Dépannage de l'intégration ACI VMM

Table des matières

Introduction

Ce document décrit les étapes à suivre pour comprendre et dépanner l'intégration VMM (Virtual Machine Manager Integration) de l'ACI.

Informations générales

Le contenu de ce document a été extrait du livre Troubleshooting Cisco Application Centric Infrastructure, Second Edition (Dépannage de l'infrastructure axée sur les applications Cisco, deuxième édition), en particulier les chapitres VMM Integration - Overview, VMM Integration - vCenter Connectivity, VMM Integration - Host Dynamic Discovery et VMM Integration - Hypervisor Uplink Load Balancing.

Présentation de Virtual Machine Manager

Les contrôleurs ACI peuvent s'intégrer à des gestionnaires de machines virtuelles (VMM) tiers.

Il s'agit de l'une des fonctions clés de l'ACI, car elle simplifie et automatise les opérations de configuration réseau de bout en bout du fabric et des charges de travail qui s'y connectent. L'ACI offre un modèle de politique de superposition unique qui peut être étendu à plusieurs types de charges de travail, c'est-à-dire les machines virtuelles, les serveurs sans système d'exploitation et les conteneurs.

Ce chapitre porte plus particulièrement sur certains scénarios de dépannage classiques liés à l'intégration de VMware vCenter VMM.

Le lecteur passera en revue les points suivants :

- Enquête sur les défaillances de communication vCenter.
- Processus de découverte dynamique des hôtes et des VM et scénarios de panne.
- Algorithmes d'équilibrage de charge hyperviseur.

connectivité vCenter

Contrôle d'accès basé sur les rôles (RBAC)

Les mécanismes par lesquels le contrôleur APIC peut interagir avec le contrôleur vCenter dépendent du compte d'utilisateur associé à un domaine VMM donné. Des exigences spécifiques sont définies pour l'utilisateur vCenter associé au domaine VMM afin de s'assurer que le contrôleur APIC peut effectuer des opérations sur le vCenter, qu'il procède à la diffusion et à la récupération d'inventaire et de configurations ou qu'il surveille et écoute les événements liés à l'inventaire géré.

Le moyen le plus simple de dissiper les inquiétudes liées à ces exigences consiste à utiliser le compte vCenter de l'administrateur qui dispose d'un accès complet. Toutefois, ce type de liberté n'est pas toujours disponible pour l'administrateur de l'ACI.

Les privilèges minimaux d'un compte utilisateur personnalisé, à partir de la version 4.2 de l'ACI, sont les suivants :

- Alarmes

    - Le contrôleur APIC crée deux alarmes sur le dossier. Un pour DVS et un autre pour le groupe de ports. Une alarme se déclenche lorsque la politique de domaine EPG ou VMM est supprimée sur le contrôleur APIC. Toutefois, vCenter ne peut pas supprimer le groupe de ports ou le DVS correspondant en raison de l'association de machines virtuelles.
- Commutateur distribué
- Groupe dvPort
- Dossier
- Réseau
    - Le contrôleur APIC gère les paramètres réseau tels que l'ajout ou la suppression de groupes de ports, la définition de MTU hôte/DVS, LLDP/CDP, LACP, etc.
- Hôte
    - Si vous utilisez AVS en plus de ce qui précède, l'utilisateur a besoin du privilège Hôte sur le centre de données où APIC va créer DVS.
    - Hôte.Configuration.Paramètres avancés
    - Hôte.Opérations locales.Reconfigurer la machine virtuelle
    - Hôte.Configuration.Configuration du réseau
    - Cela est nécessaire pour AVS et la fonction de placement automatique pour les machines virtuelles de service de couche 4 à couche 7 virtuelles. Pour AVS, APIC crée une interface VMK et la place dans le groupe de ports VTEP utilisé pour OpFlex.
- Machine virtuelle
    - Si des graphiques de services sont utilisés, le privilège de machine virtuelle pour les appliances virtuelles est également requis.
    - Machine virtuelle.Configuration.Modifier les paramètres du périphérique
    - Machine virtuelle.Configuration.Settings

Dépannage des problèmes liés au RBAC

Les problèmes RBAC sont le plus souvent rencontrés lors de la configuration initiale d'un domaine VMM, mais ils pourraient se produire si un administrateur vCenter modifiait les autorisations du compte d'utilisateur associé au domaine VMM après la configuration initiale.

Le symptôme peut se présenter de la manière suivante :

- Incapacité partielle ou complète de déployer de nouveaux services (création de DVS, création de groupes de ports, certains objets ont été déployés avec succès, mais pas tous).
- L'inventaire opérationnel est incomplet ou manquant dans les vues de l'administrateur ACI.
- Défaillances survenues pour un fonctionnement vCenter non pris en charge ou pour l'un des scénarios ci-dessus (par exemple, une défaillance de déploiement de groupe de ports).
- Le contrôleur vCenter est signalé comme étant hors ligne et des défaillances indiquent des problèmes de connectivité ou d'informations d'identification.

Solution pour les problèmes liés au RBAC

Vérifiez que toutes les autorisations ci-dessus sont accordées à l'utilisateur vCenter configuré dans le domaine VMM.

Une autre méthode consiste à se connecter directement au vCenter avec les mêmes informations d'identification que celles définies dans la configuration du domaine VMM et à tenter des opérations similaires (création de groupes de ports, etc.). Si l'utilisateur n'est pas en mesure d'effectuer ces mêmes opérations lorsqu'il est connecté directement à vCenter, il est clair que les autorisations correctes ne lui sont pas accordées.

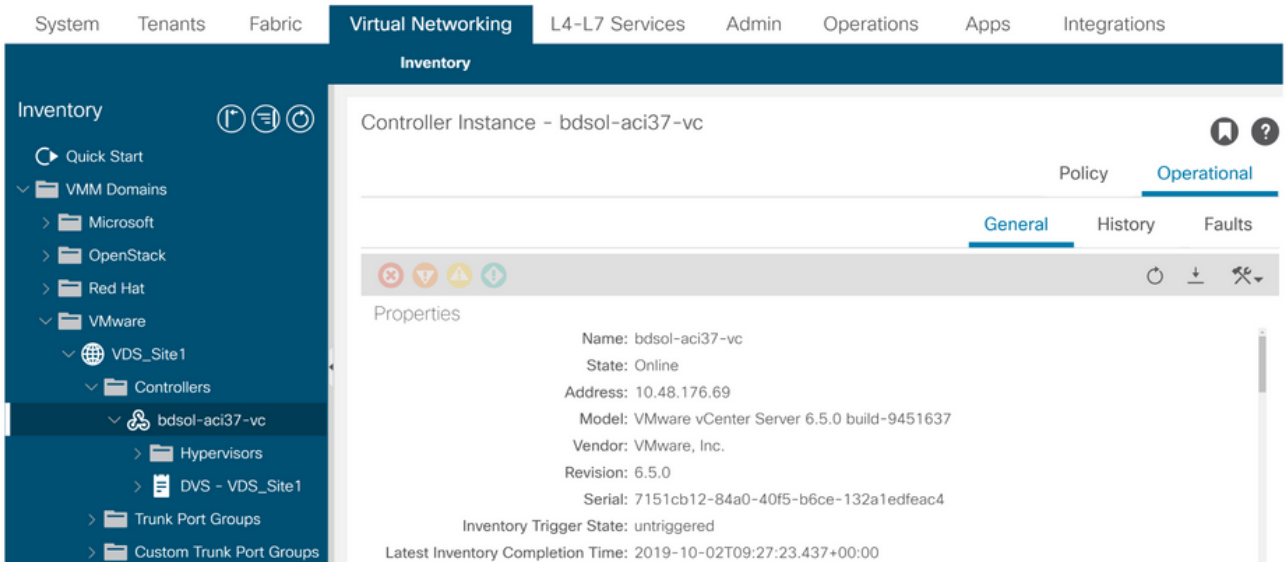
Dépannage de la connectivité

Lors du dépannage d'un problème de connectivité VMM, il est important de noter certains des comportements fondamentaux de la communication de l'ACI avec vCenter.

Le premier et le plus pertinent est qu'un seul contrôleur APIC dans le cluster envoie des informations de configuration et collecte des données d'inventaire à un point donné. Ce contrôleur APIC est désigné comme le leader partagé pour ce domaine VMM. Cependant, plusieurs APIC sont à l'écoute des événements vCenter afin de prendre en compte un scénario où le leader partagé a manqué un événement pour une raison quelconque. En suivant la même architecture distribuée de cartes APIC, un domaine VMM donné aura une carte APIC gérant les données et fonctionnalités principales (dans ce cas, le leader partagé) et deux réplicas (dans le cas de VMM, ils sont appelés suiveurs). Pour répartir la gestion de la communication et des fonctionnalités VMM entre les cartes APIC, deux domaines VMM peuvent avoir le même ou des identifiants partagés différents.

L'état de connectivité de vCenter peut être trouvé en naviguant jusqu'au contrôleur VMM concerné dans l'interface utilisateur graphique ou en utilisant la commande CLI répertoriée ci-dessous.

Domaine VMWare VMM - état de connectivité vCenter



<#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
```

Si un contrôleur VMM est indiqué comme étant hors ligne, une défaillance se produira de la manière suivante :

```
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
```

Les étapes ci-dessous peuvent être utilisées pour résoudre les problèmes de connectivité entre les circuits virtuels et les cartes APIC.

1. Identification du leader partagé

La première étape du dépannage d'un problème de connectivité entre le contrôleur APIC et vCenter consiste à déterminer quel contrôleur APIC est le leader partagé pour le domaine VMM donné. La façon la plus simple de déterminer ces informations est d'exécuter la commande « show vmware domain name <domain> » sur n'importe quel APIC.

<#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. Vérification de la connectivité à vCenter

Après avoir identifié le contrôleur APIC qui communique activement avec le vCenter, vérifiez la connectivité IP à l'aide d'outils tels que 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
```

Si le vCenter a été configuré à l'aide du nom de domaine complet plutôt que de l'adresse IP, la commande nslookup peut être utilisée pour vérifier la résolution de noms.

