

使用AVS- ACI 1.2(x)版本的GoTo(L3)模式中的ASA v

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍如何在路由/GOTO模式下使用自适应安全虚拟设备(ASA v)单防火墙部署应用虚拟交换机(AVS)交换机，作为两个终端组(EPG)之间的L4-L7服务图，以使用ACI 1.2(x)建立客户端到服务器通信释放。

先决条件

要求

Cisco 建议您了解以下主题：

- 已配置访问策略，且接口已打开和正在使用
- 已配置EPG、网桥域(BD)和虚拟路由和转发(VRF)

使用的组件

本文档中的信息基于以下软件和硬件版本：

硬件和软件：

- UCS C220 - 2.0(6d)
- ESXi/vCenter - 5.5
- ASA v - asa-device-pkg-1.2.4.8
- AVS - 5.2.1.SV3.1.10
- APIC - 1.2(1i)
- 枝叶/主干 — 11.2(1i)
- 已下载设备包*.zip

功能：

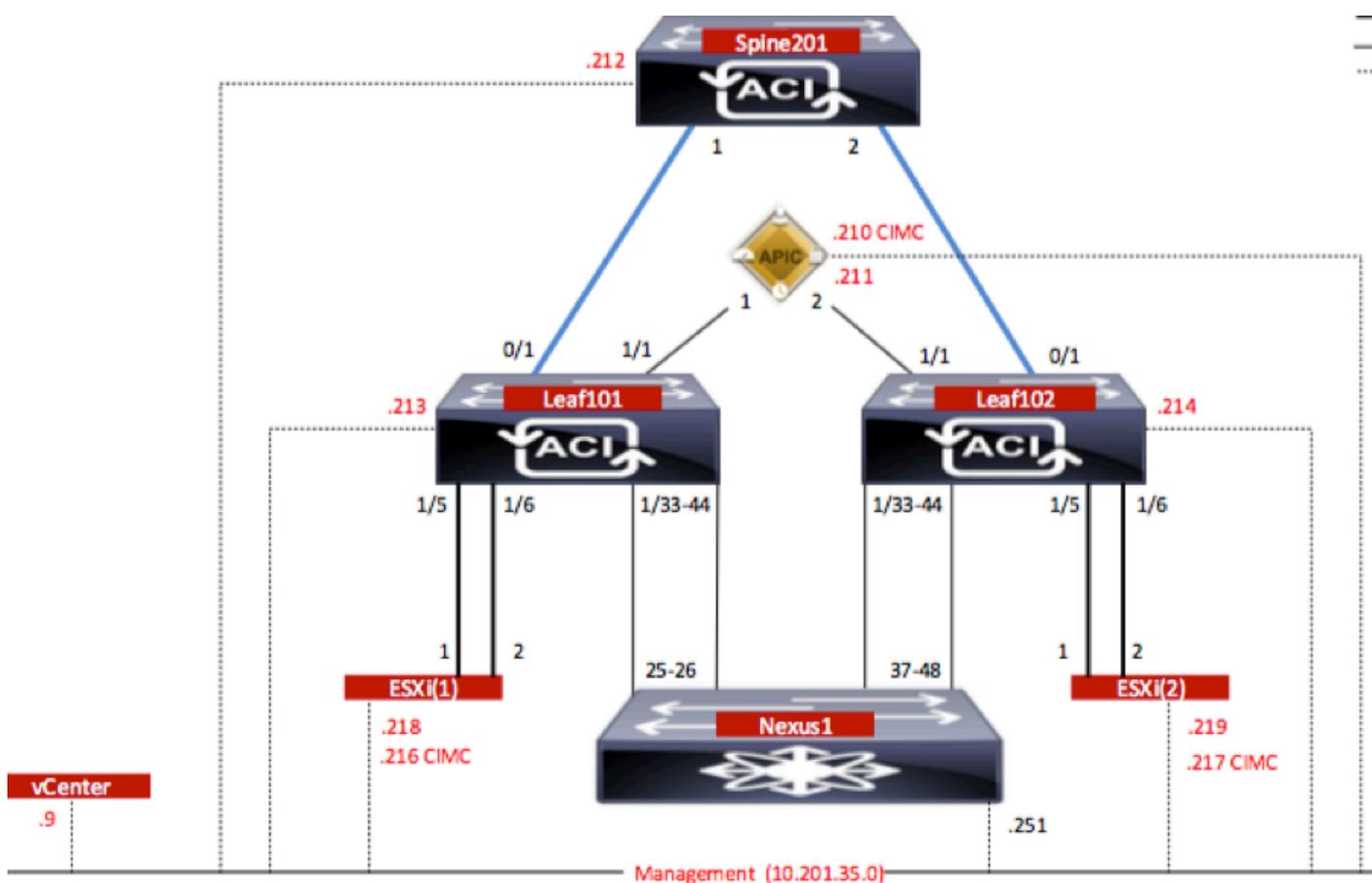
- AVS
- ASAv
- EPG、BD、VRF
- 访问控制列表(ACL)
- L4-L7服务图
- vCenter

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

网络图

如图所示，



配置

AVS初始设置创建VMware vCenter域 (VMM集成) 2

注意：

- 您可以在单个域下创建多个数据中心和分布式虚拟交换机(DVS)条目。但是，您只能将一个思科AVS分配给每个数据中心。
- 思科AVS版本1.2(1i)和思科AVS版本5.2(1)SV3(1.10)支持使用思科AVS的服务图部署。整个服

务图配置在思科应用策略基础设施控制器 (思科APIC) 上执行。

- 只有采用虚拟局域网(VLAN)封装模式的虚拟机管理器(VMM)域才支持使用思科AVS的服务虚拟机(VM)部署。但是，计算VM (提供商和消费者VM) 可以是采用虚拟可扩展LAN(VXLAN)或VLAN封装的VMM域的一部分。
- 另请注意，如果使用本地交换，则不需要组播地址和池。如果未选择本地交换，则必须配置组播池，并且AVS交换矩阵范围的组播地址不应属于组播池。从AVS发起的所有流量都将封装为VLAN或VXLAN。

导航至VM Networking > VMWare > Create vCenter Domain，如图所示：

Virtual Switch Name: AVS

Virtual Switch: VMware vSphere Distributed Switch Cisco AVS

Switching Preference: No Local Switching Local Switching

Encapsulation: VLAN VXLAN

Associated Attachable Entity Profile: AEP-AVS

VLAN Pool: VlanPool-AVS(dynamic)

Security Domains:

Name	Description
------	-------------

vCenter Credentials:

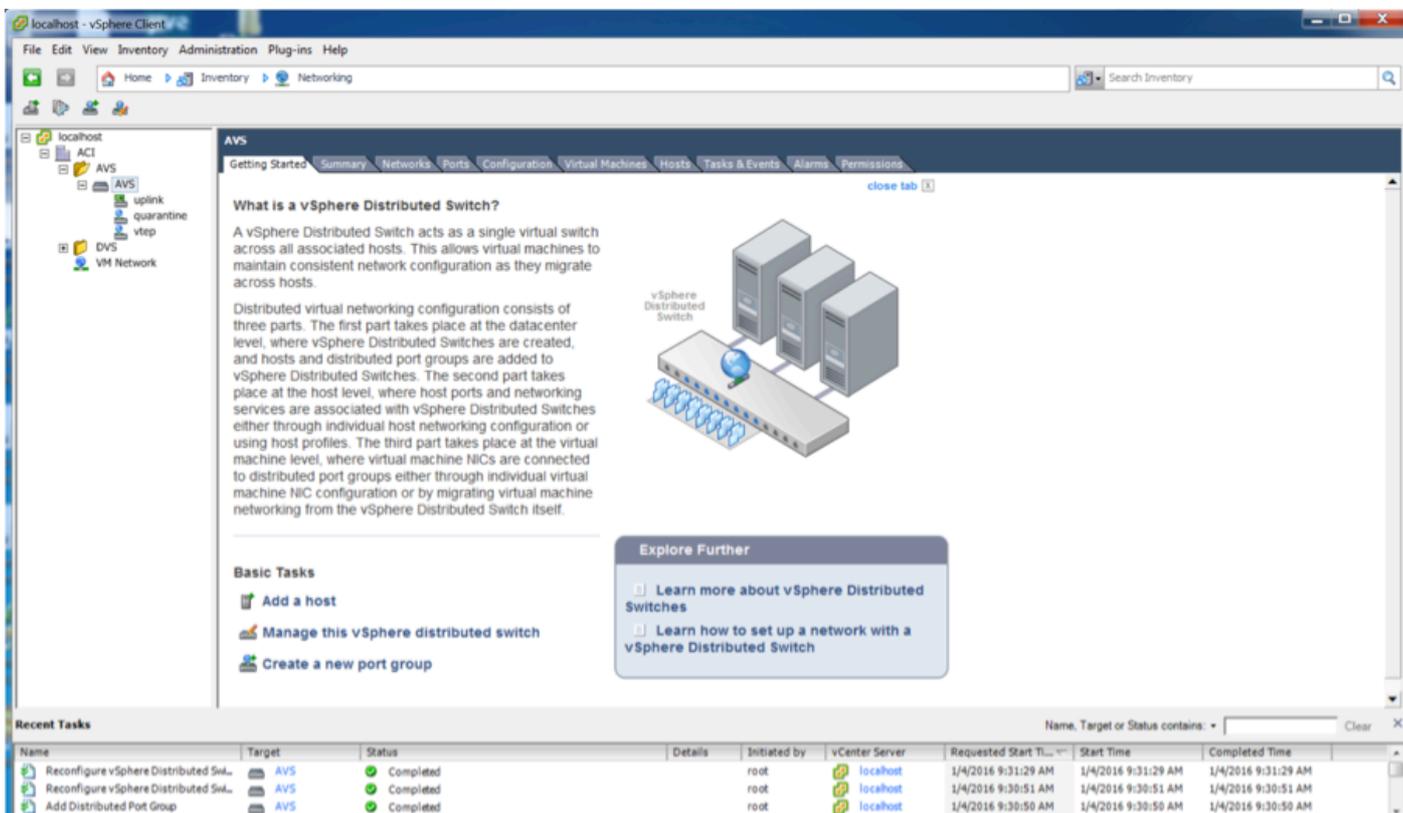
Profile Name	Username	Description
vCenterCredentials	root	

vCenter:

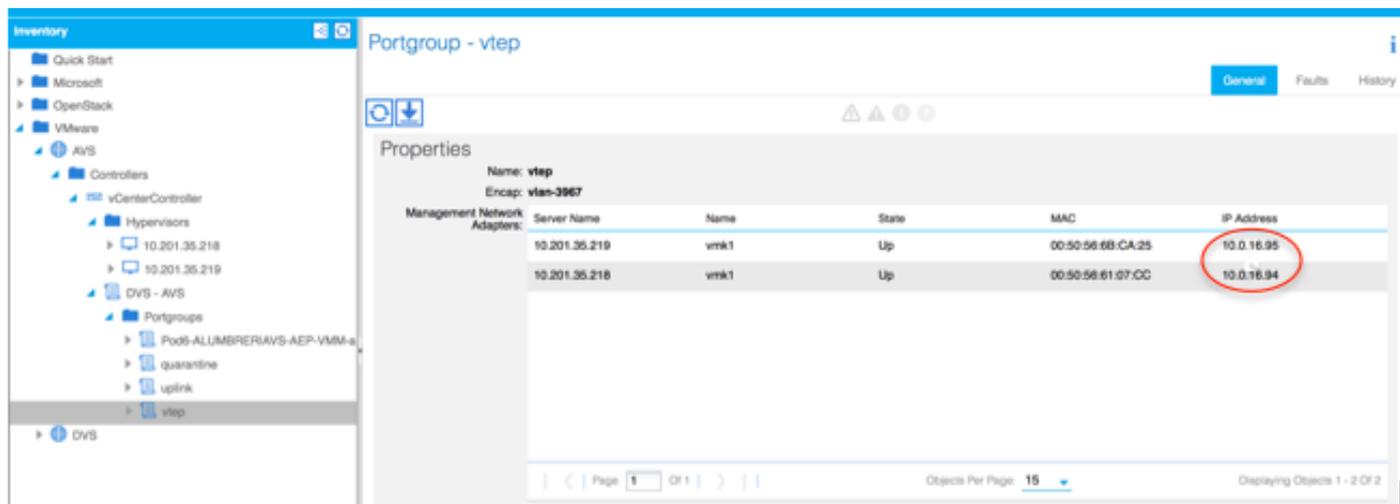
Name	IP	Type	Stats Collection
vCenterController	10.201.35.9	vCenter	Disabled

如果您使用的是端口通道或VPC (虚拟端口通道)，建议将vSwitch策略设置为使用Mac Pinning。

此后，APIC应将AVS交换机配置推送到vCenter，如图所示：



在APIC上，您可以注意到VXLAN隧道终端(VTEP)地址已分配给AVS的VTEP端口组。无论使用什么连接模式 (VLAN或VXLAN)，都会分配此地址



在vCenter中安装Cisco AVS软件

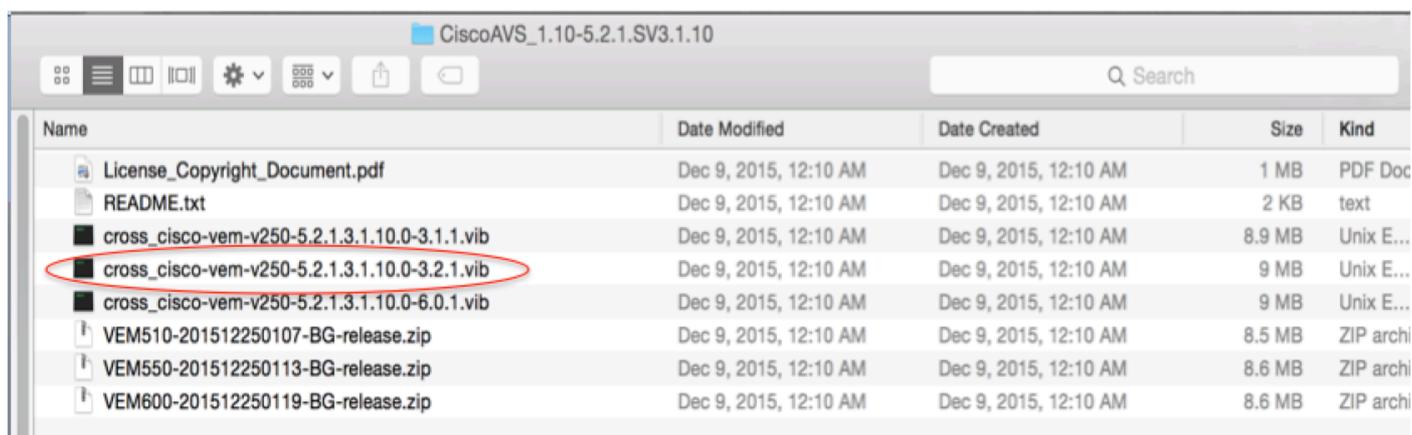
- 使用此链接从CCO下载vSphere安装捆绑包(VIB)

