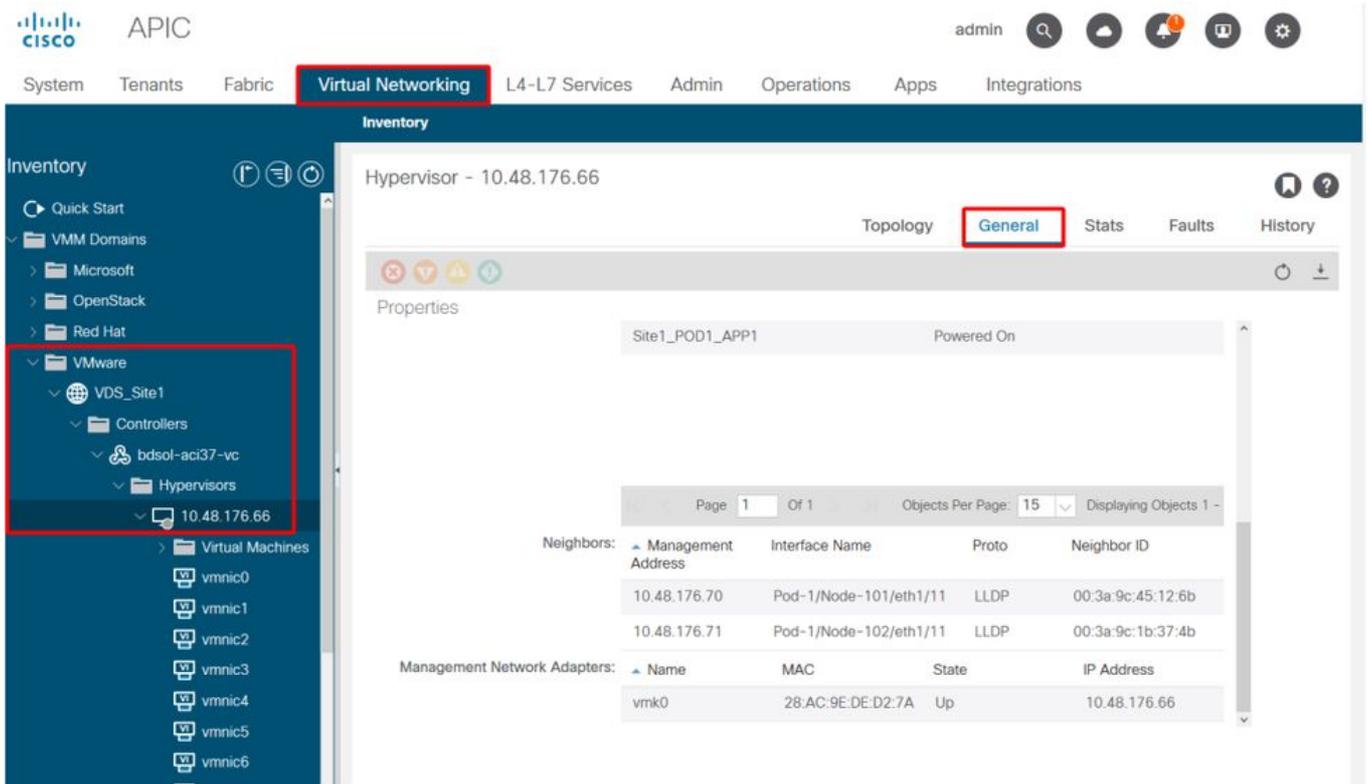
The screenshot shows the vCenter Webclient interface. On the left is a navigation sidebar with a tree view containing: Settings, Properties (selected), Topology, Private VLAN, NetFlow, Port mirroring, Health check, More, Network Protocol Profiles, and Resource Allocation. The main content area is titled 'Properties' and contains the following configuration details:

General	
Name:	VDS_Site1
Manufacturer:	VMware, Inc.
Version:	6.0.0
Number of uplinks:	8
Number of ports:	24
Network I/O Control:	Disabled
Description:	
APIC Virtual Switch	
Advanced	
MTU:	9000 Bytes
Multicast filtering mode:	Basic
Discovery protocol	
Type:	Link Layer Discovery Protocol
Operation:	Both
Administrator contact	
Name:	
Other details:	

Korrigieren Sie ggf. die LLDP-/CDP-Einstellungen.