<#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. Vérifiez si OOB ou INB est utilisé

Consultez la table de routage APIC pour vérifier si la connectivité est privilégiée en mode hors bande ou en mode intrabande et pour savoir quelle passerelle est utilisée :

<#root>

```
apic1#
```

bash

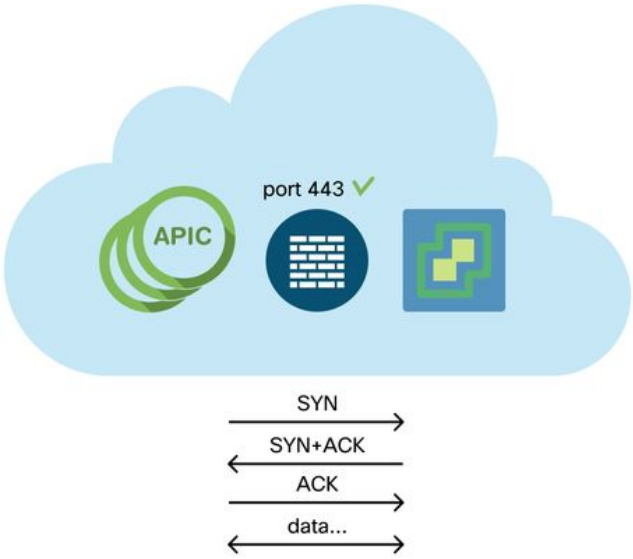
```
admin@apic1:~>
```

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. Assurez-vous que le port 443 est autorisé entre tous les APIC et le vCenter, y compris les pare-feu dans le chemin de communication.

vCenter <-> APIC - HTTPS (port TCP 443) - communication



L'accessibilité HTTPS générale des APIC vers vCenter peut être testée avec une boucle :

<#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)
...

Vérifiez que l'amorce partagée dispose d'une connexion TCP établie sur le port 443 à l'aide de la commande netstat.

<#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. Effectuer une capture de paquet

Si possible, effectuez une capture de paquets le long du chemin entre le pilote partagé et vCenter afin d'identifier si le trafic est envoyé et reçu par l'un ou l'autre périphérique.

Inventaire VMware

Le tableau suivant répertorie les paramètres VDS de VMWare et indique s'ils peuvent être configurés par le contrôleur APIC.

Paramètres VMware VDS gérés par APIC

VMware VDS	Valeur par défaut	Configurable à l'aide de la politique Cisco APIC ?
Nom	Nom de domaine VMM	Oui (Provient du domaine)
Description	'Commutateur virtuel APIC'	Non

VMware VDS	Valeur par défaut	Configurable à l'aide de la politique Cisco APIC ?
Nom du dossier	Nom de domaine VMM	Oui (Provient du domaine)
Version	Prise en charge maximale par vCenter	Oui
Protocole de découverte	protocole LLDP	Oui
Ports de liaison ascendante et noms de liaison ascendante	8	Oui (depuis Cisco APIC version 4.2(1))
Préfixe de nom de liaison ascendante	liaison montante	Oui (depuis Cisco APIC version 4.2(1))
MTU maximum	9000	Oui
politique LACP	désactivé	Oui
Mise en miroir des ports	0 session	Oui
Alarmes	2 alarmes ajoutées au niveau du dossier	Non

Le tableau suivant répertorie les paramètres du groupe de ports VDS VMWare et indique s'ils peuvent être configurés par le contrôleur APIC.

Paramètres du groupe de ports VDS VMWare gérés par APIC

Groupe de ports VMware VDS	Valeur par défaut	Configurable à l'aide de la stratégie APIC
Nom	Nom du locataire | Nom du profil d'application | Nom EPG	Oui (Provient de EPG)

Groupe de ports VMware VDS	Valeur par défaut	Configurable à l'aide de la stratégie APIC
Liaison de port	Liaison statique	Non
VLAN	Sélectionné dans le pool de VLAN	Oui
Algorithme d'équilibrage de charge	Provient de la politique de canal de port sur APIC	Oui
Mode promiscuité	Désactivé	Oui
Transmission falsifiée	Désactivé	Oui
modification MAC	Désactivé	Oui
Bloquer tous les ports	FAUX	Non

Dépannage d'inventaire VMware

Des événements de synchronisation d'inventaire se produisent pour s'assurer que le contrôleur APIC est informé des événements vCenter qui peuvent nécessiter une mise à jour dynamique de la stratégie. Deux types d'événements de synchronisation d'inventaire peuvent se produire entre vCenter et le contrôleur APIC : une synchronisation d'inventaire complète et une synchronisation d'inventaire basée sur les événements. La planification par défaut d'une synchronisation d'inventaire complète entre le contrôleur APIC et vCenter est toutes les 24 heures, mais ces synchronisations peuvent également être déclenchées manuellement. Les synchronisations d'inventaire basées sur des événements sont généralement liées à des tâches déclenchées, telles qu'un vMotion. Dans ce scénario, si une machine virtuelle se déplace d'un hôte à un autre et que ces hôtes sont connectés à deux commutateurs Leaf différents, le contrôleur APIC écoute l'événement de migration de la machine virtuelle et, dans le scénario d'immédiateté du déploiement à la demande, déprogramme l'EPG sur le Leaf source et programme l'EPG sur le Leaf de destination.

En fonction de l'immédiateté du déploiement des groupes de terminaux associés à un domaine VMM, l'échec de l'extraction de l'inventaire du vCenter peut avoir des conséquences indésirables. Dans le cas où l'inventaire n'est pas terminé ou est partiel, il y aura toujours une défaillance

indiquant l'objet ou les objets à l'origine de la défaillance.

Scénario 1 - Ordinateur virtuel avec sauvegarde non valide :

Si une machine virtuelle est déplacée d'un vCenter à un autre, ou s'il est déterminé qu'elle dispose d'une sauvegarde non valide (par exemple, une connexion de groupe de ports à un ancien DVS/DVS supprimé), la vNIC sera signalée comme présentant des problèmes de fonctionnement.

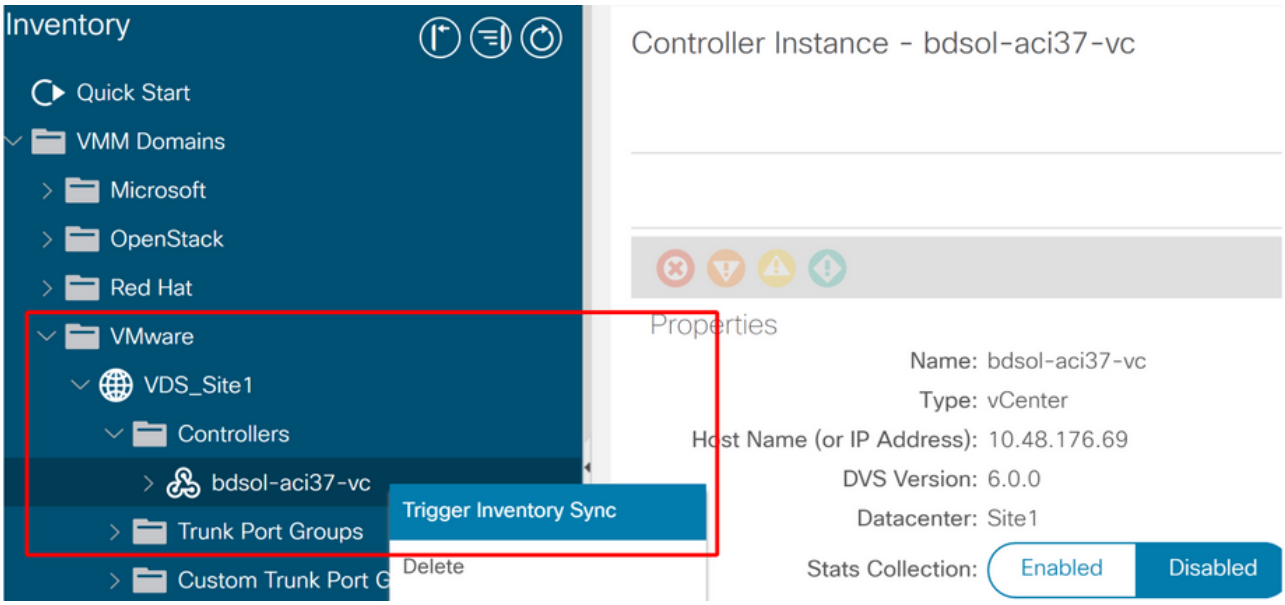
```
Fault fltCompVNicOperationalIssues
Rule ID:2842
Explanation:
This fault is raised when ACI controller failed to update the properties of a VNIC (e.g., it can not fi
Code: F2842
Message: Operational issues detected for VNic name on VM name in VMM controller: hostOrIp with name nam
Resolution:
Remediate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

Scénario 2 : l'administrateur vCenter a modifié un objet géré VMM sur le vCenter :

La modification d'objets gérés par le contrôleur APIC à partir de vCenter n'est pas une opération prise en charge. L'erreur suivante se produirait si une opération non prise en charge était effectuée sur vCenter.