注意：在本例中，我们使用ESX 5.5，表1显示ESXi 6.0、5.5、5.1和5.0的兼容性矩阵

表1 - ESXi 6.0、5.5、5.1和5.0的主机软件版本兼容性

VMware 1	VIB 2	VEM Bundle 3	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

在ZIP文件中有3个VIB文件，每个ESXi主机版本对应一个，请选择适合ESX 5.5的一个文件，如图所示：



- 将VIB文件复制到ESX Datastore — 这可以通过CLI或直接从vCenter完成

注意：如果主机上存在VIB文件，请使用esxcli软件vib remove命令将其删除。

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

或直接浏览Datastore。

- 在ESXi主机上使用以下命令安装AVS软件：

esxcli软件vib install -v /vmfs/volumes/datastore1/cross_cisco-vem-v250-5.2.1.3.10.0-3.2.1.vib
—maintenance-mode —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

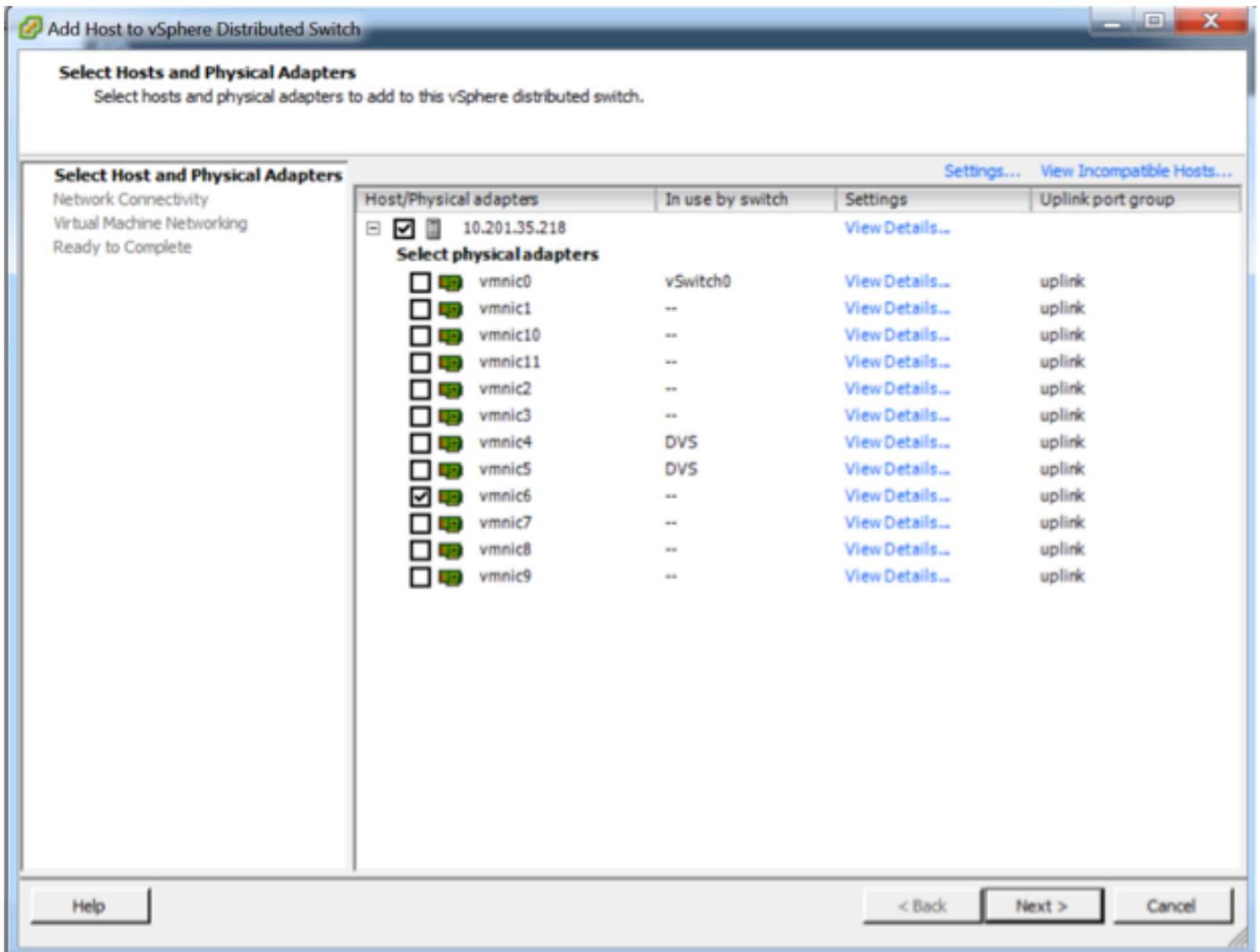
VEM Agent (vemdpa) is running

~ #

```

- 一旦虚拟以太网模块(VEM)启动，您就可以将主机添加到AVS:

在向vSphere分布式交换机添加主机对话框中，选择连接到枝叶交换机的虚拟NIC端口（在本示例中，您仅移动vmnic6），如图所示：



- 单击“下一步”
- 在Network Connectivity对话框中，单击Next(下一步)
- 在“虚拟机网络”对话框中，单击“下一步”
- 在准备完成对话框中，单击完成

注意：如果使用多台ESXi主机，则所有主机都需要运行AVS/VEM，以便从标准交换机管理到DVS或AVS。

因此，AVS集成已完成，我们已准备好继续L4-L7 ASA部署：

ASAv初始设置

- 下载Cisco ASAv设备包并将其导入APIC：
导航到L4-L7服务>包>导入设备包，如图所示：

Fabric VM Networking **L4-L7 Services** Admin Operations

Inventory | Packages

Quick Start

HELP

The **Packages** menu allows you to import L4-L7 device packages, which are used to define, configure, and monitor a network service balancer, context switch, SSL termination device, or intrusion prevention system (IPS). Device packages contain descriptions of the function and network connectivity information for each function. A network service device is deployed in the network by adding it to a service graph.

