Solucionar problemas de integración de ACI VMM

Contenido

Introducción

Este documento describe los pasos para comprender y solucionar problemas de la integración de

Virtual Machine Manager (VMM) de ACI.

Antecedentes

El material de este documento se extrajo del libro Troubleshooting de Cisco Application Centric Infrastructure, Second Edition, en concreto de los capítulos **Integración con VMM - Descripción general, Integración con VMM - Conectividad con vCenter, Integración con VMM - Detección dinámica de host** e **Integración con VMM - Equilibrio de carga de enlaces ascendentes de hipervisor**.

Descripción general de Virtual Machine Manager

Los controladores ACI tienen la capacidad de integrarse con administradores de máquinas virtuales (VMM) de terceros.

Esta es una de las funciones clave de ACI, ya que simplifica y automatiza las operaciones para la configuración de red integral del fabric y las cargas de trabajo que se conectan a él. ACI ofrece un único modelo de políticas de superposición que se puede ampliar a varios tipos de cargas de trabajo, es decir, máquinas virtuales, servidores sin software específico y contenedores.

Este capítulo se centra específicamente en algunos escenarios de solución de problemas habituales relacionados con la integración VM de VMware vCenter.

El lector recorrerá:

- Investigación de fallos de comunicación del vCenter.
- Proceso de detección dinámica de host y VM y escenarios de fallos.
- Algoritmos de equilibrio de carga del hipervisor.

Conectividad vCenter

Control de acceso basado en roles (RBAC)

Los mecanismos mediante los cuales APIC puede interactuar con el controlador vCenter dependen de la cuenta de usuario asociada a un dominio VMM determinado. Se describen los requisitos específicos para que el usuario del vCenter asociado al dominio VMM pueda garantizar que el APIC pueda realizar correctamente las operaciones en el vCenter, tanto si envía y recupera el inventario y las configuraciones como si supervisa y escucha los eventos relacionados con el inventario administrado.

La manera más fácil de eliminar la preocupación sobre estos requisitos es utilizar la cuenta de vCenter del administrador que tiene acceso completo; sin embargo, este tipo de libertad no siempre está disponible para el administrador de ACI.

Los privilegios mínimos para una cuenta de usuario personalizada, a partir de la versión 4.2 de ACI, son los siguientes:

- **Alarmas** APIC crea dos alarmas en la carpeta. Uno para DVS y otro para el grupo de puertos. Se genera una alarma cuando se elimina la política de dominio EPG o VMM en el APIC; sin

embargo, vCenter no puede eliminar el grupo de puertos o DVS correspondiente debido a que tiene VM conectadas.
- **Switch distribuido**
- **grupo dvPort**
- **Carpeta**
- **Red** APIC gestiona los parámetros de red, como la adición o eliminación de grupos de puertos, la configuración de MTU de host/DVS, LLDP/CDP, LACP, etc.
- **Host** Si utiliza AVS además de lo anterior, el usuario necesita el privilegio de host en el Data Center donde APIC creará DVS.**Host.Configuration.AdvancedHost.Operaciones locales.Reconfigurar máquina virtualHost.Configuration.Network configuration**Esto es necesario para AVS y la función de colocación automática para VM de servicio de capa 4 a capa 7 virtuales. Para AVS, APIC crea la interfaz VMK y la coloca en el grupo de puertos VTEP que se utiliza para OpFlex.
- **Máquina virtual** Si los gráficos de servicio están en uso, también se requiere el privilegio de máquina virtual para los appliances virtuales.**Máquina virtual.Configuración.Modificar configuración de dispositivoMáquina virtual.Configuration.Settings**

Solución de problemas relacionados con RBAC

Los problemas de RBAC suelen producirse durante la instalación inicial de un dominio VMM, pero podrían producirse si un administrador de vCenter modificara los permisos de la cuenta de usuario asociada al dominio VMM después de que ya se haya realizado la instalación inicial.

El síntoma puede presentarse de las siguientes maneras:

- Incapacidad parcial o total para implementar nuevos servicios (creación de DVS, creación de grupos de puertos, algunos objetos se implementan correctamente pero no todos).
- El inventario operativo está incompleto o falta en las vistas de administrador de ACI.
- Fallos provocados por un funcionamiento de vCenter no compatible o por cualquiera de los escenarios anteriores (por ejemplo, fallo en la implementación del grupo de puertos).
- El controlador vCenter se informa como desconectado y los fallos indican que hay problemas relacionados con la conectividad o las credenciales.

Solución para problemas relacionados con RBAC

Compruebe que todos los permisos anteriores se conceden al usuario del vCenter configurado en el dominio VMM.

Otro método consiste en iniciar sesión directamente en el vCenter con las mismas credenciales definidas en la configuración del dominio VMM e intentar operaciones similares (creación de grupos de puertos, etc.). Si el usuario no puede realizar estas mismas operaciones mientras está conectado directamente al vCenter, es evidente que no se le conceden los permisos correctos.

Troubleshooting de Conectividad

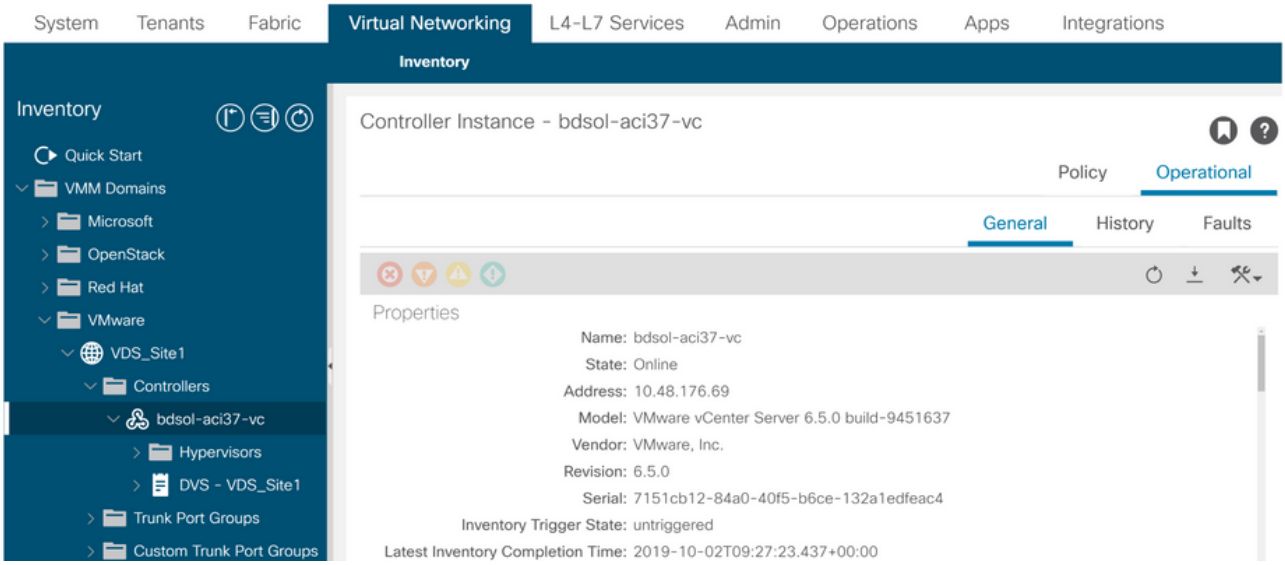
Al solucionar un problema relacionado con la conectividad de VMM, es importante tener en cuenta algunos de los comportamientos fundamentales de cómo ACI se comunica con vCenter.

El primer y más pertinente comportamiento es que solo un APIC del clúster envía la configuración

y recopila el inventario en un momento dado. Este APIC se denomina **líder compartido** para este dominio VMM. Sin embargo, hay varios APIC que están atentos a los **eventos de vCenter** para tener en cuenta un escenario en el que el líder compartido se perdió un evento por cualquier motivo. Siguiendo la misma arquitectura distribuida de los APIC, un dominio VMM determinado tendrá un APIC que gestiona los datos principales y la funcionalidad (en este caso, el líder compartido), y dos réplicas (en el caso de VMM se denominan **seguidores**). Para distribuir la administración de la comunicación y la funcionalidad de VMM entre los APIC, dos dominios VMM pueden tener los mismos controladores compartidos o uno diferente.

Puede encontrar el estado de conectividad del vCenter desplazándose al controlador VMM de su interés en la GUI o utilizando el comando CLI que se muestra a continuación.

Dominio VMware: estado de conectividad de vCenter




```
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 se indica que un controlador VMM está desconectado, se producirá un error similar al siguiente:

```
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.
```

Los siguientes pasos se pueden utilizar para resolver problemas de conectividad entre el VC y los APIC.

1. Identificación del líder del fragmento

El primer paso para solucionar un problema de conectividad entre el APIC y el vCenter consiste en saber qué APIC es el líder compartido para el dominio VMM especificado. La manera más fácil de determinar esta información es ejecutar el comando 'show vmware domain name <domain>' en cualquier APIC.

