Solucionar problemas de integração do ACI VMM

Contents

Introduction

Este documento descreve as etapas para entender e solucionar problemas da Integração do

Virtual Machine Manager (VMM) da ACI.

Informações de Apoio

O material deste documento foi extraído do livro Troubleshooting Cisco Application Centric Infrastructure, Second Edition, especificamente os capítulos **Integração do VMM - Visão geral, Integração do VMM - Conectividade do vCenter, Integração do VMM - Descoberta dinâmica do host** e **Integração do VMM - Balanceamento de carga do uplink do hipervisor** .

Visão geral do Virtual Machine Manager

Os controladores da ACI têm a capacidade de se integrar a gerenciadores de máquinas virtuais (VMMs) de terceiros.

Esse é um dos principais recursos da ACI, pois simplifica e automatiza as operações para a configuração de rede de ponta a ponta da malha e para as cargas de trabalho que se conectam a ela. A ACI oferece um único modelo de política de sobreposição que pode ser estendido para vários tipos de carga de trabalho, ou seja, máquinas virtuais, servidores bare-metal e contêineres.

Este capítulo abordará especificamente alguns cenários típicos de solução de problemas relacionados à integração do VMware vCenter VMM.

O leitor irá mostrar:

- Investigação de falhas de comunicação do vCenter.
- Cenários de falha e processo de detecção dinâmica de host e VM.
- Algoritmos de balanceamento de carga do hipervisor.

Conectividade do vCenter

Controle de acesso baseado em funções (RBAC)

Os mecanismos pelos quais o APIC pode fazer interface com o Controlador vCenter dependem da conta de usuário associada a um determinado Domínio do VMM. Os requisitos específicos são descritos para o usuário do vCenter associado ao Domínio do VMM para garantir que o APIC possa executar operações com êxito no vCenter, seja enviando e recuperando inventário e configurações ou monitorando e ouvindo eventos relacionados ao inventário gerenciado.

A maneira mais fácil de eliminar a preocupação com tais requisitos é usar a conta do vCenter do administrador que tem acesso total; no entanto, esse tipo de liberdade nem sempre está disponível para o administrador da ACI.

Os privilégios mínimos para uma conta de usuário personalizada, a partir da versão 4.2 da ACI, são os seguintes:

- **Alarmes** O APIC cria dois alarmes na pasta. Um para DVS e outro para grupo de portas. Um alarme é acionado quando a política de domínio do EPG ou VMM é excluída no APIC, no entanto o vCenter não pode excluir o Grupo de portas ou DVS correspondente devido a ter VMs anexadas a ele.

- **Switch distribuído**
- **Grupo dvPort**
- **Pasta**
- **Rede** O APIC gerencia as configurações de rede, como adicionar ou excluir grupos de portas, definir MTU de host/DVS, LLDP/CDP, LACP etc.
- **Host** Se estiver usando AVS além do mencionado acima, o usuário precisará do privilégio de host no data center onde o APIC criará DVS.**Host.Configuração.Configurações avançadasHost.Operações locais.Reconfigurar máquina virtualHost.Configuração.Configuração de rede**Isso é necessário para o AVS e o recurso de posicionamento automático para VMs de serviço virtuais da camada 4 para a camada 7. Para AVS, o APIC cria a interface VMK e a coloca no grupo de portas VTEP usado para OpFlex.
- **Máquina virtual** Se os gráficos de serviço estiverem em uso, o privilégio de máquina virtual para os dispositivos virtuais também será necessário.**Virtual machine.Configuration.Modify configurações do dispositivoMáquina virtual.Configuração.Configurações**

Solução de problemas relacionados ao RBAC

Os problemas de RBAC são encontrados com mais frequência durante a configuração inicial de um Domínio do VMM, mas podem ser encontrados se um administrador do vCenter modificar as permissões da conta de usuário associada ao Domínio do VMM após a configuração inicial já ter ocorrido.

O sintoma pode se apresentar das seguintes maneiras:

- Incapacidade parcial ou total de implantar novos serviços (criação de DVS, criação de grupo de portas, alguns objetos são implantados com êxito, mas não todos).
- O inventário operacional está incompleto ou ausente das visualizações do administrador da ACI.
- Falhas geradas por operação não suportada do vCenter ou para qualquer um dos cenários acima (por exemplo, falha na implantação do grupo de portas).
- O controlador vCenter é relatado como off-line e as falhas indicam que há problemas relacionados à conectividade ou às credenciais.

Solução para problemas relacionados a RBAC

Verifique se todas as permissões acima foram concedidas ao usuário do vCenter configurado no Domínio do VMM.

Outro método é fazer logon diretamente no vCenter com as mesmas credenciais definidas na configuração de Domínio do VMM e tentar operações semelhantes (criação de grupo de portas, etc.). Se o usuário não puder executar essas mesmas operações enquanto estiver conectado diretamente ao vCenter, claramente as permissões corretas não serão concedidas ao usuário.

Solução de problemas de conectividade

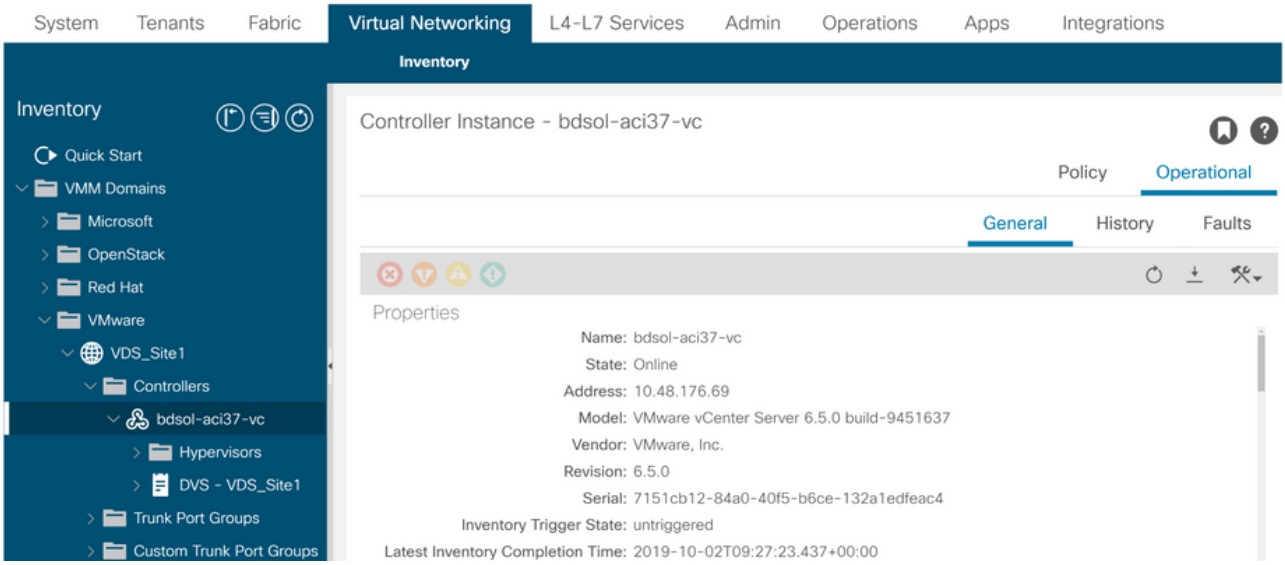
Ao solucionar um problema relacionado à conectividade do VMM, é importante observar alguns dos comportamentos fundamentais de como a ACI se comunica com o vCenter.

O primeiro e mais pertinente comportamento é que apenas um APIC no cluster está enviando

configuração e coletando inventário em um determinado momento. Este APIC é conhecido como o **líder compartilhado** para este Domínio do VMM. No entanto, vários APICs estão ouvindo os **eventos do vCenter** para explicar um cenário em que o líder compartilhado perdeu um evento por qualquer motivo. Seguindo a mesma arquitetura distribuída de APICs, um determinado domínio do VMM terá um APIC tratando de dados e funcionalidade primários (neste caso, o líder compartilhado) e duas réplicas (no caso do VMM, eles são chamados de **seguidores**). Para distribuir a manipulação da comunicação e da funcionalidade do VMM nos APICs, dois Domínios do VMM podem ter os mesmos ou líderes compartilhados diferentes.

O estado de conectividade do vCenter pode ser encontrado navegando até o controlador VMM de interesse na GUI ou usando o comando CLI listado abaixo.

Domínio do VMM do VMWare - estado de conectividade do 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
```

Se um controlador do VMM for indicado como off-line, uma falha será lançada da seguinte forma:

```
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.
```

As etapas abaixo podem ser usadas para solucionar problemas de conectividade entre VC e APICs.

1. Identificação do Líder Compartilhado

A primeira etapa na solução de um problema de conectividade entre o APIC e o vCenter é entender qual APIC é o líder compartilhado para o domínio VMM fornecido. A maneira mais fácil de determinar essas informações é executar o comando 'show vmware domain name <domain>' em qualquer 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. Verificando a conectividade com o vCenter

Após identificar o APIC que está se comunicando ativamente com o vCenter, verifique a conectividade IP com ferramentas 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
```

Se o vCenter foi configurado usando o FQDN em vez do endereço IP, o comando nslookup pode ser usado para verificar a resolução de nome.

```
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
```

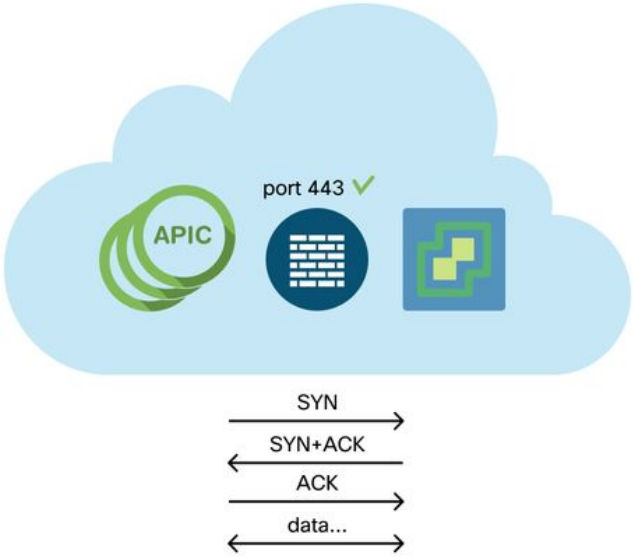
3. Verifique se OOB ou INB é usado

Verifique a tabela de roteamento APIC para verificar se a conectividade fora da banda ou dentro da banda é preferível e qual gateway é usado:

```
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. Certifique-se de que a porta 443 seja permitida entre todos os APICs e o vCenter, incluindo todos os firewalls no caminho da comunicação.

vCenter <-> APIC - HTTPS (porta TCP 443) - comunicação



A acessibilidade geral de HTTPS dos APICs para o vCenter pode ser testada com uma curva:

```
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 se o líder compartilhado tem uma conexão TCP estabelecida na porta 443 usando o 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. Executar uma captura de Pacote

Se possível, realize uma captura de pacote ao longo do caminho entre o líder compartilhado e o vCenter em um esforço para identificar se o tráfego está sendo enviado e recebido por qualquer dispositivo.