You can use the **Import a Device Package** wizard to import a device package for a function that you want to manage with APIC. We will walk you through configuring a service graph.

i X
Import Device Package

File Name: BROWSE...

SUBMIT
CLOSE

Quick Start

Import a Device Package

Device Types

- 如果一切正常，您可以看到已导入的设备包正在扩展L4-L7服务设备类型文件夹，如图所示：

L4-L7 Service Device Type - CISCO-ASA-1.2

i
General
Operational
Faults
History

↻
↓
ACTIONS ▾

Properties

Vendor: **CISCO**

Model: **ASA**

Capabilities: **GoThrough,GoTo**

Major Version: **1.2**

Minor Version: **4.8**

Minimum Required Controller Version: **1.1**

Logging Level: **DEBUG** ▾

Package Name: **device_script.py**

Supported Protocols: |

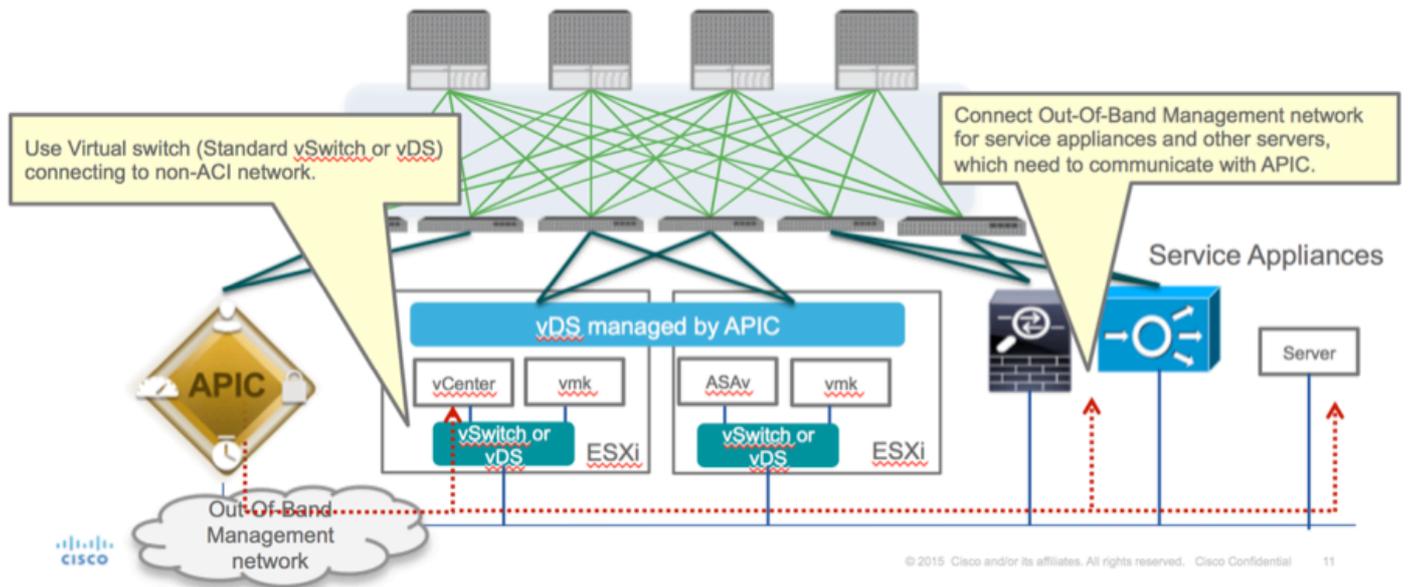
Interface Labels:

Name
cluster_ctrl_lk
external
failover_lan
failover_link
internal
mgmt
utility

在继续之前，在执行实际的L4-L7集成之前，需要确定安装的几个方面：

管理网络分为两种类型：带内管理和带外(OOB)，它们可用于管理不属于基本以应用为中心的基础设施(ACI) (枝叶、主干或apic控制器) 的设备，包括ASAv、负载均衡器等。

在这种情况下，ASAv的OOB使用标准vSwitch进行部署。对于裸机ASA或其他服务设备和/或服务器，将OOB管理端口连接到OOB交换机或网络，如图所示。



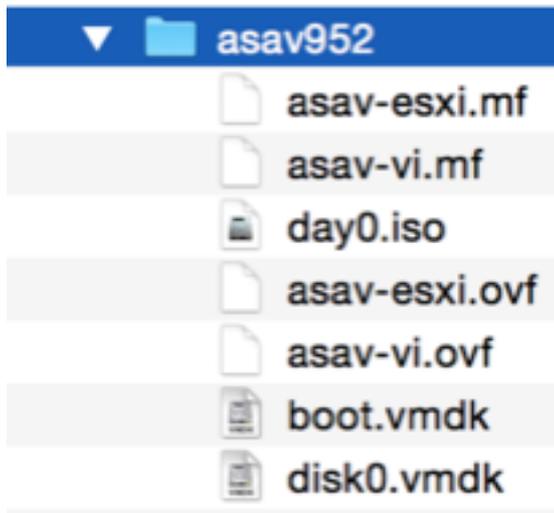
ASAv OOB管理端口管理连接需要使用ESXi上行链路端口通过OOB与APIC通信。映射vNIC接口时，网络适配器1始终与ASAv上的Management0/0接口匹配，其余数据平面接口从网络适配器2启动。

表2显示网络适配器ID和ASAv接口ID的协调：

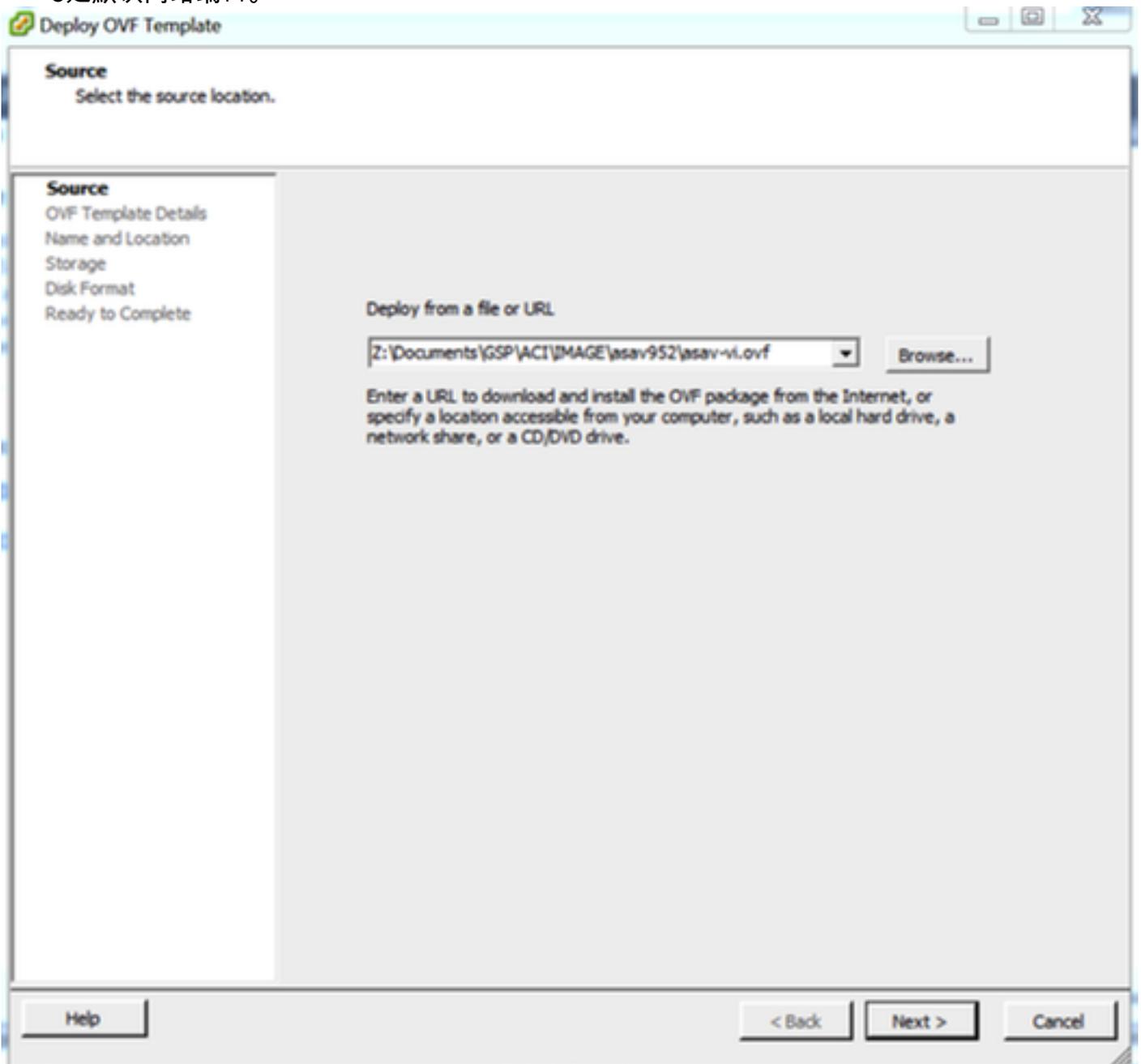
