ASAv no modo GoTo (L3) com o uso da versão AVS-ACI 1.2(x)

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Configurar](#)
[Diagrama de Rede](#)
[Configurações](#)
[Verificar](#)
[Troubleshoot](#)
[Informações Relacionadas](#)

Introduction

Este documento descreve como implantar um switch Application Virtual Switch (AVS) com um único firewall Adaptive Security Virtual Appliance (ASAv) no modo roteado/GOTO como um gráfico de serviço L4-L7 entre dois EPGs (End Point Groups) para estabelecer comunicação cliente-servidor usando a versão ACI 1.2(x).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Políticas de acesso configuradas e interfaces ativas e em serviço
- EPG, BD (Bridge Domain) e VRF (Virtual Routing and Forwarding) já configurados

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

Hardware e software:

- UCS C220 - 2.0(6d)
- ESXi/vCenter - 5.5
- ASAv - asa-device-pkg-1.2.4.8
- AVS - 5.2.1.SV3.1.10
- APIC - 1.2(1i)
- Folha/Espinha - 11.2(1i)
- Pacotes de dispositivo *.zip já baixados

Recursos:

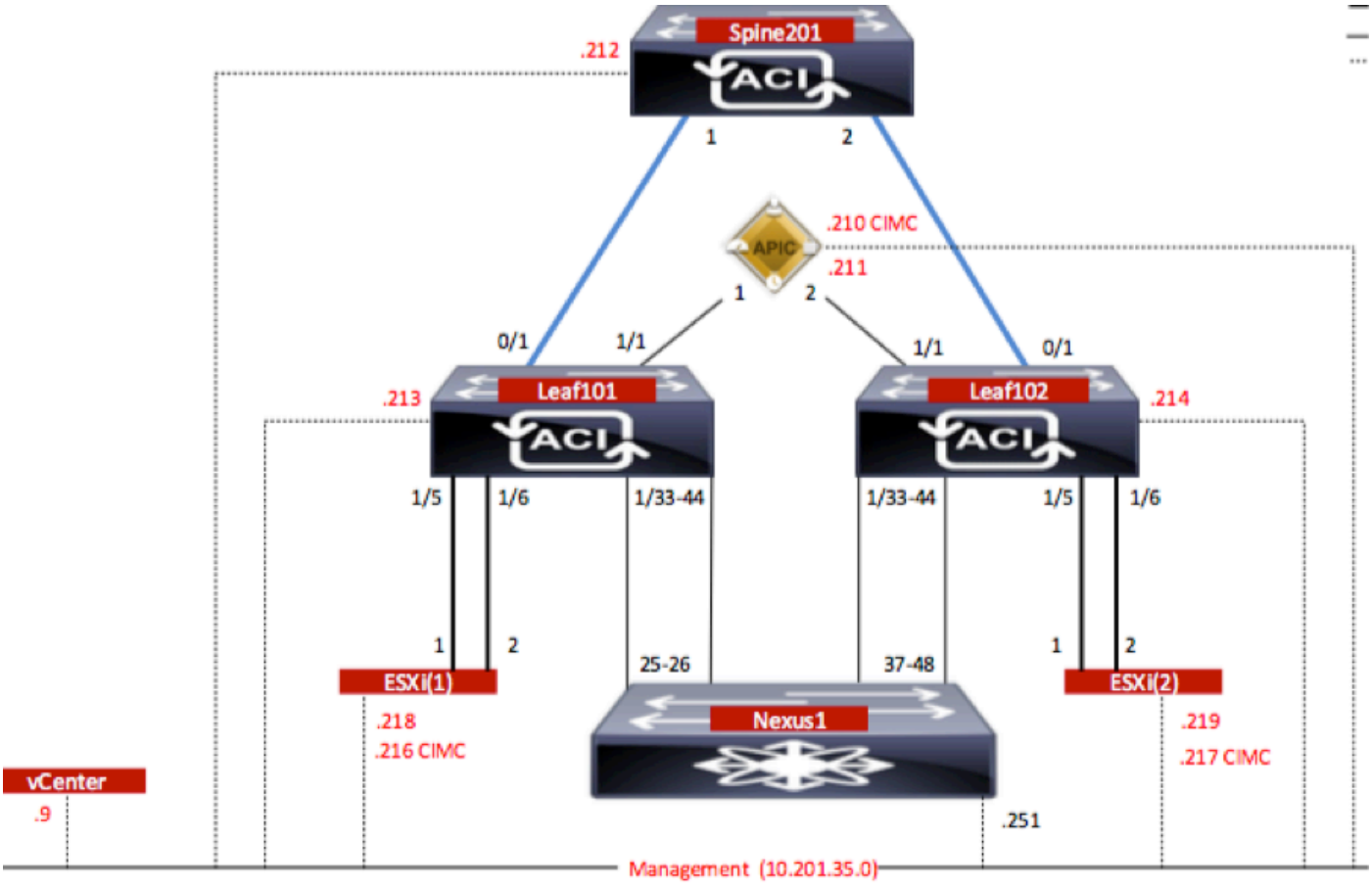
- AVS
- ASAv
- EPGs, BD, VRF
- Lista de controle de acesso (ACL)
- Gráfico de serviços L4-L7
- vCenter

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Diagrama de Rede

Conforme mostrado na imagem,



Configurações

A configuração inicial do AVS cria um domínio do VMware vCenter (integração do VMM)2

Note:

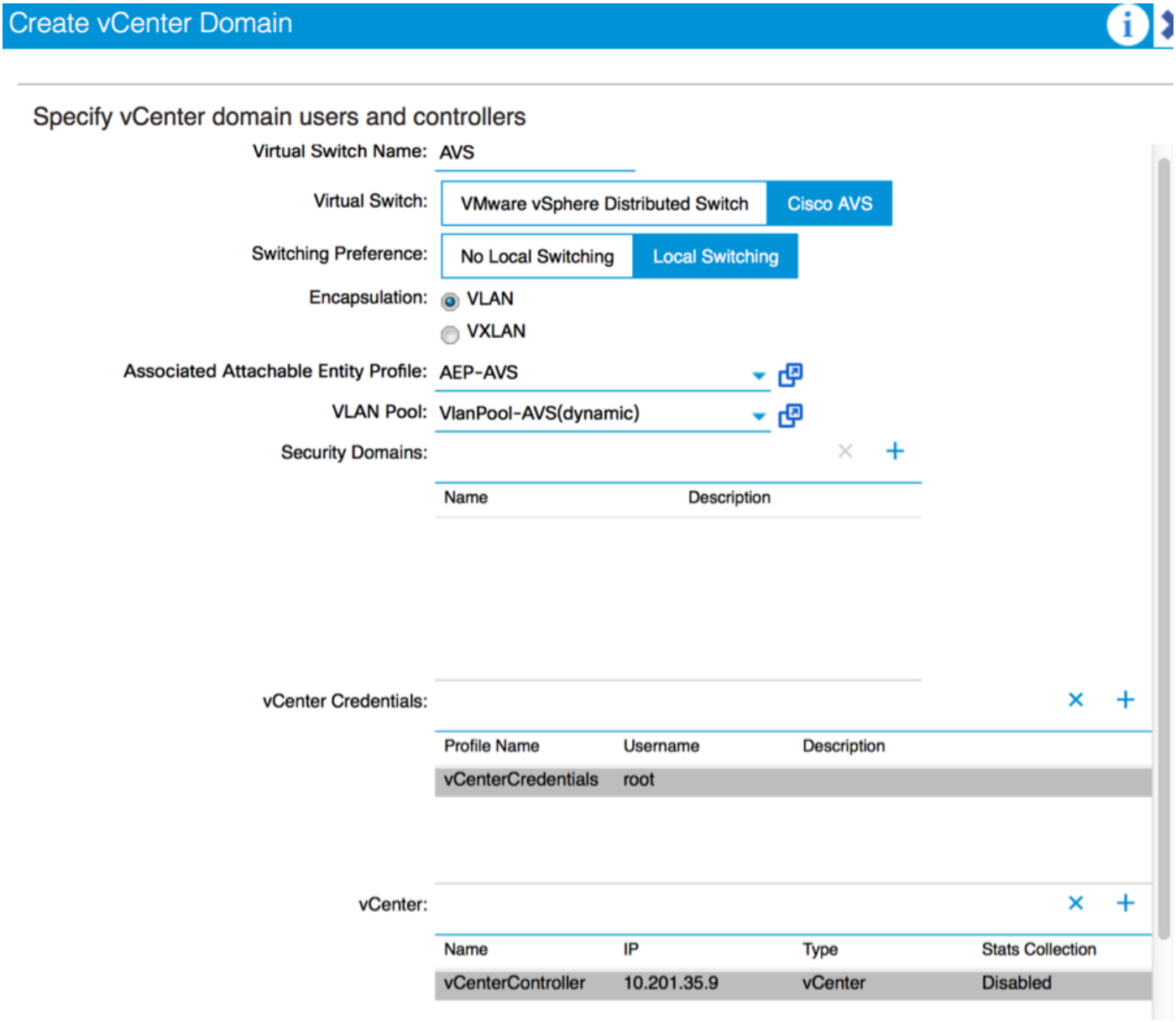
- Você pode criar vários datacenters e entradas de Distributed Virtual Switch (DVS) em um único domínio. No entanto, você pode ter apenas um Cisco AVS atribuído a cada datacenter.

- A implantação do gráfico de serviços com o Cisco AVS é suportada pela Cisco ACI versão 1.2(1i) com o Cisco AVS versão 5.2(1)SV3(1.10). Toda a configuração do gráfico de serviço é executada no Cisco Application Policy Infrastructure Controller (Cisco APIC).

- A implantação da máquina virtual de serviço (VM) com o Cisco AVS é suportada somente em domínios do Virtual Machine Manager (VMM) com modo de encapsulamento de Virtual Local Area Networks (VLAN). No entanto, as VMs de computação (as VMs do provedor e do consumidor) podem fazer parte dos domínios do VMM com Virtual Extensible LAN (VXLAN) ou encapsulamento de VLAN.

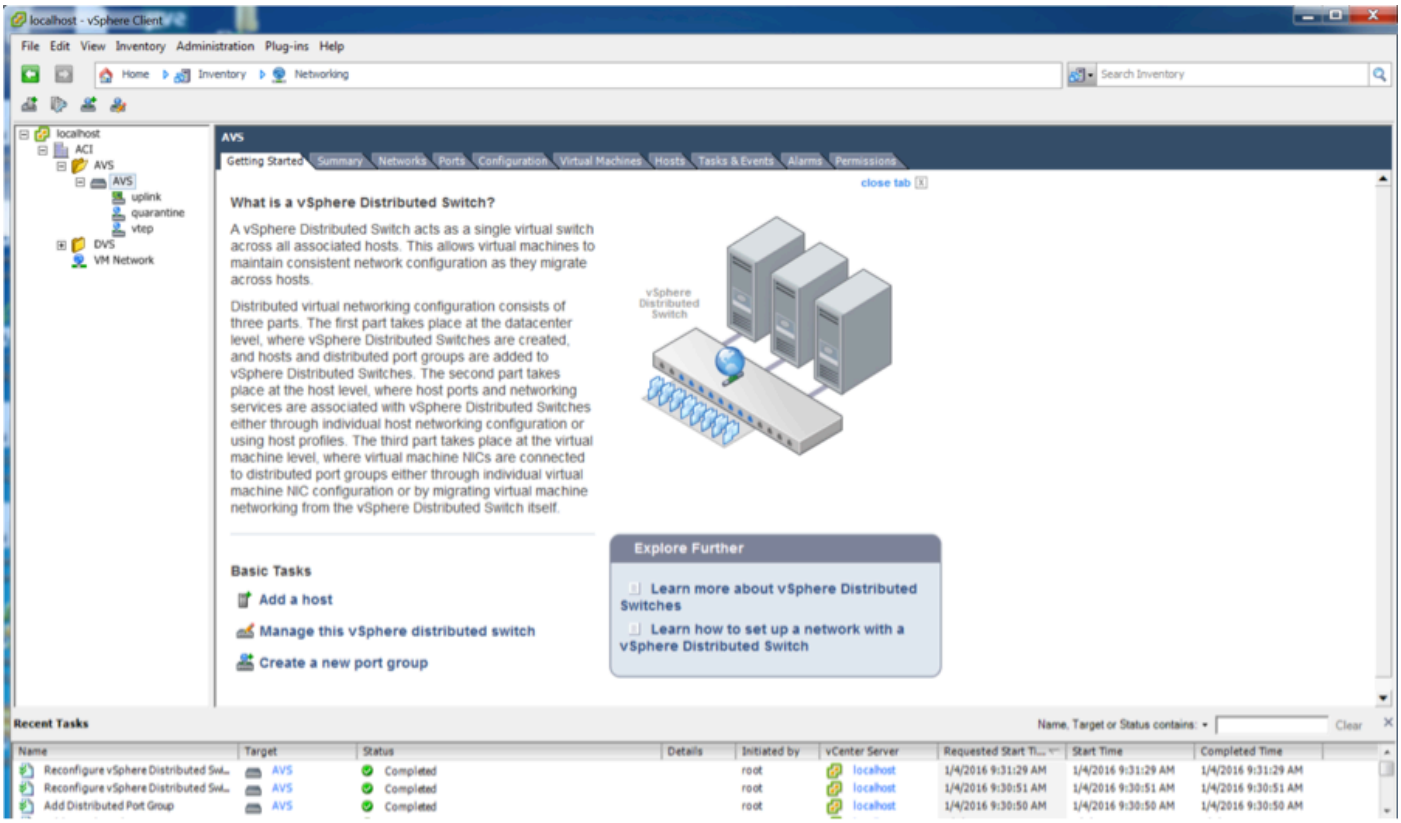
- Observe também que, se a comutação local for usada, o conjunto e o endereço multicast não serão necessários. Se nenhuma comutação local for selecionada, o pool Multicast deverá ser configurado e o endereço multicast de toda a malha AVS não deverá fazer parte do pool Multicast. Todo o tráfego originado do AVS será encapsulado em VLAN ou VXLAN.

Navegue até **Rede VM > VMWare > Criar domínio vCenter,** conforme mostrado na imagem:

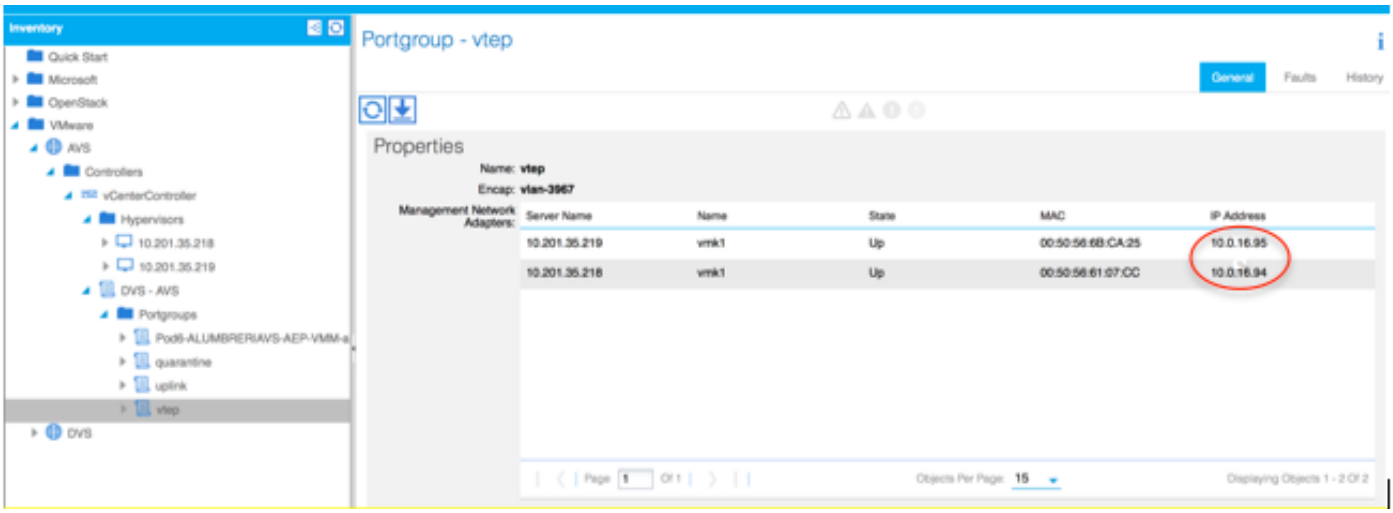


Se você estiver usando canal de porta ou VPC (canal de porta virtual), é recomendável definir as políticas do vSwitch para usar o Mac Pinning.

Depois disso, o APIC deve enviar a configuração do switch AVS para o vCenter, como mostrado na imagem:



No APIC, você pode observar que um endereço VXLAN Tunnel Endpoint (VTEP) é atribuído ao grupo de portas VTEP para AVS. Este endereço é atribuído independentemente do modo de conectividade usado (VLAN ou VXLAN)



Instalar o software Cisco AVS no vCenter

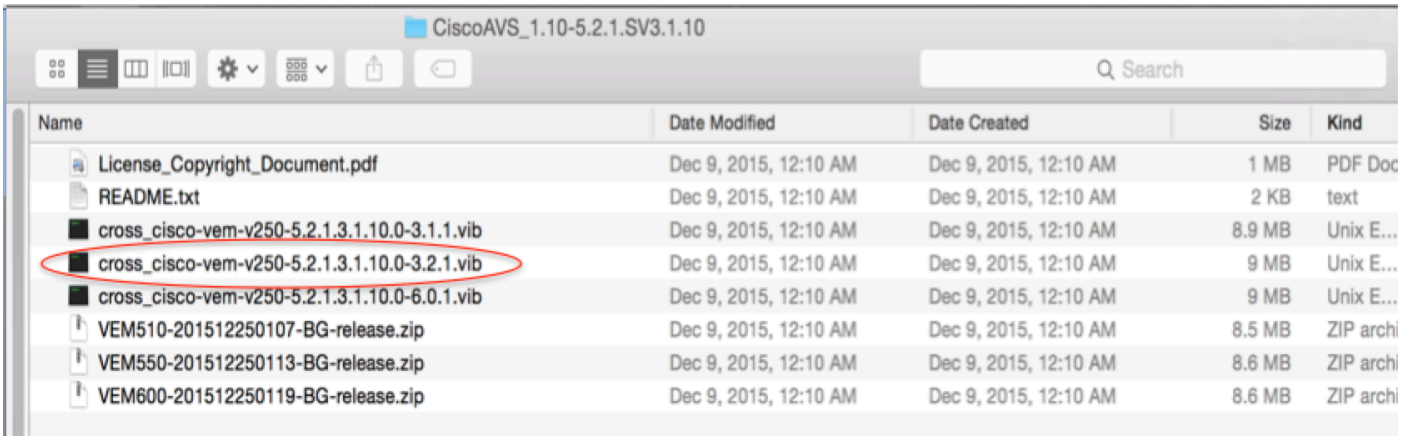
- Baixe o vSphere Installation Bundle (VIB) do CCO usando este link

  Nota:Nesse caso, estamos usando o ESX 5.5, Tabela 1, mostra a matriz de compatibilidade do ESXi 6.0, 5.5, 5.1 e 5.0

Tabela 1 - Compatibilidade da versão do software do host para ESXi 6.0, 5.5, 5.1 e 5.0

VMware	VIB	VEM Bundle	Windows VC Installer	Linux vCenter Server Appliance
ESXi 6.0	cross_cisco-vem- v250-5.2.1.3.1.10.0-6.0.1.vib	VEM600-201512250119-BG- release.zip (Offline) VEM600-201512250119-BG (Online)	6.0	6.0
ESXi 5.5	cross_cisco-vem- v250-5.2.1.3.1.10.0-3.2.1.vib	VEM550-201512250113-BG- release.zip (Offline) VEM550-201512250113-BG (Online)	5.5	5.5
ESXi 5.1	cross_cisco-vem- v250-5.2.1.3.1.10.0-3.1.1.vib	VEM510-201512250107-BG- release.zip (Offline) VEM510-201512250107-BG (Online)	5.1	5.1
ESXi 5.0	cross_cisco-vem- v250-5.2.1.3.1.10.0-3.0.1.vib	VEM500-201512250101-BG- release.zip (Offline) VEM500-201512250101-BG (Online)	5.0	5.0

No arquivo ZIP, há 3 arquivos VIB, um para cada versão do host ESXi, selecione o apropriado para o ESX 5.5, como mostrado na imagem:



- Copie o arquivo VIB para o ESX Datastore - isso pode ser feito via CLI ou diretamente do vCenter

  Note: Se houver um arquivo VIB no host, remova-o usando o comando **esxcli software vib** remove.

esxcli software vib remove -n cross_cisco-vem-v197-5.2.1.3.1.5.0-3.2.1.vib

ou navegando diretamente no Datastore.