```
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. Verificación de la conectividad con vCenter

Después de identificar el APIC que se comunica activamente con el vCenter, verifique la conectividad IP con herramientas como 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 el vCenter se configuró mediante el FQDN en lugar de la dirección IP, se puede utilizar el comando nslookup para verificar la resolución de nombres.

```
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
```

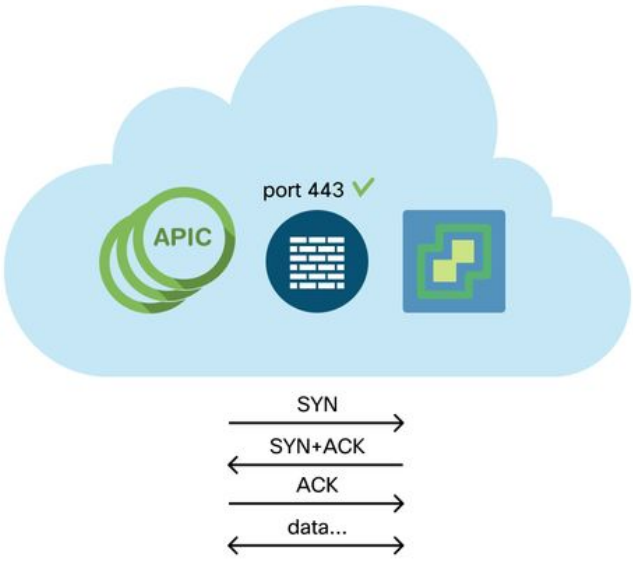
3. Compruebe si se utiliza OOB o INB

Verifique la tabla de ruteo APIC para verificar si se prefiere la conectividad fuera de banda o en banda y qué gateway se utiliza:

```
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. Asegúrese de que el puerto 443 esté permitido entre todos los APIC y el vCenter, incluidos los firewalls en la ruta de comunicación.

vCenter <-> APIC - HTTPS (puerto TCP 443) - comunicación



La disponibilidad general de HTTPS desde los APIC al vCenter se puede probar con un rizo:

```
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)
```

. . .
Verifique que el líder compartido tenga una conexión TCP establecida en el puerto 443 mediante el comando netstat.

```
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. Realice una captura de paquetes

Si es posible, realice una captura de paquetes a lo largo de la ruta entre el líder del fragmento y vCenter para identificar si el tráfico se envía y recibe en cualquier dispositivo.

Inventario de VMware

La siguiente tabla muestra una lista de parámetros VMWare VDS y especifica si el APIC puede configurarlos.

Parámetros de VMware VDS administrados por APIC

VMware VDS	Valor Predeterminado	¿Se puede configurar mediante la política Cisco APIC?
Nombre	Nombre de dominio VMM	Sí (derivado del dominio)
Descripción	'Switch virtual APIC'	No
Nombre de carpeta	Nombre de dominio VMM	Sí (derivado del dominio)
Versión	Máxima compatibilidad con vCenter	Yes
Protocolo de detección	LLDP	Yes
Puertos de enlace ascendente y nombres de enlace ascendente	8	Sí (de Cisco APIC versión 4.2(1))
Prefijo de nombre de enlace ascendente	enlace ascendente	Sí (de Cisco APIC versión 4.2(1))
MTU máxima	9000	Yes
política LACP	inhabilitado	Yes
Reflejo de Puerto	0 sesiones	Yes
Alarmas	2 alarmas añadidas en el nivel de carpeta	No

La siguiente tabla muestra una lista de parámetros de grupo de puertos VMWare VDS y especifica si el APIC puede configurarlos.

Parámetros de grupo de puertos VMWare VDS administrados por APIC

Grupo de puertos de VMware VDS	Valor Predeterminado	Configurable mediante política APIC
Nombre	Nombre del arrendatario | Nombre del perfil de aplicación | Nombre de EPG	Sí (derivado de EPG)
Enlace de puerto	Enlace estático	No
VLAN	Seleccionado del conjunto de VLAN	Yes
Algoritmo de	Derivado de la política de canal de	Yes

equilibrio de carga	puerto en APIC	
modo promiscuo	Inhabilitado	Yes
Transmisión falsificada	Inhabilitado	Yes
Cambio de MAC	Inhabilitado	Yes
Bloquear todos los puertos	FALSO	No

Solución de problemas de inventario VMware

Los eventos de sincronización del inventario se producen para garantizar que el APIC es consciente de los eventos del vCenter que pueden requerir que el APIC actualice la política de forma dinámica. Existen dos tipos de eventos de sincronización de inventario que pueden producirse entre vCenter y APIC; una sincronización de inventario completa y una sincronización de inventario basada en eventos. La programación predeterminada de una sincronización de inventario completa entre el APIC y el vCenter es cada 24 horas, aunque también se pueden activar manualmente. Las sincronizaciones de inventario basadas en eventos suelen estar vinculadas a tareas desencadenadas, como vMotion. En este escenario, si una máquina virtual se mueve de un host a otro y esos hosts están conectados a dos switches de hoja diferentes, el APIC escuchará el evento de migración de VM y, en el escenario de la inmediatez de la implementación a demanda, desprogramará el EPG en la hoja de origen y programará el EPG en la hoja de destino.

En función de la inmediatez de la implementación de los EPG asociados a un dominio VMM, el hecho de que no se extraiga el inventario del vCenter podría tener consecuencias no deseadas. En el caso de que el inventario no se haya completado o sea parcial, siempre habrá un error que indique el objeto u objetos que han causado el error.

Situación 1: máquina virtual con respaldo no válido:

Si se mueve una máquina virtual de un vCenter a otro o se determina que la máquina virtual tiene una copia de seguridad no válida (por ejemplo, un adjunto de grupo de puertos a un DVS antiguo o eliminado), se informará de que la vNIC tiene problemas operativos.

```
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.
```

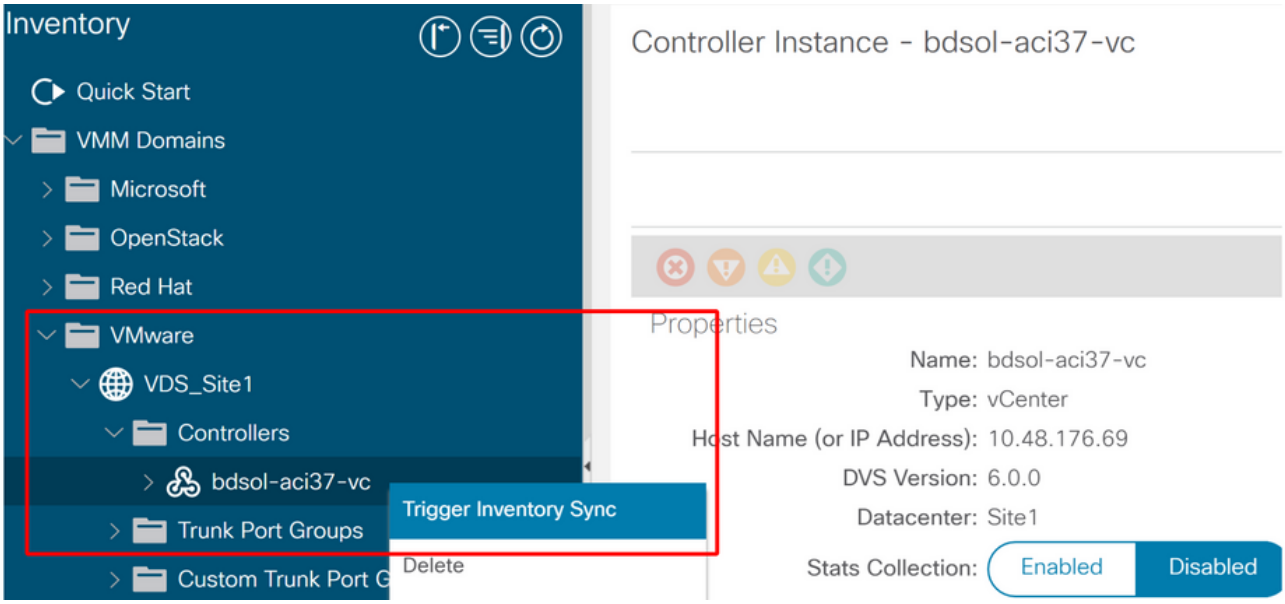
Situación 2: el administrador del vCenter modificó un objeto administrado de VMM en el vCenter:

No se admite la modificación de objetos administrados por el APIC desde vCenter. El siguiente error se observaría si se realiza una operación no admitida en 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 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.
```

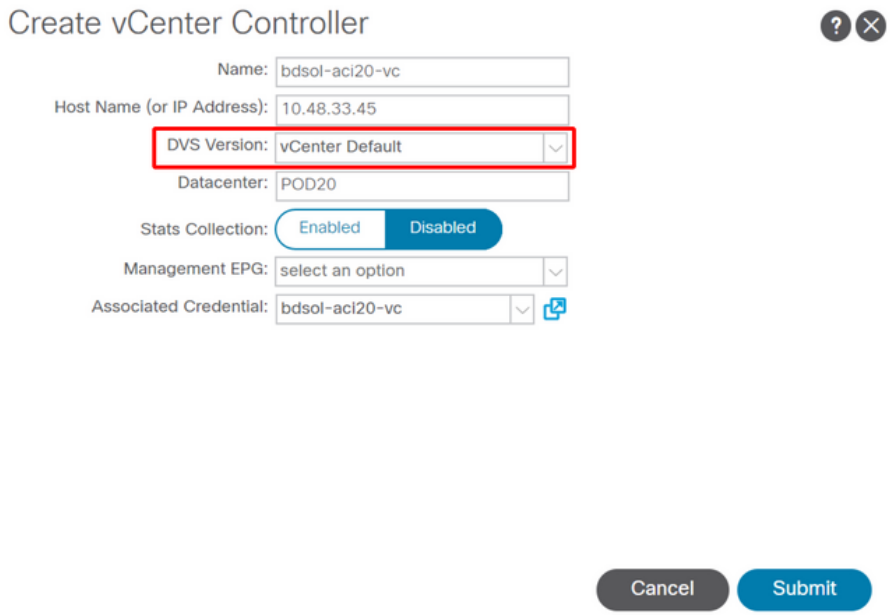
Dominio VM de VMWare - controlador vCenter - sincronización del inventario de desencadenadores



Versión de VMware DVS

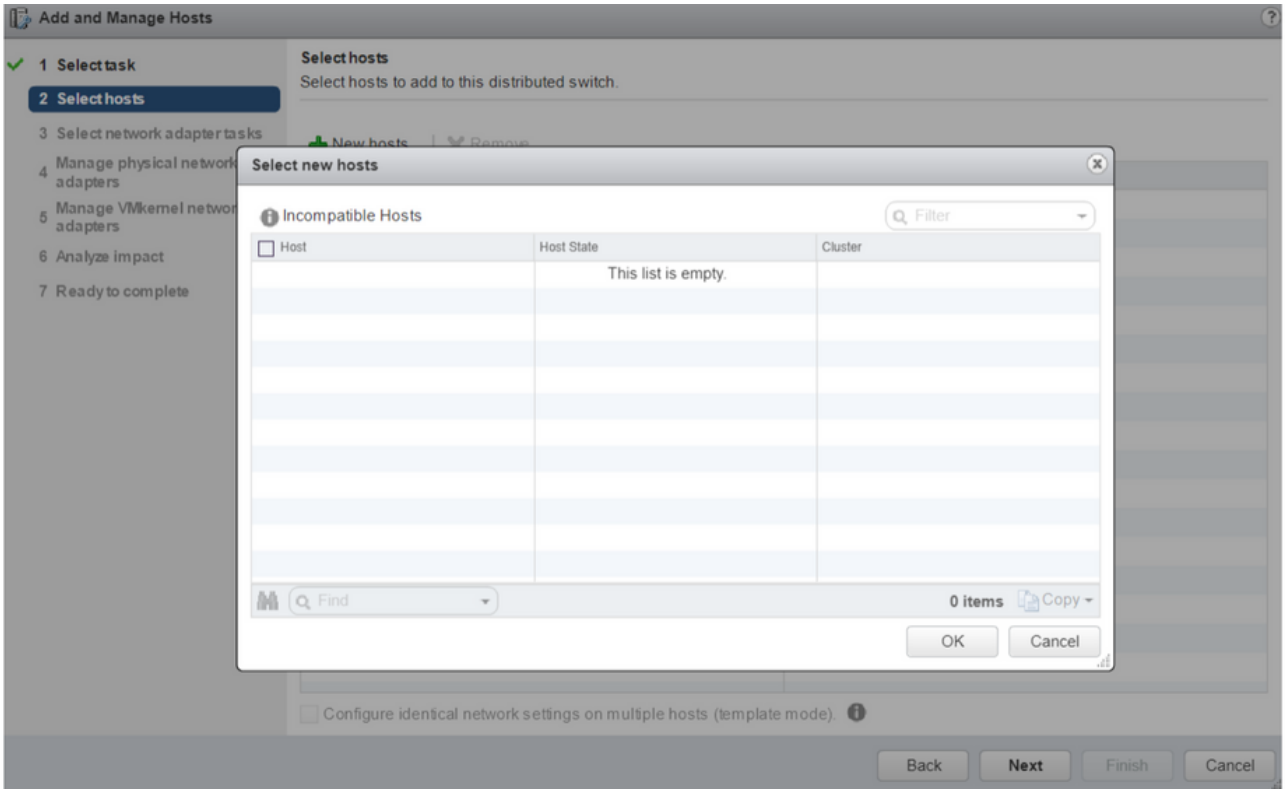
Al crear un nuevo controlador vCenter como parte de un dominio VMM, la configuración predeterminada para la versión DVS será utilizar el 'vCenter predeterminado'. Al seleccionar esta opción, la versión DVS se creará con la versión del vCenter.

Dominio VMware - creación del controlador vCenter

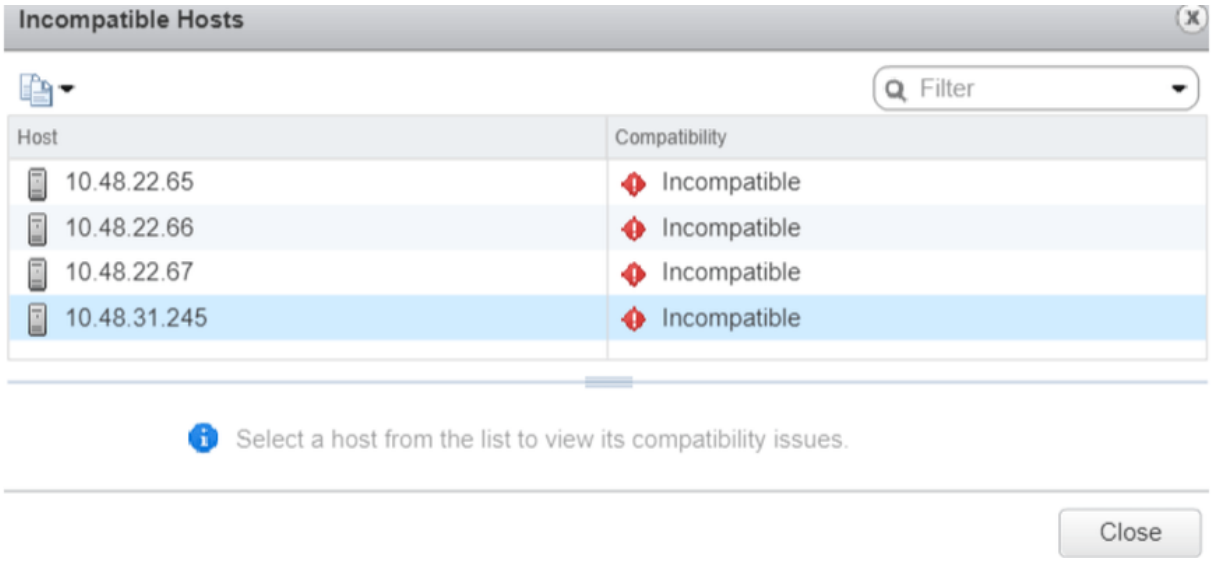


Esto significa que, en el ejemplo de un vCenter con 6.5 y servidores ESXi con 6.0, el APIC creará un DVS con la versión 6.5 y, por tanto, el administrador del vCenter no podrá agregar los servidores ESXi con 6.0 al DVS de ACI.

DVS gestionado por APIC: adición de hosts de vCenter (lista vacía)



DVS gestionado por APIC: adición de hosts vCenter; hosts incompatibles



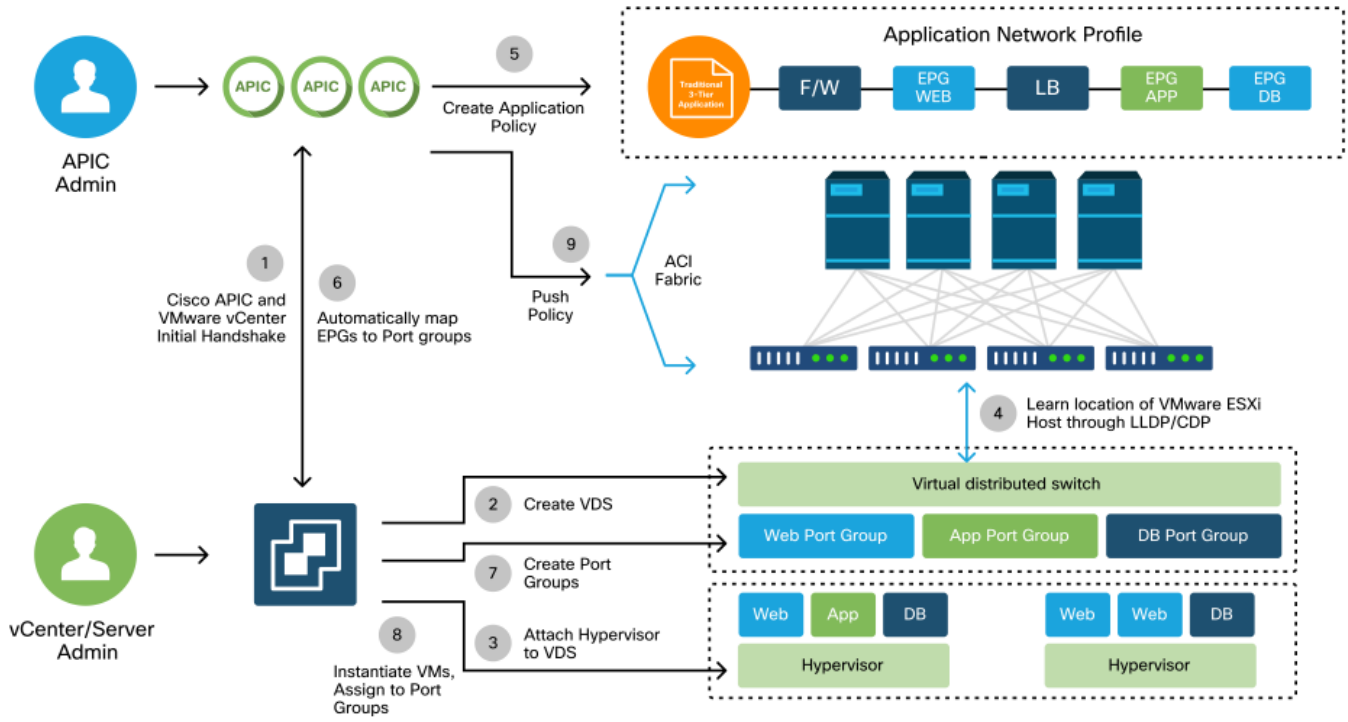
Por lo tanto, al crear un dominio VMM, asegúrese de seleccionar la 'versión DVS' correcta de modo que los servidores ESXi necesarios se puedan agregar al DVS.

Detección dinámica de host

Proceso de detección de host/VM

La integración de VMM en ACI se diferencia del aprovisionamiento manual en que el fabric puede detectar de forma dinámica dónde se conectan los hosts y las máquinas virtuales aplicables para implementar la política de forma eficaz. A través de este proceso dinámico, ACI puede optimizar el uso de los recursos de hardware en los switches de hoja, ya que las VLAN, SVI, las reglas de zonificación, etc. se implementan en los nodos solo cuando hay un terminal conectado que requiere la política. La ventaja para el administrador de red, desde una perspectiva de facilidad de uso, es que ACI proporcionará VLAN/política donde las VM se conectan de forma automatizada. Para determinar dónde se debe implementar la política, el APIC utilizará información de varias fuentes. El siguiente diagrama describe los pasos básicos del proceso de detección de hosts cuando se utiliza un dominio VMM basado en DVS.

Dominio VMware — Flujo de trabajo de implementación



En resumen, los siguientes pasos clave se producen cuando:

- LLDP o CDP se intercambia entre el hipervisor y los switches de hoja.
- Los hosts notifican la información de adyacencia al vCenter.
- vCenter notifica al APIC la información de adyacencia: APIC conoce el host mediante la sincronización del inventario.
- APIC envía la política al puerto de hoja: revise la subsección "Inmediatez de la resolución" de esta sección para comprender mejor estas condiciones.
- Si se pierde la información de adyacencia de vCenter, APIC puede eliminar la política.

Como se puede ver, CDP/LLDP juega un papel clave en el proceso de detección y es importante asegurarse de que esté configurado correctamente y que ambos lados estén usando el mismo protocolo.

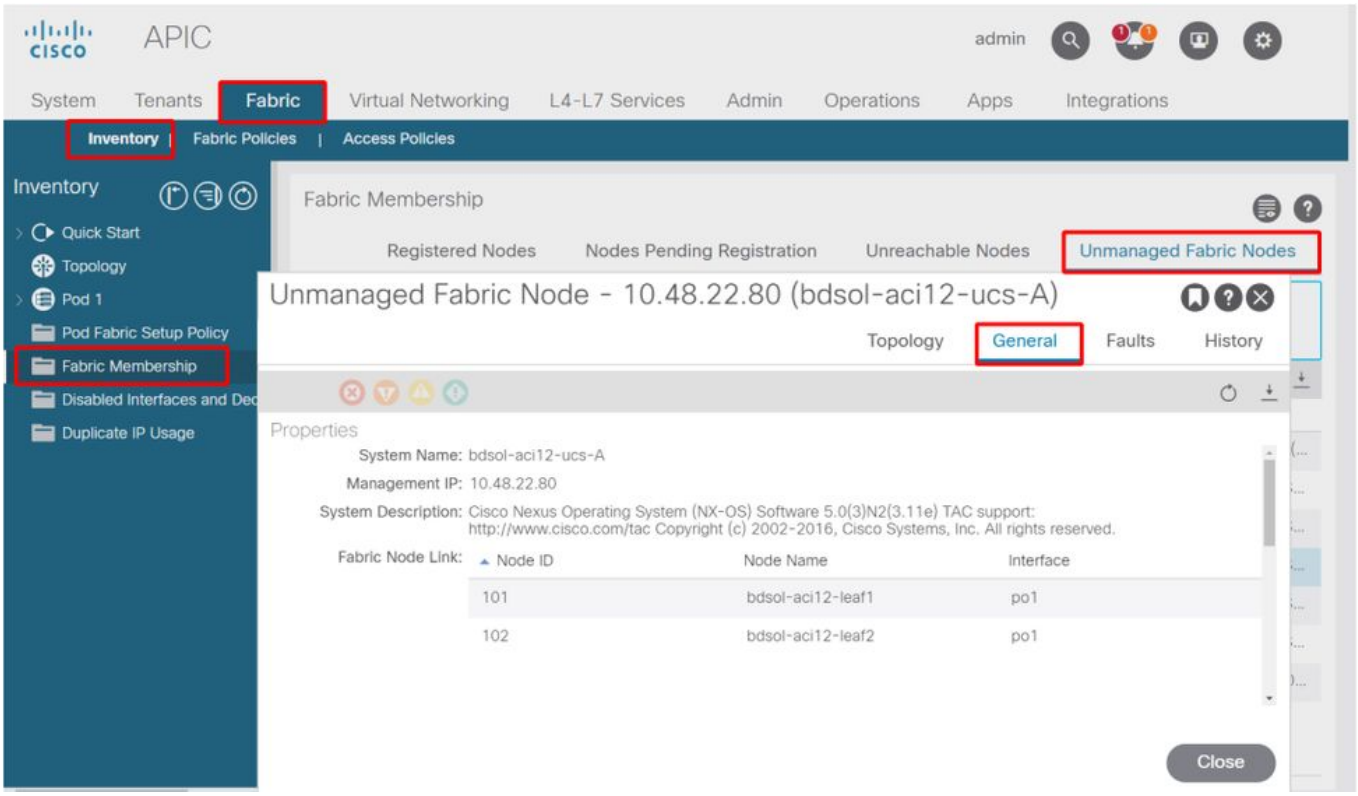
Fabric LooseNode/switch intermedio: caso práctico