Inventário VMware

A tabela a seguir mostra uma lista de parâmetros VDS do VMWare e especifica se eles podem ser configurados pelo APIC.

Parâmetros VMware VDS gerenciados pelo APIC

VDS VMware	Valor padrão	Configurável usando a política do Cisco APIC?
Nome	Nome de Domínio do VMM	Sim (Derivado do Domínio)
Descrição	'Comutador virtual APIC'	No
Nome da pasta	Nome de Domínio do VMM	Sim (Derivado do Domínio)
Versão	Maior suporte oferecido pelo vCenter	Yes
Protocolo de descoberta	LLDP	Yes
Portas de uplink e nomes de uplink	8	Sim (do Cisco APIC versão 4.2(1))
Prefixo do Nome do Uplink	uplink	Sim (do Cisco APIC versão 4.2(1))
MTU máximo	9000	Yes
política de LACP	Desabilitado	Yes
Espelhamento de portas	0 sessões	Yes
Alarmes	2 alarmes adicionados no nível da pasta	No

A tabela a seguir mostra uma lista de parâmetros do VMWare VDS Port Group e especifica se eles podem ser configurados pelo APIC.

Parâmetros do grupo de portas VDS VMWare gerenciados pelo APIC

Grupo de portas do VMware VDS	Valor padrão	Configurável usando a política APIC
Nome	Nome do Locatário | Nome do perfil do aplicativo | Nome do EPG	Sim (Derivado de EPG)
Ligação de portas	Ligação estática	No
VLAN	Selecionado do pool de VLANs	Yes
Algoritmo de	Derivado com base na política de	Yes

balanceamento de carga	canal de porta no APIC	
Modo promíscuo	Desabilitado	Yes
Transmissão forjada	Desabilitado	Yes
alteração de MAC	Desabilitado	Yes
Bloquear todas as portas	FALSO	No

Solução de problemas do VMware Inventory

Os eventos de sincronização de inventário ocorrem para garantir que o APIC esteja ciente dos eventos do vCenter que podem exigir que o APIC atualize a política dinamicamente. Há dois tipos de eventos de sincronização de inventário que podem ocorrer entre o vCenter e o APIC; uma sincronização completa de inventário e uma sincronização de inventário baseada em evento. O cronograma padrão de uma sincronização completa do inventário entre o APIC e o vCenter é a cada 24 horas, mas eles também podem ser acionados manualmente. As sincronizações de inventário baseadas em eventos normalmente estão ligadas a tarefas acionadas, como um vMotion. Neste cenário, se uma máquina virtual se mover de um host para outro e esses hosts estiverem conectados a dois switches leaf diferentes, o APIC escutará o evento de migração de VM e, no cenário de implantação imediata sob demanda, desprogramará o EPG na folha de origem e programará o EPG na folha de destino.

Dependendo da proximidade da implantação dos EPGs associados a um domínio do VMM, a falha na obtenção do inventário do vCenter pode ter consequências indesejáveis. No cenário em que o inventário não foi concluído ou é parcial, sempre haverá uma falha que indica o objeto ou objetos que causaram a falha.

Cenário 1 - Máquina virtual com suporte inválido:

Se uma máquina virtual for movida de um vCenter para outro ou se for determinado que a máquina virtual tem um suporte inválido (por exemplo, um anexo de grupo de portas a um DVS antigo/excluído), o vNIC será relatado como tendo problemas operacionais.

```
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.
```

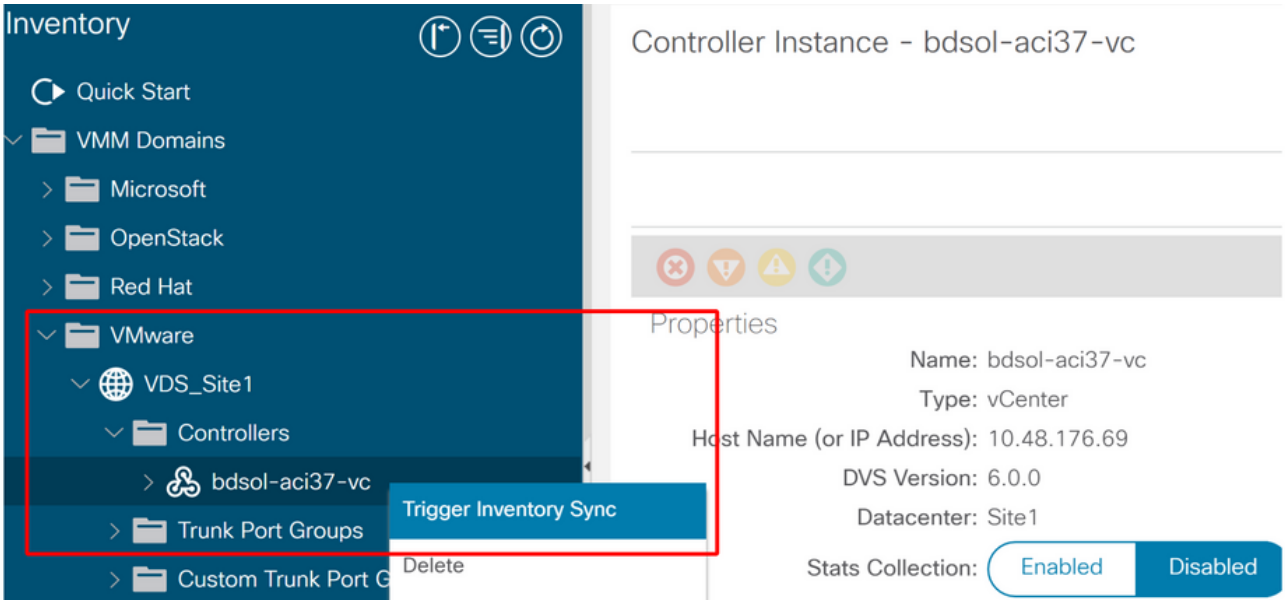
Cenário 2 — O administrador do vCenter modificou um objeto gerenciado do VMM no vCenter:

Não há suporte para a modificação de objetos gerenciados pelo APIC a partir do vCenter. A falha a seguir seria vista se uma operação não suportada fosse executada no 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.
```

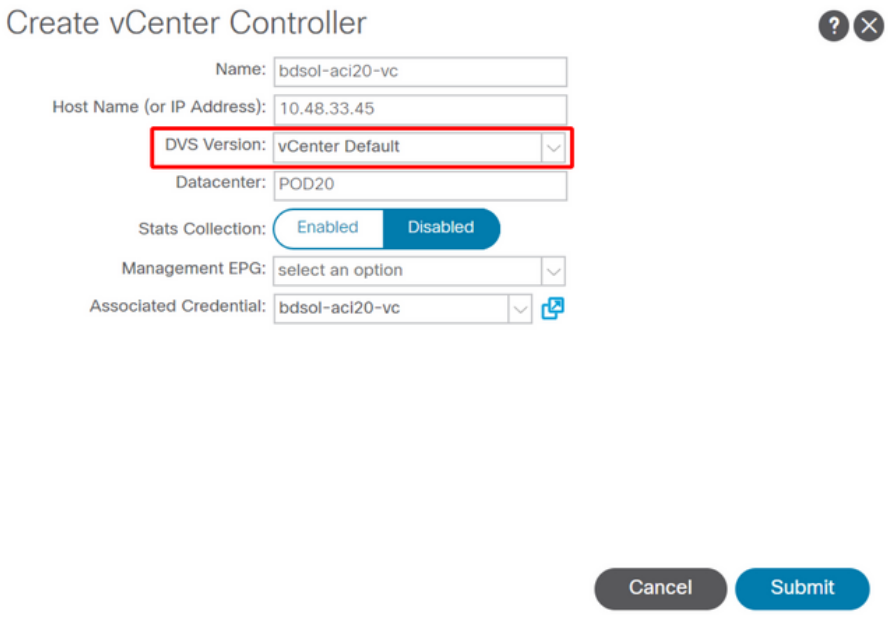
Domínio do VMM do VMWare - controlador do vCenter - acionar sincronização de inventário



Versão do VMware DVS

Ao criar um novo controlador vCenter como parte de um Domínio do VMM, a configuração padrão para a Versão DVS será usar o 'Padrão do vCenter'. Ao selecionar isso, a versão DVS será criada com a versão do vCenter.

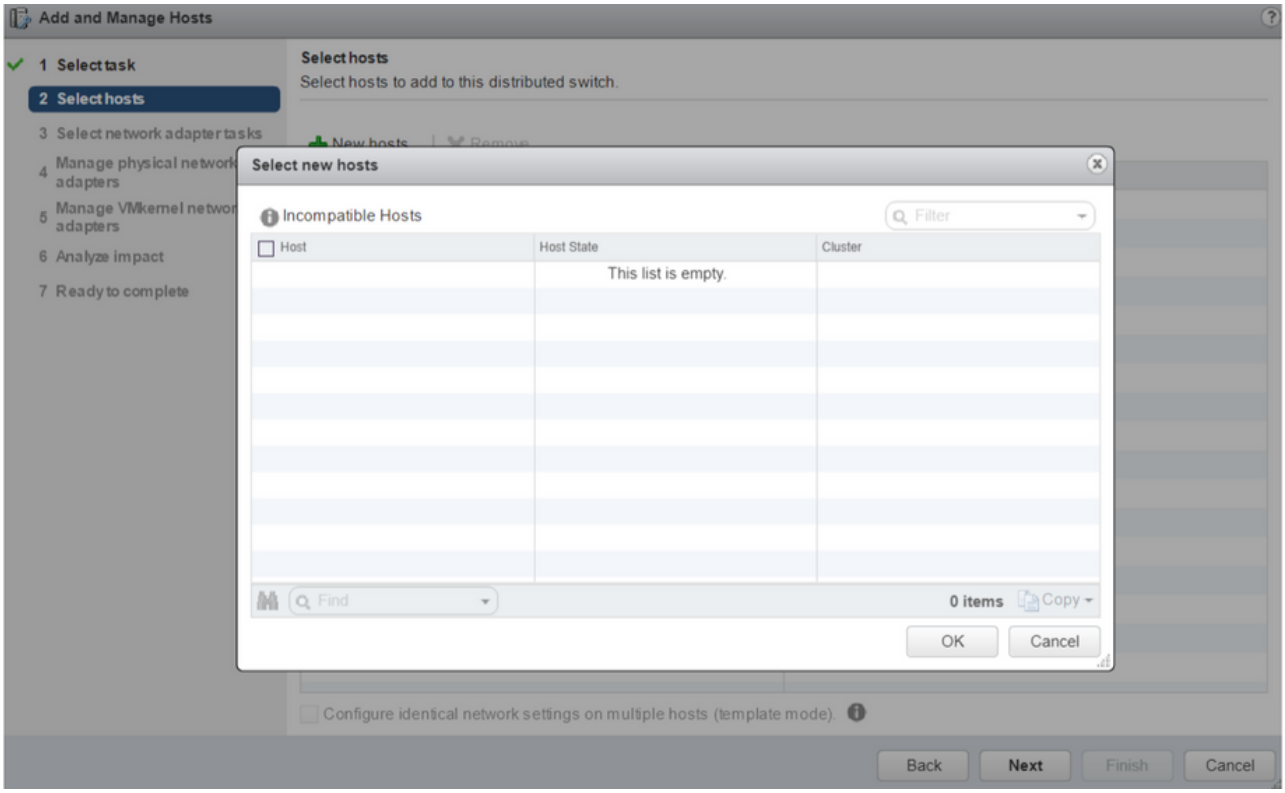
Domínio do VMM do VMWare - criação do controlador do vCenter



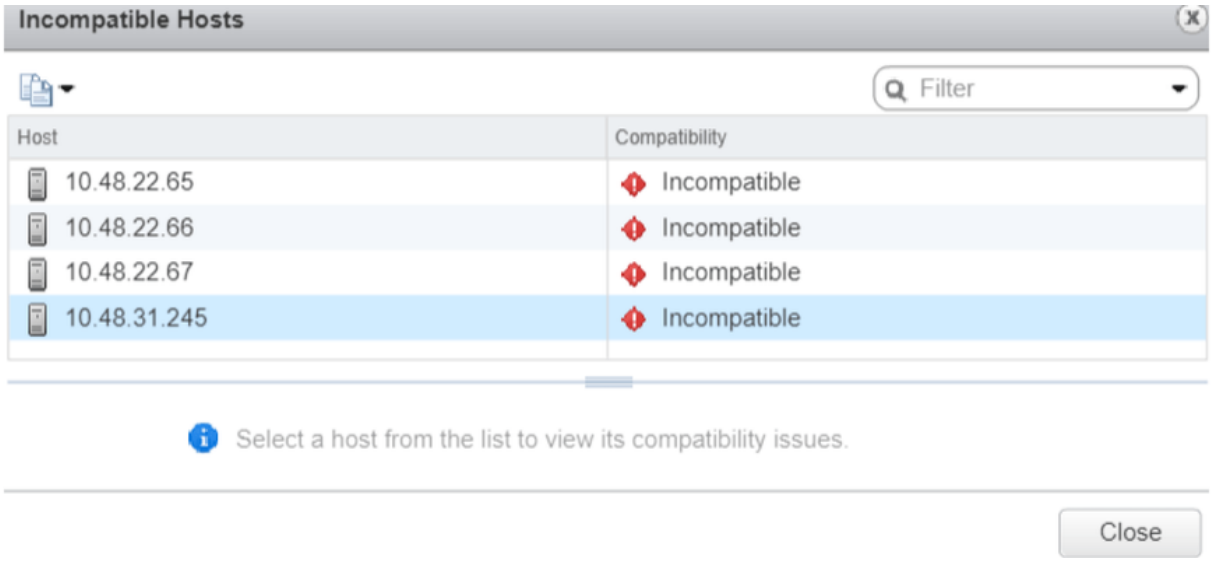
Isso significa que, no exemplo de um vCenter executando 6.5 e servidores ESXi executando 6.0, o APIC criará um DVS com a versão 6.5 e, portanto, o administrador do vCenter não poderá

adicionar os servidores ESXi executando 6.0 ao DVS da ACI.

DVS gerenciados pelo APIC - adição de host do vCenter - lista vazia



DVS gerenciado pelo APIC - adição de host vCenter - hosts incompatíveis



Portanto, ao criar um Domínio do VMM, certifique-se de selecionar a 'Versão do DVS' correta de modo que os servidores ESXi necessários possam ser adicionados ao DVS.

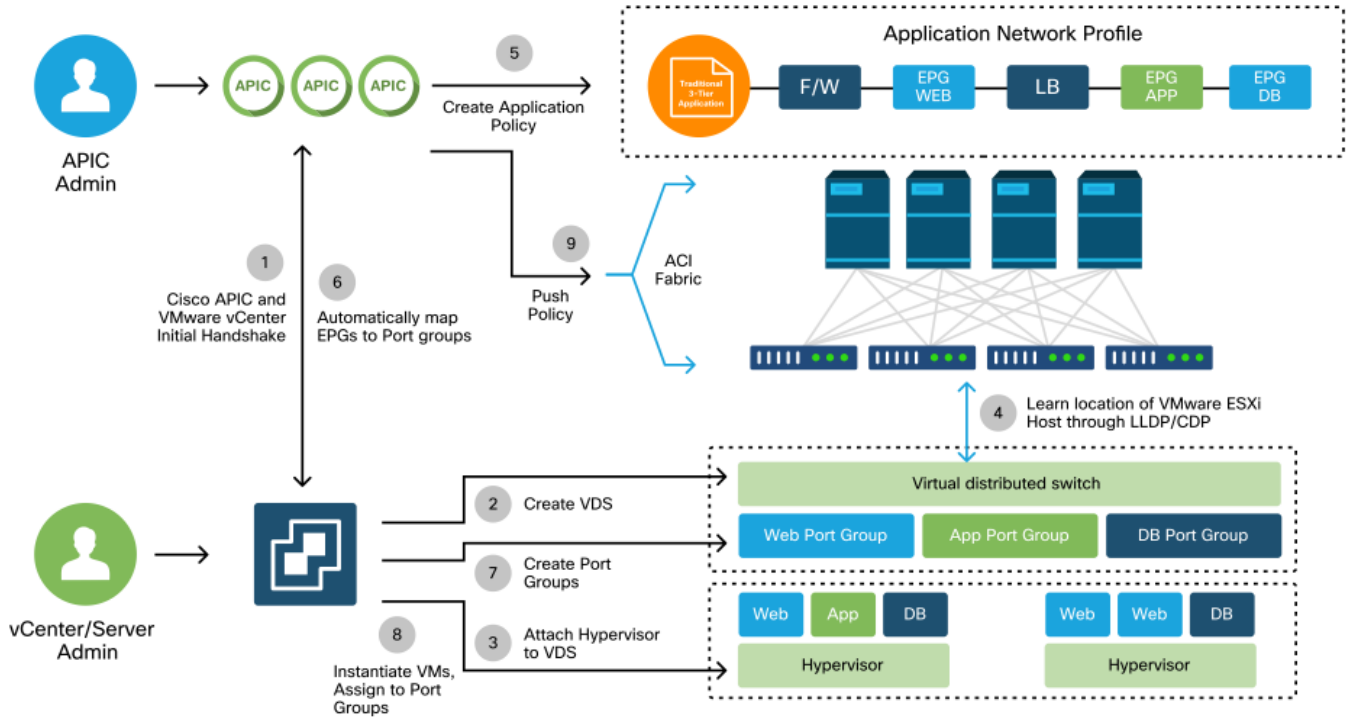
Detecção dinâmica de host

Processo de detecção de host / VM

A integração do VMM na ACI diferencia-se do provisionamento manual, pois a malha pode descobrir dinamicamente onde os hosts e as máquinas virtuais aplicáveis estão conectados para

implantar a política com eficiência. Por meio desse processo dinâmico, a ACI pode otimizar a utilização de recursos de hardware nos switches leaf, pois as VLANs, SVIs, regras de zoneamento etc. são implantadas nos nós somente quando há um endpoint conectado que requer a política. O benefício para o administrador de rede, de uma perspectiva de facilidade de uso, é que a ACI provisionará a VLAN/política onde as VMs se conectam de forma automatizada. Para determinar onde a política deve ser implantada, o APIC usará informações de várias fontes. O diagrama a seguir descreve as etapas básicas do processo de descoberta de host ao usar um domínio VMM baseado em DVS.

Domínio do VMM do VMWare — Fluxo de trabalho da implantação



Resumindo, as seguintes etapas principais ocorrem quando:

- O LLDP ou CDP é trocado entre o hipervisor e os switches leaf.
- Os hosts relatam informações de adjacência ao vCenter.
- O vCenter notifica o APIC sobre as informações de adjacência: O APIC conhece o host via sincronização de inventário.
- O APIC envia a política para a porta de folha: reveja a subseção "Imediação de resolução" nesta seção para entender melhor essas condições.
- Se as informações de adjacência do vCenter forem perdidas, o APIC poderá remover a política.

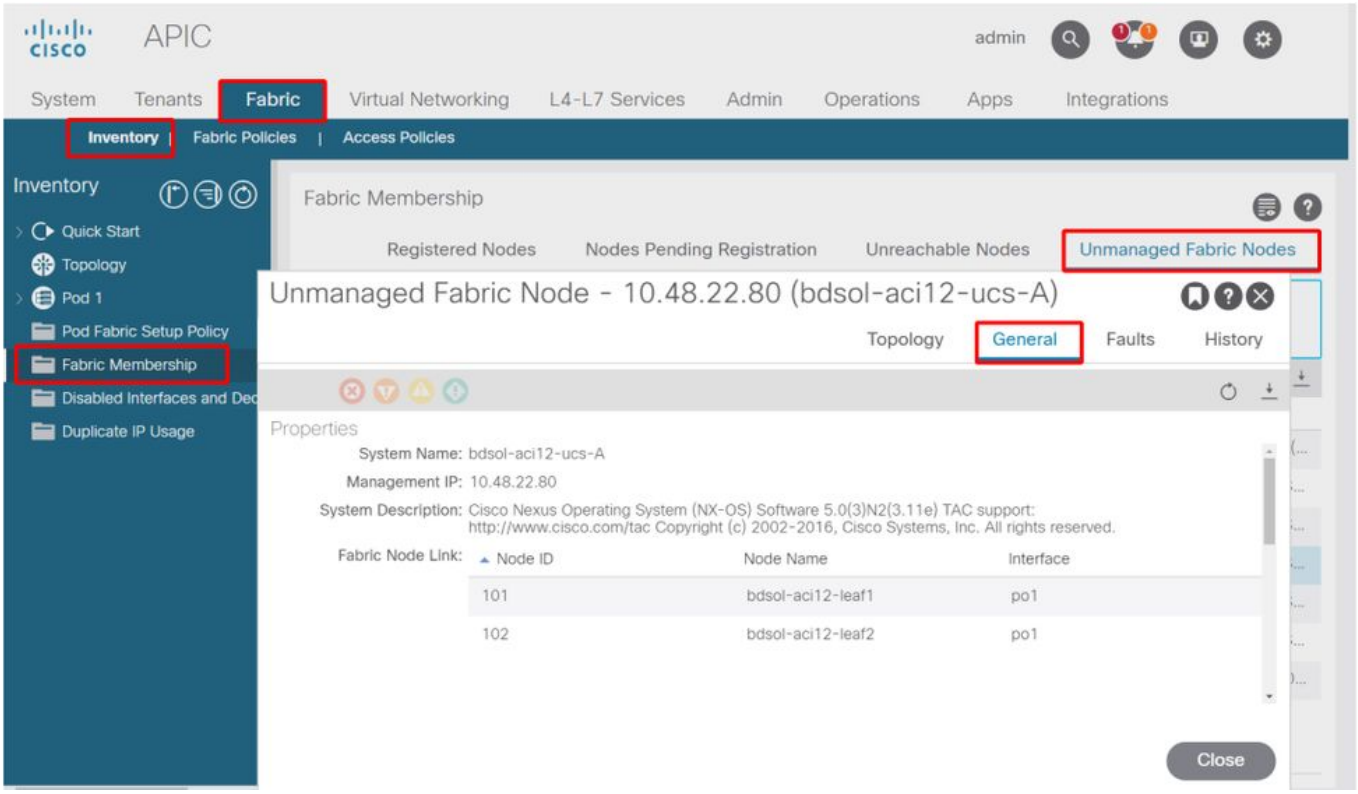
Como se pode ver, o CDP/LLDP desempenha um papel fundamental no processo de descoberta e é importante verificar se ele está configurado corretamente e se ambos os lados estão usando o mesmo protocolo.

Fabric LooseNode / switch intermediário - caso de uso