Validieren Sie anschließend, ob der APIC die LLDP/CDP-Nachbarschaft des ESXi-Hosts in der UI unter "Virtual Networking > VMM Domains > VMWare > Policy > Controller > Hypervisor > General" (Virtuelles Netzwerk > VMM-Domänen > Richtlinie > Hypervisor > Allgemein) mit dem Leaf-Switch vergleicht.

APIC-Benutzeroberfläche - VMWare VMM-Domäne - Hypervisor-Details



Wenn hier erwartete Werte angezeigt werden, kann der Benutzer überprüfen, ob das VLAN am Port zum Host vorhanden ist.

```
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-Management VMK verbunden mit APIC-gestütztem DVS

In einem Szenario, in dem der vCenter- oder ESXi-Verwaltungsdatenverkehr den integrierten VMM-DVS nutzen muss, muss besonders darauf geachtet werden, dass die Aktivierung der dynamischen Adjacencies und die Aktivierung der erforderlichen VLANs nicht zu einem Stillstand kommt.

Für vCenter, das normalerweise vor der Konfiguration der VMM-Integration erstellt wird, ist es wichtig, eine physische Domäne und einen statischen Pfad zu verwenden, um sicherzustellen, dass das Encap-VLAN des vCenter-virtuellen Systems immer auf den Leaf-Switches programmiert ist, damit es verwendet werden kann, bevor die VMM-Integration vollständig eingerichtet ist. Es wird empfohlen, diesen statischen Pfad auch nach der Einrichtung der VMM-Integration beizubehalten, um die Verfügbarkeit dieser EPG stets sicherzustellen.

Bei ESXi-Hypervisoren muss gemäß dem "Cisco ACI Virtualization Guide" unter Cisco.com bei der Migration auf den vDS sichergestellt werden, dass die EPG, mit der die VMK-Schnittstelle verbunden wird, mit der Auflösungssofortigkeit "Pre-provision" bereitgestellt wird. Dadurch wird sichergestellt, dass das VLAN immer auf den Leaf-Switches programmiert ist, ohne dass die ESXi-Hosts mithilfe von LLDP/CDP erkannt werden müssen.

Unbekannte Host-Adjacencies hinter LooseNode

Typische Ursachen für Probleme bei der LooseNode-Erkennung sind:

- CDP/LLDP ist nicht aktiviert. CDP/LLDP muss zwischen dem zwischengeschalteten Switch, den Leaf-Switches und den ESXi-Hosts ausgetauscht werden. Für das Cisco UCS erfolgt dies über eine Netzwerksteuerungsrichtlinie auf der vNIC.
- Eine Änderung der Management-IP des LLDP/CDP-Nachbarn unterbricht die Verbindung. Das vCenter erkennt die neue Management-IP in der LLDP/CDP-Adjacency, aktualisiert den APIC jedoch nicht. Manuelle Bestandssynchronisierung auslösen, um Probleme zu beheben
- VMM-VLANs werden dem zwischengeschalteten Switch nicht hinzugefügt. Der APIC programmiert keine Blade-/Zwischenswitches von Drittanbietern. Die Cisco UCSM-Integrations-App (ExternalSwitch) ist in Version 4.1(1) verfügbar. VLANs müssen konfiguriert und mit Uplinks, die mit ACI-Leaf-Knoten verbunden sind, sowie Downlinks, die mit Hosts verbunden sind, verbunden werden.

F606391 - Fehlende Adjacencies für den physischen Adapter auf dem Host

Wenn Sie den Fehler unten sehen:

```
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: bdsol-aci20-os3 (TASK:ifc:vmmmgr:CompHvGetHpNicAdj)
```

Überprüfen Sie den Workflow im Abschnitt "Das virtuelle System kann ARP nicht für sein Standard-Gateway auflösen", da CDP/LLDP-Nachbarschaften fehlen. Diese Adjacencies müssen durchgängig überprüft werden.

Hypervisor-Uplink-Lastenausgleich

Wenn Hypervisoren wie ESXi mit einer ACI-Fabric verbunden werden, werden sie in der Regel über mehrere Uplinks verbunden. Es wird empfohlen, einen ESXi-Host mit mindestens zwei Leaf-Switches zu verbinden. Dadurch werden die Auswirkungen von Fehlerszenarien oder Upgrades minimiert.

Um die Nutzung von Uplinks durch die auf einem Hypervisor ausgeführten Workloads zu optimieren, können mit VMware vCenter-Konfigurationen mehrere Load Balancing-Algorithmen für den von VM generierten Datenverkehr zu den Uplinks des Hypervisors konfiguriert werden.

Alle Hypervisoren und die ACI-Fabric müssen mit demselben Load Balancing-Algorithmus konfiguriert sein, um die korrekte Anbindung sicherzustellen. Andernfalls kann es zu unregelmäßigen Datenverkehrsverlusten und Verschiebungen von Endpunkten in der ACI-Fabric kommen.

Dies wird in einer ACI-Fabric durch übermäßige Warnungen wie die folgenden deutlich:

```
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

In diesem Kapitel wird die VMware ESXi-Host-Konnektivität mit der ACI behandelt. Dies gilt jedoch für die meisten Hypervisoren.

Rack-Server

Wenn Sie die verschiedenen Verbindungsmöglichkeiten eines ESXi-Hosts zu einer ACI-Fabric betrachten, werden diese in zwei Gruppen unterteilt: Switch-abhängig und Switch-unabhängige Lastenausgleichsalgorithmen.

Switch-unabhängige Lastenausgleichsalgorithmen sind Verbindungsmöglichkeiten, für die keine spezielle Switch-Konfiguration erforderlich ist. Für den Switch-abhängigen Lastenausgleich sind Switch-spezifische Konfigurationen erforderlich.

Überprüfen Sie, ob die vSwitch-Richtlinie mit den Anforderungen der ACI-Zugriffsrichtliniengruppe übereinstimmt (siehe Tabelle unten).

Teaming- und ACI vSwitch-Richtlinie

VMware Teaming- und Failover-Modus	ACI vSwitch-Richtlinie	Beschreibung	ACI-Zugriffsrichtliniengruppe - Port-Channel erforderlich
Routenbasiert auf dem virtuellen Ausgangs-Port	MAC Pinning	Wählen Sie einen Uplink basierend auf den virtuellen Port-IDs am Switch aus. Nachdem der virtuelle Switch einen Uplink für eine virtuelle Maschine oder einen VMKernel-Adapter ausgewählt hat, leitet er Datenverkehr immer über denselben Uplink für diese virtuelle Maschine oder diesen VMKernel-Adapter weiter.	Nein
Routenbasiert auf Quell-MAC-Hash	NA	Wählen Sie einen Uplink basierend auf einem Hash der Quell-MAC-Adresse aus.	NA
Explizite Failover-Reihenfolge	Expliziten Failover-Modus verwenden	Verwenden Sie aus der Liste der aktiven Adapter immer den Uplink höchster Ordnung, der die Failover-Erkennungskriterien erfüllt. Mit dieser Option wird kein tatsächlicher Lastenausgleich durchgeführt.	Nein
Link Aggregation (LAG) - IP Hash-basiert	Statischer Kanal - Modus Ein	Wählen Sie einen Uplink basierend auf einem Hash der Quell- und Ziel-IP-Adressen jedes Pakets aus. Bei Nicht-IP-Paketen verwendet der Switch die Daten in diesen Feldern, um den Hash zu berechnen. Für IP-basiertes Teaming muss auf Seiten der ACI ein Port-	Ja (Kanalmodus auf 'on' eingestellt)

Link Aggregation (LAG) - LACP

LACP aktiv/passiv

Channel/VPC mit dem Modus "on" (Ein) konfiguriert werden.