En una implementación que utilice un chasis de servidor blade con un switch intermedio entre los switches de hoja y el hipervisor, el APIC debe "unir" la adyacencia. En esta situación, se podrían utilizar varios protocolos de detección, ya que el switch intermedio puede tener requisitos de

protocolo diferentes a los del host.

En una configuración con un servidor en formato blade y un switch intermedio (es decir, un switch de chasis de servidor en formato blade), ACI debe detectar el switch intermedio y asignar los hipervisores detrás de él. En ACI, el switch intermedio se denomina "nodo suelto" o "nodo de fabric no administrado". Los nodos sueltos detectados se pueden ver en 'Fabric > Inventory > Fabric Membership > Unmanaged Fabric Nodes'. Si se desplaza a uno de estos tipos de servidores en la GUI, el usuario puede ver la ruta desde el switch de hoja al switch intermedio y al host.

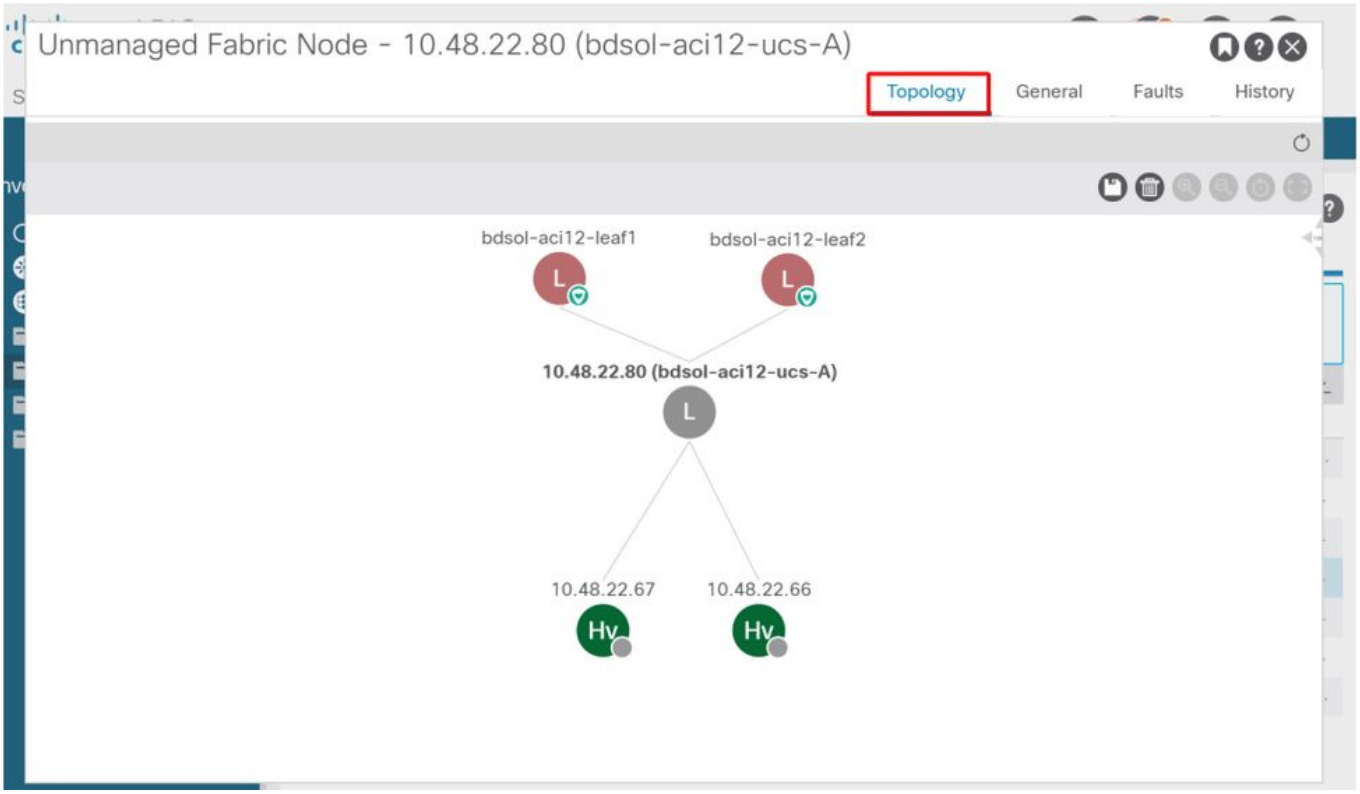
Interfaz de usuario de APIC: nodos de fabric no administrados (LooseNodes)



Con la detección de LLDP o CDP en su lugar, ACI puede determinar la topología para dichos LooseNodes, dado que el flujo descendente del hipervisor del switch intermedio se administra a través de la integración de VMM, y la hoja en sí tiene una adyacencia al switch intermedio desde el flujo descendente.

Este concepto se ilustra en la siguiente imagen.

Interfaz de usuario de APIC: ruta de nodo de fabric no administrada

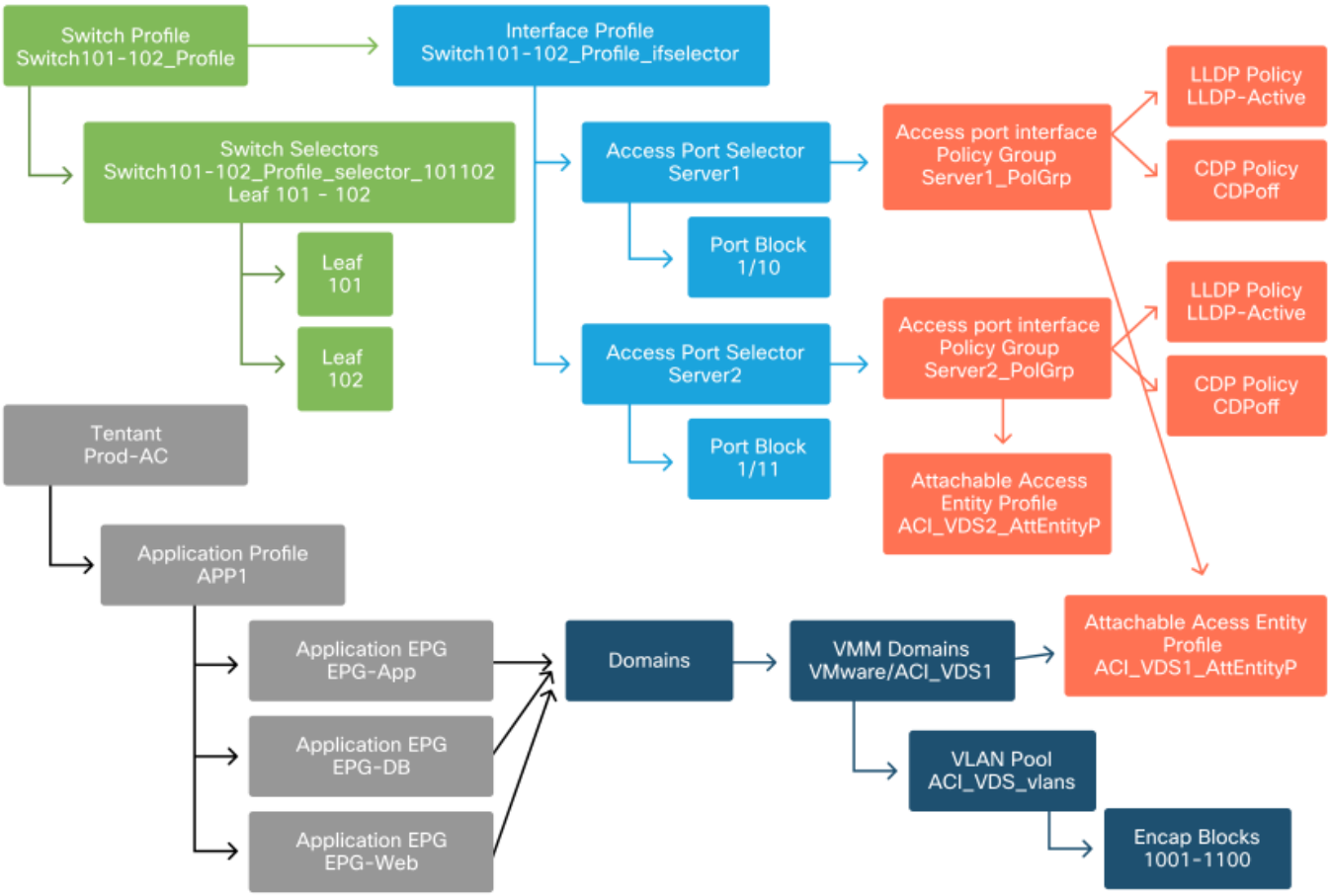


Resolución inmediata

En situaciones en las que los servicios críticos utilizan el DVS integrado en VMM, como la conectividad de gestión con vCenter/ESXi, es prudente utilizar la solución inmediata previa al aprovisionamiento. Con esta configuración, se elimina el mecanismo de detección dinámica de host y, en su lugar, las políticas/VLAN se programan estáticamente en las interfaces de cara al host. En esta configuración, las VLAN de VMM siempre se implementarán en todas las interfaces vinculadas al AEP al que hace referencia el dominio VMM. Esto elimina la posibilidad de que una VLAN crítica (como la administración) se elimine de un puerto debido a un evento de adyacencia relacionado con el protocolo de detección.

Consulte el siguiente diagrama:

Ejemplo de implementación previa al aprovisionamiento



Si se configuró la provisión previa para un EPG en el dominio VMM ACI_VDS1, las VLAN se implementarían en los enlaces para Server1 pero no para Server2, ya que el AEP de Server2 no incluye el dominio VMM ACI_VDS1.

Para resumir la configuración de inmediatez de la resolución:

- A demanda: la política se implementa cuando se establece la adyacencia entre la hoja y el host y una VM conectada al grupo de puertos.
- Inmediato: la política se implementa cuando se establece la adyacencia entre la hoja y el host.
- Preaprovisionamiento: la política se implementa en todos los puertos mediante un AEP con el dominio VMM contenido; no se requiere adyacencia.

Escenarios de resolución de problemas

La VM no puede resolver el ARP para su gateway predeterminado

En esta situación, se ha configurado la integración de VMM y el DVS se ha agregado al hipervisor, pero la VM no puede resolver el ARP para su gateway en ACI. Para que la VM tenga conectividad de red, verifique que se haya establecido la adyacencia y que se hayan implementado las VLAN.

En primer lugar, el usuario puede verificar que la hoja haya detectado el host mediante 'show lldp neighbors' o 'show cdp neighbors' en la hoja, dependiendo del protocolo seleccionado.