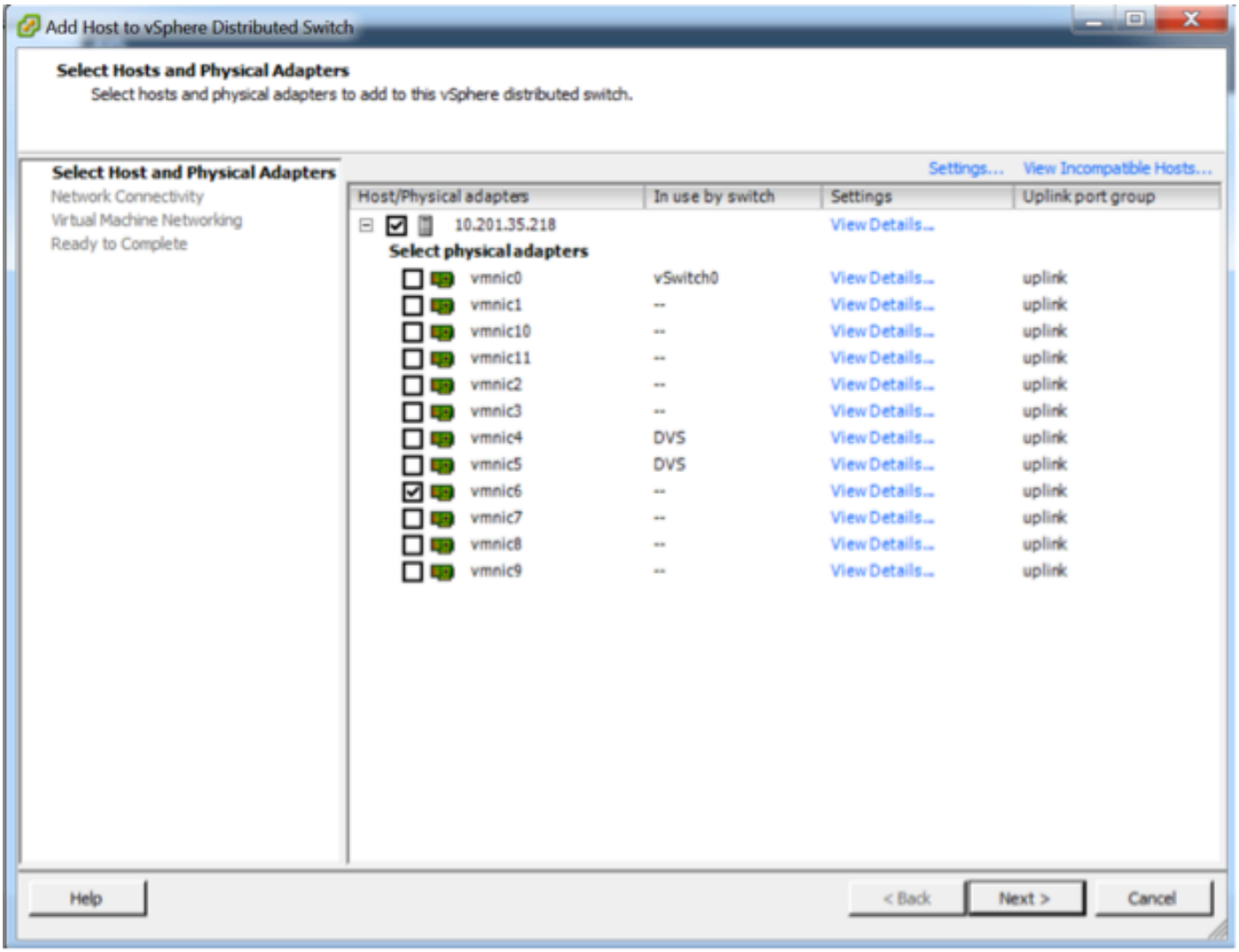
- Instale o software AVS usando o seguinte comando no host ESXi:

esxcli software vib install -v /vmfs/volumes/datastore1/cross_cisco-vem-v250-5.2.1.3.1.10.0-3.2.1.vib — modo de manutenção — no-sig-check

```
~ # esxcli software vib install -v /vmfs/volumes/datastore1/cross_cisco-vem-v250-5.2.1.3.1.10.0-3.2.1.vib --maintenance-mode --no-sig-check
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v250-esx_5.2.1.3.1.10.0-3.2.1
   VIBs Removed: Cisco_bootbank_cisco-vem-v197-esx_5.2.1.3.1.5.0-3.2.1
   VIBs Skipped:
~ # vem status

VEM modules are loaded

Switch Name      Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0         5632        8           128               1500    vmnic0
DVS Name         Num Ports   Used Ports  Configured Ports  MTU     Uplinks
DVS              5632        10          512               9000    vmnic5,vmnic4

VEM Agent (vemdpa) is running

~ #
```

- Depois que o VEM (Virtual Ethernet module) estiver ativo, você poderá adicionar hosts ao seu AVS:

Na caixa de diálogo Add Host to vSphere Distributed Switch, escolha as portas da NIC virtual conectadas ao switch leaf (Neste exemplo, você move apenas vmnic6), como mostrado na imagem:



- Clique em Next
- Na caixa de diálogo Conectividade de rede, clique em **Avançar**
- Na caixa de diálogo Rede de Máquina Virtual, clique em **Avançar**
- Na caixa de diálogo Pronto para concluir, clique em **Concluir**

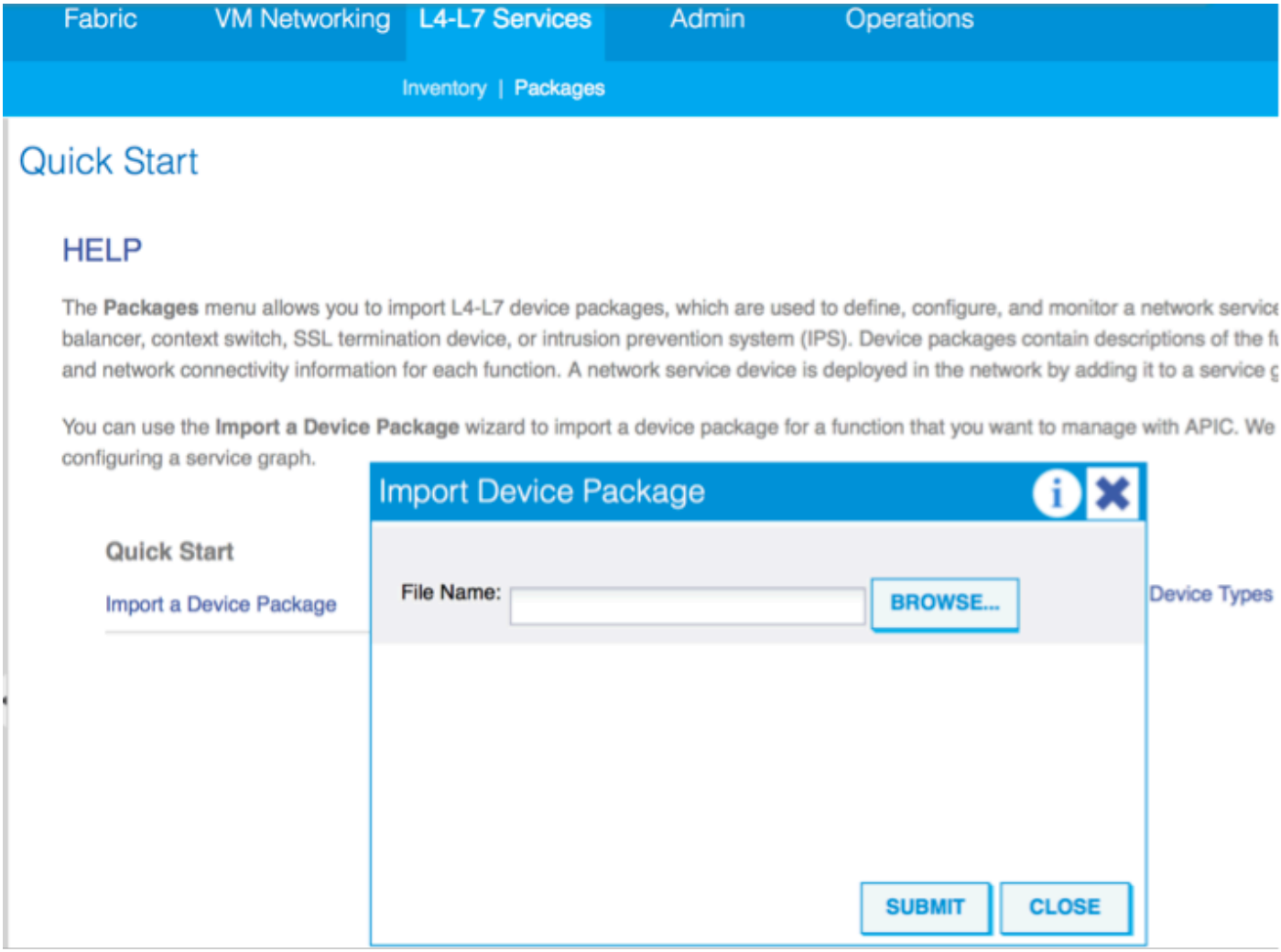
Note: Se vários hosts ESXi forem usados, todos precisarão executar o AVS/VEM para que possam ser gerenciados do switch padrão para DVS ou AVS.

Com isso, a integração do AVS foi concluída e estamos prontos para continuar com a implantação do L4-L7 ASAv:

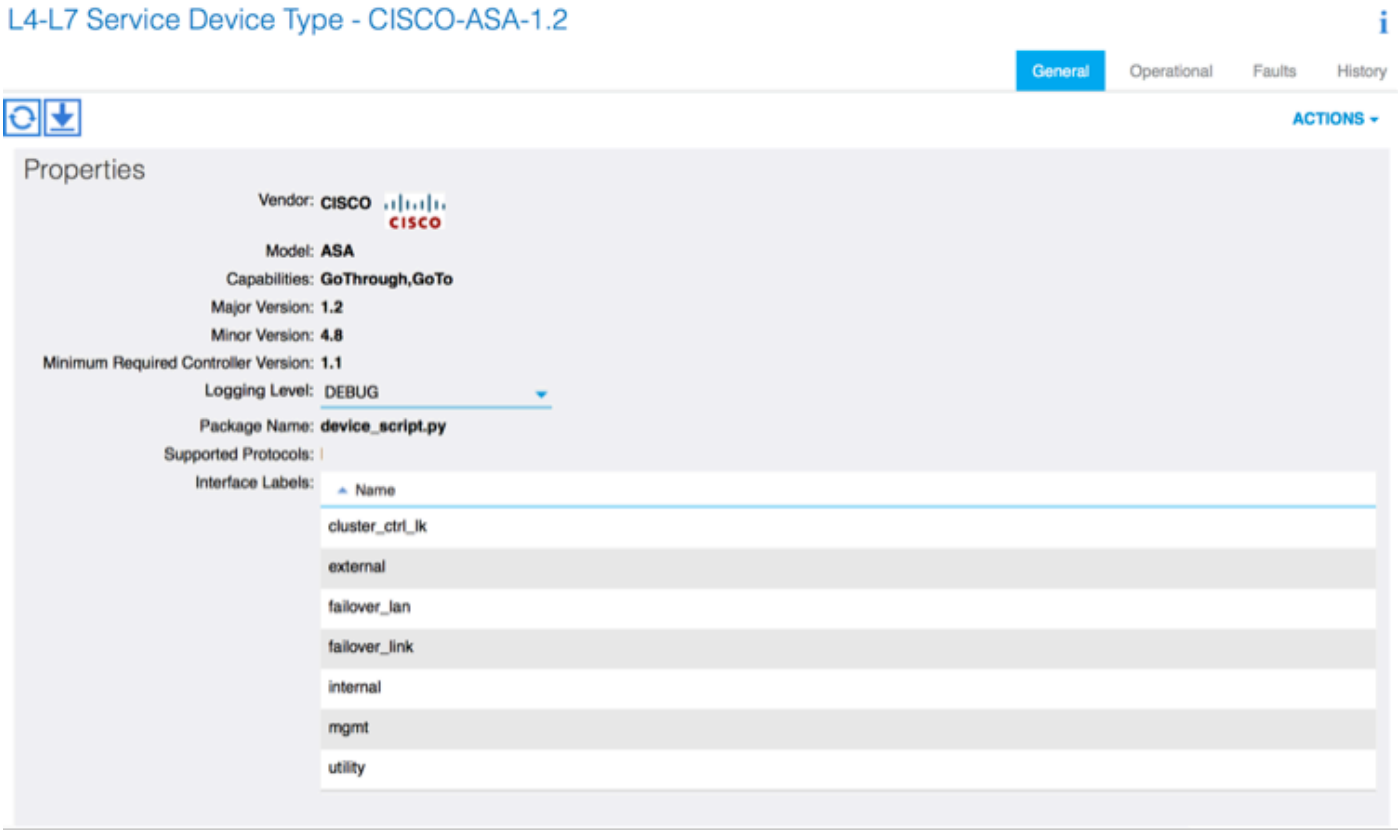
Configuração inicial do ASAv

- Faça o download do pacote de dispositivos Cisco ASAv e importe-o para o APIC:

Navegue até **L4-L7 Services > Packages > Import Device Package (Serviços L4-L7 > Pacotes > Importar pacote de dispositivo)** como mostrado na imagem:



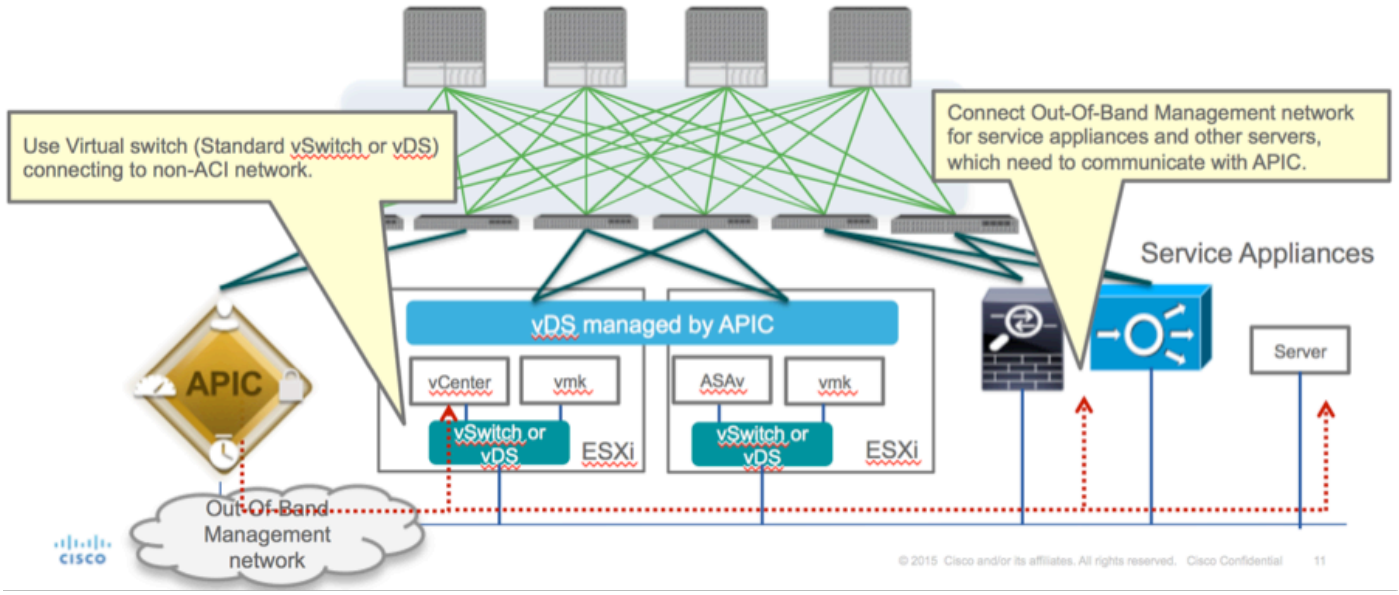
- Se tudo funcionar bem, você poderá ver o pacote de dispositivo importado expandindo a pasta Tipos de dispositivo de serviço L4-L7, como mostrado na imagem:



Antes de continuar, há alguns aspectos da instalação que precisam ser determinados antes da integração L4-L7 real ser executada:

Há dois tipos de redes de gerenciamento, gerenciamento dentro da banda e out-of-band (OOB), que podem ser usadas para gerenciar dispositivos que não fazem parte da ACI (Application Centric Infrastructure, infraestrutura básica centrada em aplicativos) (leaf, spines, controlador apic), que inclui ASAv, balanceadores de carga, etc.

Nesse caso, o OOB para ASAv é implantado com o uso do vSwitch padrão. Para ASA bare metal ou outros dispositivos e/ou servidores de serviços, conecte a porta de gerenciamento OOB ao switch OOB ou à rede, como mostrado na imagem.