Em uma implantação que usa um chassi de blade com um switch intermediário entre os switches leaf e o hipervisor, o APIC precisa "unir" a adjacência. Neste cenário, vários protocolos de descoberta podem ser usados, pois o switch intermediário pode ter requisitos de protocolo diferentes dos do host.

Em uma configuração com um servidor blade e um switch intermediário (ou seja, switch de chassi de blade), a ACI deve detectar o switch intermediário e mapear os hipervisores atrás dele. O switch intermediário é chamado na ACI de LooseNode ou "Nó de estrutura não gerenciado". Os LooseNodes detectados podem ser exibidos em 'Malha > Inventário > Associação de malha > Nós de malha não gerenciados'. Navegando para um desses tipos de servidores na GUI, o usuário pode visualizar o caminho do leaf para o switch intermediário para o host.

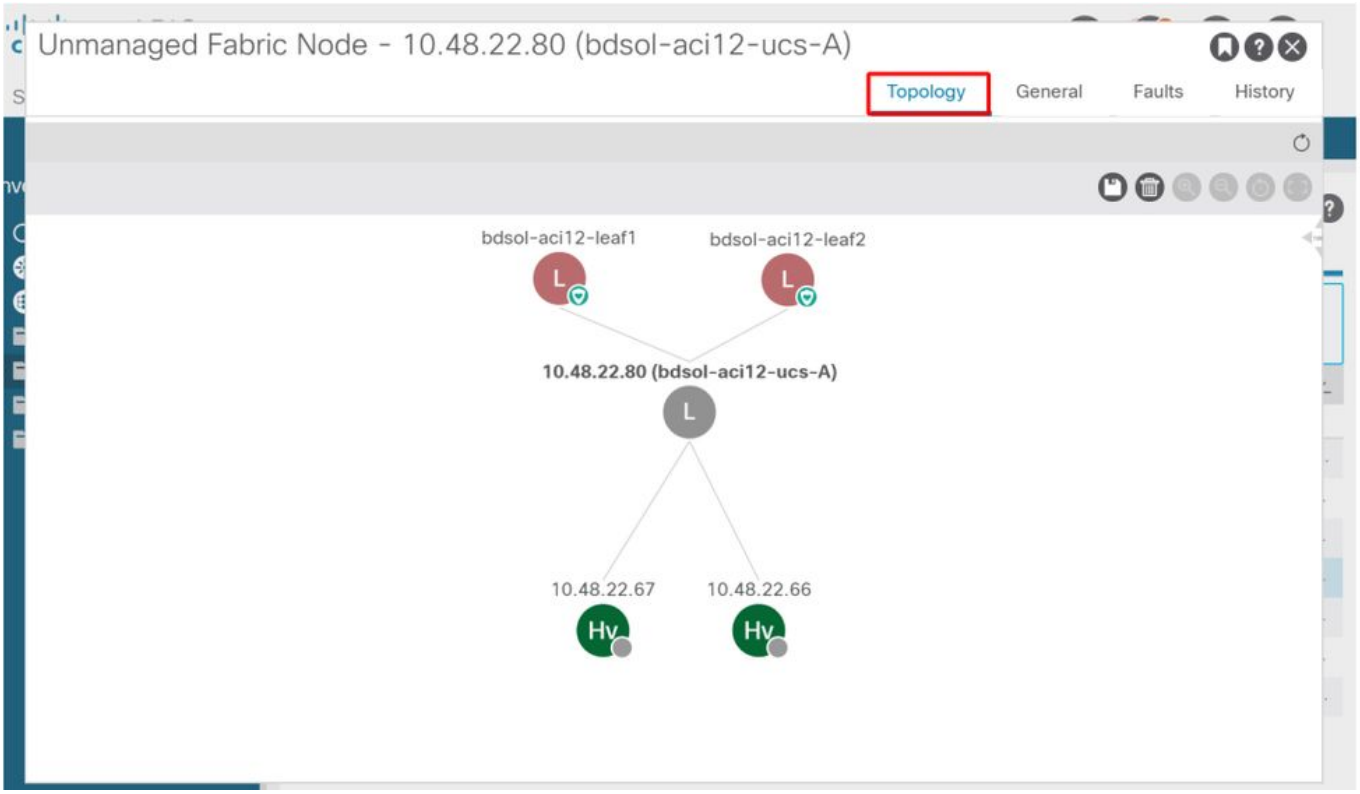
Interface do usuário do APIC — nós de estrutura não gerenciados (LooseNodes)



Com a descoberta de LLDP ou CDP implantada, a ACI pode determinar a topologia para esses LooseNodes, já que o downstream do hipervisor do switch intermediário é gerenciado por meio da integração do VMM e a própria folha tem uma adjacência para o switch intermediário a partir do downstream.

Este conceito é ilustrado pela imagem abaixo.

Interface do usuário do APIC — Caminho do nó de malha não gerenciado

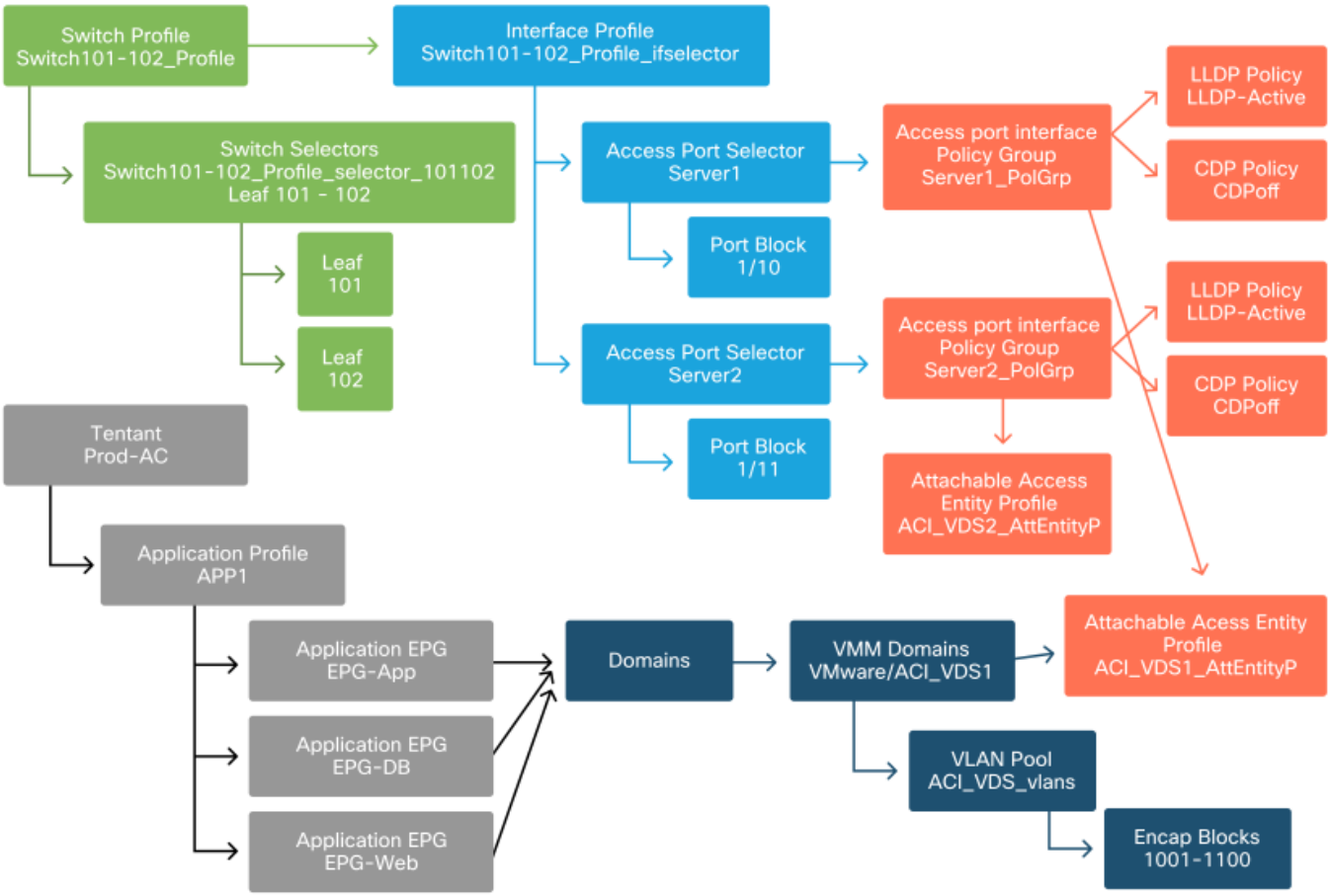


Imediato de resolução

Em cenários onde serviços críticos utilizam DVS integrados ao VMM, como conectividade de gerenciamento para vCenter/ESXi, é prudente usar a Imediação de resolução de pré-provisionamento. Com essa configuração, o mecanismo de descoberta dinâmica de hosts é removido e, em vez disso, a política/VLANs são programadas estaticamente nas interfaces voltadas para o host. Nesta configuração, as VLANs do VMM sempre serão implantadas em todas as interfaces ligadas ao AEP referenciado pelo Domínio do VMM. Isso elimina a possibilidade de que uma VLAN crítica (como gerenciamento) seja removida de uma porta devido a um evento de adjacência relacionado ao protocolo de descoberta.

Consulte o diagrama abaixo:

Exemplo de implantação pré-provisionada



Se Pré-Provisionamento tiver sido definido para um EPG no Domínio do VMM ACI_VDS1, as VLANs serão implantadas nos links para Servidor1, mas não Servidor2, pois o AEP do Servidor2 não inclui o Domínio do VMM ACI_VDS1.

Para resumir as configurações de urgência da resolução:

- Sob demanda - a política é implantada quando a adjacência é estabelecida entre o leaf e o host e uma VM conectada ao grupo de portas.
- Imediata - a política é implantada quando a adjacência é estabelecida entre o leaf e o host.
- Pré-provisionamento - A política é implantada em todas as portas usando um AEP com o Domínio do VMM contido, nenhuma adjacência é necessária.

Cenários de Troubleshooting

A VM não pode resolver o ARP para seu gateway padrão

Neste cenário, a integração do VMM foi configurada e o DVS foi adicionado ao hipervisor, mas a VM não pode resolver o ARP para seu gateway na ACI. Para que a VM tenha conectividade de rede, verifique se a adjacência foi estabelecida e se as VLANs estão implantadas.

Primeiro, o usuário pode verificar se a folha detectou o host usando 'show lldp neighbors' ou 'show cdp neighbors' na folha, dependendo do protocolo selecionado.