```
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 es necesario desde el punto de vista de la solución de problemas, esto se puede validar desde el lado de ESXi tanto en la CLI como en la GUI:

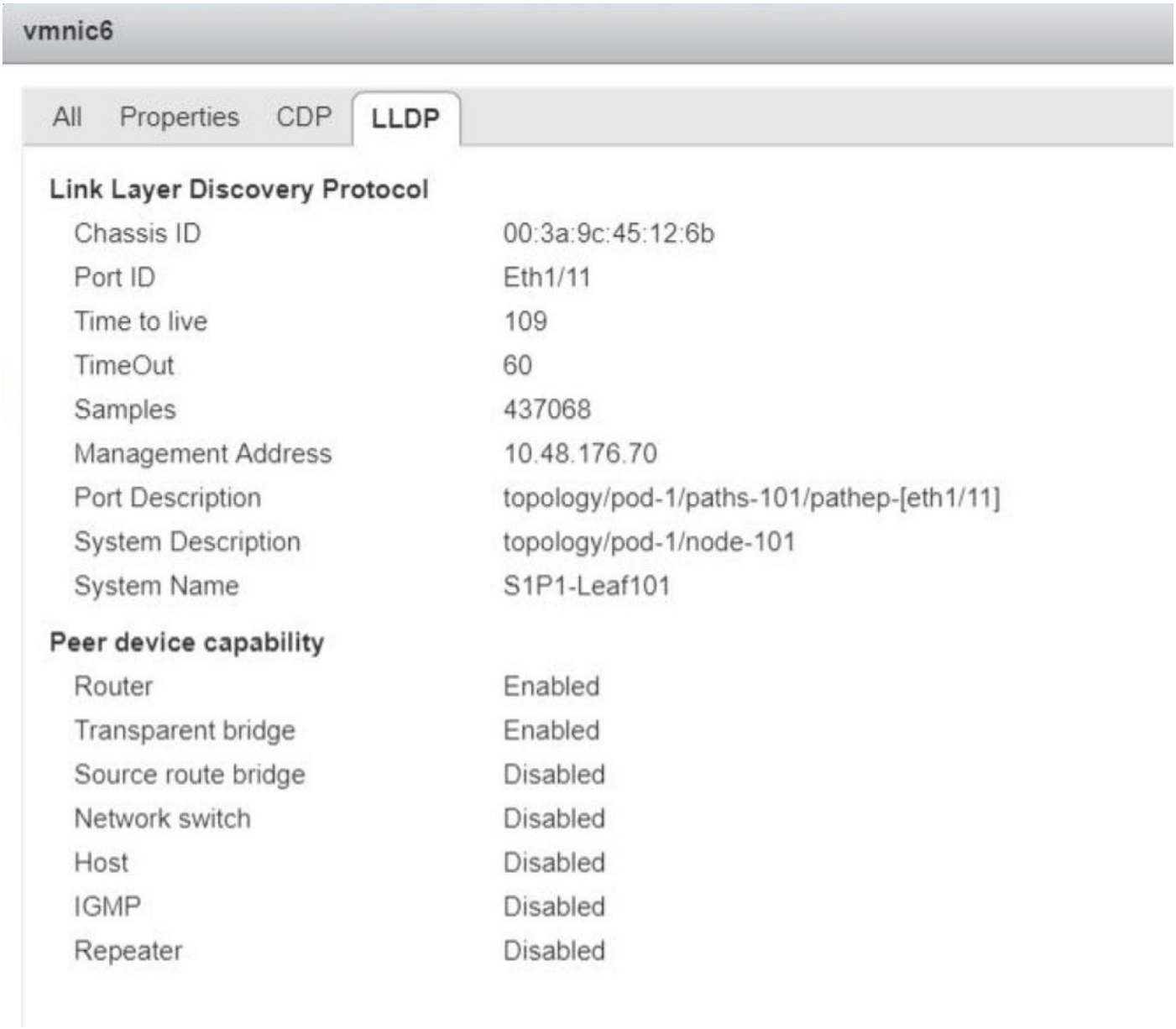
```
[root@host:~] esxcli network vswitch dvs vmware list
VDS_Site1
  Name: VDS_Site1
 ...
  Uplinks: vmnic7, vmnic6
  VMware Branded: true
  DVPort:
        Client: vmnic6
        DVPortgroup ID: dvportgroup-122
        In Use: true
        Port ID: 0

        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 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 --pnic-name=vmnic6 | grep -A2 "System Name"
              key = "System Name",
              value = "Leaf101"
           }
```

Detalles de adyacencia de vCenter Web Client - host - vmnic LLDP/CDP

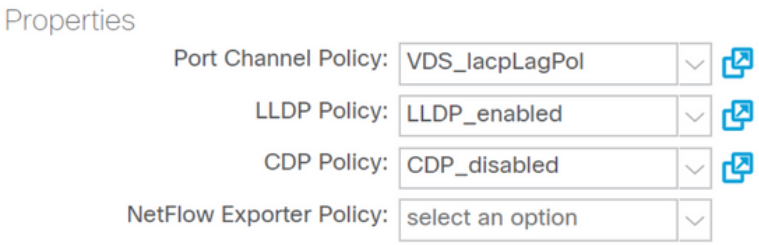


Si no se puede ver la adyacencia de LDP de hoja desde el host de ESXi, a menudo se debe a que se usa un adaptador de red configurado para generar LLDPDU en lugar del sistema operativo de ESXi. Asegúrese de validar si el adaptador de red tiene habilitado LLDP y, por lo tanto, consume toda la información LLDP. Si este es el caso, asegúrese de inhabilitar LLDP en el adaptador para que se controle a través de la política vSwitch.