表 2

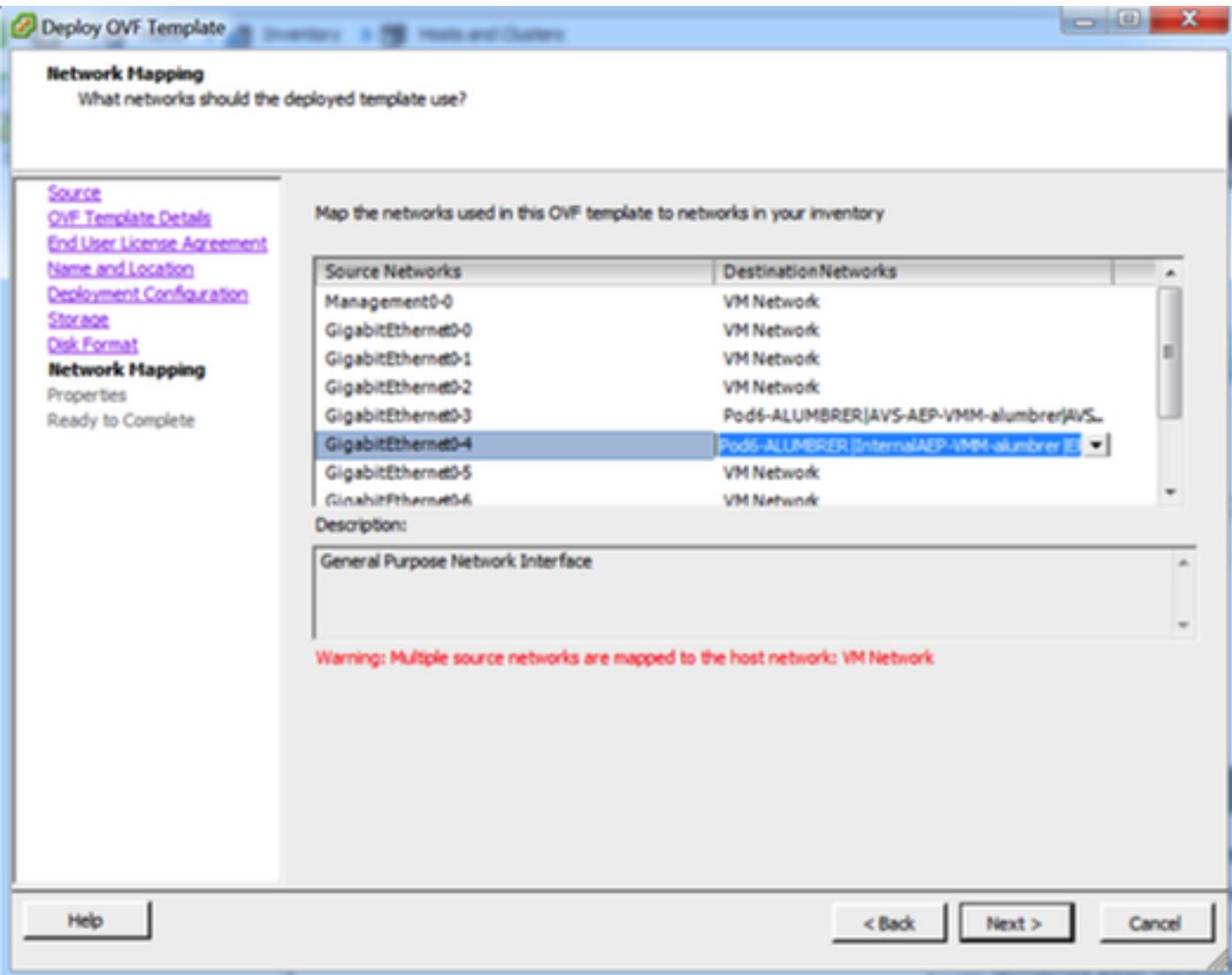
Network Adapter ID	ASAv Interface ID
Network Adapter 1	Management0/0
Network Adapter 2	GigabitEthernet0/0
Network Adapter 3	GigabitEthernet0/1
Network Adapter 4	GigabitEthernet0/2
Network Adapter 5	GigabitEthernet0/3
Network Adapter 6	GigabitEthernet0/4
Network Adapter 7	GigabitEthernet0/5
Network Adapter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

- 通过File>Deploy OVF(Open Virtualization Format)Template中的向导部署ASAv VM
- 如果要将独立ESX Server或asav-vi用于vCenter，请选择asav-esxi。在本例中，使用vCenter。



- 通过安装向导，接受条款和条件。在向导的中间，您可以确定多个选项，如主机名、管理、IP地址、防火墙模式和与ASA v相关的其他特定信息。切记对ASA v使用OOB管理，在本例中，您需要在使用VM网络（标准交换机）时保留接口Management0/0，而接口GigabitEthernet0-8是默认网络端口。





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 ASA v 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

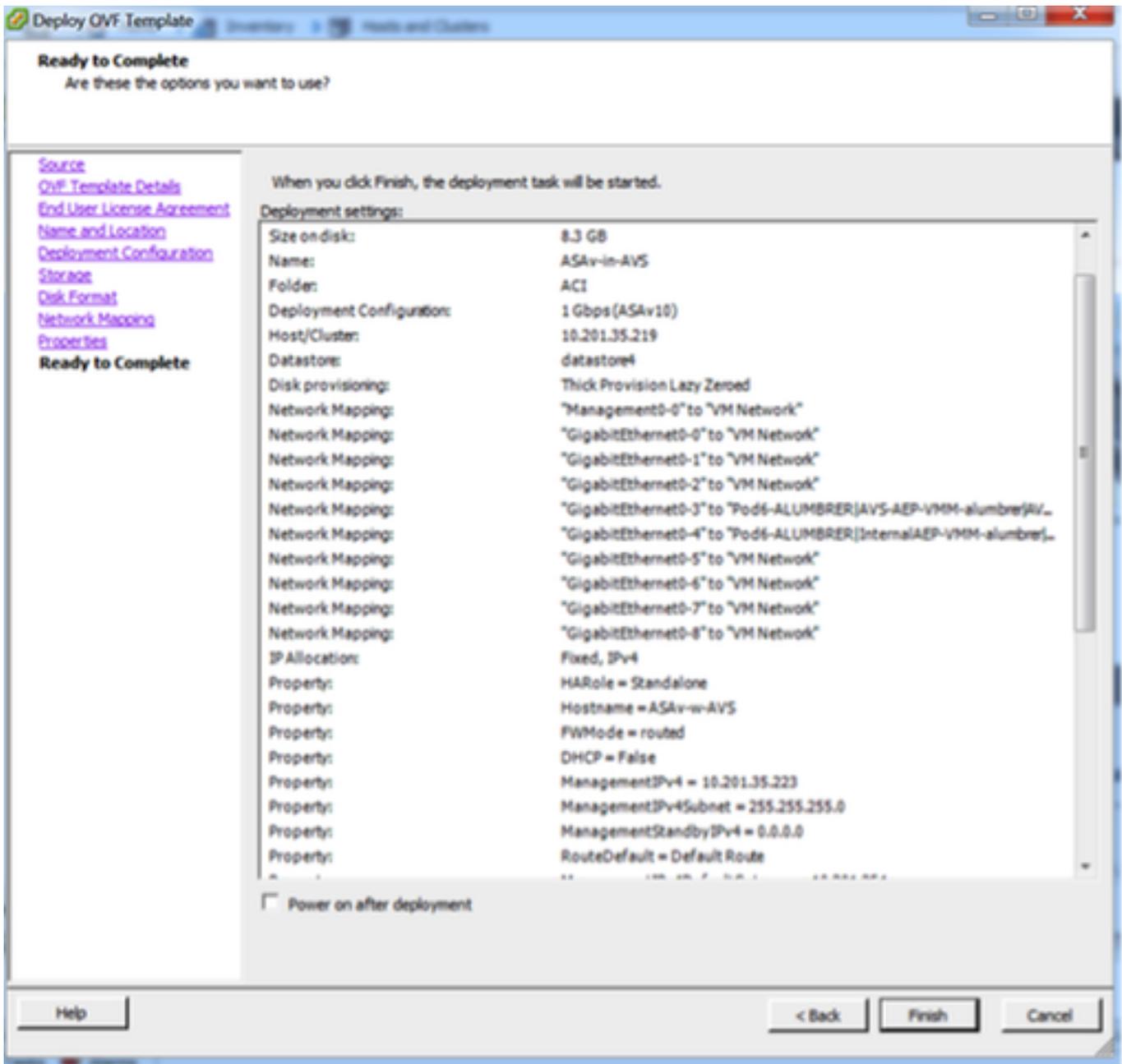
Firewall Properties
Firewall Mode
Select the Firewall Mode
routed

Management Interface Settings
Management Interface DHCP mode
Choose whether to use DHCP for Management interface configuration.

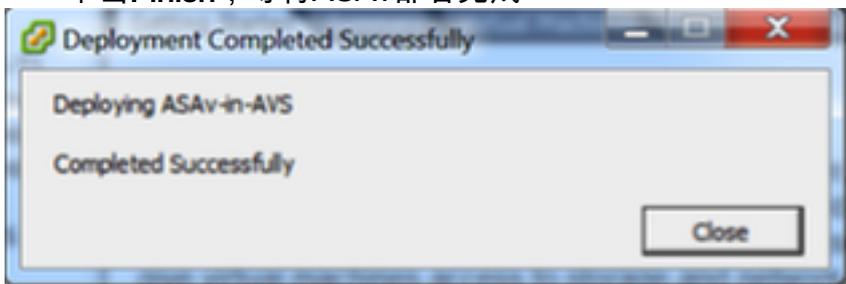
Management IP Address
Enter the Management IPv4 Address. For HA-type deployments, this property specifies the Management IPv4 address of the Active HA host.
10 . 201 . 35 . 223

Management IP Subnet Mask

Help < Back Next > Cancel



- 单击Finish，等待ASAv部署完成



- 打开ASAv VM电源并通过控制台登录以验证初始配置