```
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
```

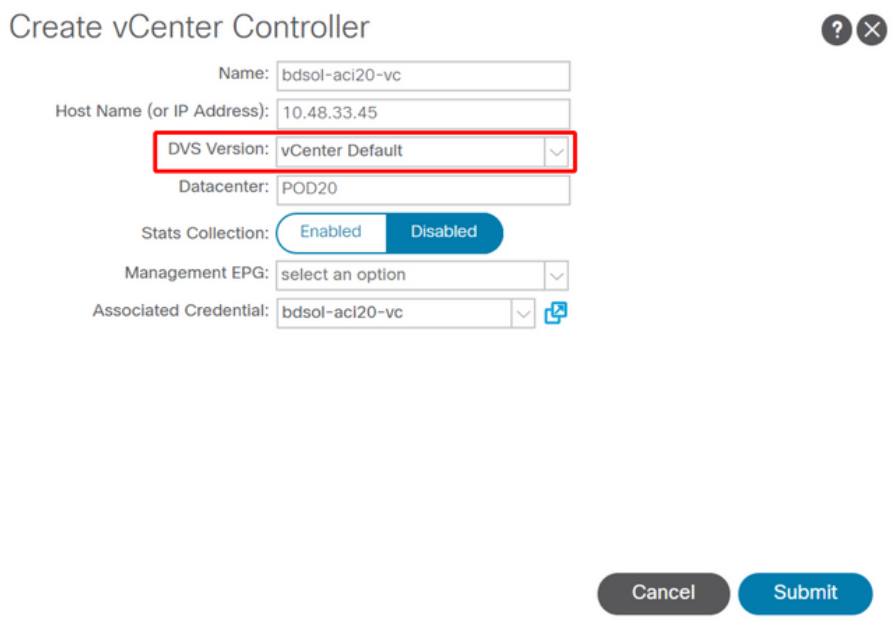
Domaine VMWare VMM - Contrôleur vCenter - Déclenchement de la synchronisation d'inventaire



Version VMware DVS

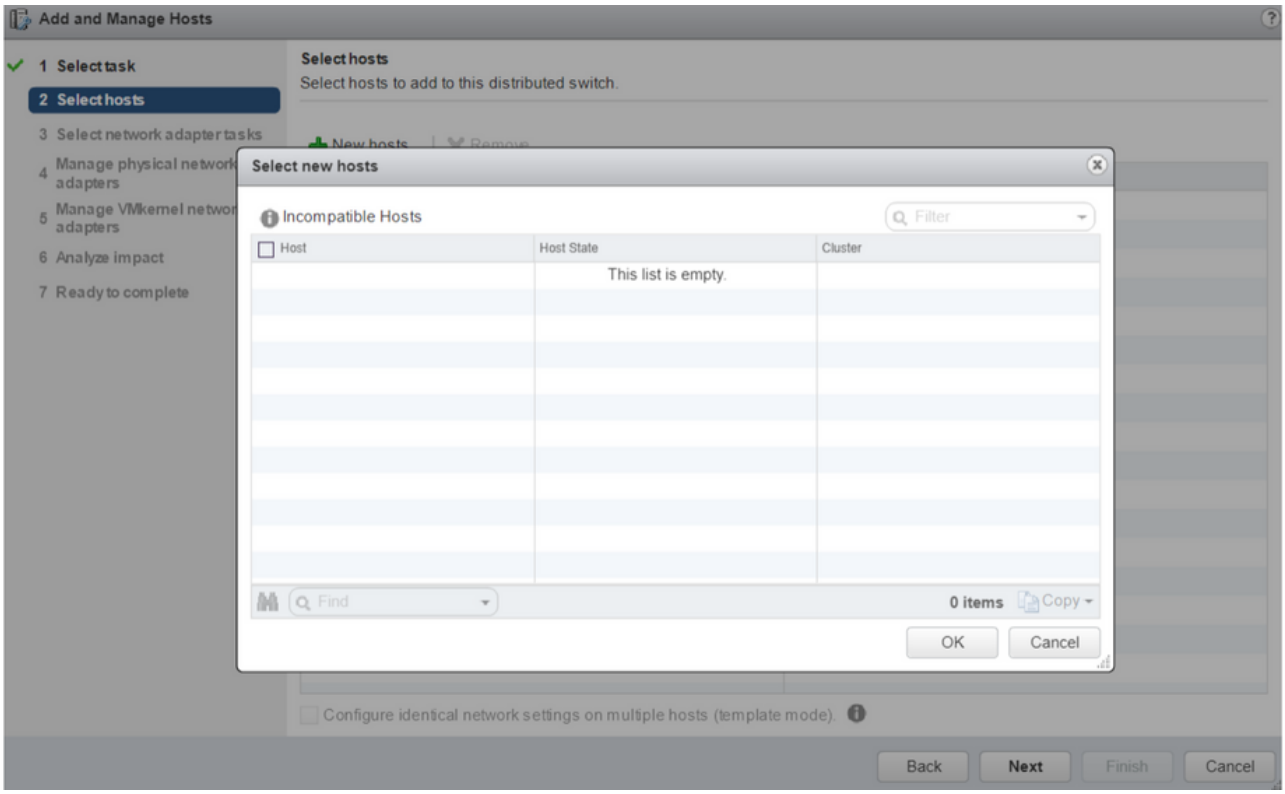
Lors de la création d'un nouveau contrôleur vCenter dans le cadre d'un domaine VMM, le paramètre par défaut de la version DVS sera d'utiliser le paramètre « Valeur par défaut vCenter ». Lorsque vous sélectionnez cette option, la version DVS est créée avec la version de vCenter.

Domaine VMWare VMM - création du contrôleur vCenter

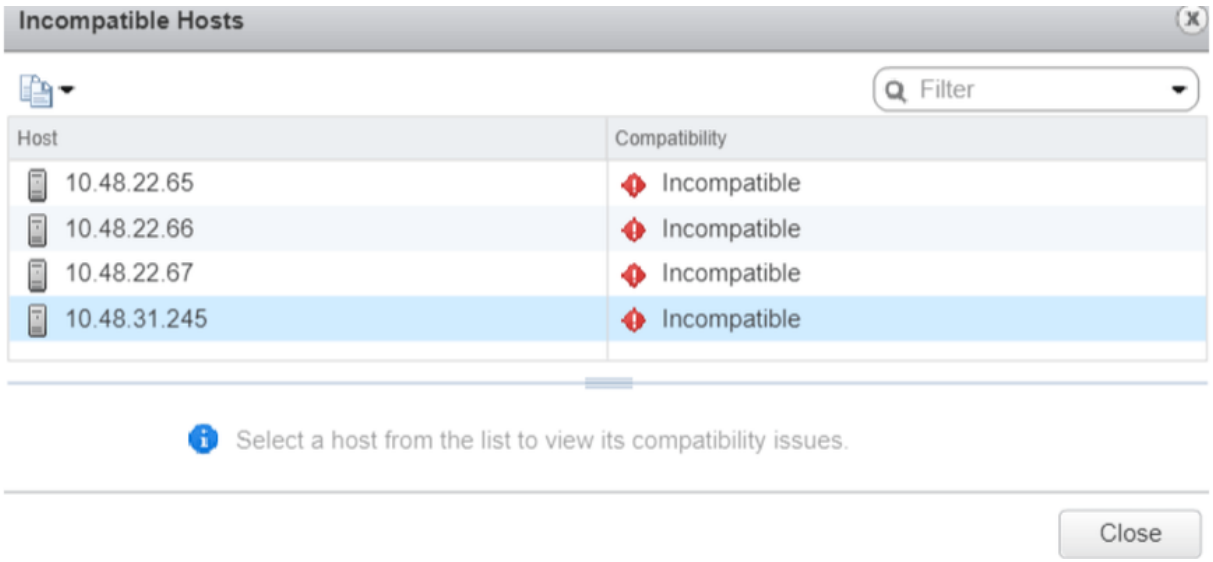


Cela signifie que dans l'exemple d'un serveur vCenter exécutant 6.5 et d'un serveur ESXi exécutant 6.0, le contrôleur APIC va créer un DVS avec la version 6.5 et par conséquent l'administrateur vCenter ne pourra pas ajouter les serveurs ESXi exécutant 6.0 dans le DVS ACI.

DVS géré APIC - ajout d'hôte vCenter - liste vide



DVS géré par APIC - ajout d'hôtes vCenter - hôtes incompatibles



Par conséquent, lors de la création d'un domaine VMM, veillez à sélectionner la version DVS appropriée afin que les serveurs ESXi nécessaires puissent être ajoutés au DVS.

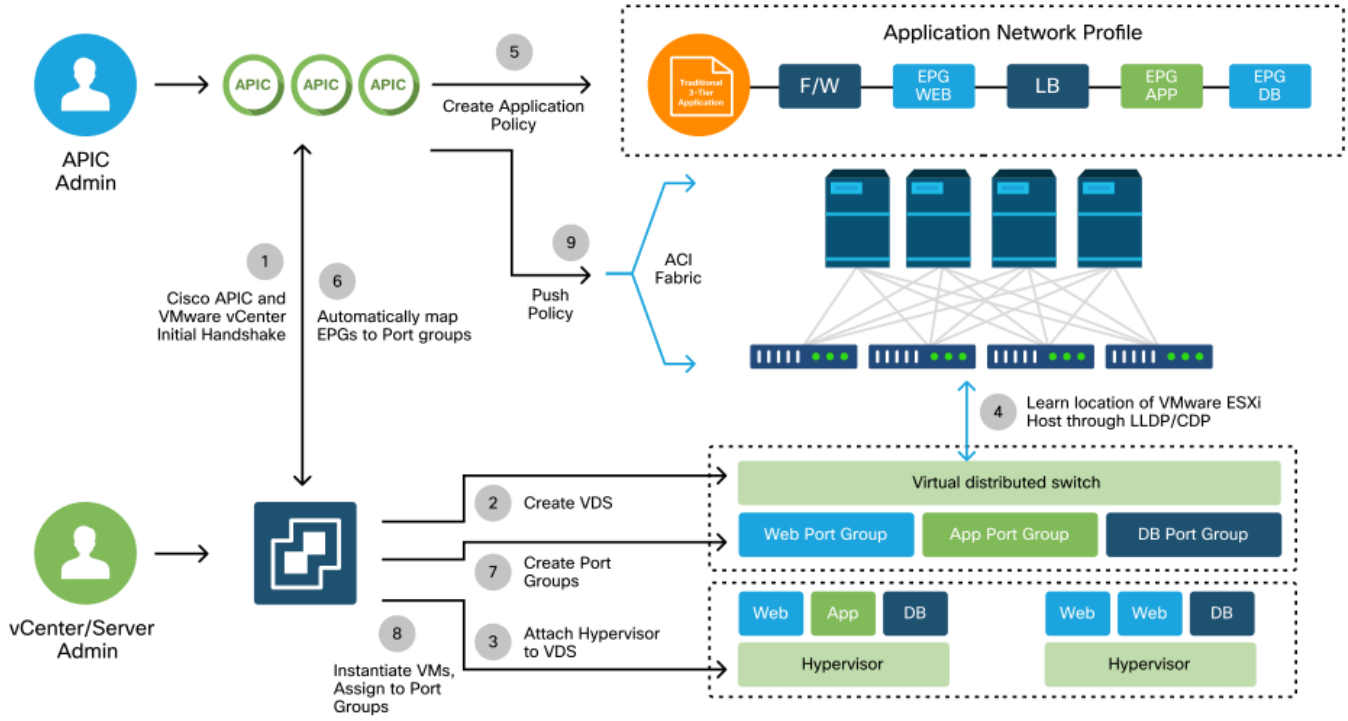
Détection dynamique des hôtes

Processus de découverte hôte/machine virtuelle

L'intégration de VMM dans l'ACI se distingue du provisionnement manuel en ce que le fabric peut détecter dynamiquement où les hôtes et les machines virtuelles applicables sont connectés pour déployer efficacement la politique. Grâce à ce processus dynamique, l'ACI peut optimiser l'utilisation des ressources matérielles sur les commutateurs Leaf, car les VLAN, les SVI, les

règles de zonage, etc. sont déployés sur les noeuds uniquement lorsqu'un terminal connecté requiert la politique. L'avantage pour l'administrateur réseau, du point de vue de la facilité d'utilisation, est que l'ACI provisionnera les VLAN/politiques là où les machines virtuelles se connectent de manière automatisée. Pour déterminer où la politique doit être déployée, le contrôleur APIC utilise des informations provenant de plusieurs sources. Le schéma suivant décrit les étapes de base du processus de détection d'hôte lors de l'utilisation d'un domaine VMM basé sur DVS.

Domaine VMWare VMM — Workflow de déploiement



En bref, les étapes clés suivantes se produisent lorsque :

- Le protocole LLDP ou CDP est échangé entre l'hyperviseur et les commutateurs Leaf.
- Les hôtes signalent les informations de contiguïté à vCenter.
- vCenter informe le contrôleur APIC des informations de contiguïté :
  - APIC connaît l'hôte via la synchronisation d'inventaire.
- Le contrôleur APIC transmet la politique au port leaf :
  - veuillez consulter la sous-section « Immédiateté de la résolution » de cette section pour mieux comprendre ces conditions.
- Si les informations de contiguïté vCenter sont perdues, le contrôleur APIC peut supprimer la stratégie.

Comme vous pouvez le constater, le protocole CDP/LLDP joue un rôle clé dans le processus de découverte et il est important de s'assurer que ce protocole est correctement configuré et que les deux parties utilisent le même protocole.

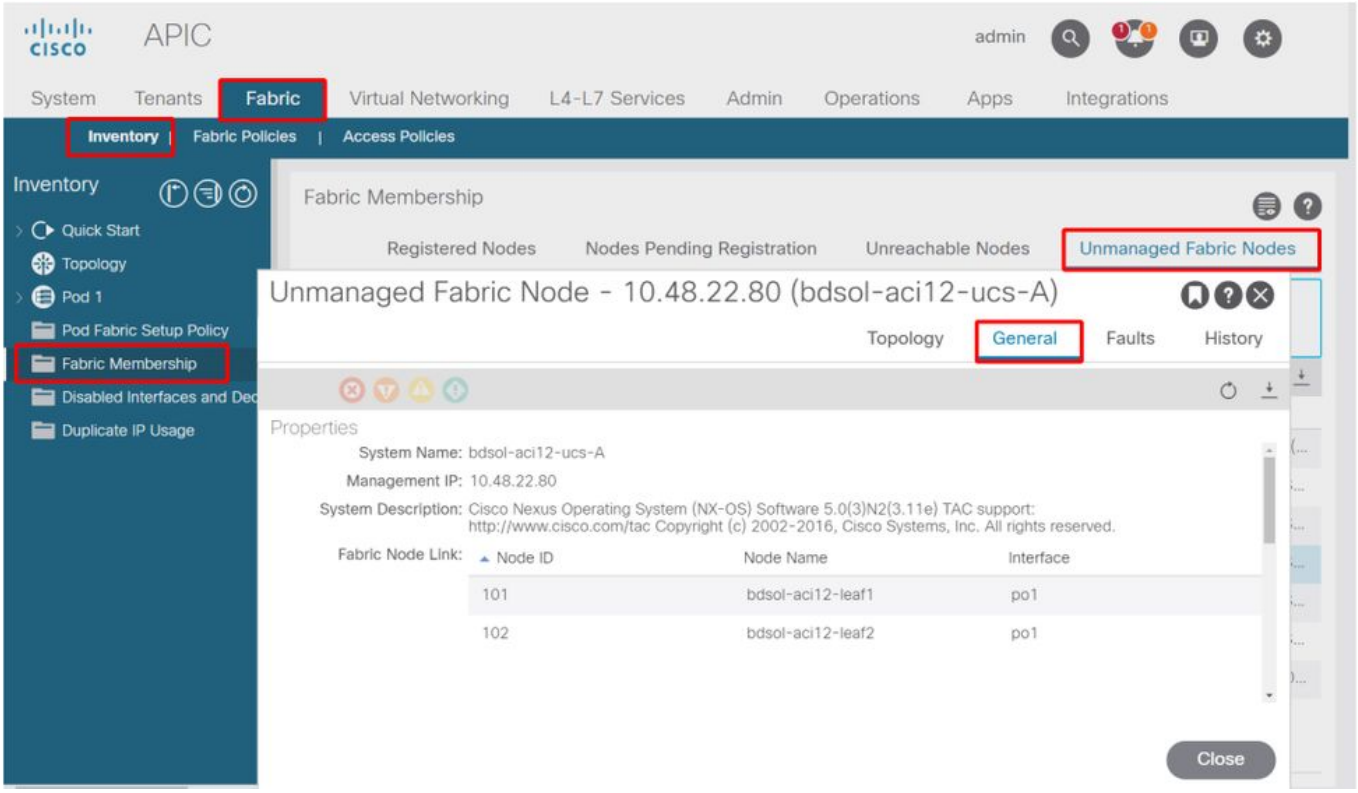
Fabric LooseNode / commutateur intermédiaire - cas d'utilisation

Dans un déploiement utilisant un châssis lame avec un commutateur intermédiaire entre les