A conexão de gerenciamento de porta OOB ASAv precisa usar portas de uplink ESXi para se comunicar com o APIC via OOB. Ao mapear interfaces vNIC, o adaptador de rede 1 sempre corresponde à interface Management0/0 no ASAv, e o restante das interfaces do plano de dados é iniciado do adaptador de rede 2.

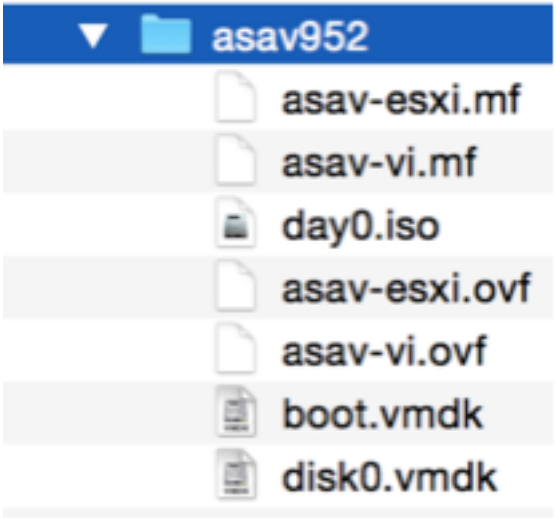
A Tabela 2 mostra a concordância das IDs dos adaptadores de rede e IDs de interface do ASAv:

Tabela 2

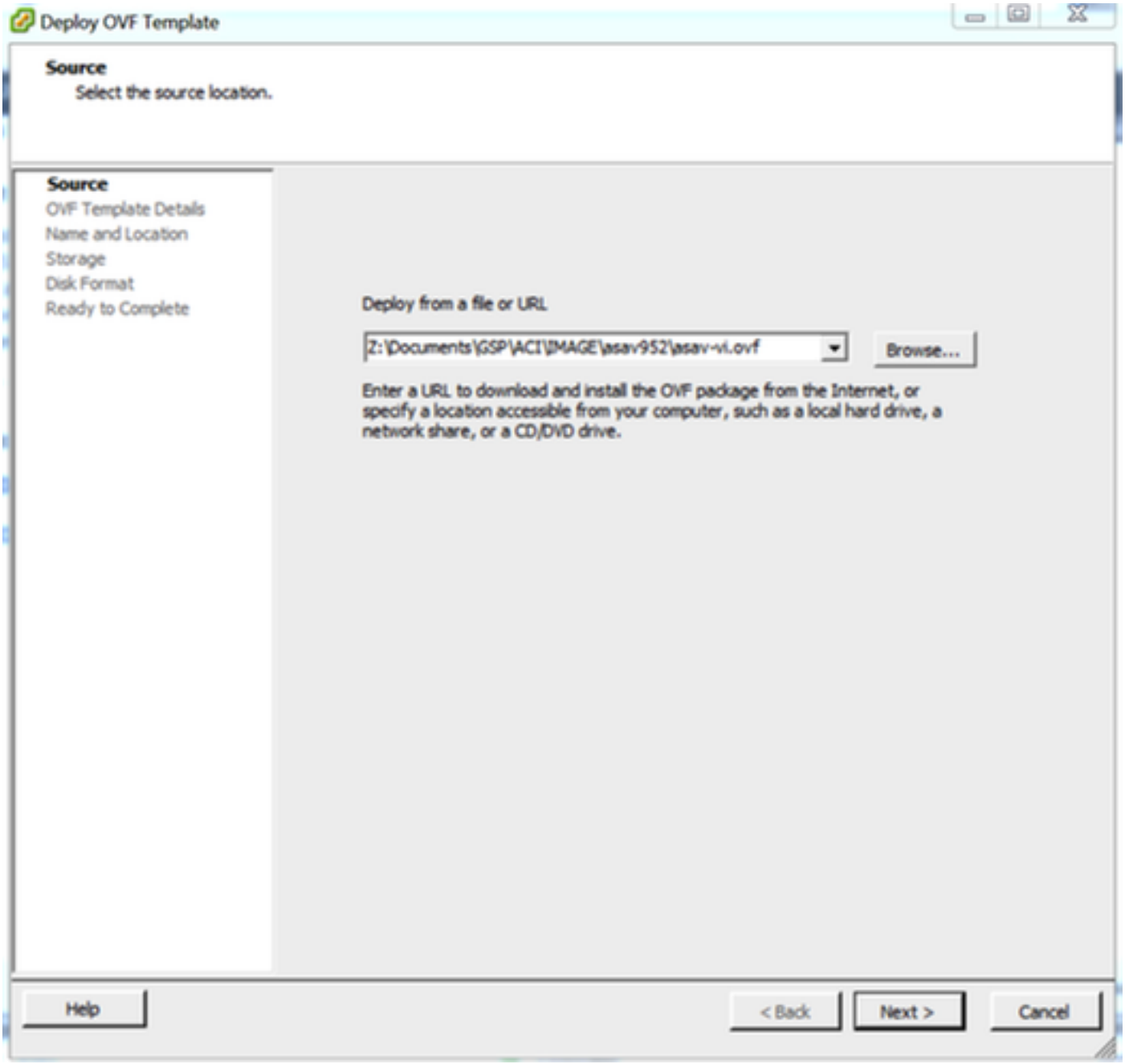
Network Adapter ID	ASAv Interface ID
Network Adapter 1	Management0/0
Network Adapter 2	GigabitEthernet0/0
Network Adapter 3	GigabitEthernet0/1
Network Adapter 4	GigabitEthernet0/2
Network Adapter 5	GigabitEthernet0/3
Network Adapter 6	GigabitEthernet0/4
Network Adapter 7	GigabitEthernet0/5
Network Adapter 8	GigabitEthernet0/6
Network Adapter 9	GigabitEthernet0/7
Network Adapter 10	GigabitEthernet0/8

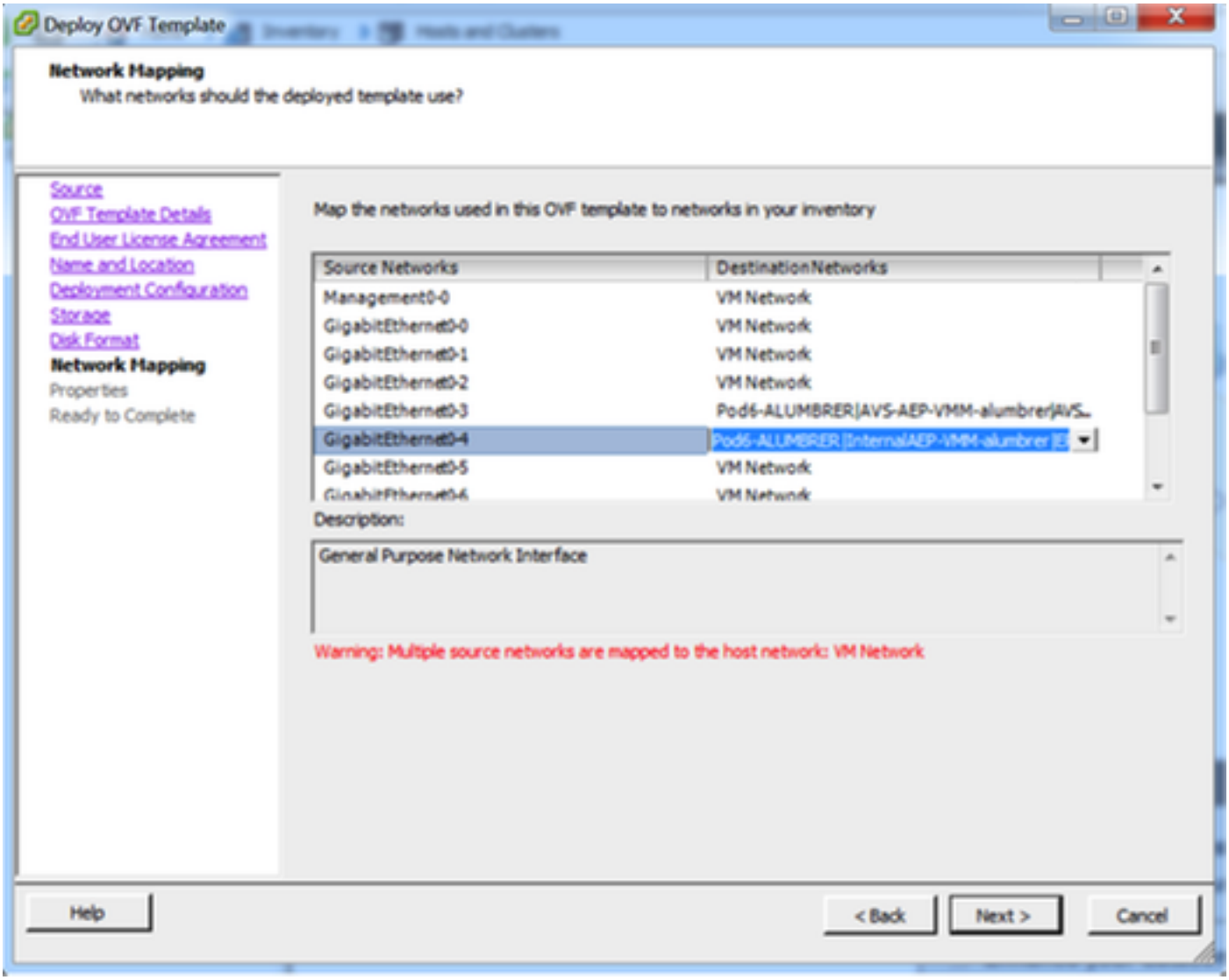
- Implantar a VM ASAv através do assistente de **Arquivo > Implantar modelo OVF (Open Virtualization Format)**
- Selecione **asav-esxi** se quiser usar o ESX Server independente ou **asav-vi** para vCenter.

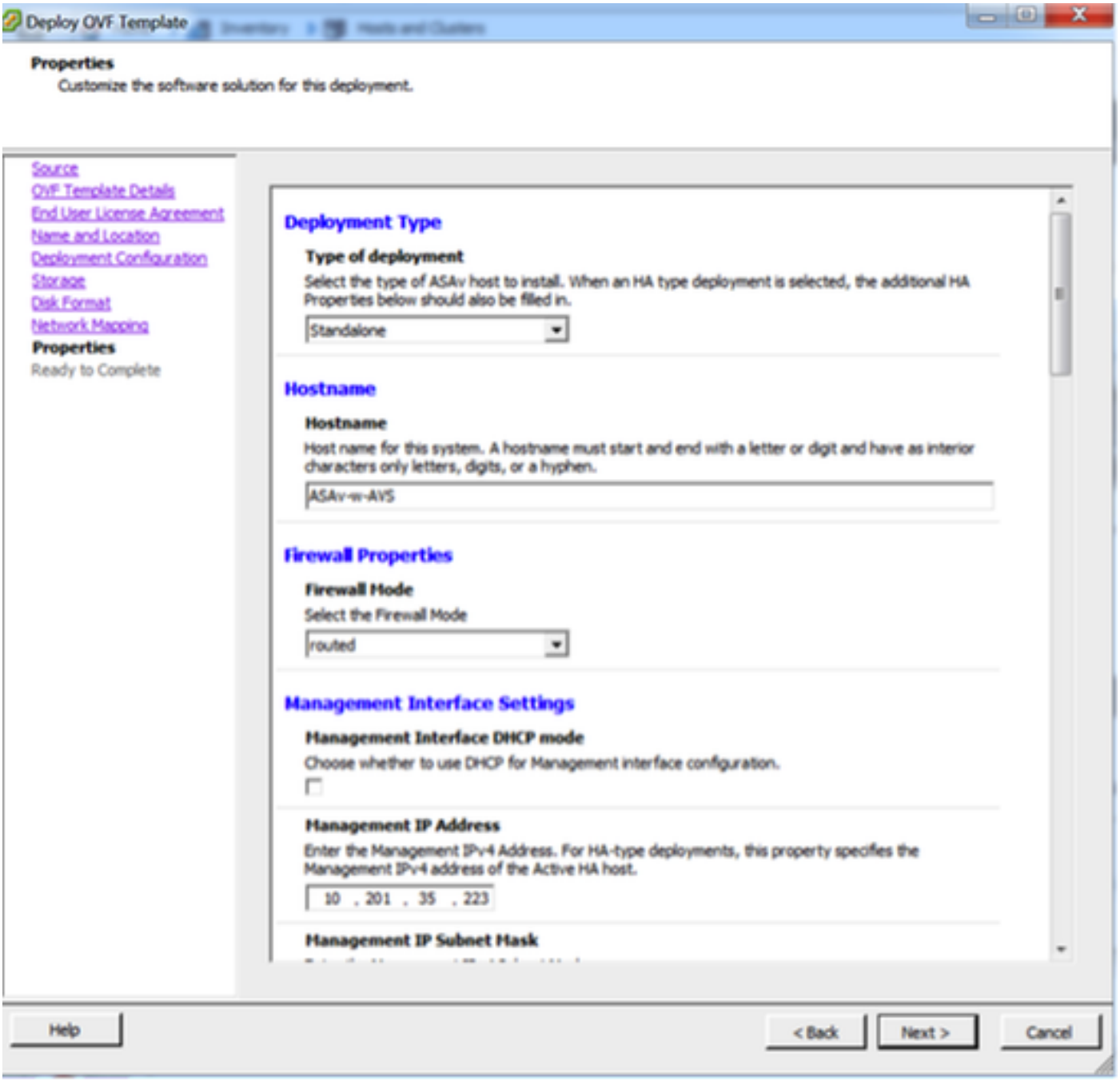
Nesse caso, o vCenter é usado.

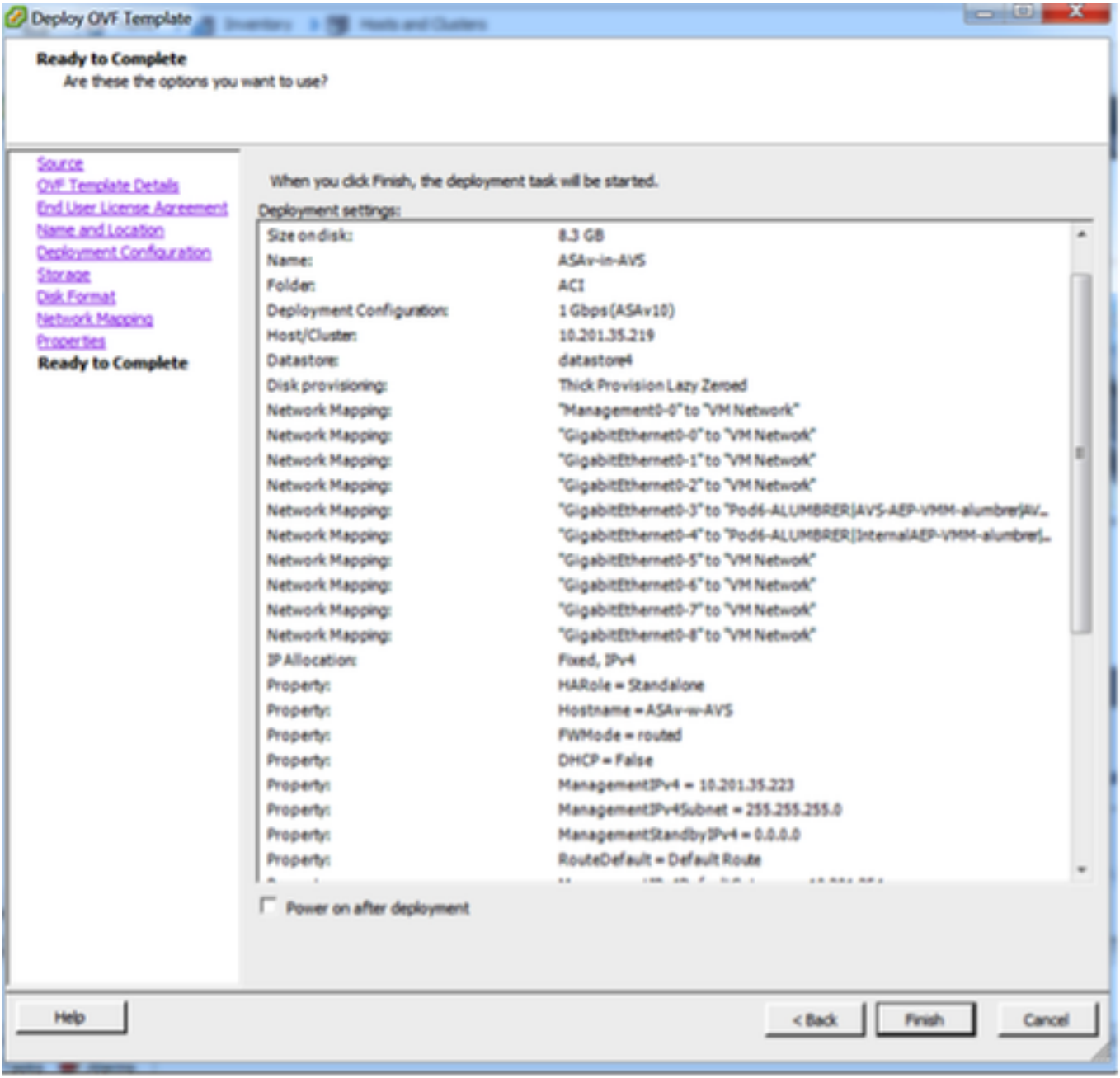


- Vá até o assistente de instalação, aceite os termos e condições. No meio do assistente, você pode determinar várias opções, como nome do host, gerenciamento, endereço ip, modo de firewall e outras informações específicas relacionadas ao ASAv. Lembre-se de usar o gerenciamento OOB para ASAv, pois nesse caso você precisa manter a interface Management0/0 enquanto usa a Rede VM (Switch Padrão) e a interface GigabitEthernet0-8 é a porta de rede padrão.