```
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
```

Se necessário, de uma perspectiva de solução de problemas, isso pode ser validado do lado do ESXi na CLI e na GUI:

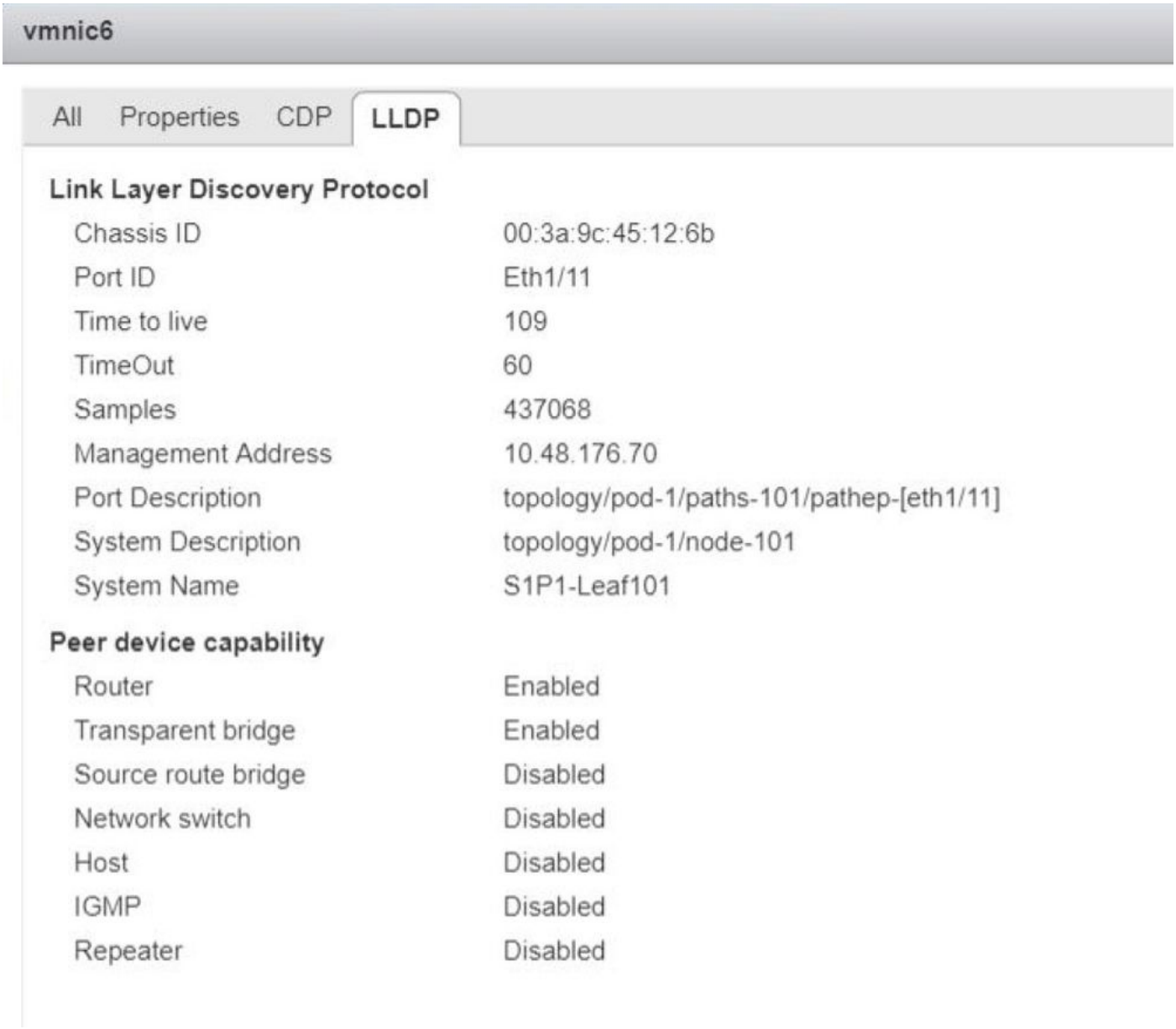
```
[root@host:~] esxcli network vswitch dvs vmware list
VDS_Site1
  Name: VDS_Site1
 ...
  Uplinks: vmnic7, vmnic6
  VMware Branded: true
  DVPort:
        Client: vmnic6
        DVPortgroup ID: dvportgroup-122
        In Use: true
        Port ID: 0