commutateurs Leaf et l'hyperviseur, l'APIC doit « assembler » les contiguïtés. Dans ce scénario, plusieurs protocoles de détection peuvent être utilisés car le commutateur intermédiaire peut avoir des exigences de protocole différentes de celles de l'hôte.

Dans une configuration avec un serveur lame et un commutateur intermédiaire (par exemple, un commutateur de châssis lame), l'ACI doit détecter le commutateur intermédiaire et mapper les hyperviseurs derrière lui. Dans l'ACI, le commutateur intermédiaire est appelé « noeud libre » ou « noeud de fabric non géré ». Les noeuds flottants détectés peuvent être affichés sous « Fabric > Inventory > Fabric Membership > Unmanaged Fabric Nodes ». En accédant à l'un de ces types de serveurs dans l'interface utilisateur graphique, l'utilisateur peut visualiser le chemin entre le noeud terminal et le commutateur intermédiaire, puis entre l'hôte et le commutateur intermédiaire.

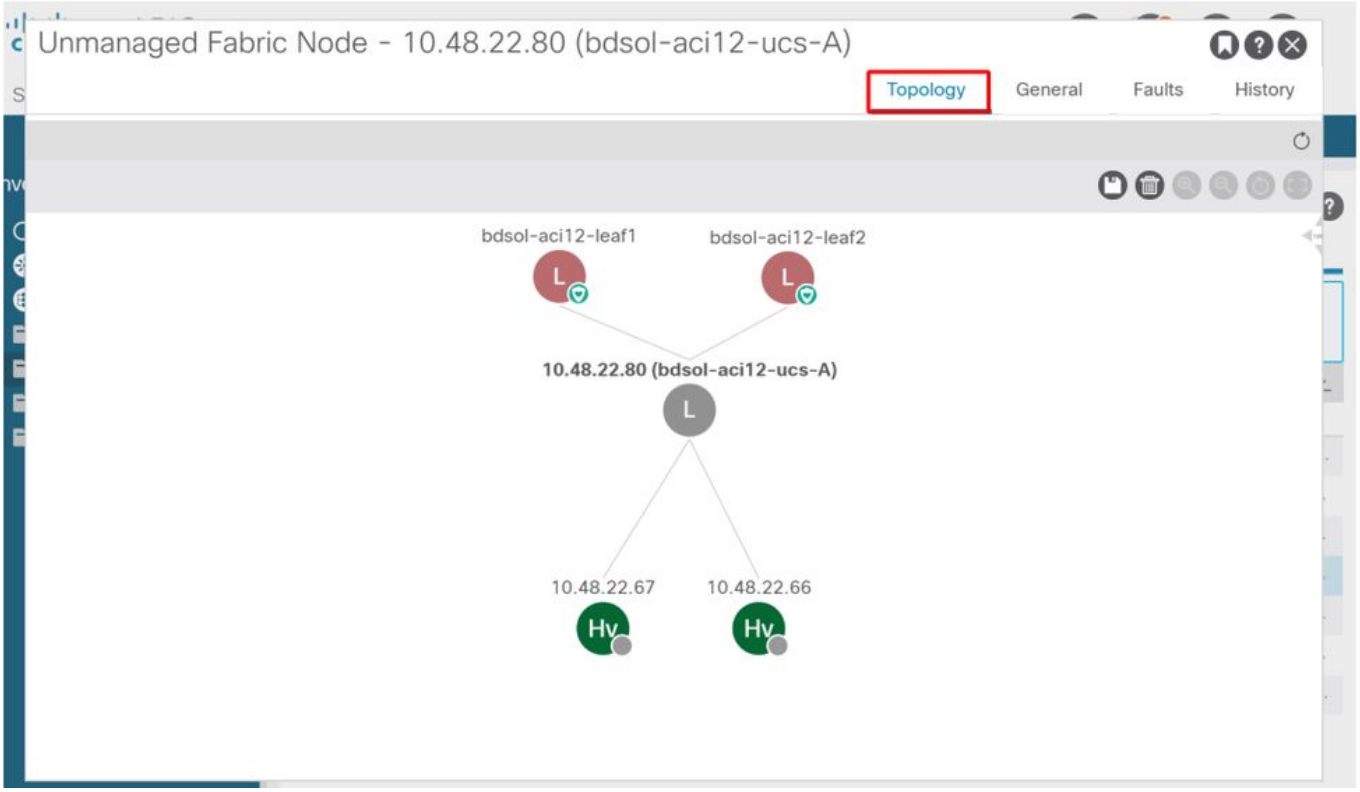
Interface utilisateur APIC : noeuds de fabric non gérés (LooseNodes)



Avec la détection LLDP ou CDP en place, l'ACI peut déterminer la topologie pour ces noeuds desserrés, étant donné que l'hyperviseur en aval du commutateur intermédiaire est géré par intégration VMM et que le noeud leaf lui-même a une contiguïté avec le commutateur intermédiaire en aval.

Ce concept est illustré par l'image ci-dessous.

Interface utilisateur APIC — Chemin de noeud de fabric non géré

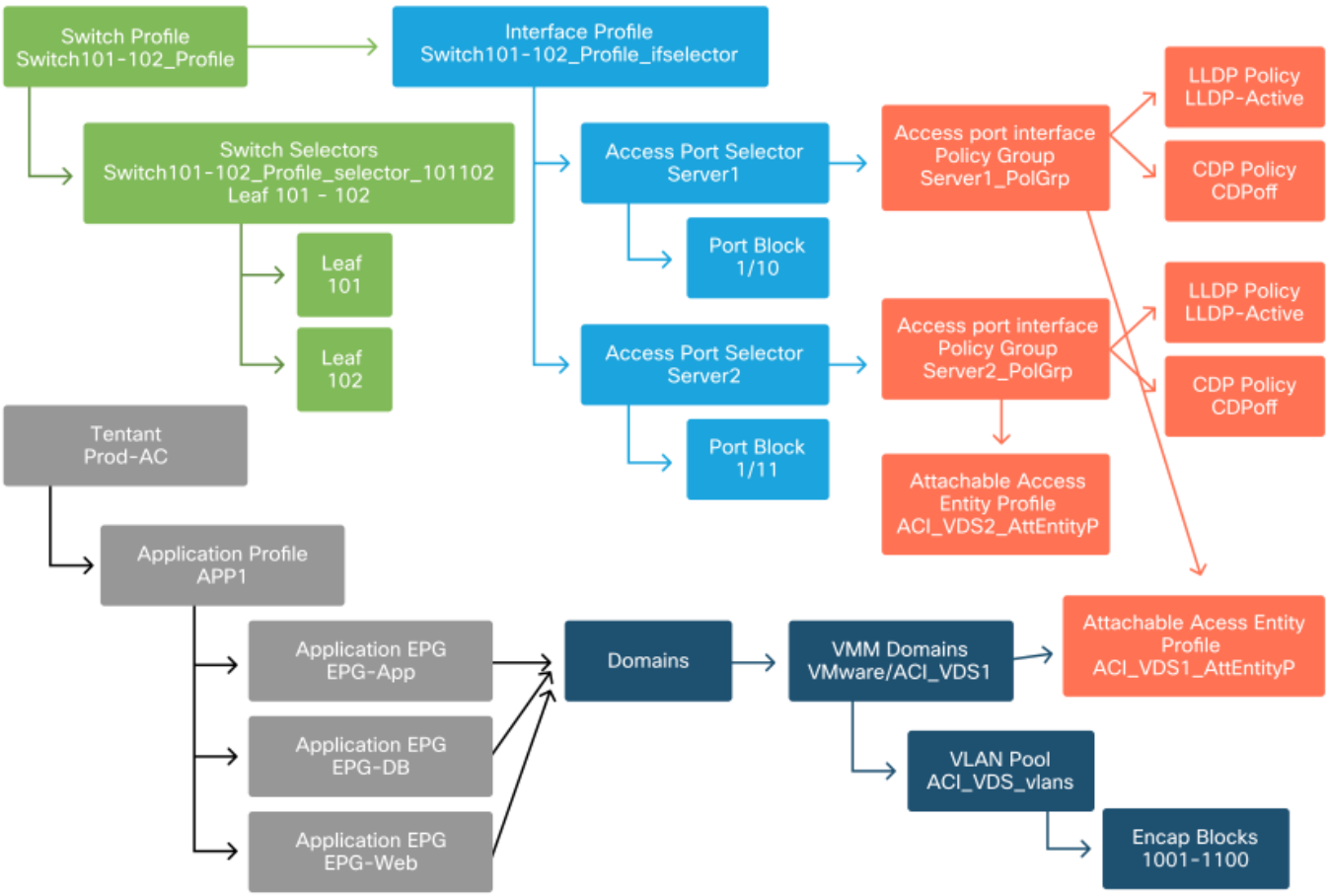


Immédiateté De La Résolution

Dans les scénarios où les services critiques utilisent le DVS intégré à VMM, comme la connectivité de gestion vers vCenter/ESXi, il est prudent d'utiliser l'Immédiateté de la résolution de pré-provisionnement. Avec ce paramètre, le mécanisme de détection dynamique d'hôte est supprimé et les politiques/VLAN sont programmés de manière statique sur les interfaces orientées hôte. Dans cette configuration, les VLAN VMM seront toujours déployés sur toutes les interfaces liées à l'AEP référencé par le domaine VMM. Cela supprime la possibilité qu'un VLAN critique (tel que la gestion) soit supprimé d'un port en raison d'un événement de contiguïté lié au protocole de détection.

Reportez-vous au schéma ci-dessous :

Exemple de déploiement pré-provisionnement



Si le pré-provisionnement a été défini pour un EPG dans le domaine VMM ACI_VDS1, les VLAN seront déployés sur les liaisons pour Server1 mais pas Server2, car l'AEP de Server2 n'inclut pas le domaine VMM ACI_VDS1.

Pour résumer les paramètres d'immédiateté de la résolution :

- À la demande : la politique est déployée lorsque la contiguïté est établie entre le terminal et l'hôte et une machine virtuelle connectée au groupe de ports.
- Immédiat : la stratégie est déployée lorsque la contiguïté est établie entre le noeud Leaf et l'hôte.
- Pré-provisionnement : la politique est déployée sur tous les ports à l'aide d'un AEP avec le domaine VMM contenu, aucune contiguïté n'est requise.

Scénarios de dépannage

VM ne peut pas résoudre ARP pour sa passerelle par défaut

Dans ce scénario, l'intégration VMM a été configurée et le DVS a été ajouté à l'hyperviseur, mais la machine virtuelle ne peut pas résoudre le protocole ARP pour sa passerelle dans l'ACI. Pour que la machine virtuelle dispose d'une connectivité réseau, vérifiez que la contiguïté a été établie et que les VLAN sont déployés.

Tout d'abord, l'utilisateur peut vérifier que le leaf a détecté l'hôte en utilisant « show lldp neighbors

» ou « show cdp neighbors » sur le leaf, selon le protocole sélectionné.

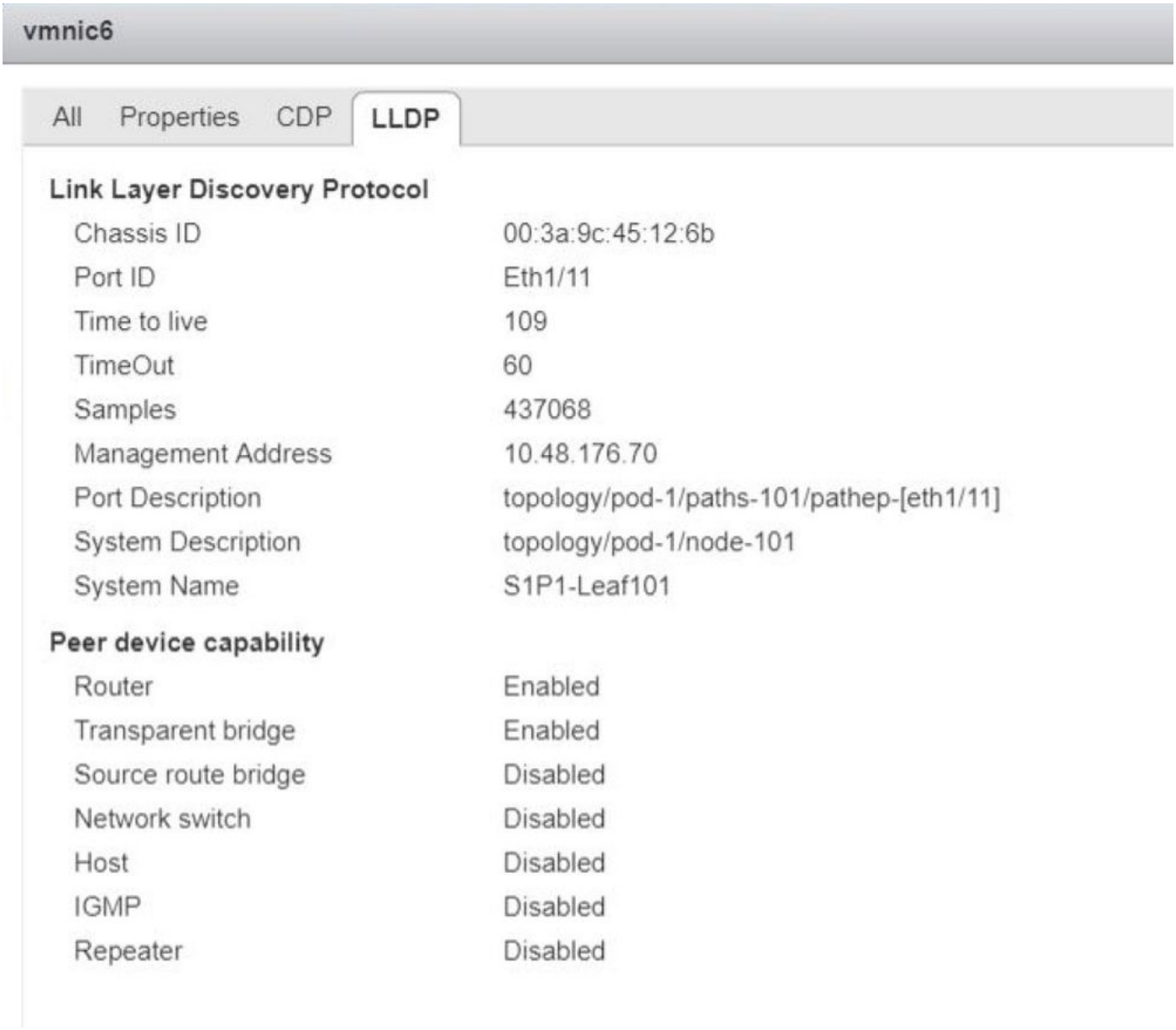
```
<#root>