```

?
interface Management0/0
 management-only
 nameif management
 security-level 0
 ip address 10.201.35.223 255.255.255.0
?
ftp mode passive
pager lines 23
mtu management 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
route management 0.0.0.0 0.0.0.0 10.201.35.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
<--- More --->_

```

- 如图所示，某些管理配置已推送到ASAv防火墙。配置管理员用户名和密码。此用户名和密码由 APIC用于登录和配置ASA。ASA应能连接到OOB网络，并且应能到达APIC。

username admin password <device_password> encrypted privilege 15

```

ASA-v-w-AUS(config)# username admin password Cisc0123 privilege 15
ASA-v-w-AUS(config)# wr mem
Building configuration...
Cryptochecksum: d491b980 86fa522f 6f937baf b5bfb318

7977 bytes copied in 0.250 secs
[OK]
ASA-v-w-AUS(config)# ping 10.201.35.211
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.201.35.211, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
ASA-v-w-AUS(config)# _

```

此外，在全局配置模式下启用http服务器：

HTTP服务器启用

http 0.0.0.0 0.0.0.0管理

APIC中ASAv集成的L4-L7:

- 登录ACI GUI，点击将部署服务图的租户。展开导航窗格底部的L4-L7服务，右键单击L4-L7设备，然后单击创建L4-L7设备以打开向导
- 对于此实施，将应用以下设置：
 - 托管模式

— 防火墙服务

— 虚拟设备

— 通过单节点连接到AVS域

-ASAv型号

— 路由模式(GoTo)

— 管理地址 (必须与之前分配给Mgmt0/0接口的地址匹配)

- 默认情况下，将HTTPS用作APIC使用最安全的协议与ASAv通信

Create L4-L7 Devices

STEP 1 > General

Please select device package and enter connectivity information.

General

Managed:

Name: ASAv-AVS-Routed

Service Type: Firewall

Device Type: PHYSICAL VIRTUAL

VMM Domain: AVS

Mode: Single Node HA Cluster

Device Package: CISCO-ASA-1.2

Model: ASAv

Function Type: GoThrough GoTo

Connectivity

APIC to Device Management Connectivity: Out-Of-Band In-Band

Credentials

Username: admin

Password:

Confirm Password:

Device 1

Management IP Address: 10.201.35.3

Management Port: https

VM: vCenterController/ASAv-in-AVS

Device Interfaces:

Name	VNIC	Path (Only For Route Peering)
GigabitEthernet0/0	Network adapter 2	Node-102/MAC_Pinning
GigabitEthernet0/1	Network adapter 3	Node-102/MAC_Pinning

Cluster

Management IP Address: 10.201.35.3

Management Port: https

Cluster Interfaces:

Type	Name	Concrete Interfaces
provider	ServerInt	Device1/GigabitEthernet0/0
consumer	ClientInt	Device1/GigabitEthernet0/1

- 正确定义设备接口和集群接口对于成功部署至关重要

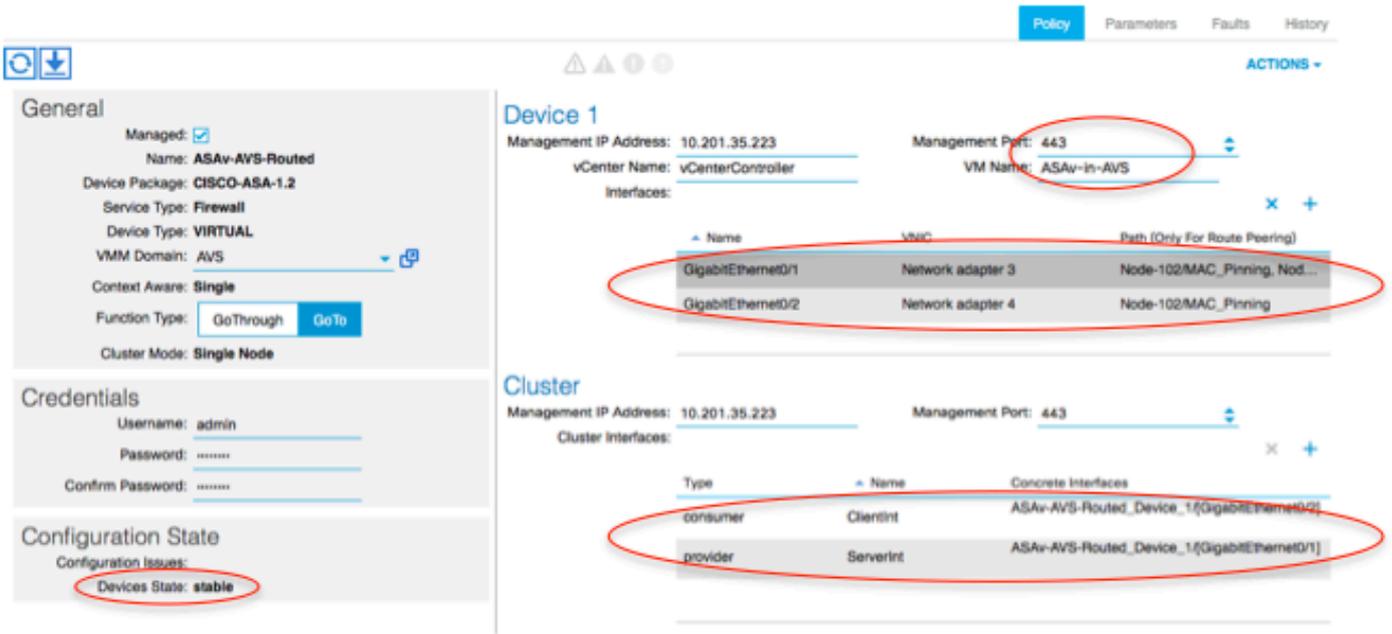
对于第一部分，使用上一节中显示的表2，将网络适配器ID与要使用的ASAv接口ID正确匹配。路径是指启用进出防火墙接口的方式的物理端口或端口通道或VPC。在这种情况下，ASA位于ESX主机中，其中传入和传出对于两个接口都是相同的。在物理设备中，防火墙(FW)的内部和外部是不同的物理端口。

对于第二部分，必须始终定义集群接口，而不例外 (即使不使用集群HA)，这是因为对象模型在 **mlf** 接口 (设备包上的元接口)、**Lif** 接口 (枝叶接口，如外部、内部、内部等) 与 **Clif** (具体接口)。L4-L7具体设备必须在设备集群配置中配置，这种抽象称为逻辑设备。逻辑设备具有逻辑接口，这些逻辑接口映射到具体设备上的具体接口。

在本例中，将使用以下关联：

Gi0/0 = vnic2 =服务器接口/提供商/服务器> EPG1

Gi0/1 = vnic3 =客户端接口/消费者/客户端> EPG2

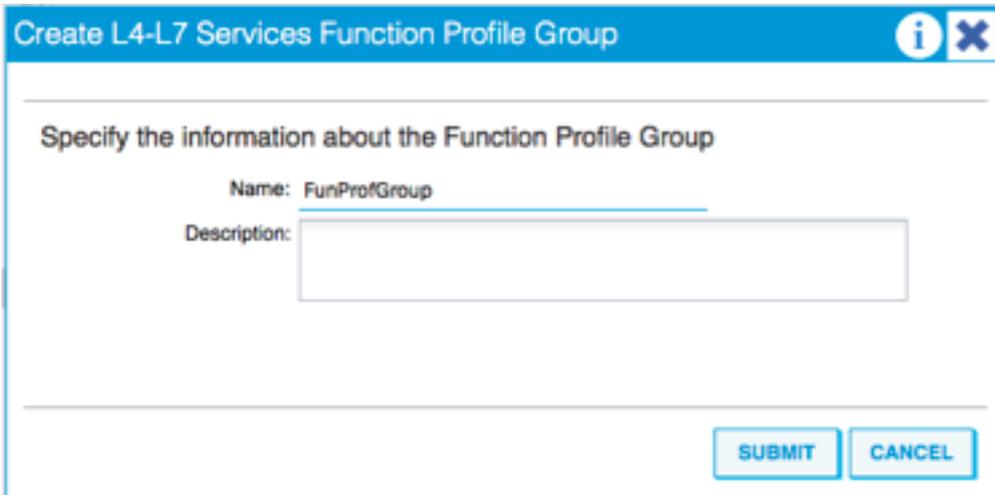


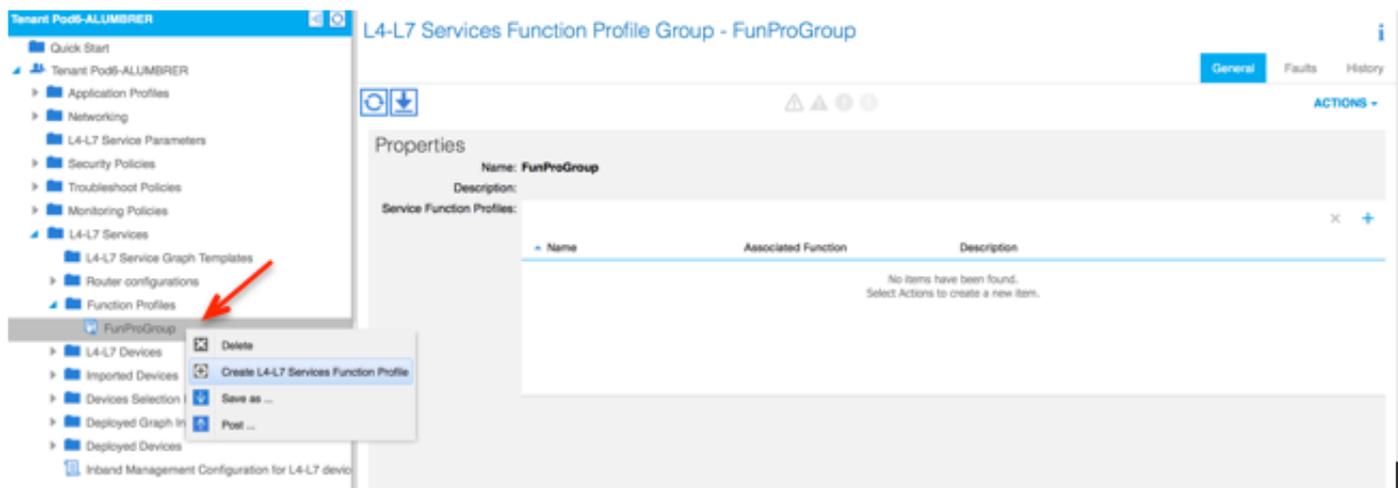
注意：对于故障切换/HA部署，GigabitEthernet 0/8已预配置为故障切换接口。

设备状态应为“稳定”，您应准备好部署功能配置文件和服务图模板

服务图庙

首先，为ASAv创建功能配置文件，但在此之前，您需要在该文件夹下创建功能配置文件组，然后创建L4-L7服务功能配置文件，如图所示：





- 从下拉菜单中选择WebPolicyForRoutedMode 配置文件，然后继续配置防火墙上的接口。从此开始，这些步骤是可选的，可以稍后实施/修改。这些步骤可在部署的几个不同阶段执行，具体取决于服务图的可重用性或自定义程度。

在本练习中，路由防火墙（GoTo模式）要求每个接口都有唯一的IP地址。标准ASA配置还具有接口安全级别（外部接口安全性较低，内部接口安全性较高）。您还可以根据需要更改接口的名称。本示例中使用默认值。

- 展开接口特定配置，为ServerInt添加IP地址和安全级别，IP地址为x.x.x.x/y.y.y.y或x.x.x.x/yy，格式如下。对ClientInt接口重复该过程。

Create Function Profile

Name: FunProf-ASA
 Description: optional
 Copy Existing Profile Parameters:
 Profile: CISCO-ASA-1.2/WebPolicyForRoutedMode

Features and Parameters

In order to auto apply new values to the parameters of existing graph instance when users modify function profiles, the name of top folder must be ended with -Default.

Folder/Param	Name	Value	Mandatory	Locked	Shared
Device Config	Device				
Bridge Group Interface					
Interface Related Configuration	externallif			false	false
Access Group	ExtAccessGroup			false	
IPv6 Enforce EUI-64					
Interface Specific Configur...	externallCfIg			false	
IPv4 Address Configur...	ipv4_address	192.168.10.1/24		<input type="checkbox"/>	<input type="checkbox"/>
IPv4 Standby Address					
IPv6 Address Configur...					
IPv6 Link Local Address...					

UPDATE RESET CANCEL

SUBMIT CANCEL

注意：您还可以修改默认访问列表设置并创建您自己的基本模板。默认情况下，路由模式模板将包含HTTP和HTTPS规则。在本练习中，SSH和ICMP将添加到允许的外部访问列表。