        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"
           }
```

vCenter Web Client - host - detalhes de adjacência de LLDP/CDP da vmnic

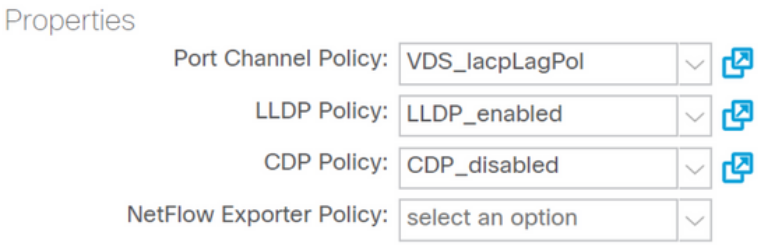


Se a adjacência de LLDP folha não puder ser vista do host ESXi, isso geralmente é causado pelo uso de um adaptador de rede que é configurado para gerar LLDPDUs em vez do sistema operacional ESXi. Verifique se o adaptador de rede tem LLDP habilitado e, portanto, está consumindo todas as informações de LLDP. Se esse for o caso, desabilite o LLDP no próprio adaptador para que ele seja controlado pela política do vSwitch.

Outra causa pode ser que há um desalinhamento entre os protocolos de detecção usados entre o leaf e o hipervisor ESXi. Verifique se ambas as extremidades usam o mesmo protocolo de descoberta.

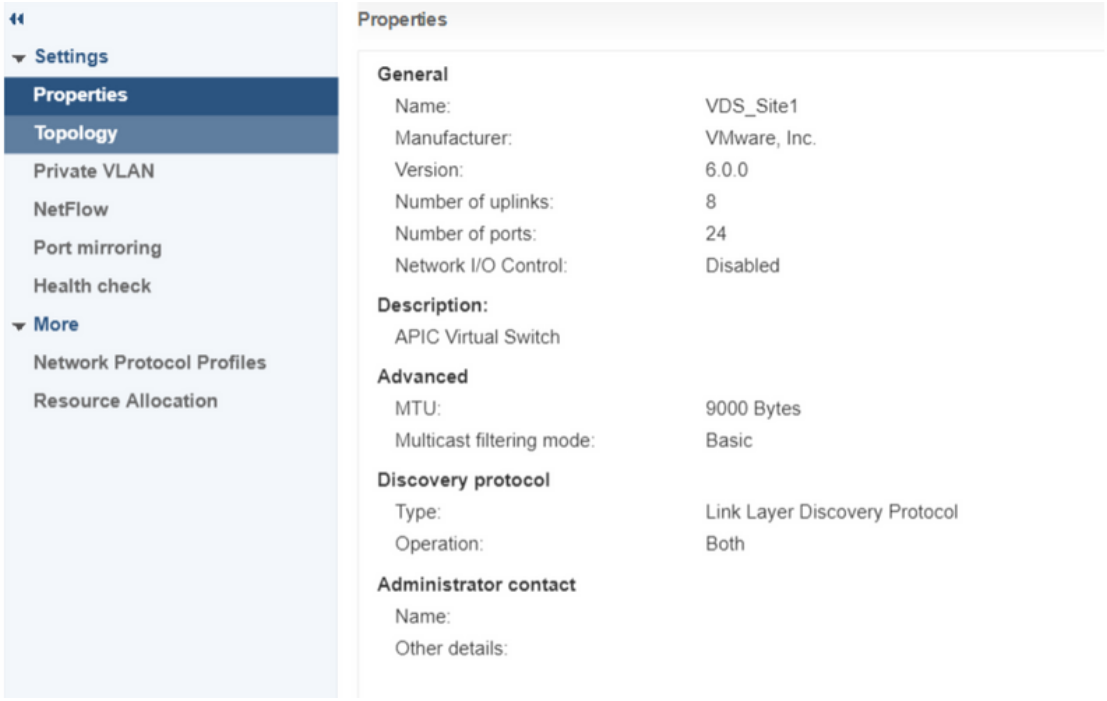
Para verificar se as configurações de CDP/LLDP estão alinhadas entre a ACI e o DVS na interface do usuário do APIC, navegue para "Virtual Networking > VMM Domains > VMWare > Policy > vSwitch Policy" (Rede virtual > Domínios VMM > VMWare > Política > Política vSwitch). Certifique-se de ativar somente a política LLDP ou CDP, pois elas são mutuamente exclusivas.

Interface do usuário do APIC - Domínio VMM do VMWare - política vSwitch



No vCenter, vá para: 'Rede > VDS > Configurar'.

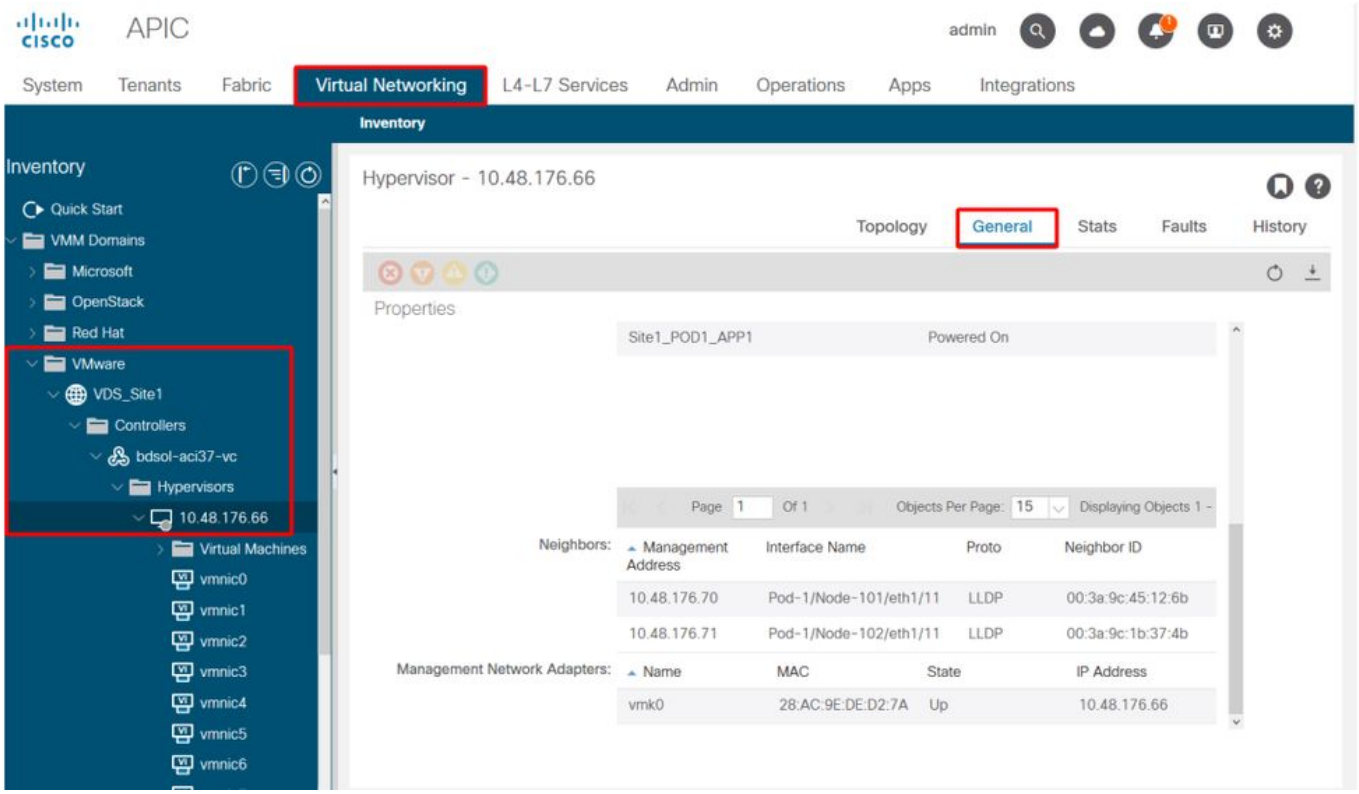
IU do vCenter Web Client - propriedades do VDS



Corrija as configurações de LLDP/CDP se necessário.

Em seguida, confirme se o APIC observa a vizinhança LLDP/CDP do host ESXi em relação ao switch leaf na interface do usuário em "Virtual Networking > VMM Domains > VMWare > Policy > Controller > Hypervisor > General".

Interface do usuário do APIC - Domínio VMM do VMWare - Detalhes do hipervisor



Se isso estiver mostrando os valores esperados, o usuário poderá validar se a VLAN está presente na porta em direção ao 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
```