Otra causa podría ser que existe una falta de alineación entre los protocolos de detección utilizados entre el hipervisor de hoja y el de ESXi. Asegúrese de que ambos extremos utilicen el mismo protocolo de detección.

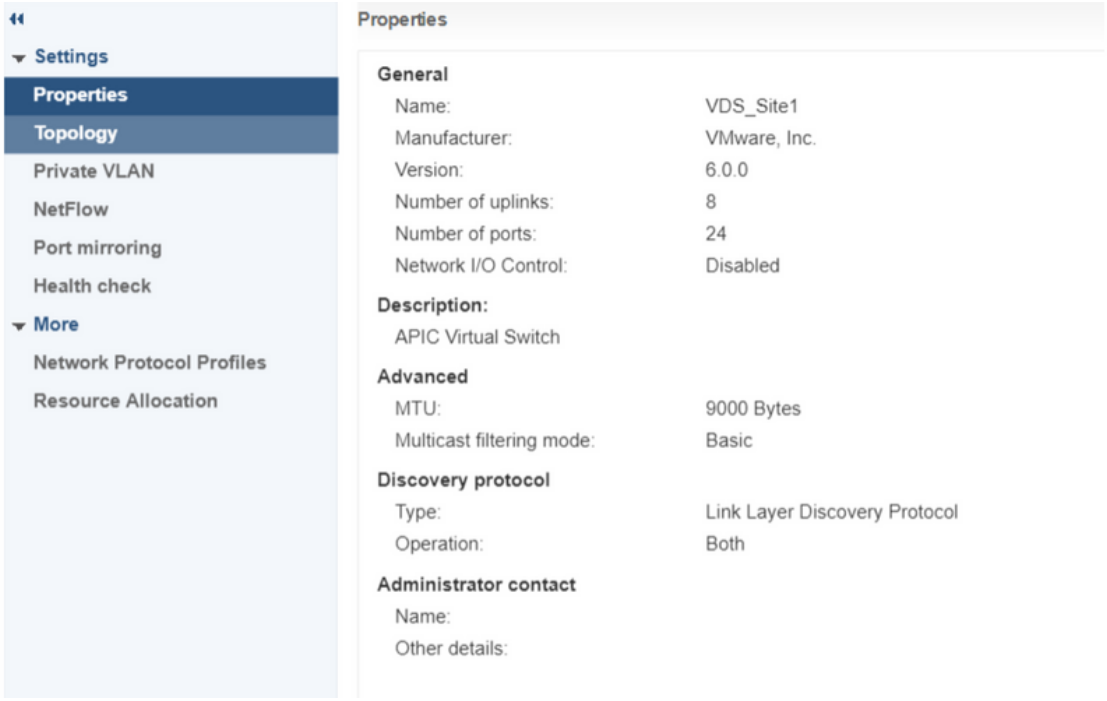
Para comprobar si los parámetros CDP/LLDP están alineados entre ACI y DVS en la interfaz de usuario de APIC, vaya a 'Red virtual > Dominios VMM > VMware > Política > Política vSwitch'. Asegúrese de habilitar solamente la política LLDP o CDP ya que son mutuamente excluyentes.

UI de APIC: dominio VM de VMWare: política de vSwitch



En vCenter, vaya a: 'Networking > VDS > Configure'.

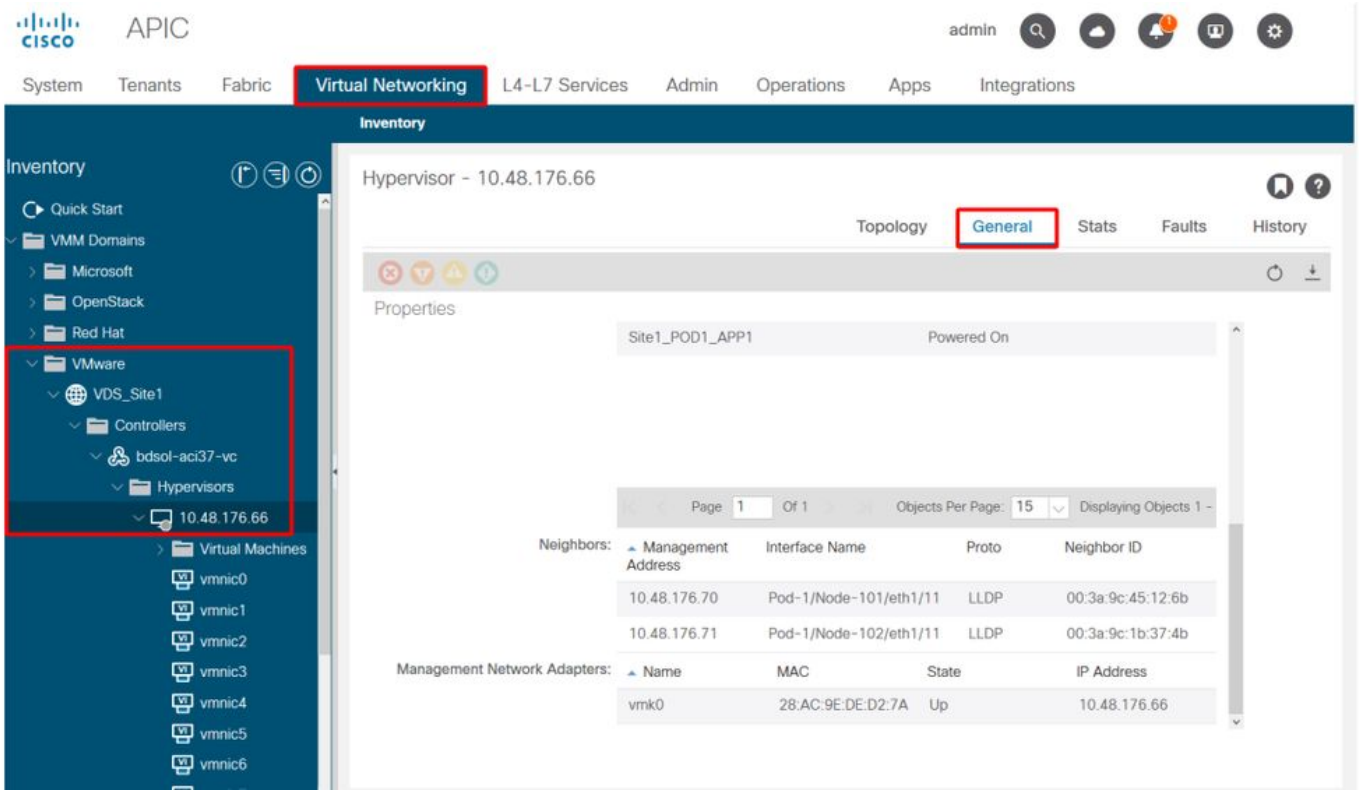
Interfaz de usuario de vCenter Web Client: propiedades de VDS



Corrija la configuración LLDP/CDP si es necesario.

A continuación, valide el APIC y observe la vecindad LLDP/CDP del host de ESXi en el switch de hoja de la interfaz de usuario en 'Red virtual > Dominios VMM > VMware > Política > Controlador > Hipervisor > General'.

Interfaz de usuario de APIC: dominio VM de VMWare: detalles del hipervisor



Si muestra los valores esperados, el usuario puede validar que la VLAN está presente en el puerto hacia el host.

```
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
```

Administración de vCenter/ESXi VMK conectada a DVS insertadas por APIC

En una situación en la que el tráfico de administración de vCenter o ESXi necesita utilizar el DVS integrado de VMM, es importante tener un cuidado especial para evitar un punto muerto en la activación de las adyacencias dinámicas y activar las VLAN necesarias.

Para vCenter, que suele crearse antes de configurar la integración de VMM, es importante utilizar un dominio físico y una ruta estática para garantizar que la VLAN encap de la VM de vCenter esté siempre programada en los switches de hoja, de modo que se pueda utilizar antes de que la integración de VMM esté completamente configurada. Incluso después de configurar la integración de VMM, se recomienda dejar esta ruta estática en su lugar para garantizar siempre la disponibilidad de este EPG.

Para los hipervisores ESXi, según la "Guía de virtualización de Cisco ACI" de Cisco.com, al migrar a vDS es importante asegurarse de que el EPG al que se conectará la interfaz VMK se implemente con la inmediatez de resolución establecida en Preaprovisionamiento. Esto garantizará que la VLAN esté siempre programada en los switches de hoja sin depender de la detección LLDP/CDP de los hosts ESXi.

Adyacencias de host no detectadas detrás de LooseNode

Las causas típicas de los problemas de detección de LooseNode son:

- CDP/LLDP no está habilitado El CDP/LLDP se debe intercambiar entre el switch intermedio, los switches de hoja y los hosts ESXiPara Cisco UCS, esto se consigue mediante una política de control de red en la vNIC
- Un cambio en la IP de administración del vecino LLDP/CDP interrumpe la conectividad El vCenter verá la nueva IP de administración en la adyacencia LLDP/CDP, pero no actualizará APICActivar una sincronización manual del inventario para corregir
- Las VLAN de VMM no se agregan al switch intermedio El APIC no programa switches blade/intermedios de terceros.La aplicación de integración Cisco UCSM (ExternalSwitch) está disponible en la versión 4.1(1).Las VLAN deben configurarse y conectarse mediante enlaces troncales a los enlaces ascendentes conectados a los nodos de hoja de ACI y a los enlaces descendentes conectados a los hosts

F606391 - Faltan adyacencias para el adaptador físico en el host

Al observar el siguiente fallo:

```
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)
```

Revise el flujo de trabajo en la sección "La VM no puede resolver ARP para su gateway predeterminado", ya que esto significa que faltan adyacencias CDP/LLDP. Estas adyacencias deben verificarse de extremo a extremo.