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
```

Si nécessaire, du point de vue du dépannage, cela peut être validé du côté d'ESXi à la fois sur l'interface de ligne de commande et l'interface utilisateur graphique :

```
<#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"
    }
```

Client Web vCenter - hôte - détails de contiguïté LLDP/CDP vmnic

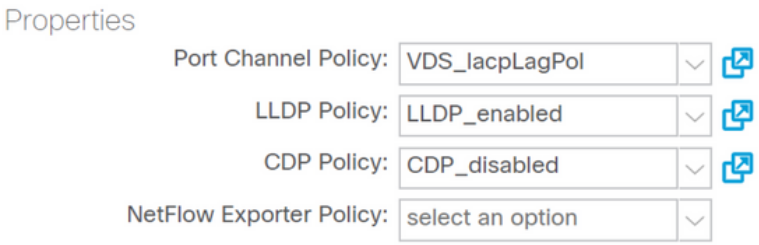


Si la contiguïté LLDP leaf ne peut pas être vue depuis l'hôte ESXi, cela est souvent dû à l'utilisation d'une carte réseau qui est configurée pour générer des LLDPDU au lieu du système d'exploitation ESXi. Assurez-vous que le protocole LLDP est activé sur la carte réseau et qu'il utilise donc toutes les informations LLDP. Si c'est le cas, assurez-vous de désactiver LLDP sur la carte elle-même afin qu'elle soit contrôlée via la stratégie vSwitch.

Une autre cause peut être un mauvais alignement entre les protocoles de détection utilisés entre leaf et l'hyperviseur ESXi. Assurez-vous que les deux extrémités utilisent le même protocole de détection.

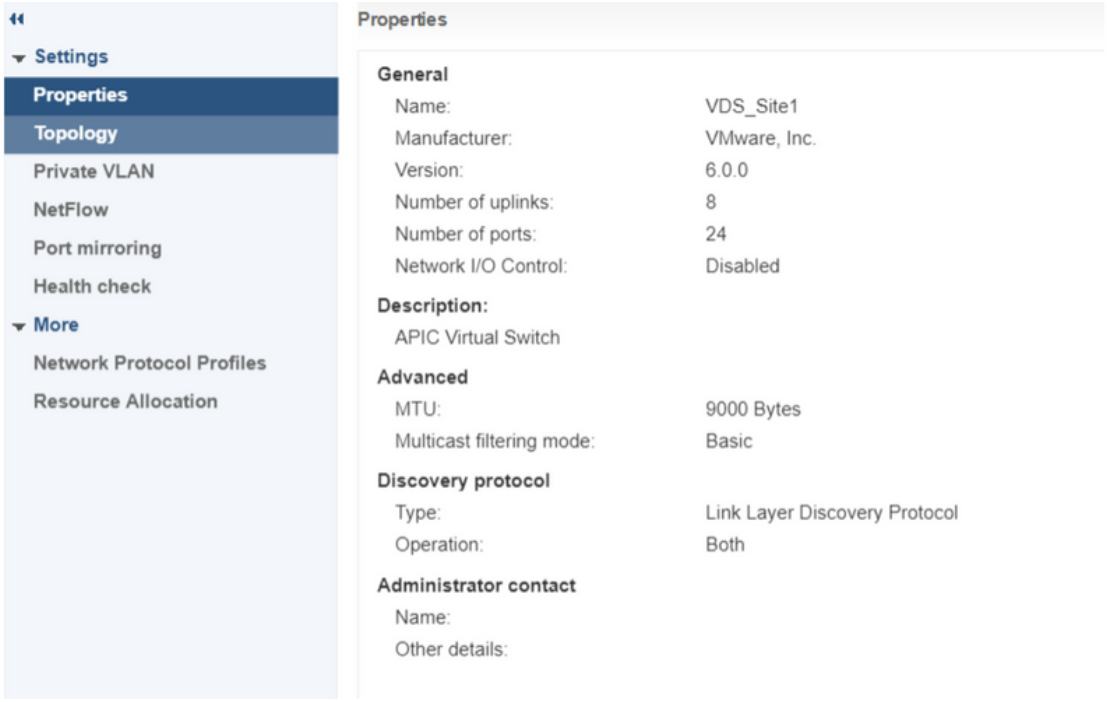
Pour vérifier si les paramètres CDP/LLDP sont alignés entre l'ACI et le DVS dans l'interface utilisateur APIC, accédez à « Virtual Networking > VMM Domains > VMWare > Policy > vSwitch Policy ». Veillez à activer uniquement la stratégie LLDP ou CDP car elles s'excluent mutuellement.

Interface utilisateur APIC - Domaine VMM VMWare - Stratégie vSwitch



Dans vCenter, accédez à : 'Mise en réseau > VDS > Configurer'.

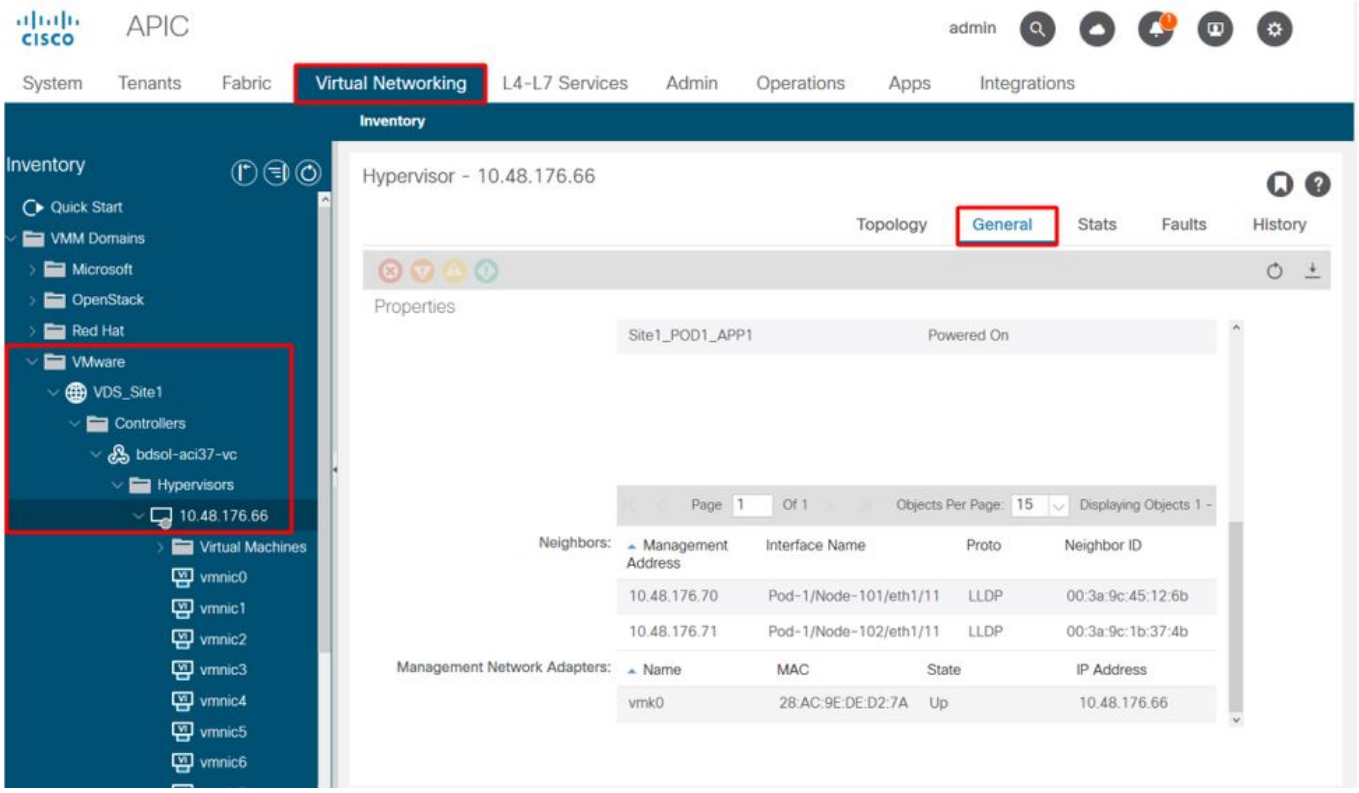
Interface utilisateur du client Web vCenter - Propriétés VDS



Corrigez les paramètres LLDP/CDP si nécessaire.

Ensuite, validez le contrôleur APIC observe le voisinage LLDP/CDP de l'hôte ESXi par rapport au commutateur leaf dans l'interface utilisateur sous « Mise en réseau virtuelle > Domaines VMM > VMWare > Stratégie > Contrôleur > Hyperviseur > Général ».

Interface utilisateur APIC - Domaine VMM VMWare - Détails de l'hyperviseur



Si les valeurs attendues s'affichent, l'utilisateur peut confirmer que le VLAN est présent sur le port en direction de l'hôte.

<#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
```