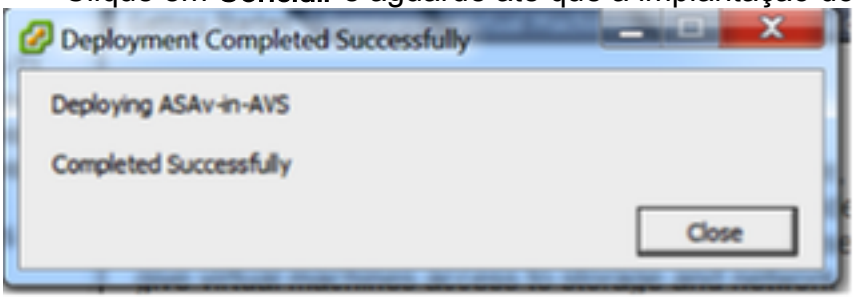

Deploy OVF Template
Source
Select the source location.
Source
OVF Template Details
Name and Location
Storage
Disk Format
Ready to Complete
Deploy from a file or URL
Z:\Documents\GSP\ACI\IMAGE\asav952\asav-vi.ovf
Browse...
Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.
Help
< Back
Next >
Cancel


Deploy OVF Template
Network Mapping
What networks should the deployed template use?
Source
OVF Template Details
End User License Agreement
Name and Location
Deployment Configuration
Storage
Disk Format
Network Mapping
Properties
Ready to Complete
Map the networks used in this OVF template to networks in your inventory
Source Networks
Destination Networks
Management0-0
VM Network
GigabitEthernet0-0
VM Network
GigabitEthernet0-1
VM Network
GigabitEthernet0-2
VM Network
GigabitEthernet0-3
Pod6-ALUMBRER|AVS-AEP-VMM-alumbrer|AVS...
GigabitEthernet0-4
Pod6-ALUMBRER|InternalAEP-VMM-alumbrer|E
GigabitEthernet0-5
VM Network
Description:
General Purpose Network Interface
Warning: Multiple source networks are mapped to the host network: VM Network
Help
< Back
Next >
Cancel

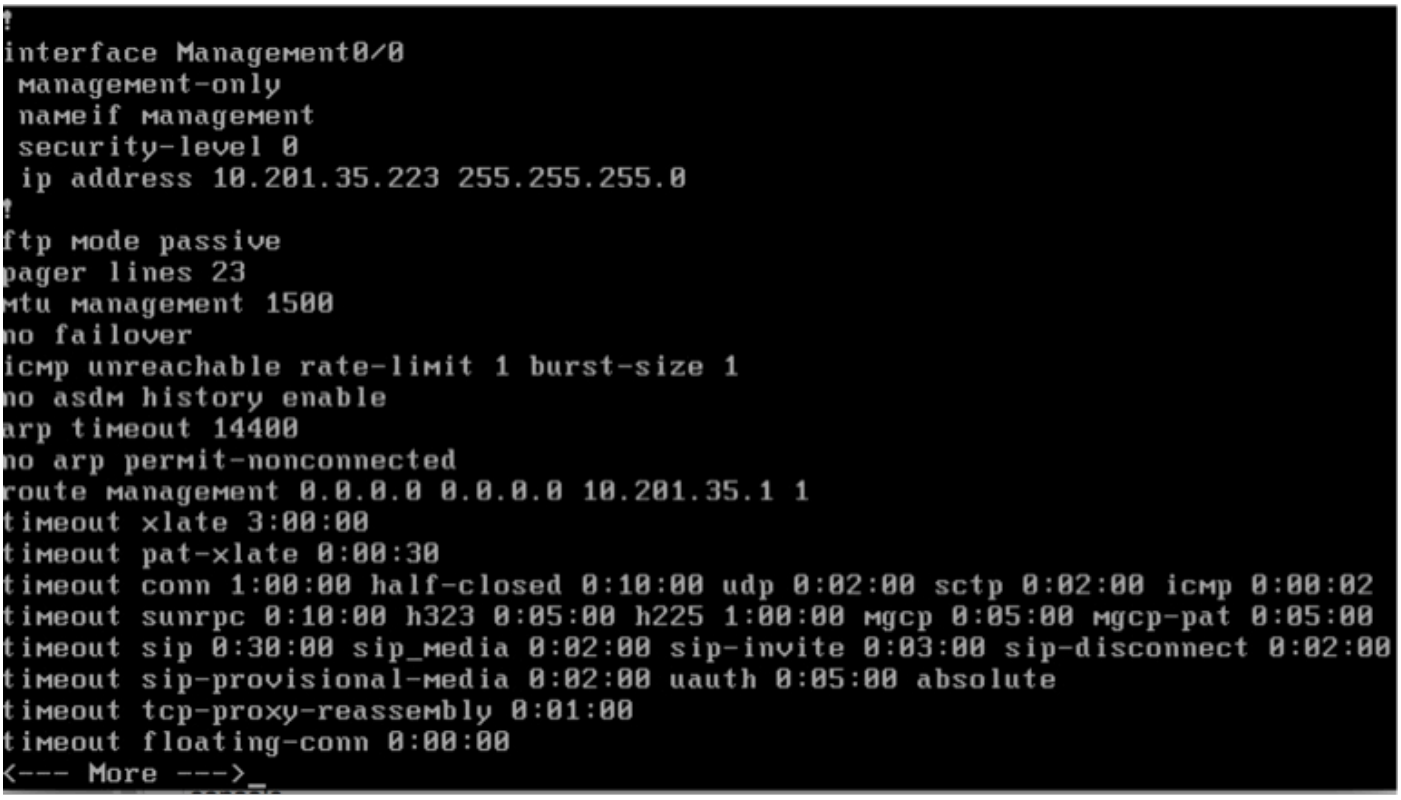

Deploy OVF Template
Properties
Customize the software solution for this deployment.
Source
OVF Template Details
End User License Agreement
Name and Location
Deployment Configuration
Storage
Disk Format
Network Mapping
Properties
Ready to Complete
Deployment Type
Type of deployment
Select the type of ASAv host to install. When an HA type deployment is selected, the additional HA Properties below should also be filled in.
Standalone
Hostname
Hostname
Host name for this system. A hostname must start and end with a letter or digit and have as interior characters only letters, digits, or a hyphen.
ASAv-w-AVS
Firewall Properties
Firewall Mode
Select the Firewall Mode
routed
Management Interface Settings
Management Interface DHCP mode
Choose whether to use DHCP for Management interface configuration.
Management IP Address
Enter the Management IPv4 Address. For HA-type deployments, this property specifies the Management IPv4 address of the Active HA host.
10 . 201 . 35 . 223
Management IP Subnet Mask
Help
< Back
Next >
Cancel



- Clique em **Concluir** e aguarde até que a implantação do ASAv seja concluída

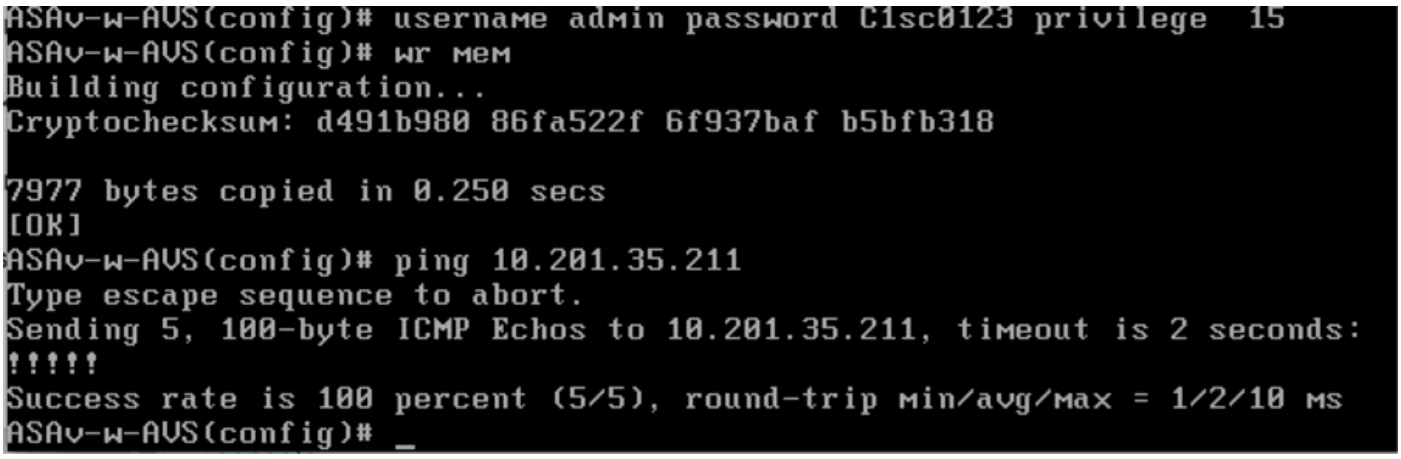


- Ligue o ASAv VM e faça login via console para verificar a configuração inicial



- Como mostrado na imagem, alguma configuração de gerenciamento já foi enviada para o Firewall ASAv. Configure o nome de usuário e a senha do administrador. Esse nome de usuário e senha são usados pelo APIC para fazer login e configurar o ASA. O ASA deve ter conectividade com a rede OOB e deve conseguir acessar o APIC.

username admin password <device_password> privilégio criptografado 15



Além disso, no modo de configuração global, habilite o servidor http:

http server enable

http 0.0.0.0 0.0.0.0 gerenciamento

L4-L7 para integração do ASAv no APIC:

- Faça login na GUI da ACI, clique no Espaço onde o gráfico de serviços será implantado. Expanda os serviços L4-L7 na parte inferior do painel de navegação e clique com o botão direito do mouse em **Dispositivos L4-L7** e clique em **Criar dispositivos L4-L7** para abrir o assistente

- Para esta implementação, serão aplicadas as seguintes definições:
  -Modo gerenciado

  -Serviço de firewall

  -Dispositivo virtual

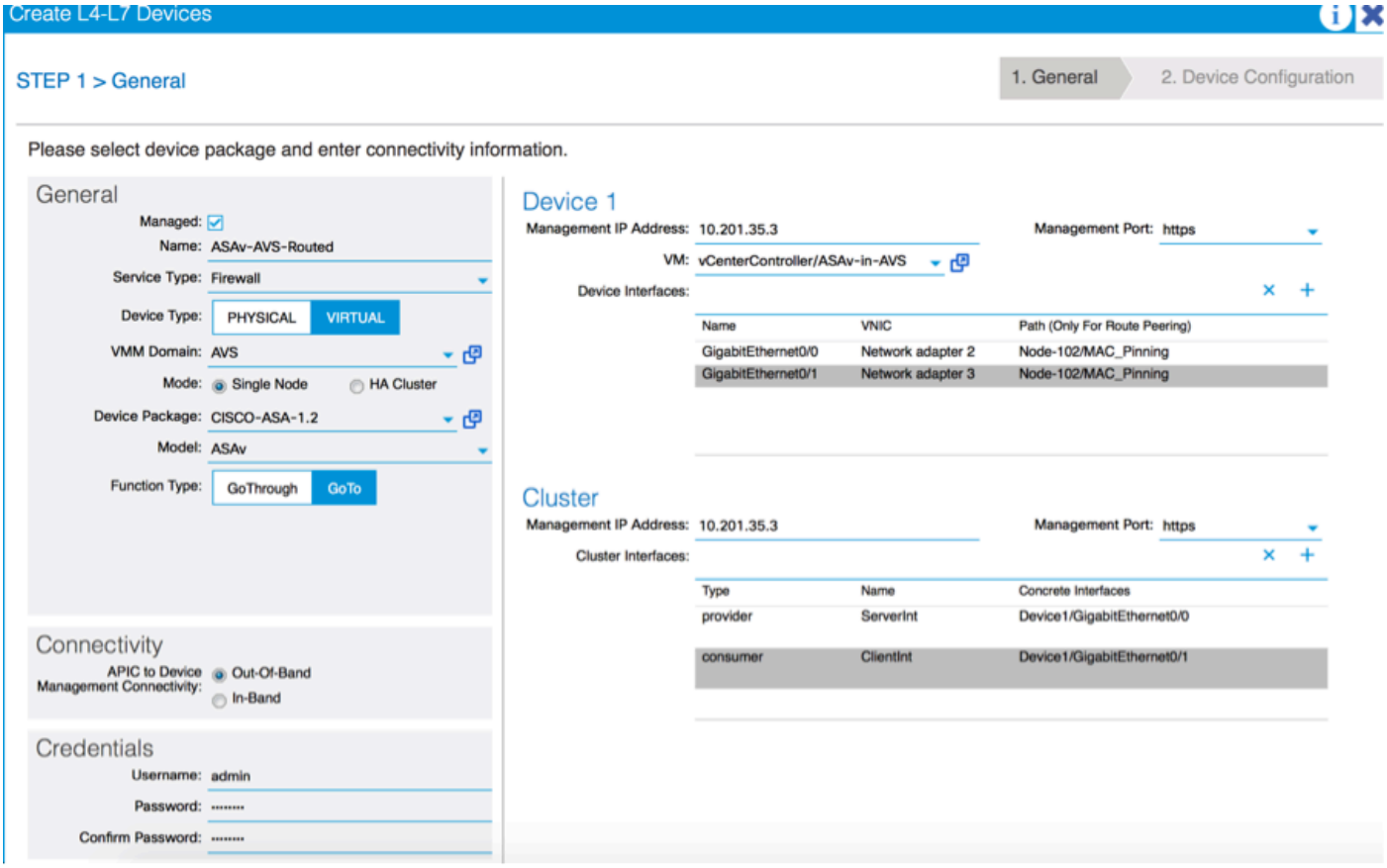
  -Conectado ao domínio AVS com um nó único

  -Modelo ASAv

  -Modo roteado (GoTo)

  -Management Address (Endereço de gerenciamento) (precisa corresponder ao endereço anterior atribuído à interface Mgmt0/0)

- Usar HTTPS como APIC por padrão usa o protocolo mais seguro para se comunicar com o ASAv



- A definição correta das interfaces do dispositivo e das interfaces do cluster é essencial para uma implantação bem-sucedida

Para a primeira parte, use a Tabela 2 mostrada na seção anterior para corresponder corretamente as IDs do adaptador de rede com as IDs de interface do ASAv que você gostaria de usar. O Caminho refere-se à porta física ou canal de porta ou VPC que permite a entrada e saída das interfaces de firewall. Nesse caso, o ASA está localizado em um host ESX, em que entrada e saída são iguais para ambas as interfaces. Em um dispositivo físico, dentro e fora do firewall (FW) seriam portas físicas diferentes.

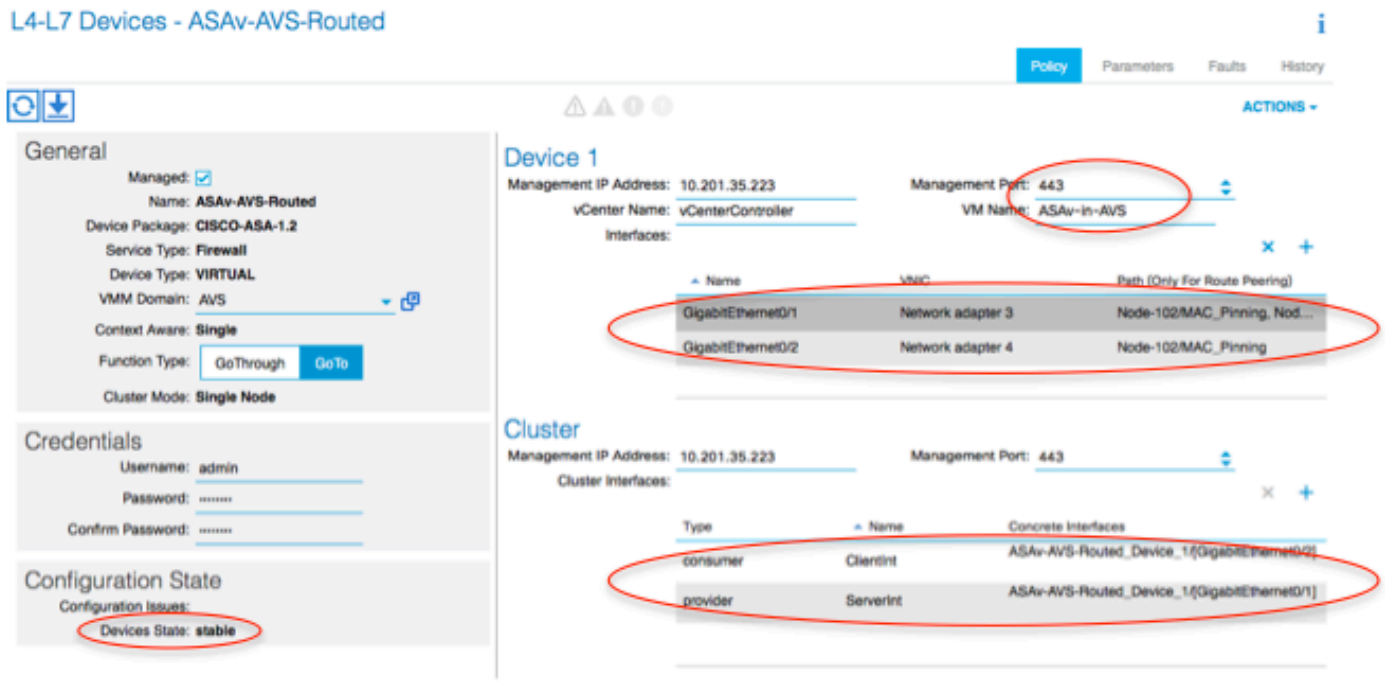
Para a segunda parte, as interfaces de cluster devem ser definidas sempre sem exceções

(mesmo que o Cluster HA não seja usado), isso ocorre porque o Modelo de objeto tem uma associação entre a interface **mIf** (meta interface no pacote de dispositivos), a interface **LIf** (interface leaf, como externa, interna, interna, etc.) e a **CIf** (interface concreta). Os dispositivos concretos L4-L7 precisam ser configurados em uma configuração de cluster de dispositivos e essa abstração é chamada de dispositivo lógico. O dispositivo lógico tem interfaces lógicas que são mapeadas para interfaces concretas no dispositivo concreto.