Equilibrio de carga de link ascendente de hipervisor

Al conectar hipervisores como ESXi a un fabric ACI, normalmente se conectarán con varios enlaces ascendentes. De hecho, se recomienda tener un host de ESXi conectado al menos a dos switches de hoja. Esto minimizará el impacto de los escenarios de fallos o las actualizaciones.

Para optimizar el uso de los enlaces ascendentes por parte de las cargas de trabajo que se ejecutan en un hipervisor, las configuraciones de VMware vCenter permiten configurar varios algoritmos de equilibrio de carga para el tráfico generado por VM hacia los enlaces ascendentes del hipervisor.

Es fundamental tener todos los hipervisores y el fabric de ACI alineados con la misma configuración de algoritmo de equilibrio de carga para garantizar que se dispone de la conectividad correcta. Si no lo hace, se pueden producir caídas intermitentes del flujo de tráfico y movimientos de terminales en el fabric de ACI.

Esto se puede observar en un fabric de ACI mediante alertas excesivas como:

```
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
```

Este capítulo trata sobre la conectividad del host VMWare ESXi en ACI, pero es aplicable a la mayoría de los hipervisores.

Servidor en rack

Al analizar las distintas formas en las que un host ESXi puede conectarse a un fabric ACI, se dividen en 2 grupos: algoritmos de equilibrio de carga dependientes del switch e independientes del switch.

Los algoritmos de balanceo de carga independiente del switch son maneras de conectarse donde no se necesita una configuración específica del switch. Para el balanceo de carga dependiente del switch, se requieren configuraciones específicas del switch.

Asegúrese de validar si la política del vSwitch está en línea con los requisitos del 'Grupo de políticas de acceso de ACI' según la tabla siguiente.

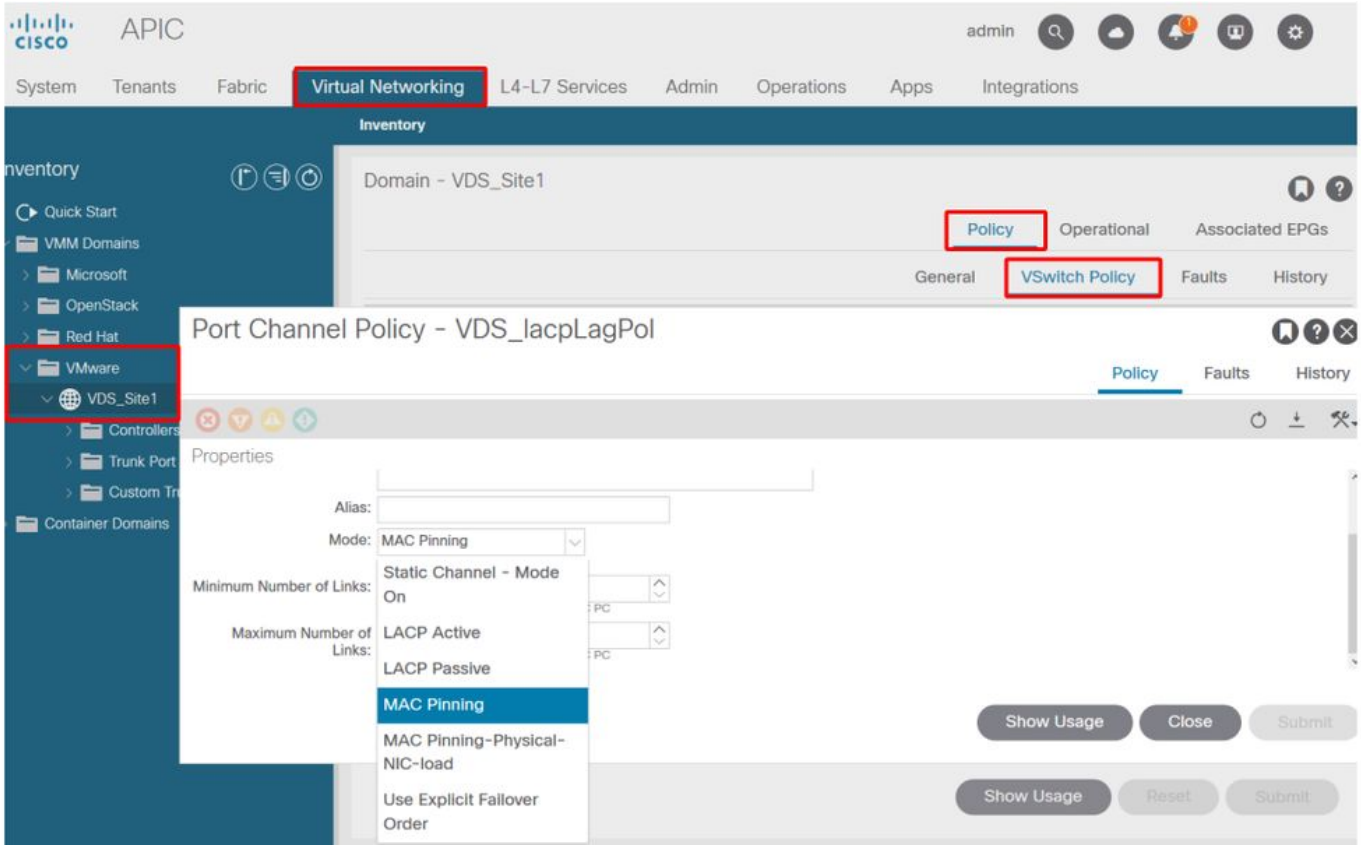
Política de Teaming y ACI vSwitch

Teaming y modo de failover de VMware	Política de vSwitch de ACI	Descripción	Grupo de políticas de acceso de ACI: canal de puerto necesario
Ruta basada en el puerto virtual de origen	Fijación MAC	Seleccione un enlace ascendente basado en los ID de puertos virtuales del switch. Una vez que el switch virtual selecciona un enlace ascendente para una máquina virtual o un adaptador VMKernel, siempre reenvía el tráfico a través del mismo enlace ascendente para esta máquina virtual o adaptador VMKernel.	No
Ruta basada en hash de MAC de origen	NA	Seleccione un enlace ascendente basado en un hash de la dirección MAC de origen	NA
Orden explícito de failover	Usar modo de conmutación por fallo explícito	En la lista de adaptadores activos, utilice siempre el enlace ascendente de mayor orden que supere los criterios de detección de conmutación por error. Con esta opción no se realiza ningún equilibrio de carga real.	No
Agregación de enlaces (LAG): basada en hash IP	Canal estático - Modo activado	Seleccione un enlace ascendente basado en un hash de las direcciones IP de origen y destino de cada paquete. Para los paquetes no IP, el switch utiliza los datos de esos campos para calcular el hash. El agrupamiento basado en IP	Sí (modo de canal establecido en 'activado')

Agregación de enlaces (LAG): LACP	LACP activo/pasivo	requiere que en el lado de ACI se configure un canal de puerto / VPC con 'mode on'. Seleccione un enlace ascendente basado en un hash seleccionado (20 opciones de hash diferentes disponibles). El agrupamiento basado en LACP requiere que en el lado de ACI se configure un canal de puerto/VPC con LACP habilitado. Asegúrese de crear una política de retraso mejorada en ACI y aplicarla a la política de VSwitch. Disponible para grupos de puertos distribuidos o puertos distribuidos.	Sí (modo de canal establecido en 'LACP activo/pasivo')
Ruta basada en carga NIC física (LBT)	Fijación MAC: carga NIC física	Seleccione un enlace ascendente basado en la carga actual de los adaptadores de red físicos conectados al grupo de puertos o al puerto. Si un enlace ascendente permanece ocupado al 75% o más durante 30 segundos, el vSwitch del host mueve una parte del tráfico de la máquina virtual a un adaptador físico con capacidad libre.	No

Consulte la captura de pantalla siguiente sobre cómo validar la política de canal de puerto como parte de la política de vSwitch en vigor.

Política de vSwitch de ACI: política de canal de puerto



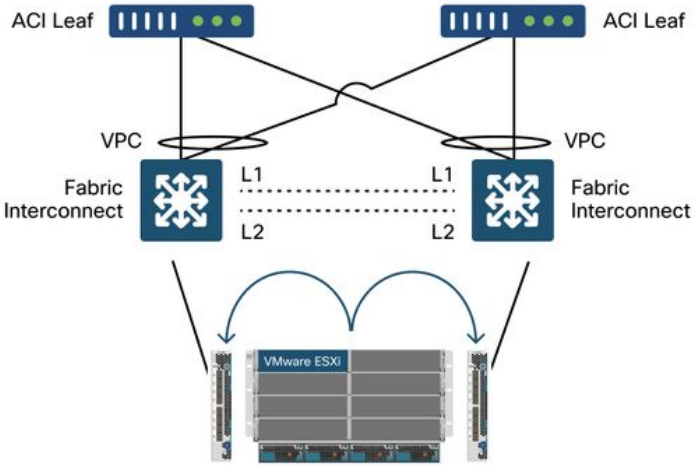
Nota: Para obtener una descripción más detallada de las funciones de red de VMware, consulte vSphere Networking en https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.networking.doc/GUID-D34B1ADD-B8A7-43CD-AA7E-2832A0F7EE76.html

Caso práctico de Cisco UCS serie B

Al utilizar servidores de la serie B de Cisco UCS, es importante tener en cuenta que se conectan dentro de su chasis a Fabric Interconnects (FI) de UCS que no tienen un plano de datos unificado. Este caso práctico se aplica igualmente a otros proveedores que emplean una topología similar. Debido a esto, puede haber una diferencia entre el método de equilibrio de carga utilizado desde un lado de switch de hoja ACI y el lado vSwitch.