VMK de gestion vCenter/ESXi attaché à un DVS poussé par APIC

Dans un scénario où le trafic de gestion vCenter ou ESXi doit utiliser le DVS intégré VMM, il est important de prendre des précautions supplémentaires pour éviter une impasse dans l'activation des contiguïtés dynamiques et l'activation des VLAN requis.

Pour vCenter, qui est généralement construit avant la configuration de l'intégration VMM, il est important d'utiliser un domaine physique et un chemin statique pour s'assurer que le VLAN d'encapsulation de la VM vCenter est toujours programmé sur les commutateurs Leaf afin qu'il puisse être utilisé avant la configuration complète de l'intégration VMM. Même après avoir

configuré l'intégration VMM, il est conseillé de laisser ce chemin statique en place pour toujours assurer la disponibilité de cet EPG.

Pour les hyperviseurs ESXi, comme indiqué dans le « Guide de virtualisation de l'ACI Cisco » sur Cisco.com, lors de la migration vers le vDS, il est important de s'assurer que l'EPG où l'interface VMK sera connectée est déployé avec l'immédiateté de résolution définie sur Pré-provisionnement. Cela garantit que le VLAN est toujours programmé sur les commutateurs Leaf sans dépendre de la découverte LLDP/CDP des hôtes ESXi.

Contiguïtés d'hôtes non découvertes derrière LooseNode

Les causes typiques des problèmes de détection LooseNode sont :

- CDP/LLDP non activé
  - Les protocoles CDP/LLDP doivent être échangés entre le commutateur intermédiaire, les commutateurs Leaf et les hôtes ESXi
  - Pour Cisco UCS, cette opération est effectuée via une politique de contrôle du réseau sur la vNIC
- Une modification de l’adresse IP de gestion du voisin LLDP/CDP interrompt la connectivité
  - Le vCenter verra la nouvelle adresse IP de gestion dans la contiguïté LLDP/CDP, mais ne mettra pas à jour le contrôleur APIC
  - Déclencher une synchronisation manuelle de l'inventaire à corriger
- Les VLAN VMM ne sont pas ajoutés au commutateur intermédiaire
  - Le contrôleur APIC ne programme pas les commutateurs intermédiaires/lames tiers.
  - Application d'intégration Cisco UCSM (ExternalSwitch) disponible dans la version 4.1(1).
  - Les VLAN doivent être configurés et agrégés aux liaisons ascendantes connectées aux noeuds leaf ACI et aux liaisons descendantes connectées aux hôtes

F606391 : contiguïtés manquantes pour la carte physique sur l'hôte

Lorsque vous voyez le défaut ci-dessous :

```
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:
```

Revoyez le workflow dans la section « La machine virtuelle ne peut pas résoudre le protocole ARP pour sa passerelle par défaut », car cela signifie qu'il manque des contiguïtés CDP/LLDP. Ces contiguïtés doivent être vérifiées de bout en bout.