VMK de gerenciamento do vCenter/ESXi anexado aos DVS enviados pelo APIC

Em um cenário em que o tráfego de gerenciamento do vCenter ou ESXi precisa utilizar o VMM integrado ao DVS, é importante tomar algum cuidado extra para evitar um impasse na ativação das adjacências dinâmicas e ativar as VLANs necessárias.

Para o vCenter, que normalmente é criado antes da integração do VMM ser configurada, é importante usar um domínio físico e um caminho estático para garantir que a VLAN de encapsulamento da VM do vCenter seja sempre programada nos switches leaf para que possa ser usada antes da integração do VMM ser totalmente configurada. Mesmo depois de configurar a integração do VMM, é aconselhável deixar esse caminho estático no lugar para sempre garantir a disponibilidade desse EPG.

Para os hipervisores ESXi, de acordo com o "Guia de virtualização da Cisco ACI" em Cisco.com, ao migrar para o vDS, é importante garantir que o EPG onde a interface VMK será conectada seja implantado com a resolução imediata definida como Pré-provisionamento. Isso garantirá que a VLAN seja sempre programada nos switches leaf sem depender da descoberta LLDP/CDP dos hosts ESXi.

Adjacências de host não descobertas por trás do LooseNode

As causas típicas de problemas de descoberta do LooseNode são:

- O CDP/LLDP não está ativado O CDP/LLDP deve ser trocado entre o switch intermediário, os switches leaf e os hosts ESXiPara o Cisco UCS, isso é feito por meio de uma política de controle de rede no vNIC
- Uma alteração no IP de gerenciamento do vizinho LLDP/CDP interrompe a conectividade O vCenter verá o novo IP de gerenciamento na adjacência LLDP/CDP, mas não atualizará o APICDisparar uma sincronização de inventário manual para corrigir
- As VLANs VMM não são adicionadas ao switch intermediário O APIC não programa switches blade/intermediários de terceiros.Aplicativo de integração Cisco UCSM (ExternalSwitch) disponível na versão 4.1(1).As VLANs devem ser configuradas e colocadas em tronco nos uplinks conectados aos nós leaf da ACI e nos downlinks conectados aos hosts