Para este exemplo, será usada a seguinte associação:

Gi0/0 = vmnic2 = ServerInt/provider/server > EPG1

Gi0/1 = vmnic3 = ClientInt/consumer/client > EPG2

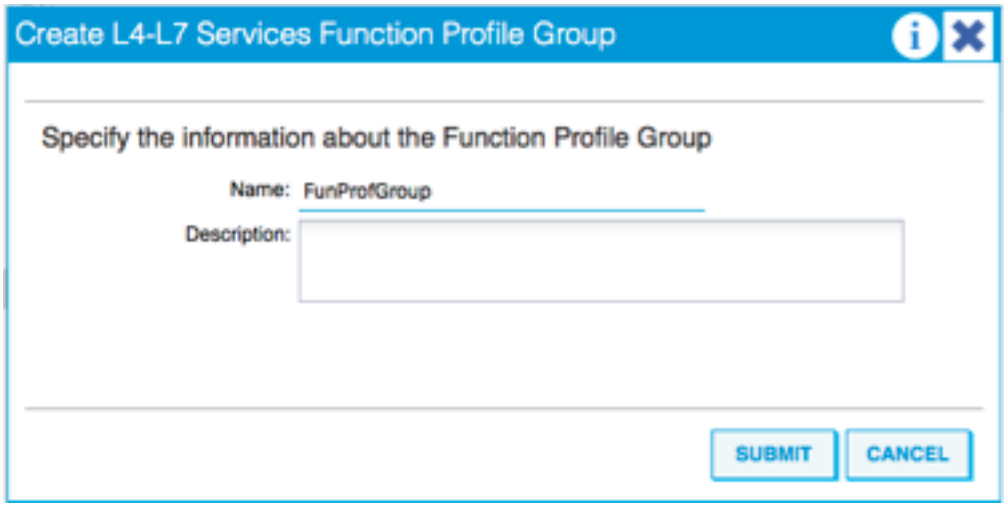


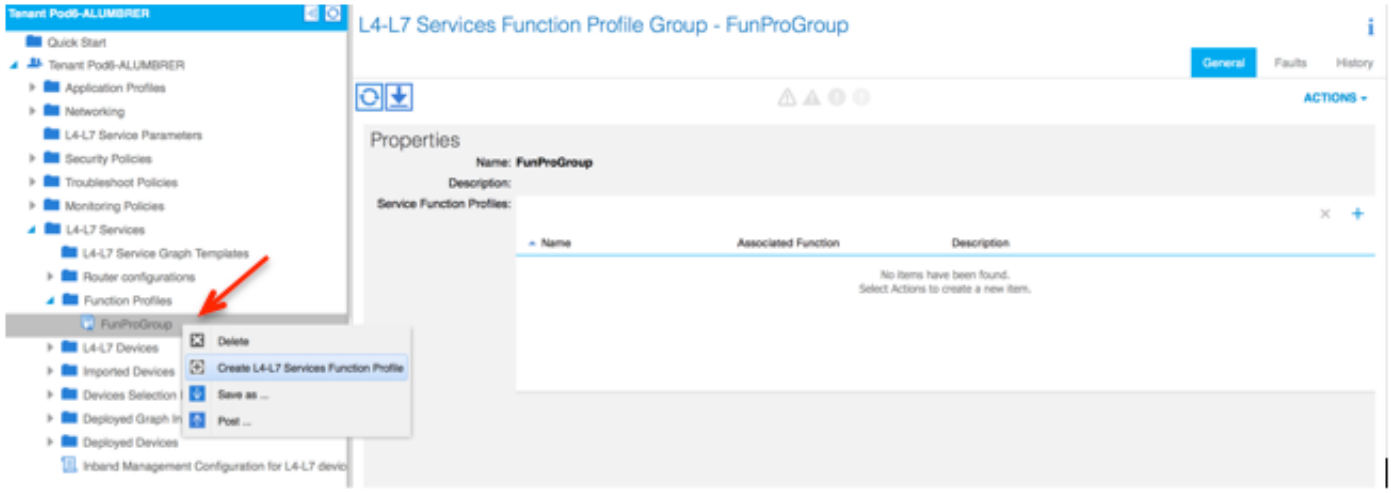
> **Note**: Para implantações de failover/HA, o GigabitEthernet 0/8 é pré-configurado como a interface de failover.

O estado do dispositivo deve ser Estável e você deve estar pronto para implantar o Perfil de função e o Modelo de Gráfico de serviços

Templo do Gráfico de Serviços

Primeiro, crie um perfil de função para o ASAv, mas antes disso você precisa criar o grupo de perfis de função e, em seguida, o perfil de função de serviços L4-L7 nessa pasta, como mostrado na imagem:

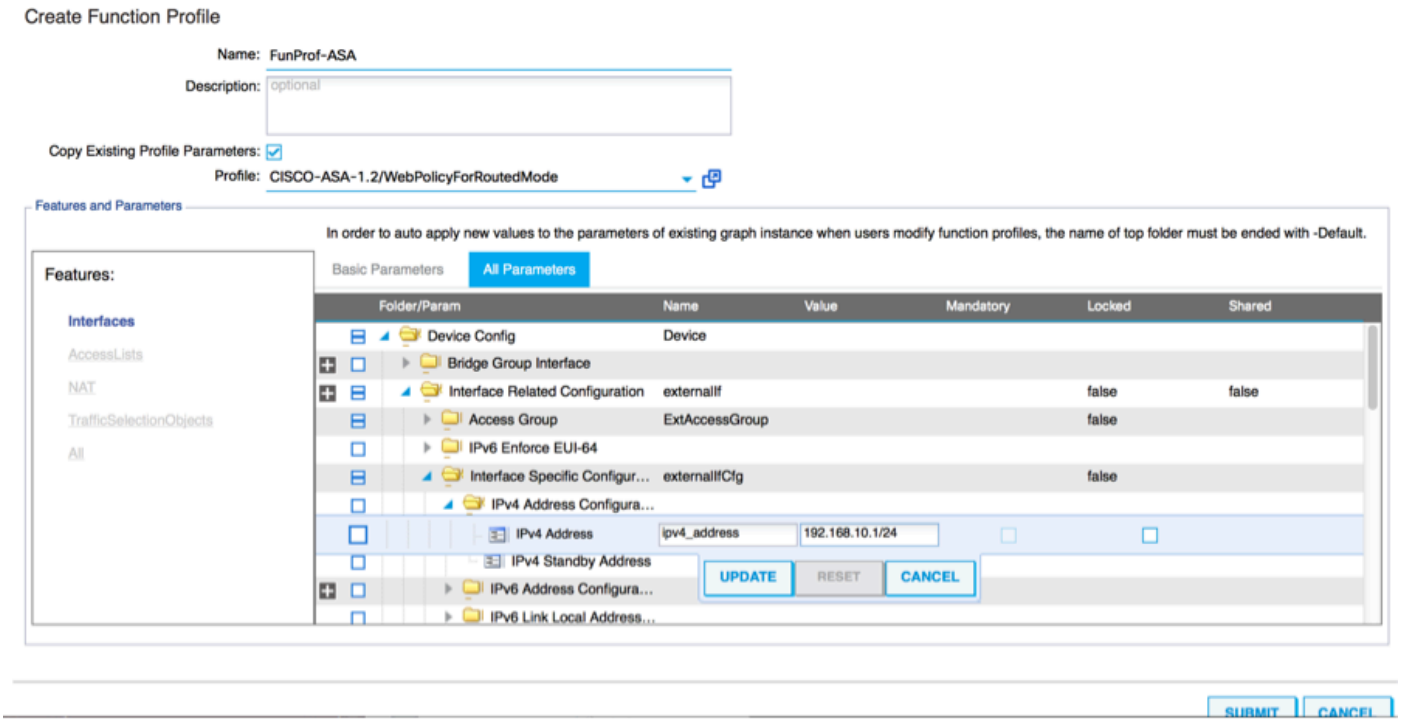




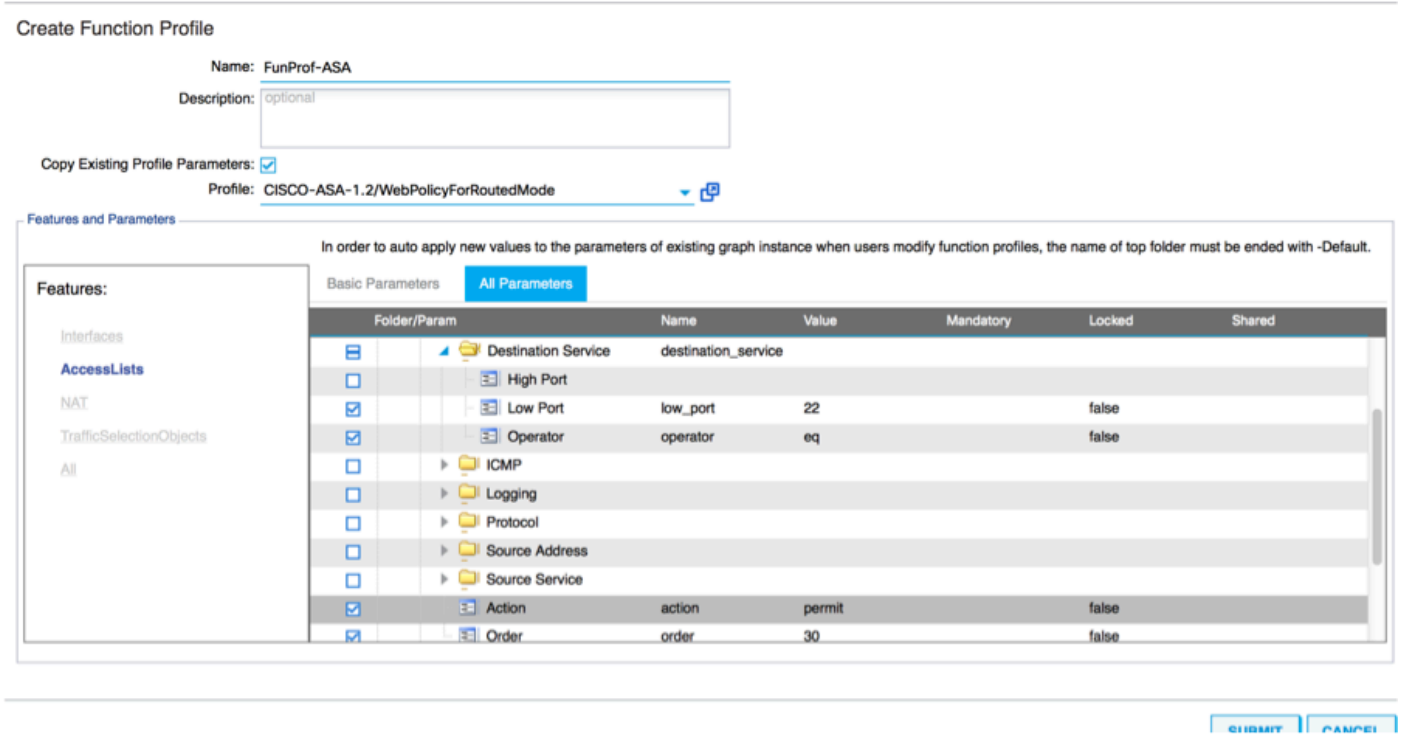
- Selecione o **WebPolicyForRoutedMode** Profile no menu suspenso e continue a configurar as interfaces no firewall. A partir daqui, as etapas são opcionais e podem ser implementadas/modificadas posteriormente. Essas etapas podem ser executadas em alguns estágios diferentes na implantação, dependendo de como o Service Graph pode ser reutilizável ou personalizado.

Para este exercício, um firewall roteado (modo GoTo) exige que cada interface tenha um endereço IP exclusivo. A configuração ASA padrão também tem um nível de segurança de interface (a interface externa é menos segura, a interface interna é mais segura). Você também pode alterar o nome da interface de acordo com seu requisito. Os padrões são usados neste exemplo.

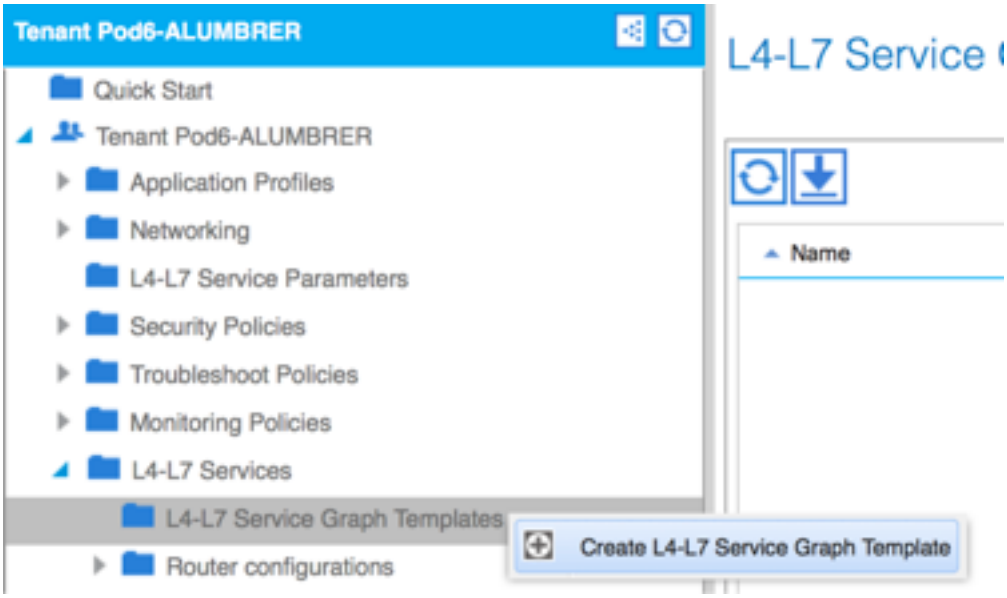
- Expanda a configuração específica da interface, adicione o endereço IP e o nível de segurança para ServerInt com o seguinte formato para o endereço IP **x.x.x.x/y.y.y.y ou x.x.x.x/yy**. Repita o processo para a interface ClientInt.



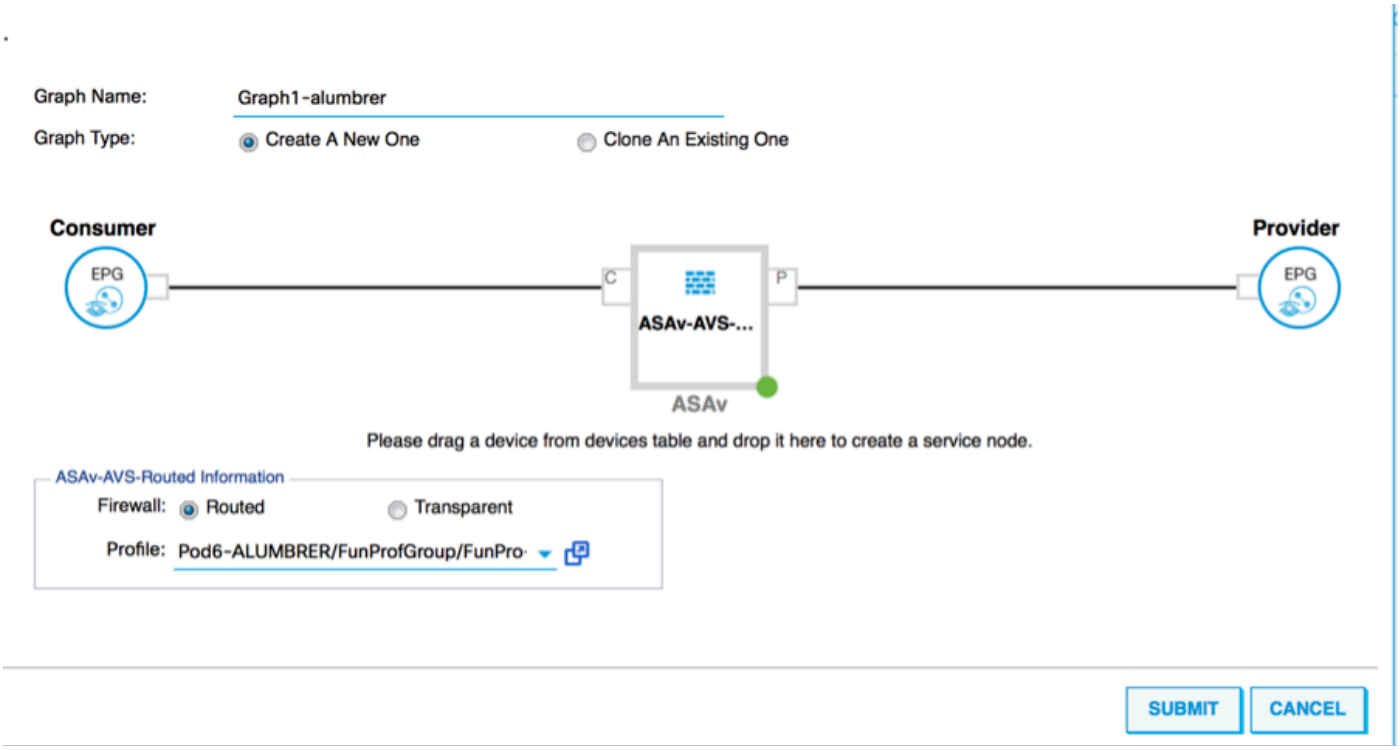
Note: Você também pode modificar as configurações padrão da Lista de acesso e criar seu próprio modelo base. Por padrão, o modelo RoutedMode incluirá regras para HTTP e HTTPS. Para este exercício, SSH e ICMP serão adicionados à lista de acesso externo permitida.



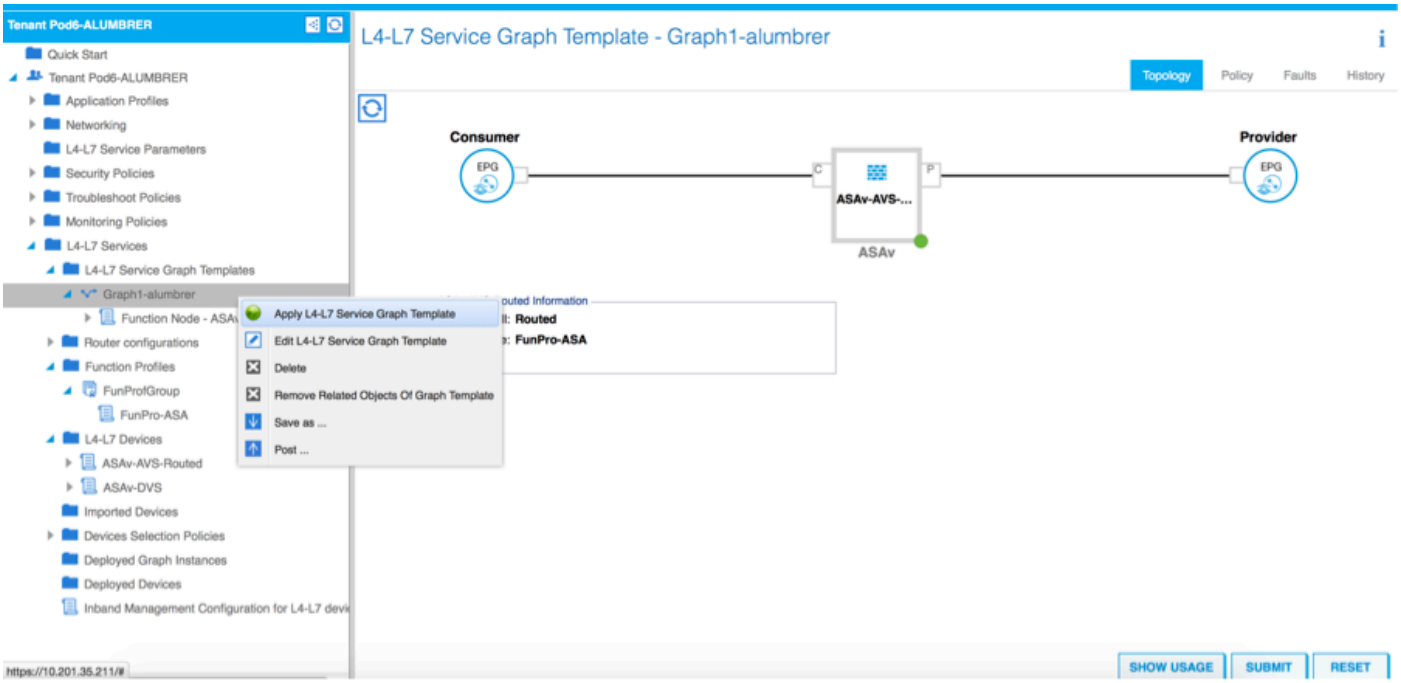
- Em seguida, clique em **Enviar**
- Agora, crie o modelo de gráfico de serviço