Wählen Sie einen Uplink basierend auf einem ausgewählten Hash aus (20 verschiedene Hash-Optionen sind verfügbar). Für LACP-basiertes Teaming Ja muss auf Seiten der ACI ein Port-Channel/VPC mit aktiviertem LACP konfiguriert werden. Stellen Sie sicher, dass Sie in der ACI eine erweiterte Richtlinie für Verzögerungen erstellen und auf die VSwitch-Richtlinie anwenden.

(Kanalmodus auf 'LACP Active/Passive' eingestellt)

Routenbasiert auf physischer NIC-Last (LBT) MAC Pinning - Laden physischer NICs

Verfügbar für verteilte Portgruppen oder verteilte Ports. Wählen Sie einen Uplink basierend auf der aktuellen Last der physischen Netzwerkadapter aus, die mit der Portgruppe oder dem Port verbunden sind. Wenn ein Uplink mit 75 Prozent oder mehr 30 Sekunden lang belegt bleibt, verlagert der vSwitch des Hosts einen Teil des Datenverkehrs des virtuellen Systems auf einen physischen Adapter mit freier Kapazität.

Im Screenshot unten wird gezeigt, wie die Port-Channel-Richtlinie im Rahmen der vorhandenen vSwitch-Richtlinie validiert wird.

ACI vSwitch-Richtlinie - Port-Channel-Richtlinie

The screenshot displays the Cisco APIC web interface. The top navigation bar includes 'System', 'Tenants', 'Fabric', 'Virtual Networking' (highlighted with a red box), 'L4-L7 Services', 'Admin', 'Operations', 'Apps', and 'Integrations'. The left sidebar shows a tree view with 'VMware' and 'VDS_Site1' highlighted. The main content area shows the configuration for 'Domain - VDS_Site1'. A 'Port Channel Policy - VDS_lacpLagPol' window is open, showing a 'Properties' section with a dropdown menu for 'Mode' set to 'MAC Pinning'. Other options include 'Static Channel - Mode' (On), 'LACP Active', 'LACP Passive', 'MAC Pinning-Physical-NIC-load', and 'Use Explicit Failover Order'. The 'VSwitch Policy' tab is also visible in the background.

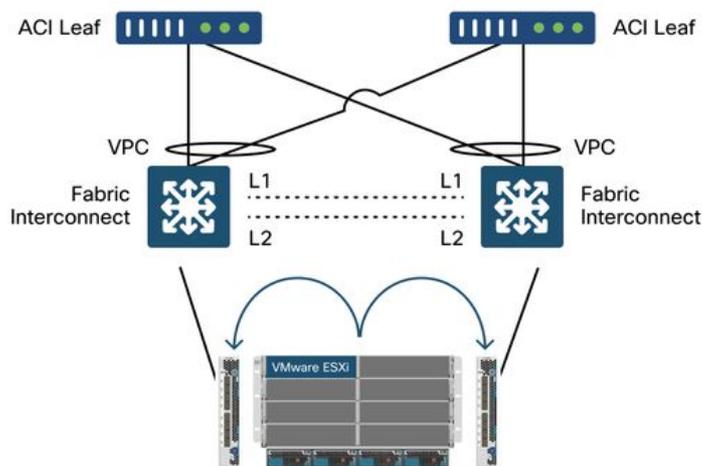
Hinweis: Eine ausführliche Beschreibung der VMware-Netzwerkfunktionen finden Sie unter vSphere Networking unter <https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.networking.doc/GUID-D34B1ADD-B8A7-43CD-AA7E-2832A0F7EE76.html>

Anwendungsfall der Cisco UCS B-Serie

Bei der Verwendung von Cisco UCS Servern der B-Serie müssen Sie darauf achten, dass diese innerhalb ihres Chassis mit UCS Fabric Interconnects (FIs) verbunden sind, die über kein einheitliches Datenflugzeug verfügen. Dieser Anwendungsfall gilt auch für andere Anbieter mit einer ähnlichen Topologie. Aus diesem Grund kann ein Unterschied zwischen der Lastverteilungsmethode auf Seiten der ACI-Leaf-Switches und der vSwitch-Seite bestehen.