F606391 - Adjacências ausentes para o adaptador físico no host

Ao observar a falha abaixo:

```
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 o fluxo de trabalho na seção "A VM não pode resolver o ARP para seu gateway padrão", pois isso significa que há adjacências CDP/LLDP ausentes. Essas adjacências devem ser verificadas de ponta a ponta.

Balanceamento de carga do uplink do hipervisor

Ao conectar hipervisores como o ESXi a uma malha da ACI, eles normalmente estarão conectados com vários uplinks. Na verdade, é recomendável ter um host ESXi conectado a pelo menos dois switches leaf. Isso minimizará o impacto de cenários de falha ou atualizações.

Para otimizar como os uplinks são usados pelas cargas de trabalho em execução em um hipervisor, as configurações do VMware vCenter permitem configurar vários algoritmos de balanceamento de carga para o tráfego gerado pela VM em direção aos uplinks do hipervisor.

Éessencial ter todos os hipervisores e a estrutura da ACI alinhados com a mesma configuração de algoritmo de balanceamento de carga para garantir que a conectividade correta esteja em vigor. Se isso não for feito, o fluxo de tráfego cai de forma intermitente e o endpoint se move na estrutura da ACI.

Isso pode ser observado em uma estrutura da ACI por alertas excessivos, 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 abordará a conectividade do host VMWare ESXi na ACI, mas é aplicável à maioria dos hipervisores.

Servidor rack

Ao examinar as várias maneiras pelas quais um host ESXi pode se conectar a uma estrutura ACI, eles são divididos em 2 grupos, dependendo do switch e algoritmos de balanceamento de carga independentes do switch.

Os algoritmos de balanceamento de carga independentes do switch são maneiras de se conectar quando não for necessária uma configuração específica do switch. Para o balanceamento de carga dependente do switch, são necessárias configurações específicas do switch.

Certifique-se de validar se a política vSwitch está de acordo com os requisitos do "Grupo de política de acesso da ACI", conforme a tabela abaixo.

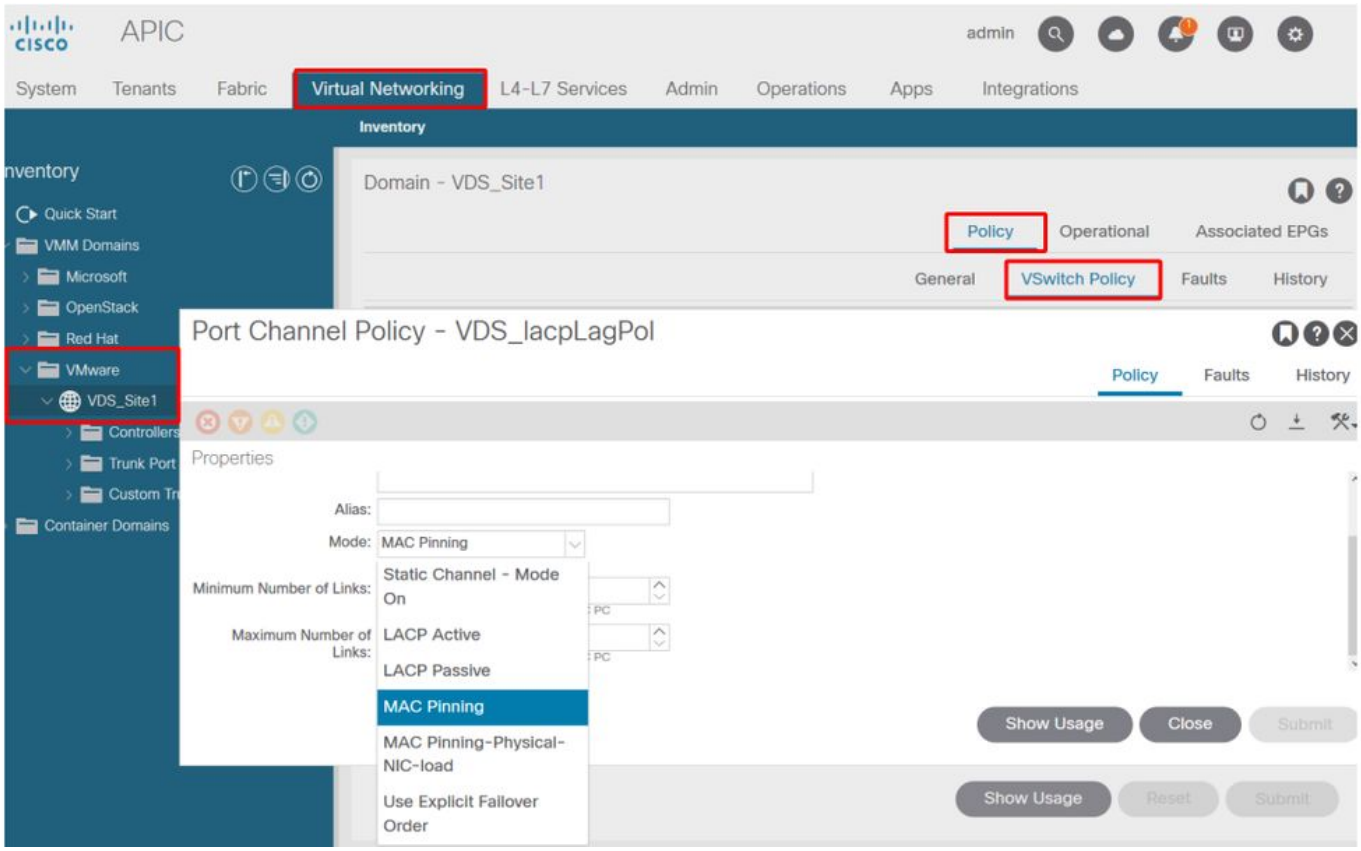
Política de agrupamento e vSwitch da ACI

Modo de agrupamento e failover do VMware	Política vSwitch da ACI	Descrição	Grupo de política de acesso da ACI - canal de porta necessário
Rota baseada na porta virtual de origem	Fixação de MAC	Selecione um uplink baseado nas IDs de porta virtual no switch. Depois que o switch virtual seleciona um uplink para uma máquina virtual ou um adaptador VMKernel, ele sempre encaminha o tráfego através do mesmo uplink para essa máquina virtual ou adaptador VMKernel.	No
Rota baseada no hash MAC de origem	NA	Selecionar um uplink com base em um hash do endereço MAC origem	NA
Ordem de Failover Explícito	Usar Modo de Failover Explícito	Na lista de adaptadores ativos, sempre use o uplink de ordem mais alta que passe critérios de detecção de failover. Nenhum balanceamento de carga real é executado com essa opção.	No
Agregação de link (LAG) - Baseado em hash IP	Canal estático - Modo ativado	Selecione um uplink com base em um hash dos endereços IP origem e destino de cada pacote. Para pacotes não IP, o switch usa os dados nesses campos para calcular o hash. O agrupamento baseado em IP exige que, no lado da ACI, um canal de porta/VPC seja configurado com o "modo ativado".	Sim (modo de canal definido como 'ativado')
Agregação de links (LAG) -	LACP ativo/passivo	Selecione um uplink com base em um hash selecionado (20 opções de hash	Sim (modo de canal

LACP		diferentes disponíveis). O agrupamento baseado em LACP requer que, no lado da ACI, um canal de porta/VPC seja configurado com LACP habilitado. Certifique-se de criar uma política de retardo aprimorada na ACI e aplicá-la à política VSwitch. Disponível para grupos de portas distribuídas ou portas distribuídas.	definido como 'LACP ativo/passivo')
Rota baseada em carga de NIC física (LBT)	Fixação de MAC - Physical-NIC-load	Selecione um uplink com base na carga atual dos adaptadores de rede física conectados ao grupo de portas ou porta. Se um uplink permanecer ocupado a 75 por cento ou mais por 30 segundos, o vSwitch do host move uma parte do tráfego da máquina virtual para um adaptador físico que tem capacidade livre.	No

Veja a captura de tela abaixo sobre como validar a política de canal de porta como parte da política vSwitch em vigor.

Política vSwitch ACI — Política de canal de porta



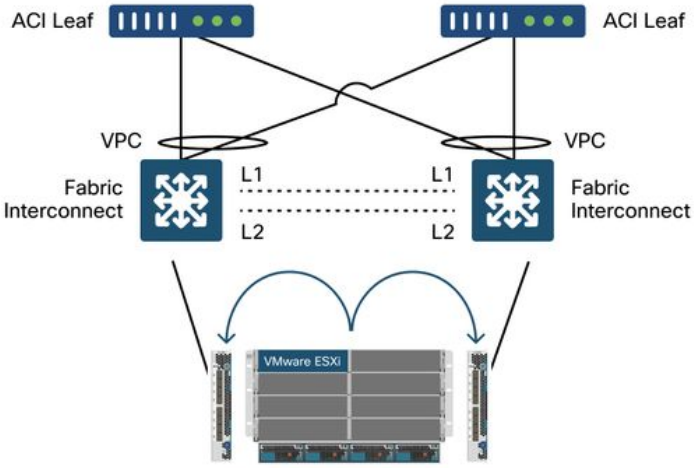
Nota: Para obter uma descrição mais detalhada dos recursos de rede da VMware, consulte a vSphere Networking em https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.networking.doc/GUID-D34B1ADD-B8A7-43CD-AA7E-2832A0F7EE76.html

Caso de uso do Cisco UCS B-Series

Ao usar servidores Cisco UCS B-Series, é importante observar que eles se conectam dentro de seus chassis a UCS Fabric Interconnects (FIs) que não têm um plano de dados unificado. Este caso de uso aplica-se igualmente a outros fornecedores que empregam uma topologia semelhante. Por isso, pode haver uma diferença entre o método de balanceamento de carga usado de um lado do switch leaf da ACI e o lado do vSwitch.

Veja abaixo uma topologia UCS FI com ACI:

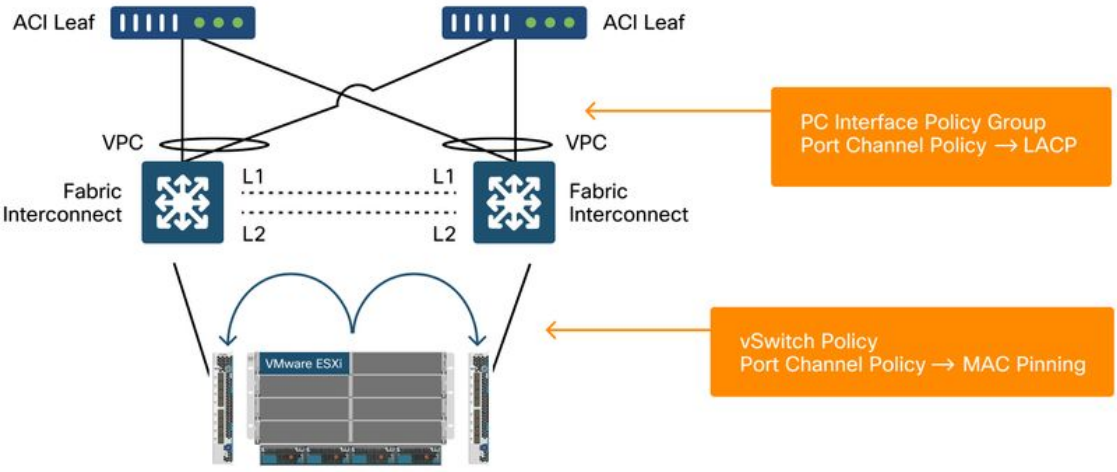
Cisco UCS FI com switches leaf ACI - topologia



Principais pontos a serem observados:

- Cada Cisco UCS FI tem um canal de porta para os switches leaf da ACI.
- Os FIs do UCS são interconectados diretamente apenas para fins de pulsação (não usados para dataplane).
- O vNIC de cada servidor blade é fixado a um UCS FI específico ou usa um caminho em direção a um dos FIs usando o failover de malha do UCS (Ative-Standby).
- Usar algoritmos de hash IP no vSwitch do host ESXi causará oscilações de MAC nos FIs do UCS.

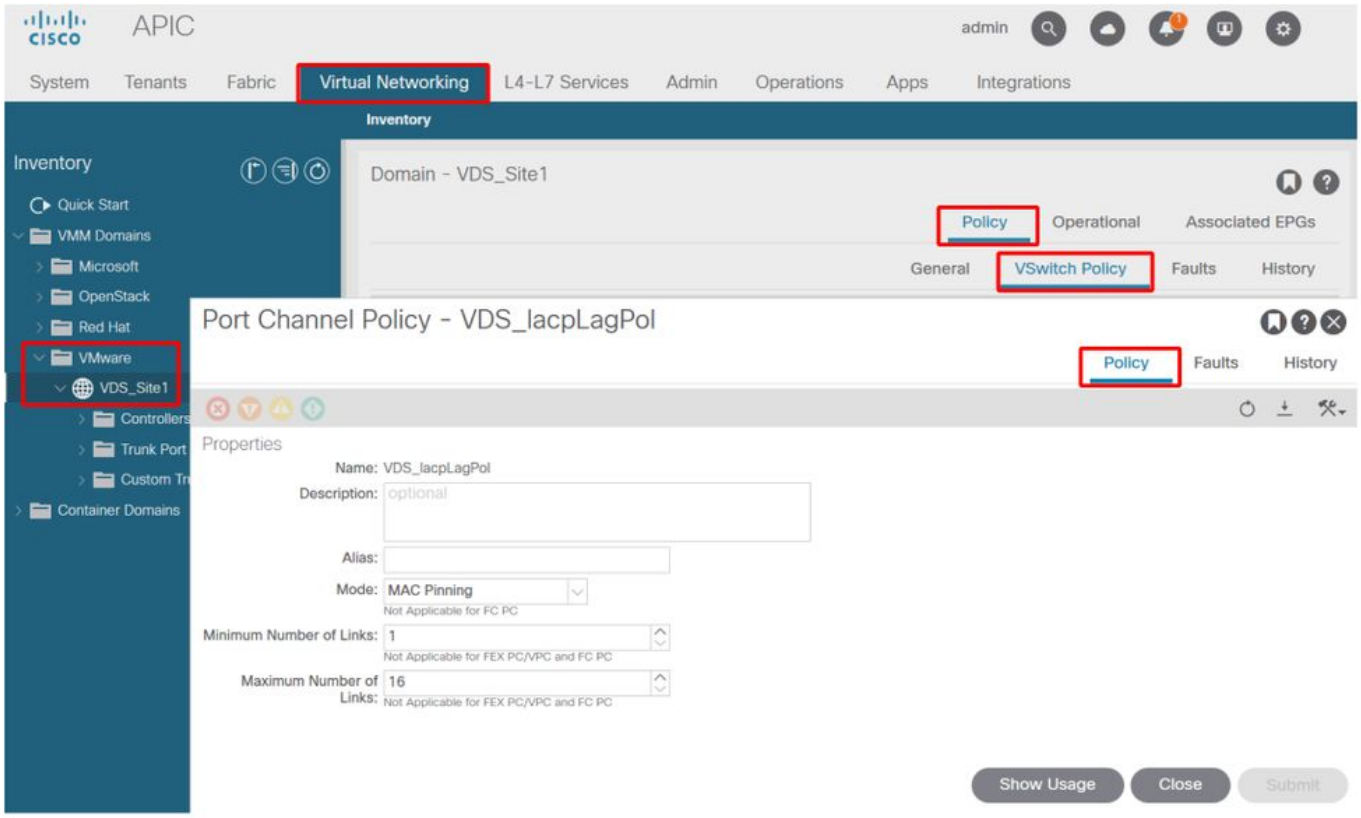
Para configurar corretamente isso, faça o seguinte:



Quando a Fixação de MAC é configurada na Política de Canal de Porta como parte da Política vSwitch na ACI, isso será mostrado como configuração de agrupamento 'Rota baseada na porta

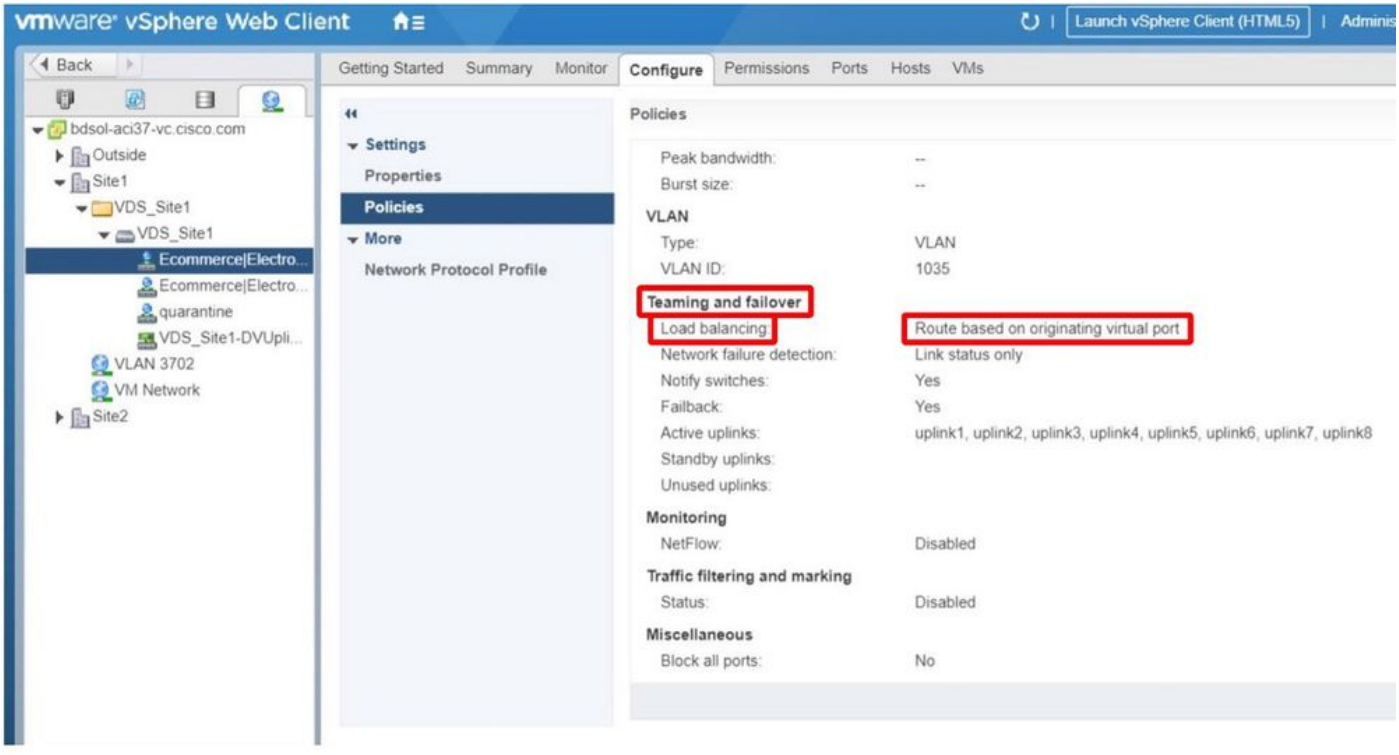
virtual de origem' dos grupos de porta no VDS.

ACI — Port Channel Policy como parte da vSwitch Policy



A política de canal de porta usada no exemplo acima é nomeada automaticamente pelo assistente, portanto, é chamada de "CDS_lacpLagPol", embora usemos o modo "Fixação MAC".

VMWare vCenter — ACI VDS — Grupo de portas — configuração de balanceamento de carga



Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.