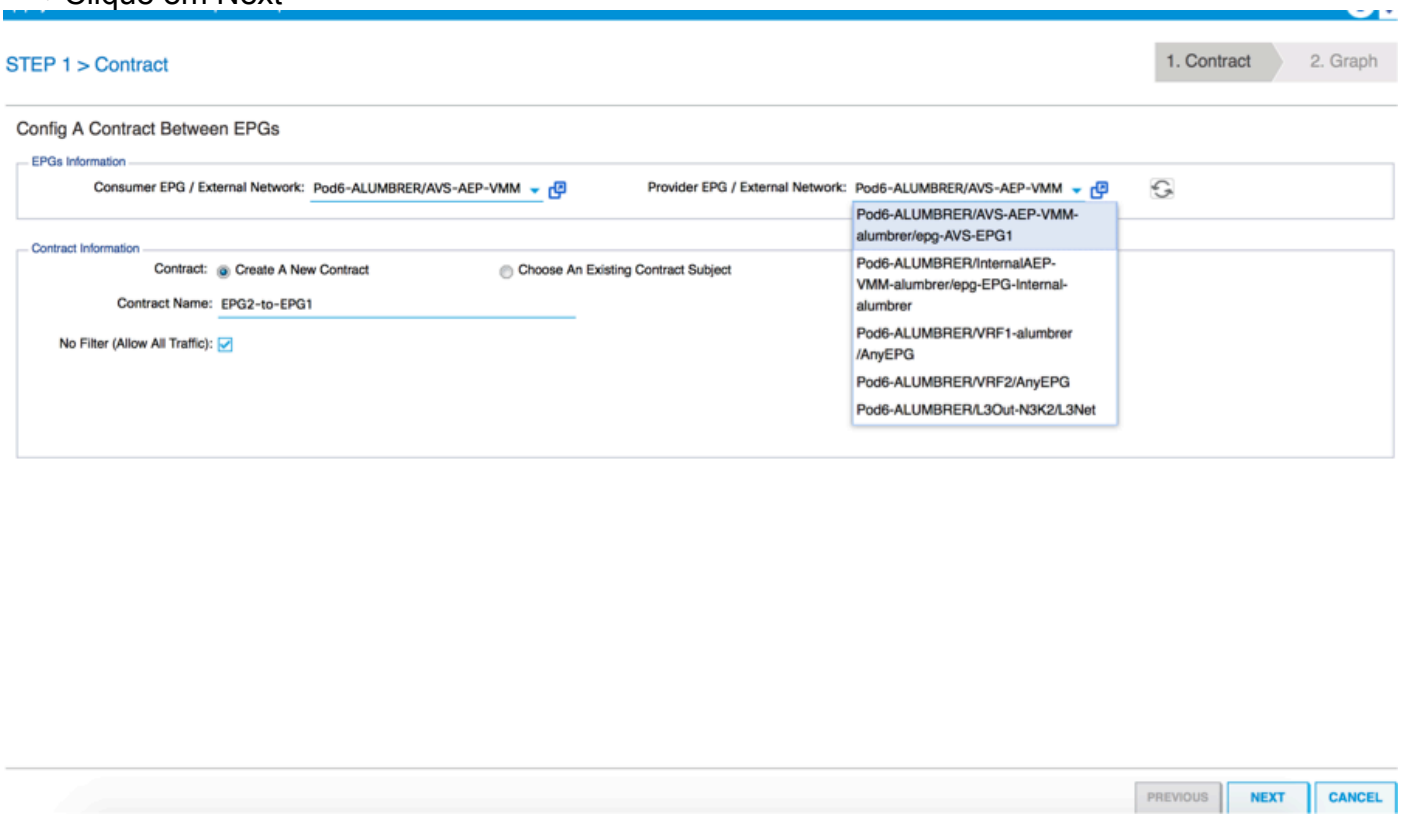
- Arraste e solte o cluster de dispositivos à direita para formar a relação entre consumidor e provedor, selecione Routed Mode (Modo roteado) e o Function Profile (Perfil de função) criado anteriormente.



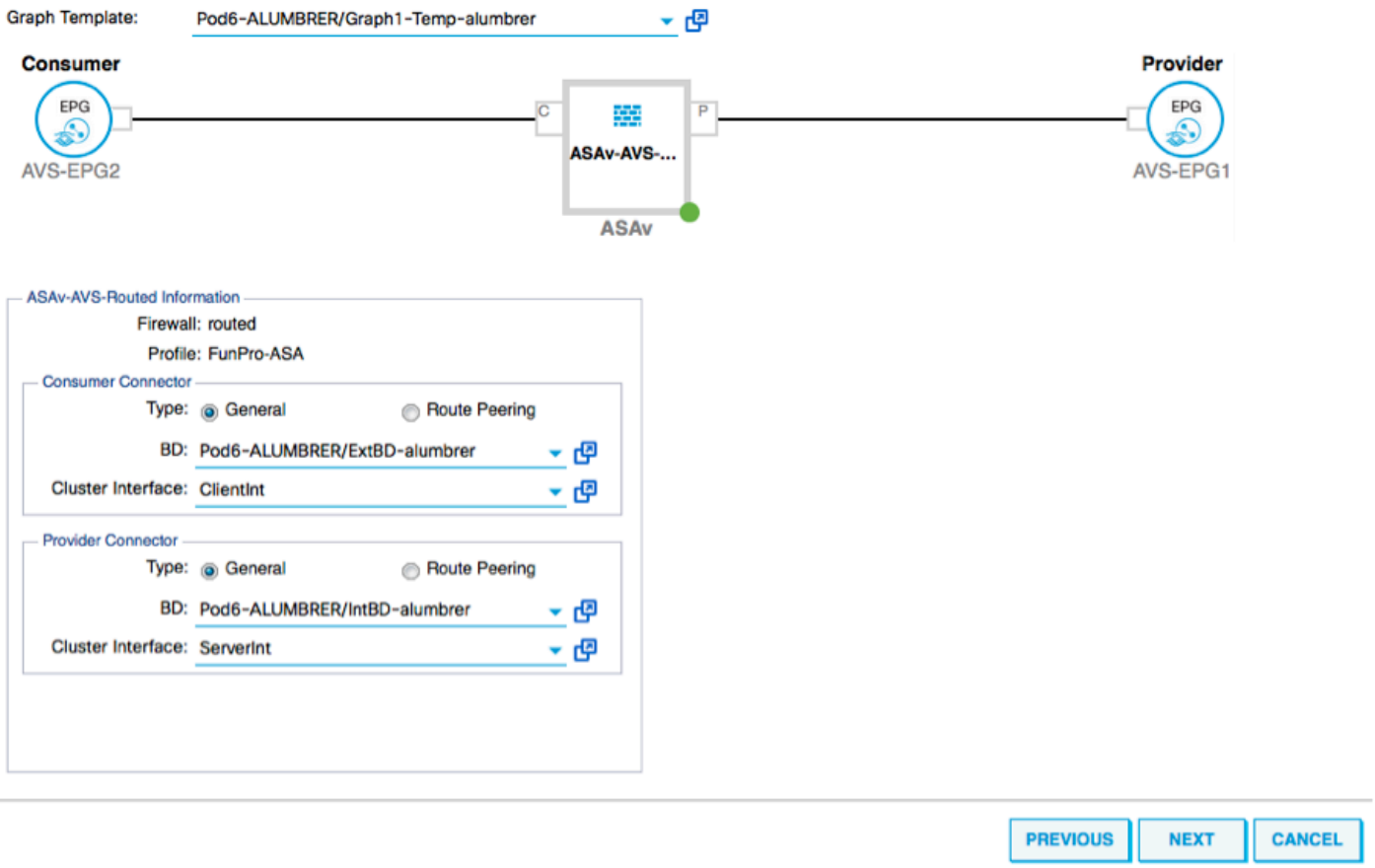
- Verifique se há falhas no modelo. Os modelos são criados para serem reutilizáveis, devem ser aplicados a EPGs específicos, etc.
- Para aplicar um modelo, clique com o botão direito do mouse e selecione Aplicar modelo de gráfico de serviço L4-L7



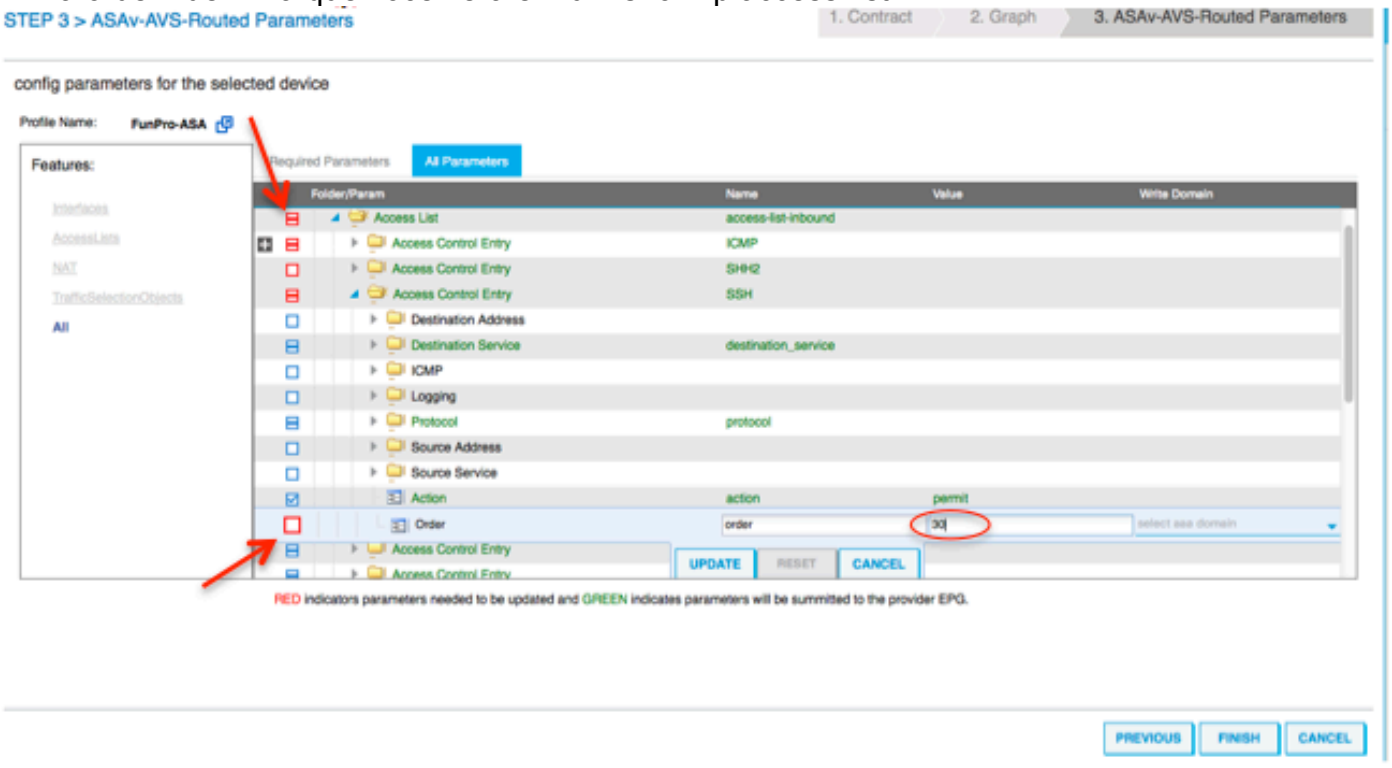
- Defina qual EPG estará no lado do consumidor e do provedor. Neste exercício, AVS-EPG2 é o consumidor (cliente) e AVS-EPG1 é o provedor (servidor). Lembre-se de que nenhum filtro é aplicado, isso permitirá que o firewall faça toda a filtragem com base na lista de acesso definida na última seção deste assistente.
- Clique em Next



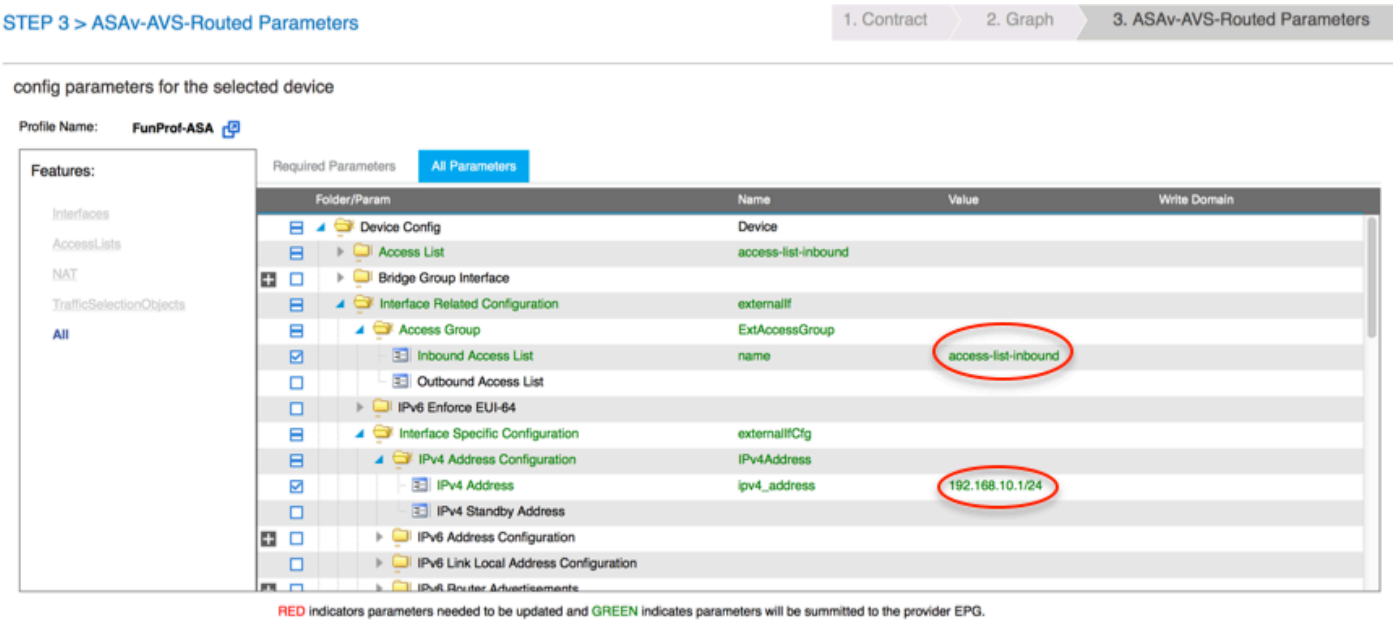
- Verifique as informações da BD para cada um dos EPGs. Nesse caso, EPG1 é o provedor no IntBD DB e EPG2 é o consumidor no BD ExtBD. EPG1 se conectará na interface de firewall ServerInt e EPG2 será conectado na interface ClientInt. As duas interfaces de FW se tornarão a DG de cada EPGs, de modo que o tráfego é forçado a cruzar o firewall o tempo todo.
- Clique em Next



- Na seção Parâmetros de configuração, clique em **Todos os parâmetros** e verifique se há indicadores RED que precisam ser atualizados/configurados. Na saída, como mostrado na imagem, pode-se observar que a ordem na lista de acesso não foi encontrada. Isso equivale à ordem de linha que você verá em um show ip access-list X.



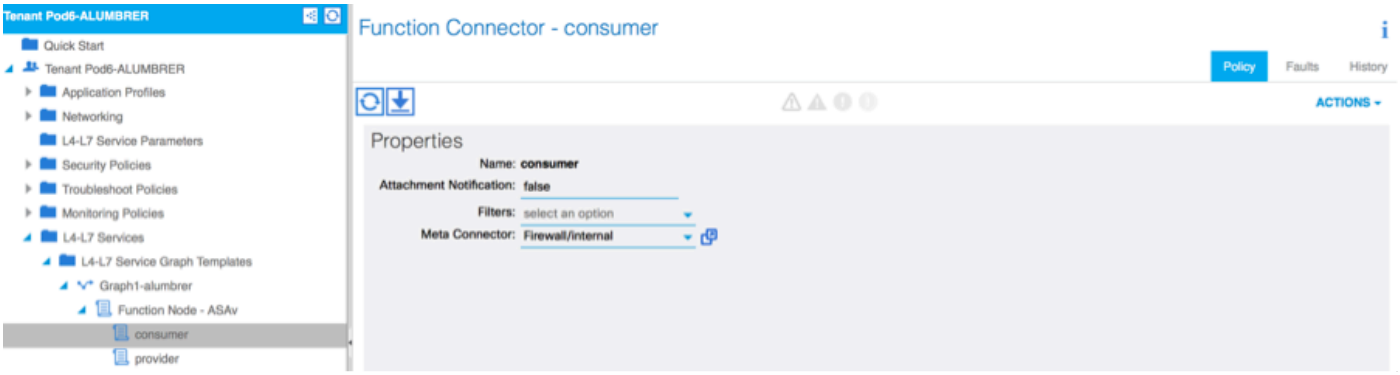
- Você também pode verificar o endereçamento IP atribuído do Perfil de função definido anteriormente, aqui está uma boa chance de alterar informações, se necessário. Quando todos os parâmetros estiverem definidos, clique em **Concluir**, como mostrado na imagem:



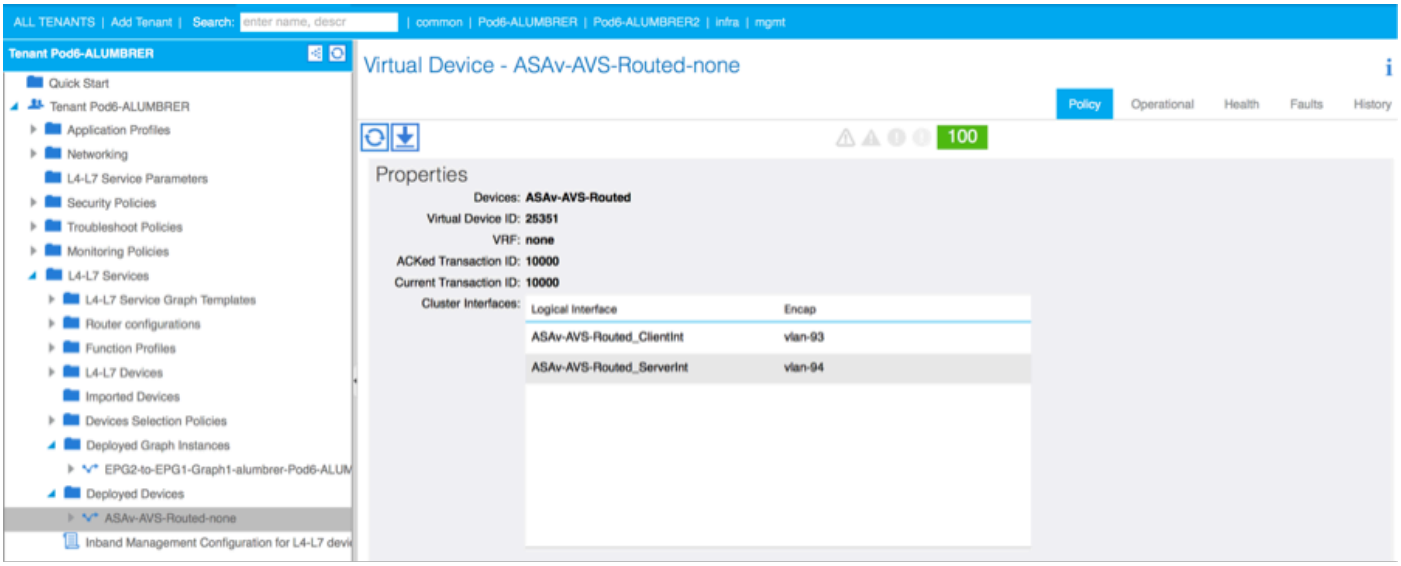
- Se tudo correr bem, um novo dispositivo implantado e uma instância de gráfico serão exibidos.