Nachfolgend finden Sie eine UCS FI-Topologie mit ACI:

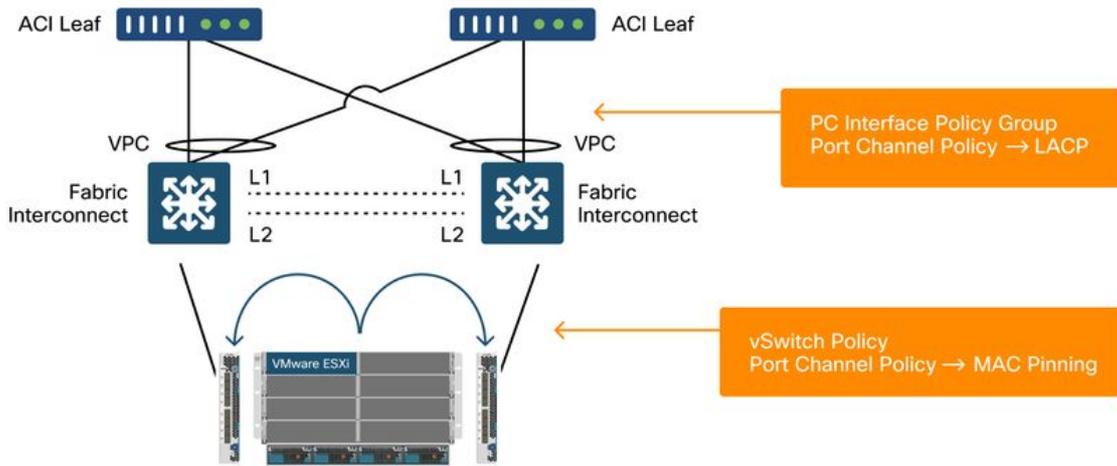
Cisco UCS FI mit ACI-Leaf-Switches - Topologie



Wichtige Punkte:

- Jede Cisco UCS FI verfügt über einen Port-Channel zu den ACI-Leaf-Switches.
- Die UCS FIs sind nur für Heartbeat-Zwecke direkt miteinander verbunden (nicht für Datenflugzeuge verwendet).
- Die vNIC jedes Blade-Servers ist an ein bestimmtes UCS FI gebunden oder verwendet einen Pfad zu einem FI mithilfe von UCS Fabric Failover (Aktiv/Standby).
- Die Verwendung von IP-Hash-Algorithmen auf dem vSwitch des ESXi-Hosts verursacht MAC-Flaps auf den UCS-FIs.

Gehen Sie folgendermaßen vor, um die Konfiguration korrekt durchzuführen:



Wenn MAC Pinning in der Port-Channel-Richtlinie als Teil der vSwitch-Richtlinie in der ACI konfiguriert ist, wird dies als Teaming-Konfiguration der Portgruppen auf dem VDS für "Route based on the original virtual port" angezeigt.

ACI - Port-Channel-Richtlinie als Teil der vSwitch-Richtlinie

The screenshot shows the APIC web interface. The 'Virtual Networking' tab is selected. The 'Inventory' section shows 'Domain - VDS_Site1'. The 'Port Channel Policy - VDS_lacpLagPol' configuration is displayed, with 'Mode' set to 'MAC Pinning', 'Minimum Number of Links' set to 1, and 'Maximum Number of Links' set to 16.

Die im obigen Beispiel verwendete Port-Channel-Richtlinie wird vom Assistenten automatisch benannt. Daher heißt sie "CDS_lacpLagPol", obwohl der Modus "MAC Pinning" verwendet wird.

VMware vCenter - ACI VDS - Portgruppe - Lastenausgleichseinstellung

vmware vSphere Web Client

Getting Started Summary Monitor **Configure** Permissions Ports Hosts VMs

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

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