Équilibrage de charge de liaison ascendante hyperviseur

Lors de la connexion d'hyperviseurs tels qu'ESXi à un fabric ACI, ils sont généralement connectés à plusieurs liaisons ascendantes. En fait, il est recommandé de connecter un hôte ESXi à au

moins deux commutateurs Leaf. Cela minimisera l'impact des scénarios de panne ou des mises à niveau.

Afin d'optimiser l'utilisation des liaisons ascendantes par les charges de travail exécutées sur un hyperviseur, les configurations VMware vCenter permettent de configurer plusieurs algorithmes d'équilibrage de charge pour le trafic généré par la VM vers les liaisons ascendantes de l'hyperviseur.

Il est essentiel que tous les hyperviseurs et le fabric ACI soient alignés sur la même configuration d'algorithme d'équilibrage de charge pour garantir une connectivité correcte. Si vous ne le faites pas, le trafic risque d'être interrompu et les terminaux déplacés dans le fabric ACI.

Ceci peut être constaté dans un fabric ACI par des alertes excessives telles que :

```
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
```

Ce chapitre traite de la connectivité des hôtes VMware ESXi à l'ACI, mais s'applique à la plupart des hyperviseurs.

Serveur rack

Lorsqu'un hôte ESXi examine les différentes manières dont il peut se connecter à un fabric ACI, il est divisé en 2 groupes, avec des algorithmes d'équilibrage de charge dépendants et indépendants du commutateur.

Les algorithmes d’équilibrage de charge indépendants du commutateur permettent de se connecter sans configuration de commutateur spécifique. Pour l'équilibrage de charge dépendant du commutateur, des configurations spécifiques au commutateur sont requises.

Assurez-vous de valider si la stratégie vSwitch est conforme aux exigences du « groupe de stratégies d'accès ACI », comme indiqué dans le tableau ci-dessous.

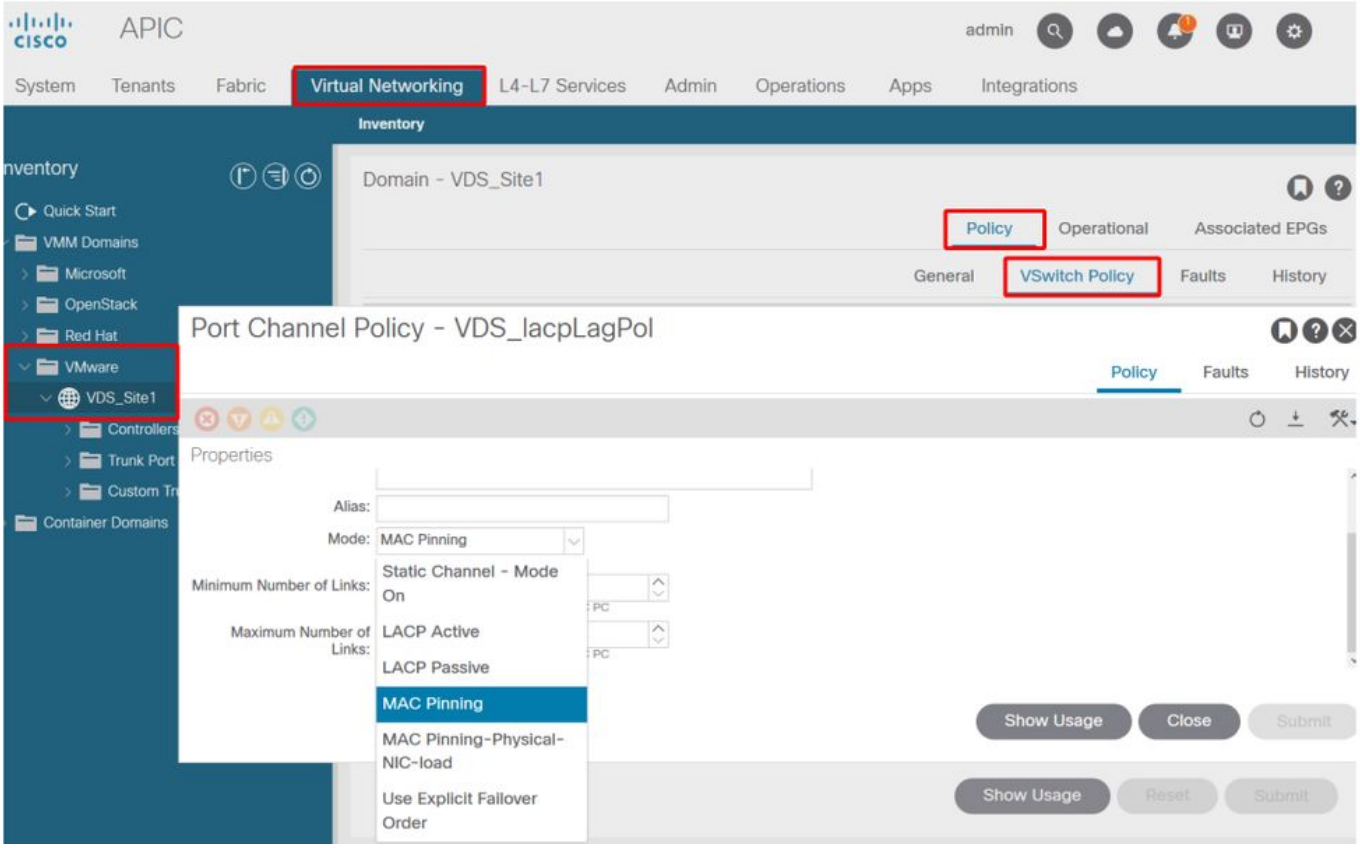
Stratégie de collaboration et ACI vSwitch

Mode de collaboration et de basculement VMware	Politique vSwitch ACI	Description	Groupe de politiques d'accès ACI - Port Channel requis
Route basée sur le port virtuel d'origine	Épinglage MAC	Sélectionnez une liaison ascendante en fonction des ID de port virtuel sur le commutateur. Une fois que le commutateur virtuel a sélectionné une liaison ascendante pour une machine virtuelle ou une carte VMKernel, il transfère toujours le trafic via la même liaison ascendante pour cette machine virtuelle ou cette carte VMKernel.	Non
Route basée sur le hachage MAC source	S. O.	Sélectionnez une liaison ascendante basée sur un hachage de l'adresse MAC source	S. O.
Ordre de basculement explicite	Utiliser le mode de basculement explicite	Dans la liste des adaptateurs actifs, utilisez toujours la liaison ascendante d'ordre le plus élevé qui répond aux critères de détection de basculement. Cette option n'effectue aucun équilibrage de charge réel.	Non
Agrégation de liens (LAG) - Basée sur le hachage IP	Canal statique - Mode Activé	Sélectionnez une liaison ascendante en fonction d'un hachage des adresses IP source et de destination de chaque paquet. Pour les paquets non IP, le commutateur utilise les données de ces champs pour calculer le hachage. L'association basée sur IP nécessite que du côté de l'ACI un port-channel / VPC soit configuré avec 'mode on'.	Oui (mode canal activé)
Agrégation de liens (LAG) - LACP	LACP actif/passif	Sélectionnez une liaison ascendante en fonction d'un hachage sélectionné (20 options de hachage différentes sont disponibles). L'association basée sur LACP nécessite que du côté ACI un	Oui (mode de canal défini sur « LACP actif/passif »)

Mode de collaboration et de basculement VMware	Politique vSwitch ACI	Description	Groupe de politiques d'accès ACI - Port Channel requis
		port-channel / VPC soit configuré avec LACP activé. Veillez à créer une politique de décalage améliorée dans l'ACI et à l'appliquer à la politique de VSwitch.	
Route basée sur la charge physique de la carte réseau (LBT)	Épinglage MAC - Physical-NIC-load	Disponible pour les groupes de ports distribués ou les ports distribués. Sélectionnez une liaison ascendante en fonction de la charge actuelle des cartes réseau physiques connectées au groupe de ports ou au port. Si une liaison ascendante reste occupée à 75 pour cent ou plus pendant 30 secondes, le commutateur virtuel de l'hôte déplace une partie du trafic de la machine virtuelle vers une carte physique qui a une capacité libre.	Non

Reportez-vous à la capture d'écran ci-dessous pour savoir comment valider la stratégie Port-Channel dans le cadre de la stratégie vSwitch en place.

Politique vSwitch ACI - Politique de canal de port



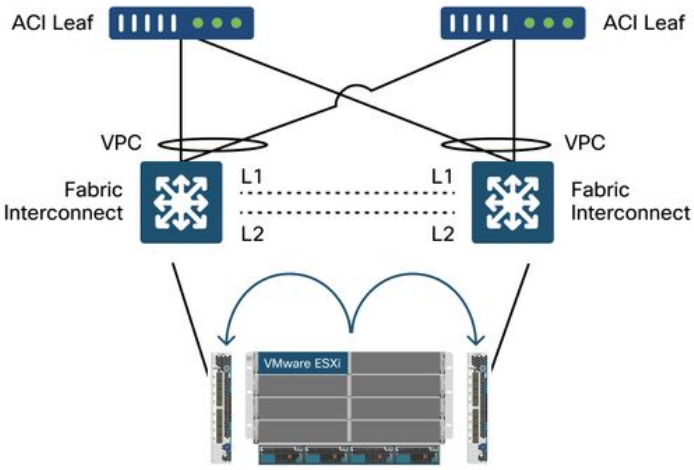
Remarque : pour obtenir une description plus détaillée des fonctionnalités de mise en réseau VMware, consultez la section consacrée à la mise en réseau vSphere à l'adresse https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.networking.doc/GUID-D34B1ADD-B8A7-43CD-AA7E-2832A0F7EE76.html

Exemple d'utilisation de Cisco UCS série B

Lors de l'utilisation de serveurs Cisco UCS série B, il est important de noter qu'ils se connectent au sein de leur châssis à des interconnexions de fabric UCS (FI) ne disposant pas d'un plan de données unifié. Cet exemple d'utilisation s'applique également aux autres fournisseurs qui utilisent une topologie similaire. De ce fait, il peut y avoir une différence entre la méthode d'équilibrage de charge utilisée du côté d'un commutateur leaf ACI et du côté du commutateur virtuel.