Verificar

- Uma coisa importante a ser verificada após a criação do gráfico de serviços é que a relação consumidor/provedor foi criada com o Meta Connector apropriado. Verifique nas Propriedades do conector de função.



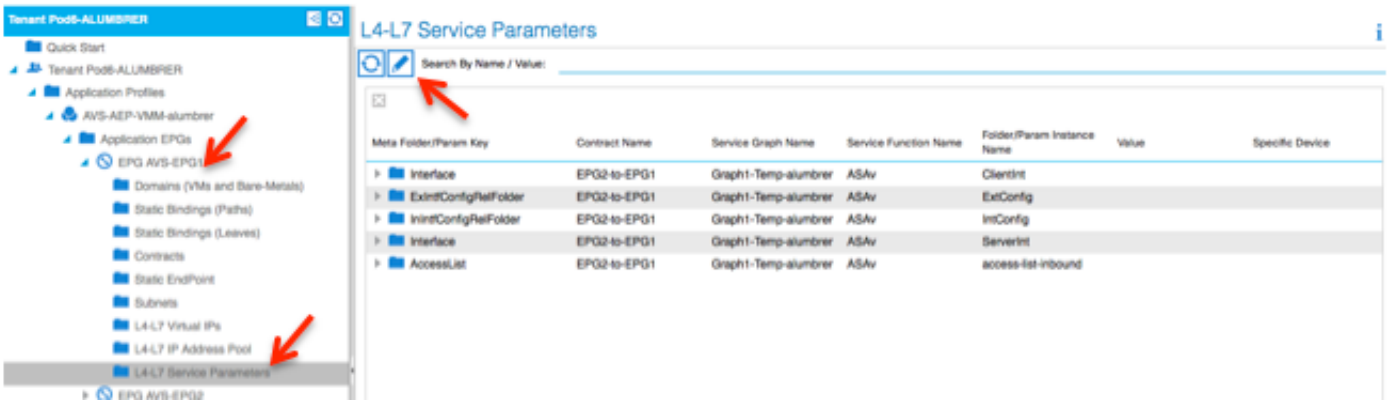
Note: Cada interface do Firewall será atribuída com uma encap-vlan do Pool Dinâmico do AVS. Verifique se não há falhas.



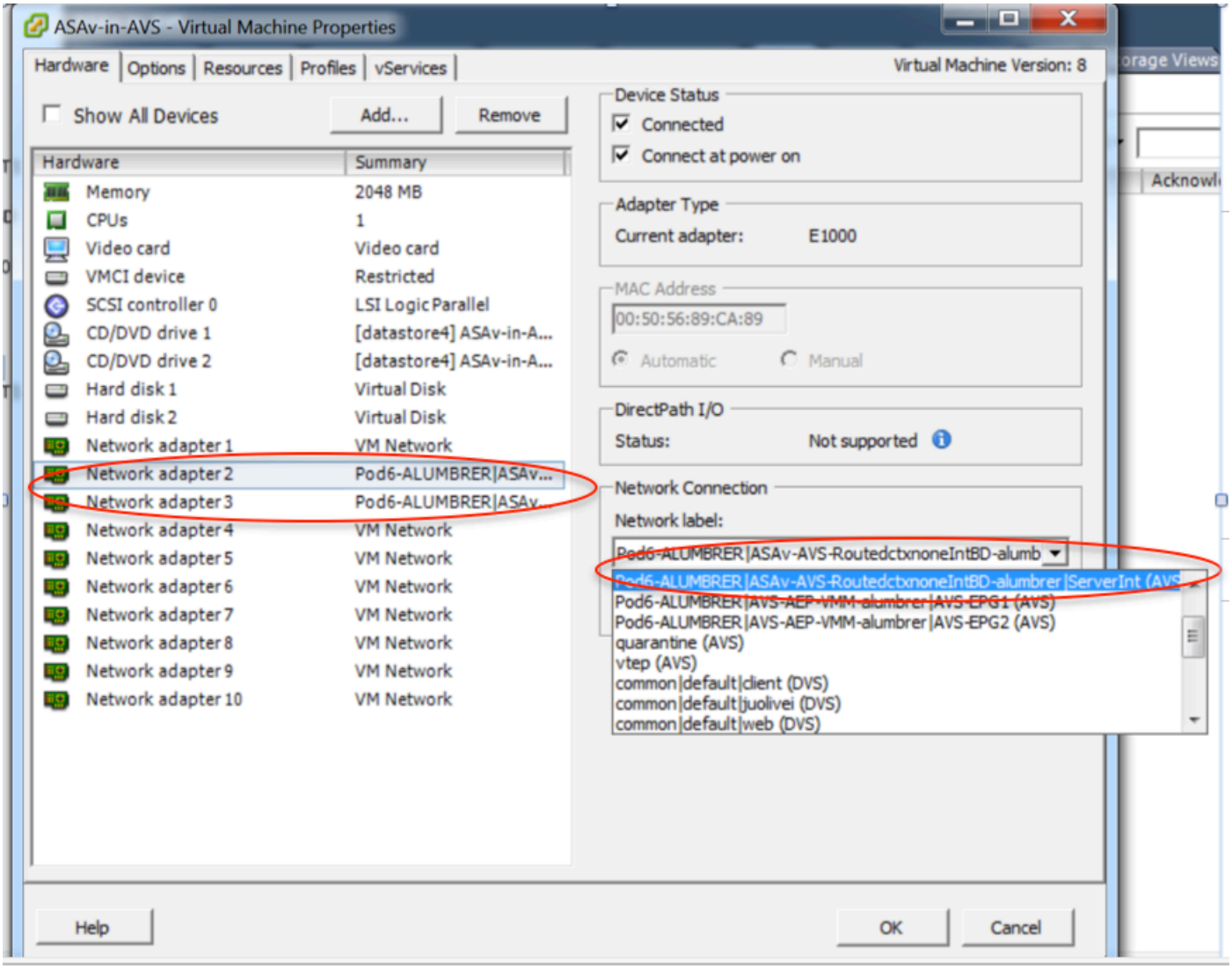
- Agora, você também pode verificar as informações enviadas para o ASAv

```
ASAv-w-AVS# show interface ip brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
GigabitEthernet0/0         192.168.10.1    YES manual up                    up
GigabitEthernet0/1         172.16.1.1      YES manual up                    up
GigabitEthernet0/2         unassigned      YES unset  administratively down up
GigabitEthernet0/3         unassigned      YES unset  administratively down up
GigabitEthernet0/4         unassigned      YES unset  administratively down up
GigabitEthernet0/5         unassigned      YES unset  administratively down up
GigabitEthernet0/6         unassigned      YES unset  administratively down up
GigabitEthernet0/7         unassigned      YES unset  administratively down up
GigabitEthernet0/8         unassigned      YES unset  administratively down up
Management0/0              10.201.35.223   YES CONFIG up                    up
ASAv-w-AVS# show run access-list
access-list access-list-inbound extended permit tcp any any eq www
access-list access-list-inbound extended permit tcp any any eq https
access-list access-list-inbound extended permit tcp any any eq ssh
access-list access-list-inbound extended permit icmp any any
ASAv-w-AVS#
```

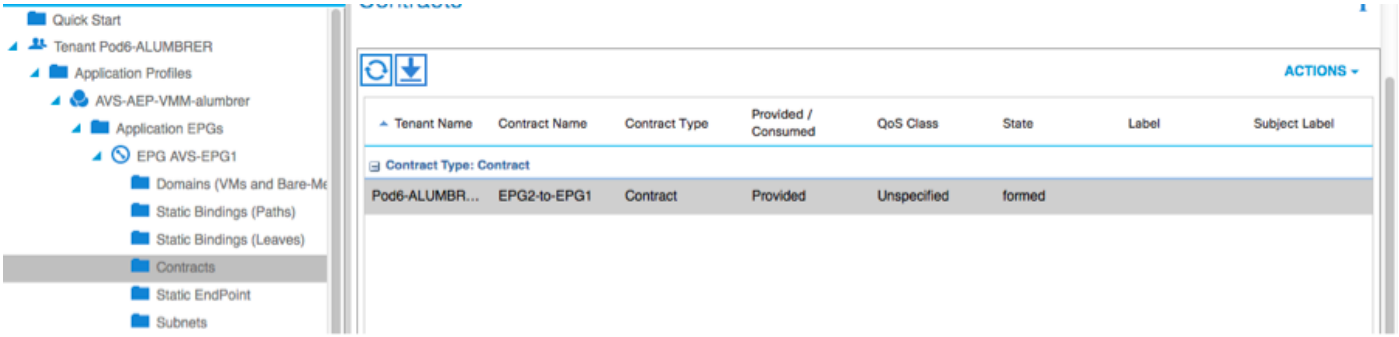
- Um novo contrato é atribuído nos EPGs. A partir de agora, se você precisar modificar alguma coisa na lista de acesso, a alteração deverá ser feita a partir dos parâmetros de serviço L4-L7 do EPG do provedor.



- No vCenter, você também pode verificar se os EPGs de sombra estão atribuídos a cada uma das interfaces de FW:



Para esse teste, tive os 2 EPGs se comunicando com contratos padrão, esses 2 EPGs estão em domínios diferentes e VRFs diferentes, portanto, o vazamento de rota entre eles foi configurado anteriormente. Isso simplifica um pouco após a inserção do Service Graph, pois o FW configura o roteamento e a filtragem entre os 2 EPGs. A DG previamente configurada no EPG e na BD pode agora ser removida da mesma forma que os contratos. Apenas o contrato proposto pelo L4-L7 deve permanecer sob os EPG.



Àmedida que o contrato padrão é removido, você pode confirmar que o tráfego agora flui através do ASAv, o comando show access-list deve exibir a contagem de ocorrências para a regra que é incrementada sempre que o cliente envia uma solicitação ao servidor.

```
ASAv-w-AVS#
ASAv-w-AVS# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list access-list-inbound; 4 elements; name hash: 0xcb5bd6c7
access-list access-list-inbound line 1 extended permit tcp any any eq www (hitcn
t=0) 0xc873a747
access-list access-list-inbound line 2 extended permit tcp any any eq https (hit
cnt=0) 0x48bedbdd
access-list access-list-inbound line 3 extended permit tcp any any eq ssh (hitcn
t=4) 0x532fd57a
access-list access-list-inbound line 4 extended permit icmp any any (hitcnt=4) 0
xe4b5a75d
ASAv-w-AVS# _
```

No leaf, os endpoints devem ser aprendidos para VMs cliente e servidor, bem como para as interfaces ASAv

```
leaf2# show endpoint
Legend:
 O - peer-attached    H - vtep            a - locally-aged     S - static
 V - vpc-attached     p - peer-aged       L - local            M - span
 s - static-arp       B - bounce
+--------------------------------+---------------+----------------+-------------+-------------+
     VLAN/                          Encap           MAC Address      MAC Info/      Interface
     Domain                         VLAN            IP Address       IP Info
+--------------------------------+---------------+----------------+-------------+-------------+
Pod6-ALUMBRER:VRF1-alumbrer                                50.50.50.50 L
14/Pod6-ALUMBRER:VRF1-alumbrer   vxlan-14778359     5897.bda4.f9bc L                 eth1/13
30                                     vlan-98      0050.5689.fa08 L                 eth1/7
Pod6-ALUMBRER:VRF1-alumbrer            vlan-98       192.168.10.10 L
25                                     vlan-94      0050.5689.ca89 L                 po4
Pod6-ALUMBRER:VRF1-alumbrer            vlan-94        192.168.10.1 L
mgmt:inb                                                192.168.2.11 S
21                                     vlan-97      0050.5689.3fca L                 eth1/7
Pod6-ALUMBRER:VRF2                     vlan-97        172.16.1.10 L
26                                     vlan-93      0050.5689.e7dd L                 po4
Pod6-ALUMBRER:VRF2                     vlan-93         172.16.1.1 L
overlay-1                                              10.0.104.93
overlay-1                                               10.0.96.67 L
13                               vxlan-16777209     0050.5677.18a5 H    unspecified
overlay-1                        vxlan-16777209        10.0.32.93 H
13                               vxlan-16777209     0050.5660.ddab H    unspecified
overlay-1                        vxlan-16777209        10.0.32.64 H
```

Server IP & MAC

Client IP & MAC

FW interface (ServerInt)

FW interface (ClientInt)

consulte as duas interfaces de firewall conectadas ao VEM.

ESX-1

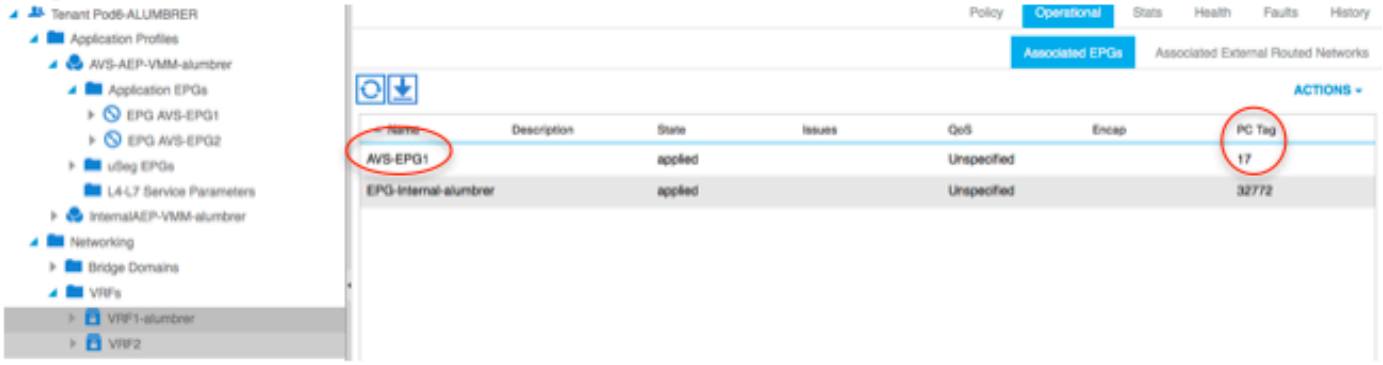
```
~ # vemcmd show port vlan
  LTL   VSM Port  Admin Link  State    Cause  PC-LTL  SGID  ORG  svcpath  Type    Vem Port
   22     Eth1/5     UP   UP    FWD        -    1040     4    0        0                vmnic4
   23     Eth1/6     UP   UP    FWD        -    1040     5    0        0                vmnic5
   50                UP   UP    FWD        -       0     4    0        0                 vmk1
   51                UP   UP    FWD        -       0     4    0        0          ASAv-in-AVS.eth1
   52                UP   UP    FWD        -       0     4    0        0          ASAv-in-AVS.eth2
 1040        Po1     UP   UP    FWD        -       0          0        0
```

ESX-2

```
~ # vemcmd show port vlan
  LTL   VSM Port  Admin Link  State    Cause  PC-LTL  SGID  ORG  svcpath  Type    Vem Port
   24     Eth1/7     UP   UP    FWD        -    1040     6    0        0                vmnic6
   50                UP   UP    FWD        -       0     6    0        0                 vmk1
   51                UP   UP    FWD        -       0     6    0        0          Client1-AVS.eth0
   52                UP   UP    FWD        -       0     6    0        0          Server1-AVS.eth0
 1040        Po1     UP   UP    FWD        -       0          0        0
~ #
```

Finalmente, as regras de firewall também podem ser verificadas no nível de folha se soubermos as Marcas do PC para EPGs de origem e de destino:

EPG1



EPG2

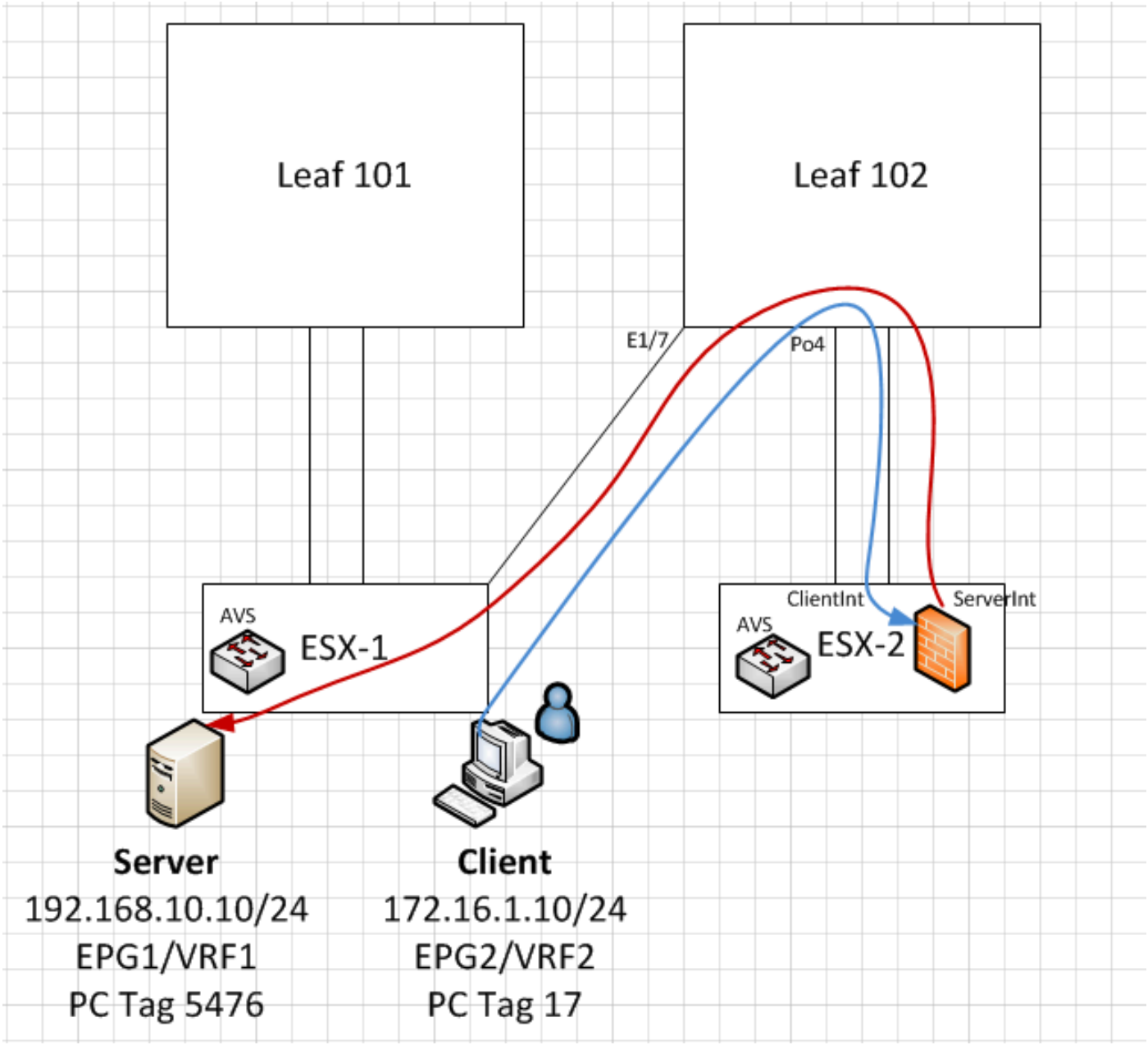
As IDs de filtro podem ser combinadas com as marcas de PC na folha para verificar as regras de FW.

```
leaf2# show zoning-rule | grep '17\|5476'
4141          17      32775    default         enabled         2916352         permit          src_dst_any(5)
4142          32775   17       default         enabled         2916352         permit          src_dst_any(5)
4139          5476    49156    14              enabled         2555904         permit          src_dst_any(5)
4140          49156   5476     14              enabled         2555904         permit          src_dst_any(5)
leaf2#
```

Note: Os EPG PCTags/Sclass nunca se comunicam diretamente. A comunicação é interrompida ou vinculada através dos EPGs de sombra criados pela inserção do gráfico do serviço L4-L7.