A continuación se muestra una topología UCS FI con ACI:

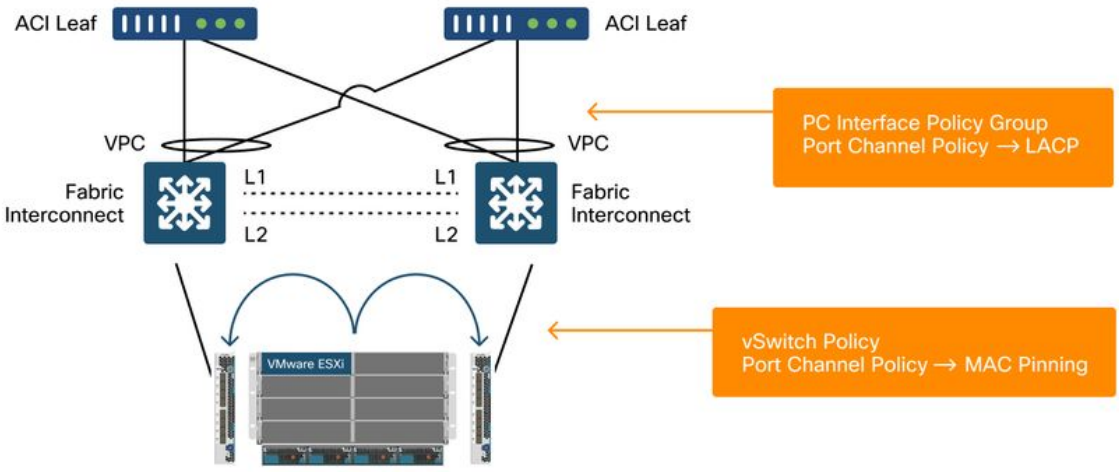
Cisco UCS FI con switches de hoja ACI: topología



Aspectos clave a tener en cuenta:

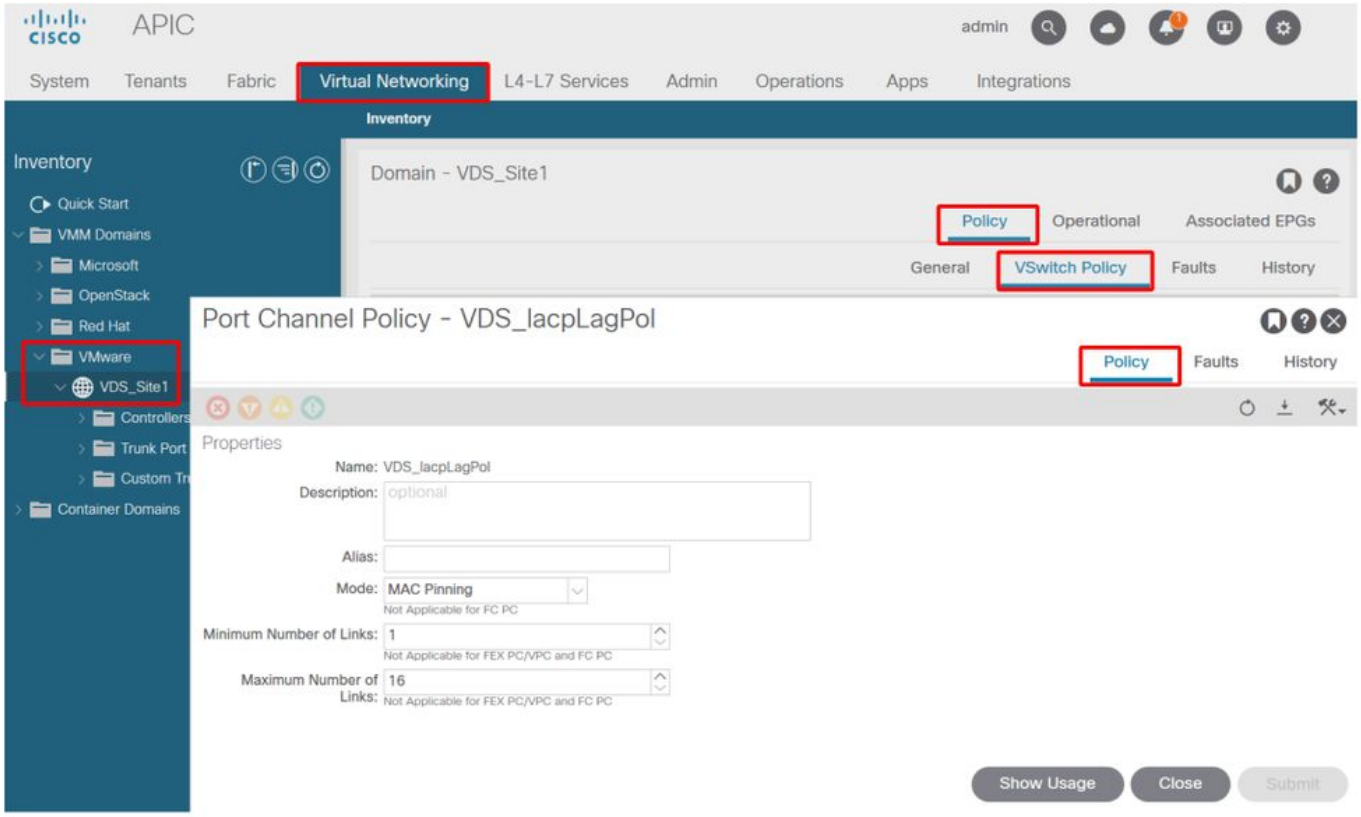
- Cada FI de Cisco UCS tiene un canal de puerto hacia los switches de hoja de ACI.
- Los FI de UCS se interconectan directamente solo para fines de latidos (no se utilizan para el plano de datos).
- La vNIC de cada servidor blade se fija a una FI de UCS específica o utiliza una ruta hacia una de las FI mediante la conmutación por fallo del fabric de UCS (Activo-En espera).
- El uso de algoritmos de hash de IP en el vSwitch del host ESXi provocará inestabilidad de MAC en los UCS FI.

Para configurar esto correctamente, haga lo siguiente:



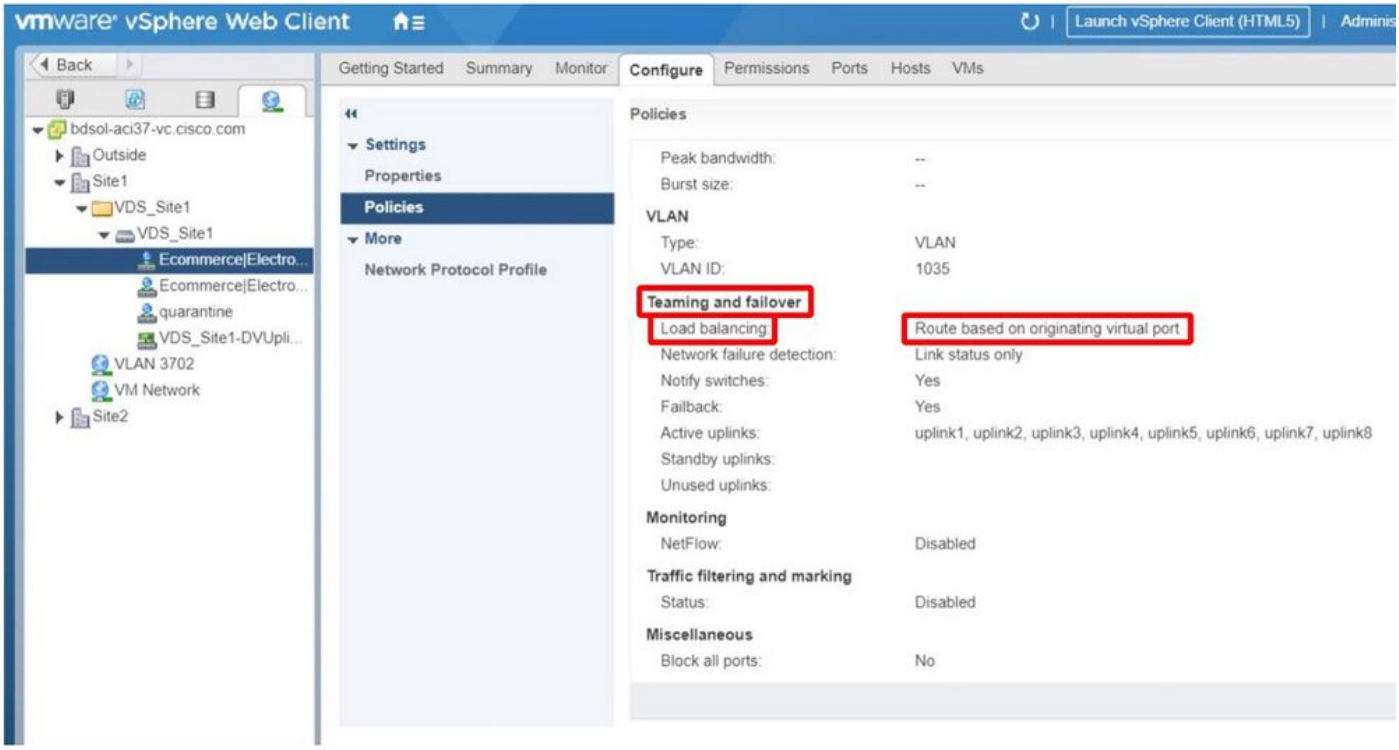
Cuando se configura el anclaje MAC en la política de canal de puerto como parte de la política de vSwitch en ACI, esto se mostrará como configuración de agrupamiento 'Ruta basada en el puerto virtual de origen' de los grupos de puertos en el VDS.

ACI: política de canal de puerto como parte de la política de vSwitch



El asistente denomina automáticamente la política de canal de puerto utilizada en el ejemplo anterior, por lo que se denomina "CDS_lacpLagPol", aunque utilizamos el modo "Fijación de MAC".

VMWare vCenter — ACI VDS — Grupo de puertos — Configuración de equilibrio de carga


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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).