Voici une topologie UCS FI avec ACI :

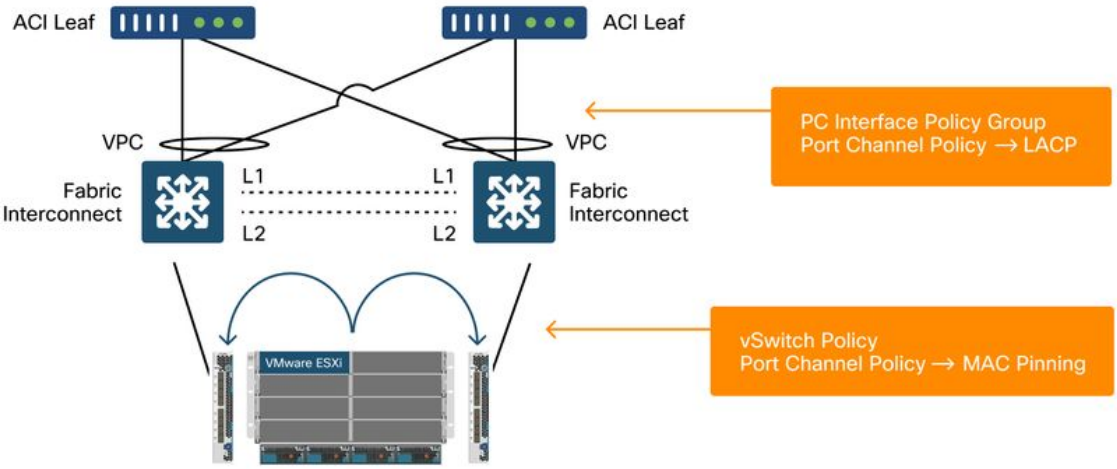
Cisco UCS FI avec commutateurs leaf ACI - topologie



Points importants à noter :

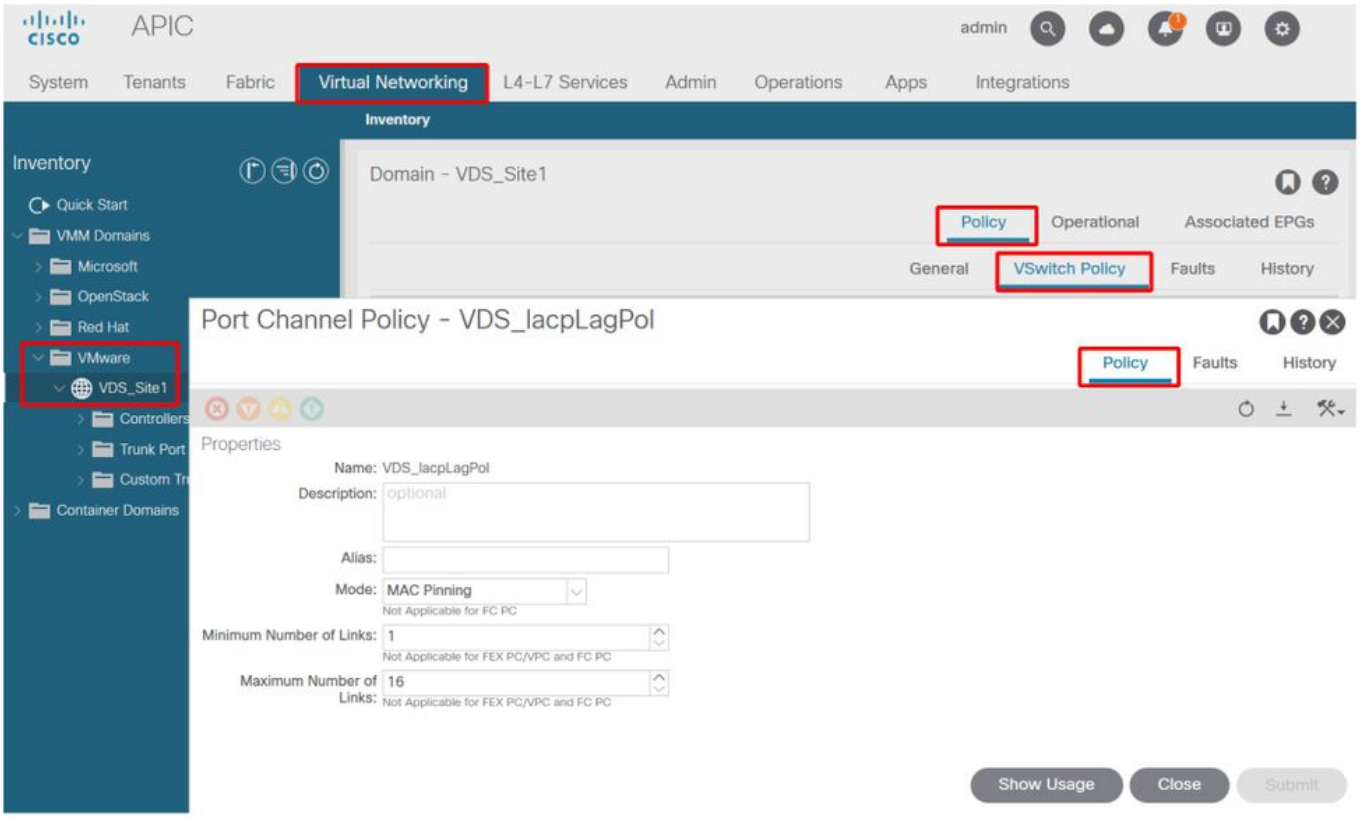
- Chaque interface FI Cisco UCS dispose d'un canal de port vers les commutateurs Leaf ACI.
- Les interfaces de ligne de commande UCS sont directement interconnectées à des fins de pulsation uniquement (non utilisées pour le plan de données).
- La vNIC de chaque serveur lame est épinglée à un FI UCS spécifique ou utilise un chemin vers l'un des FI à l'aide du basculement de fabric UCS (Active-Standby).
- L'utilisation d'algorithmes de hachage IP sur le commutateur virtuel de l'hôte ESXi entraînera des battements MAC sur les interfaces de ligne de commande UCS.

Afin de configurer correctement ceci, faites ce qui suit :



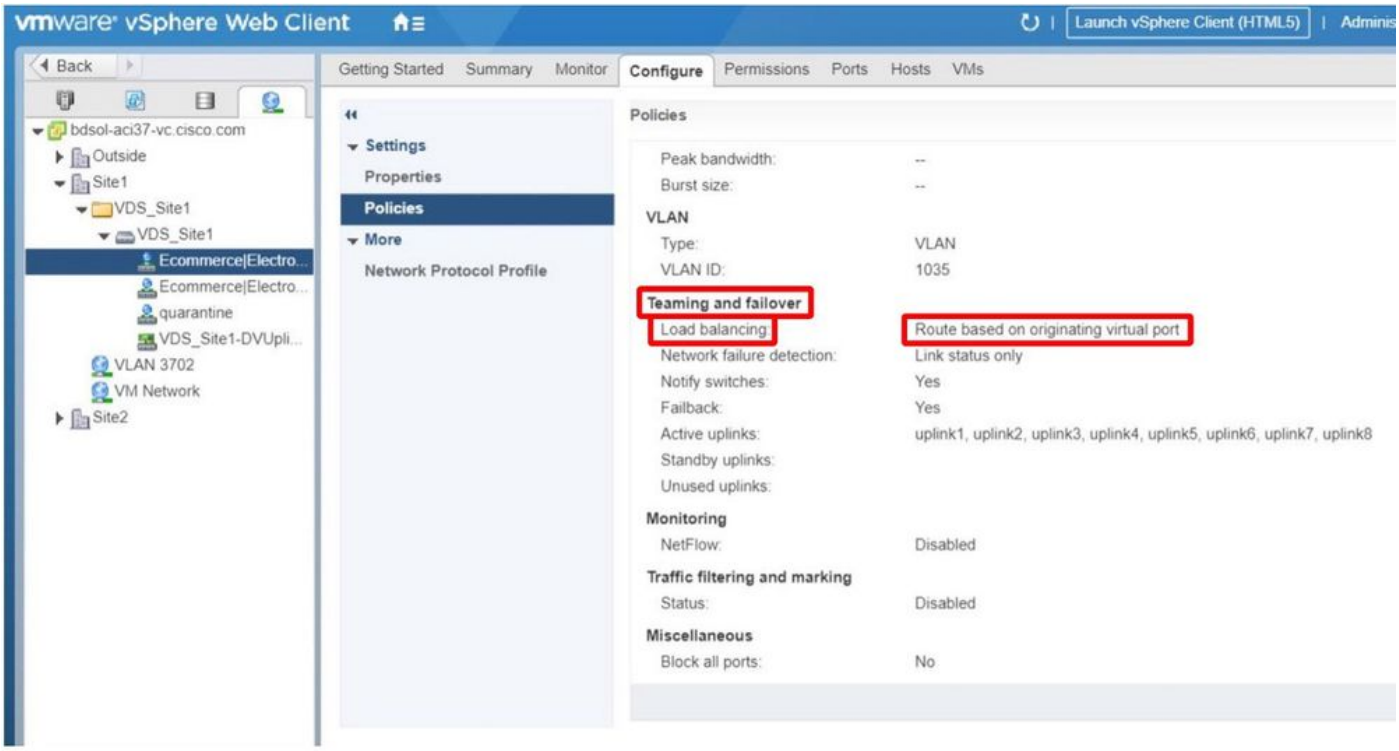
Lorsque l'épinglage MAC est configuré sur la politique Port-Channel dans le cadre de la politique vSwitch de l'ACI, il s'affiche comme « Route basée sur le port virtuel d'origine » dans la configuration d'association des groupes de ports sur le VDS.

ACI - Politique de canal de port dans le cadre de la politique vSwitch



La politique de canal de port utilisée dans l'exemple ci-dessus est nommée automatiquement par l'assistant. Elle est donc appelée « CDS_lacpLagPol » bien que nous utilisions le mode « MAC Pinning ».

VMWare vCenter — ACI VDS — Groupe de ports — Paramètre d'équilibrage de charge



À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.