E o cliente de comunicação para servidor funciona.

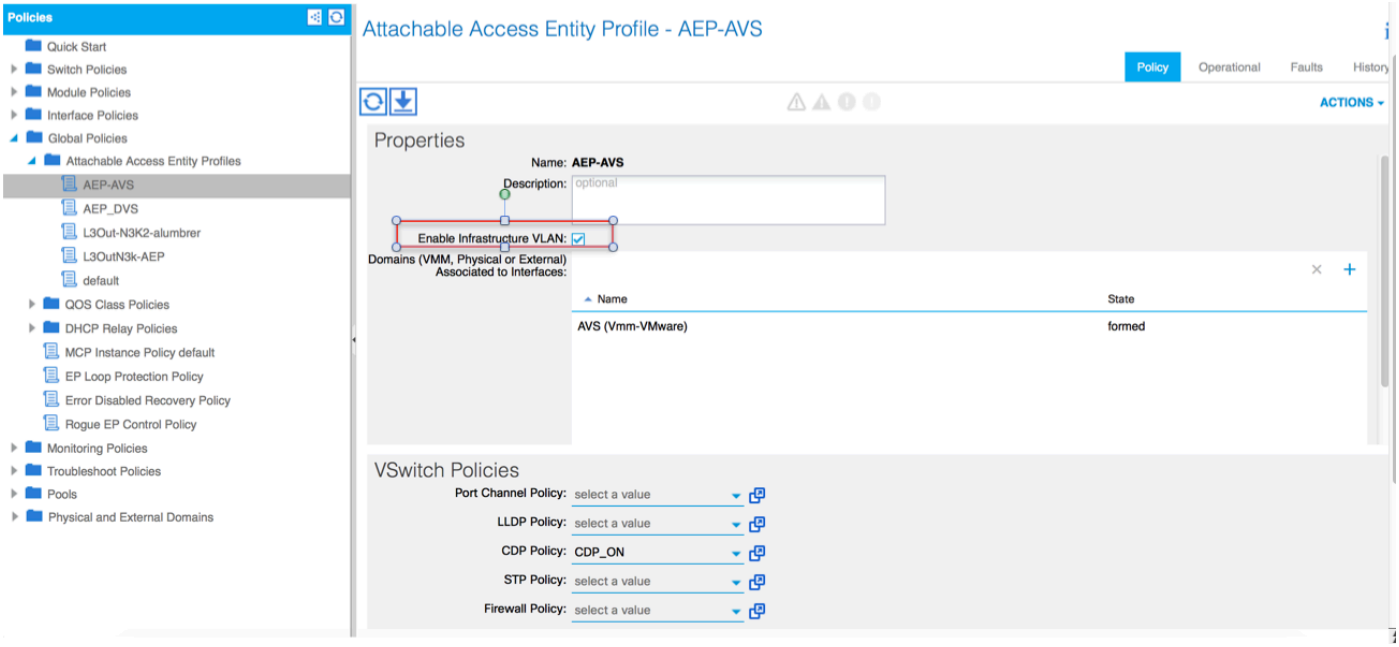
```
cisco@cisco-UbuntuClient:~$ ifconfig
eth1      Link encap:Ethernet  HWaddr 00:50:56:89:3f:ca
          inet addr:172.16.1.10  Bcast:172.16.1.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe89:3fca/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:346596 errors:0 dropped:97 overruns:0 frame:0
          TX packets:533034 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:33670388 (33.6 MB)  TX bytes:42734068 (42.7 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:170350 errors:0 dropped:0 overruns:0 frame:0
          TX packets:170350 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:18739044 (18.7 MB)  TX bytes:18739044 (18.7 MB)

cisco@cisco-UbuntuClient:~$ ssh 192.168.10.10
cisco@192.168.10.10's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

Last login: Mon Feb  1 10:14:11 2016 from 172.16.1.10
cisco@cisco-UbuntuClient:~$ $
```



Troubleshoot

O endereço VTEP não está atribuído

Verifique se Infrastructure Vlan está marcada no AEP:



Versão não suportada

Verifique se a versão do VEM está correta e ofereça suporte ao sistema ESXi VMWare apropriado.

```
~ # vem version
Running esx version -1746974 x86_64
VEM Version: 5.2.1.3.1.10.0-3.2.1
OpFlex SDK Version: 1.2(1i)
System Version: VMware ESXi 5.5.0 Releasebuild-1746974
ESX Version Update Level: 0
```

Comunicação de VEM e malha não está funcionando

```
- Check VEM status
vem status

- Try reloading or restating the VEM at the host:
vem reload
vem restart

- Check if there’s connectivity towards the Fabric. You can try pinging 10.0.0.30 which is
(infra:default) with 10.0.0.30 (shared address, for both Leafs)

~ # vmkping -I vmk1 10.0.0.30
PING 10.0.0.30 (10.0.0.30): 56 data bytes

--- 10.0.0.30 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss

If ping fails, check:

- Check OpFlex status - The DPA (DataPathAgent) handles all the control traffic between AVS and
APIC (talks to the immediate Leaf switch that is connecting to) using OpFlex (opflex
client/agent).
All EPG communication will go thru this opflex connection. ~ # vemcmd show opflex Status: 0
(Discovering) Channel0: 0 (Discovering), Channel1: 0 (Discovering) Dvs name: comp/prov-
VMware/ctrlr-[AVS]-vCenterController/sw-dvs-129 Remote IP: 10.0.0.30 Port: 8000 Infra vlan: 3967
FTEP IP: 10.0.0.32 Switching Mode: unknown Encap Type: unknown NS GIPO: 0.0.0.0 you can also
check the status of the vmnics at the host level: ~ # esxcfg-vmknic -l Interface Port
```

```
Group/DVPort IP Family IP Address Netmask Broadcast MAC Address MTU TSO MSS Enabled Type vmk0
Management Network IPv4 10.201.35.219 255.255.255.0 10.201.35.255 e4:aa:5d:ad:06:3e 1500 65535
true STATIC vmk0 Management Network IPv6 fe80::e6aa:5dff:fead:63e 64 e4:aa:5d:ad:06:3e 1500
65535 true STATIC, PREFERRED vmk1 160 IPv4 10.0.32.65 255.255.0.0 10.0.255.255 00:50:56:6b:ca:25
1500 65535 true STATIC vmk1 160 IPv6 fe80::250:56ff:fe6b:ca25 64 00:50:56:6b:ca:25 1500 65535
true STATIC, PREFERRED ~ # - Also on the host, verify if DHCP requests are sent back and forth:
~ # tcpdump-uw -i vmk1 tcpdump-uw: verbose output suppressed, use -v or -vv for full protocol
decode listening on vmk1, link-type EN10MB (Ethernet), capture size 96 bytes 12:46:08.818776 IP
truncated-ip - 246 bytes missing! 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request
from 00:50:56:6b:ca:25 (oui Unknown), length 300 12:46:13.002342 IP truncated-ip - 246 bytes
missing! 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 00:50:56:6b:ca:25
(oui Unknown), length 300 12:46:21.002532 IP truncated-ip - 246 bytes missing! 0.0.0.0.bootpc >
255.255.255.255.bootps: BOOTP/DHCP, Request from 00:50:56:6b:ca:25 (oui Unknown), length 300
12:46:30.002753 IP truncated-ip - 246 bytes missing! 0.0.0.0.bootpc > 255.255.255.255.bootps:
BOOTP/DHCP, Request from 00:50:56:6b:ca:25 (oui Unknown), length 300
```

Neste ponto, pode-se determinar que a comunicação de estrutura entre o host ESXi e o Folaf não funciona corretamente. Alguns comandos de verificação podem ser verificados no lado da folha para determinar a causa raiz.

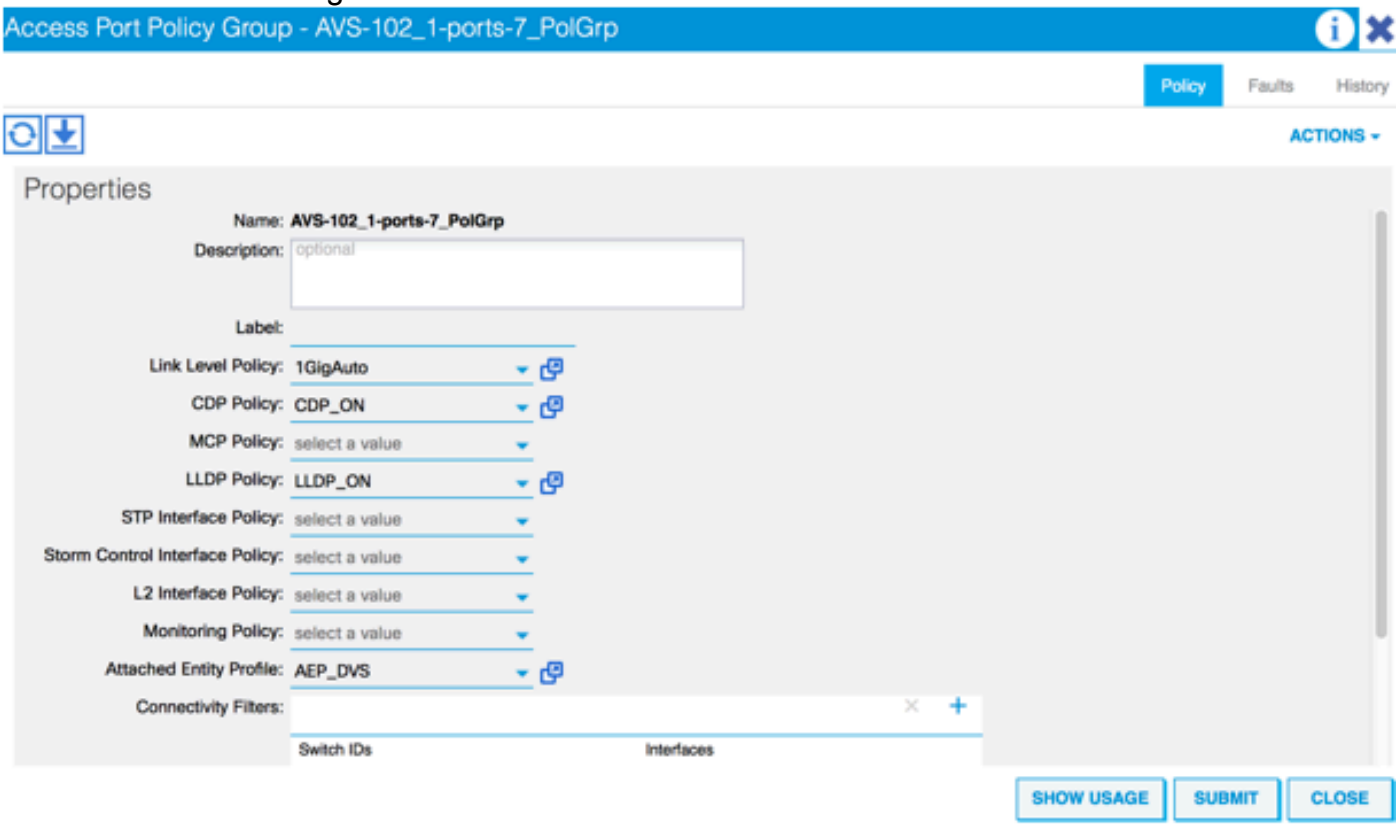
```
leaf2# show cdp ne

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme  Capability  Platform      Port ID
AVS:localhost.localdomainmain
                     Eth1/5          169     S I s      VMware ESXi    vmnic4
AVS:localhost.localdomainmain
                     Eth1/6          169     S I s      VMware ESXi    vmnic5
N3K-2(FOC1938R02L)
                     Eth1/13         166     R S I s    N3K-C3172PQ-1  Eth1/13

leaf2# show port-c sum
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
        F - Configuration failed
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
5     Po5(SU)     Eth      LACP      Eth1/5(P)    Eth1/6(P)
```

Há duas portas usadas no ESXi conectadas através de um Po5

```
leaf2# show vlan extended

 VLAN Name                            Status    Ports
 ---- ------------------------------- --------- -------------------------------
 13   infra:default                   active    Eth1/1, Eth1/20
 19   --                              active    Eth1/13
 22   mgmt:inb                        active    Eth1/1
 26   --                              active    Eth1/5, Eth1/6, Po5
 27   --                              active    Eth1/1
 28   ::                              active    Eth1/5, Eth1/6, Po5
```

```
36   common:pod6_BD                  active    Eth1/5, Eth1/6, Po5

VLAN Type  Vlan-mode  Encap
---- ----- ---------- --------------------------------
13   enet  CE         vxlan-16777209, vlan-3967
19   enet  CE         vxlan-14680064, vlan-150
22   enet  CE         vxlan-16383902
26   enet  CE         vxlan-15531929, vlan-200
27   enet  CE         vlan-11
28   enet  CE         vlan-14
36   enet  CE         vxlan-15662984
```

A partir da saída acima, pode-se observar que a Vlan de infravermelho não é permitida ou passa pelas portas de uplinks que vão para o host ESXi (1/5-6). Isso indica uma configuração incorreta com a política de interface ou a política de switch configurada no APIC.
Verifique ambos:
Políticas de acesso > Políticas de interface > Políticas de acesso a perfis > Políticas de switch > Perfis
Nesse caso, os perfis de interface são anexados ao AEP errado (AEP antigo usado para DVS), como mostrado na imagem:



Depois de definir o AEP correto para AVS, podemos ver que a Vlan de infravermelho é vista através do Unlinks apropriados no Folha:

```
leaf2# show vlan extended

VLAN Name                            Status    Ports
---- ------------------------------- --------- -------------------------------
13   infra:default                   active    Eth1/1, Eth1/5, Eth1/6,
                                               Eth1/20, Po5
19   --                              active    Eth1/13
22   mgmt:inb                        active    Eth1/1
26   --                              active    Eth1/5, Eth1/6, Po5
27   --                              active    Eth1/1
28   ::                              active    Eth1/5, Eth1/6, Po5
36   common:pod6_BD                  active    Eth1/5, Eth1/6, Po5
```

```
 VLAN Type  Vlan-mode  Encap
 ---- ----- ---------- --------------------------------
 13   enet  CE         vxlan-16777209, vlan-3967
 19   enet  CE         vxlan-14680064, vlan-150
 22   enet  CE         vxlan-16383902
 26   enet  CE         vxlan-15531929, vlan-200
 27   enet  CE         vlan-11
 28   enet  CE         vlan-14
 36   enet  CE         vxlan-15662984
```

and Opflex connection is restablised after restarting the VEM module:

```
~ # vem restart
stopDpa
VEM SwISCSI PID is
Warn: DPA running host/vim/vimuser/cisco/vem/vemdpa.213997
Warn: DPA running host/vim/vimuser/cisco/vem/vemdpa.213997
watchdog-vemdpa: Terminating watchdog process with PID 213974

~ # vemcmd show opflex
Status: 0 (Discovering)
Channel0: 14 (Connection attempt), Channel1: 0 (Discovering)
Dvs name: comp/prov-VMware/ctrlr-[AVS]-vCenterController/sw-dvs-129
Remote IP: 10.0.0.30 Port: 8000
Infra vlan: 3967
FTEP IP: 10.0.0.32
Switching Mode: unknown
Encap Type: unknown
NS GIPO: 0.0.0.0

~ # vemcmd show opflex
Status: 12 (Active)
Channel0: 12 (Active), Channel1: 0 (Discovering)
Dvs name: comp/prov-VMware/ctrlr-[AVS]-vCenterController/sw-dvs-129
Remote IP: 10.0.0.30 Port: 8000
Infra vlan: 3967
FTEP IP: 10.0.0.32
Switching Mode: LS
Encap Type: unknown
NS GIPO: 0.0.0.0
```

Informações Relacionadas

Instalação do Switch Virtual de Aplicativo

Cisco Systems, Inc. Guia de instalação do Cisco Application Virtual Switch, versão 5.2(1)SV3(1.2)

Implante o ASAv usando o VMware

Cisco Systems, Inc. Guia de início rápido do Cisco Adaptive Security Virtual Appliance (ASAv), 9.4

Cisco ACI e Cisco AVS

Cisco Systems, Inc. Guia de virtualização da Cisco ACI, versão 1.2(1i)

White paper Design do Service Graph com a infraestrutura centrada em aplicativos da Cisco

White paper Design do Service Graph com a infraestrutura centrada em aplicativos da Cisco

Suporte Técnico e Documentação - Cisco Systems