Create Function Profile

Name: FunProf-ASA

Description: optional

Copy Existing Profile Parameters:

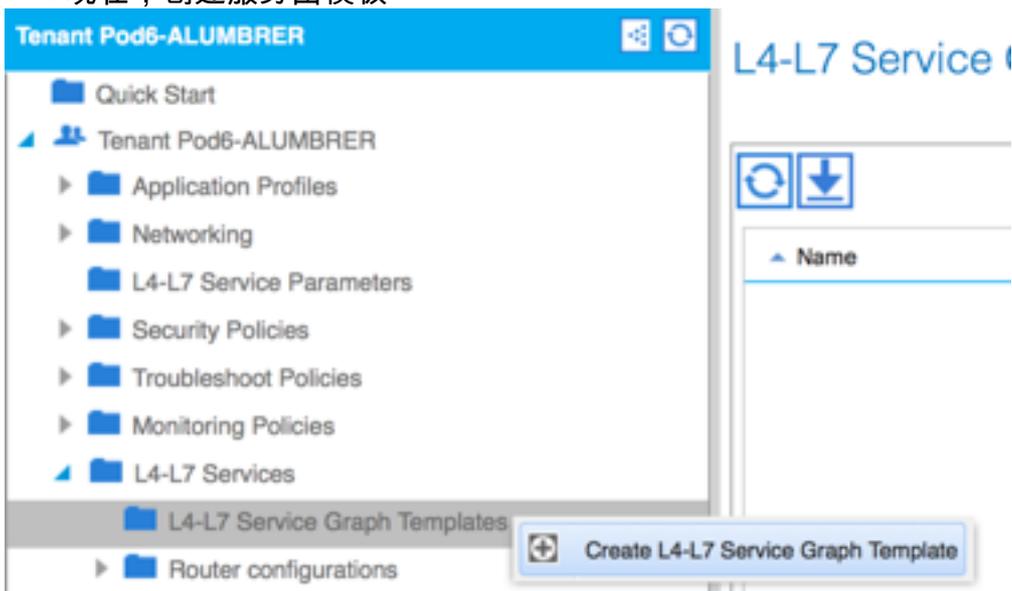
Profile: CISCO-ASA-1.2/WebPolicyForRoutedMode

Features and Parameters

In order to auto apply new values to the parameters of existing graph instance when users modify function profiles, the name of top folder must be ended with -Default.

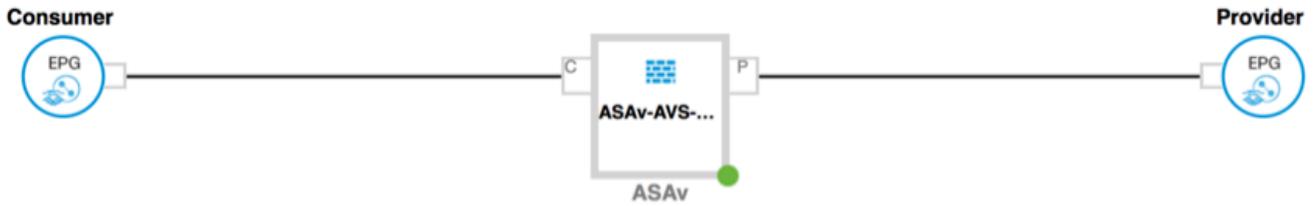
Folder/Param	Name	Value	Mandatory	Locked	Shared
Destination Service	destination_service				
High Port					
Low Port	low_port	22		false	
Operator	operator	eq		false	
ICMP					
Logging					
Protocol					
Source Address					
Source Service					
Action	action	permit		false	
Order	order	30		false	

- 然后单击**Submit**
- 现在，创建服务图模板



- 将设备集群拖放到右侧以形成消费者和提供商之间的关系，选择路由模式和先前创建的功能配置文件。

Graph Name: Graph1-alumbrrer
Graph Type: Create A New One Clone An Existing One



ASAv-AVS-Routed Information

Firewall: Routed Transparent

Profile: Pod6-ALUMBRER/FunProfGroup/FunPro

- 检查模板是否存在故障。模板创建为可重用，然后必须应用于特定EPG等。
- 要应用模板，请右键单击并选择应用L4-L7服务图模板

- 定义哪个EPG将位于消费者端和提供商端。在本练习中，AVS-EPG2是消费者（客户端），AVS-EPG1是提供商（服务器）。请记住，未应用过滤器，这将允许防火墙根据此向导最后一节中定义的访问列表执行所有过滤。
- 单击“下一步”

Config A Contract Between EPGs

EPGs Information

Consumer EPG / External Network: Pod6-ALUMBRER/AVS-AEP-VMM

Provider EPG / External Network: Pod6-ALUMBRER/AVS-AEP-VMM

Contract Information

Contract: Create A New Contract Choose An Existing Contract Subject

Contract Name: EPG2-to-EPG1

No Filter (Allow All Traffic):

Pod6-ALUMBRER/AVS-AEP-VMM-alubr/epg-AVS-EPG1

Pod6-ALUMBRER/InternalAEP-VMM-alubr/epg-EPG-Internal-alubr

Pod6-ALUMBRER/VRF1-alubr/AnyEPG

Pod6-ALUMBRER/VRF2/AnyEPG

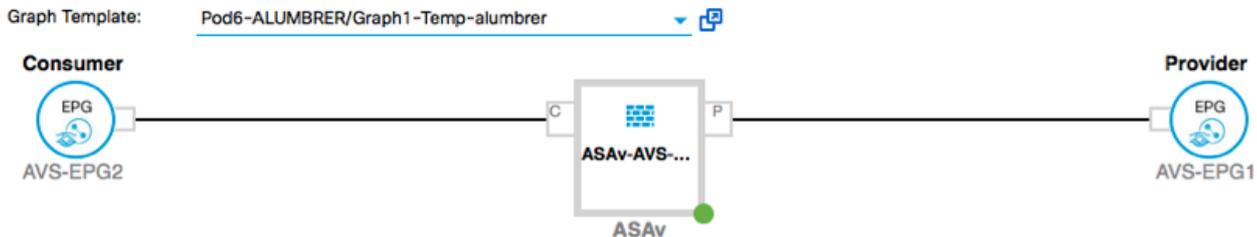
Pod6-ALUMBRER/L3Out-N3K2/L3Net

PREVIOUS

NEXT

CANCEL

- 验证每个EPG的BD信息。在这种情况下，EPG1是IntBD DB上的提供商，EPG2是BD ExtBD上的消费者。EPG1将连接到防火墙接口ServerInt，EPG2将连接到接口ClientInt。两个防火墙接口将成为每个EPG的DG，因此流量会被迫始终通过防火墙。
- 单击“下一步”



ASAv-AVS-Routed Information

Firewall: routed

Profile: FunPro-ASA

Consumer Connector

Type: General Route Peering

BD: Pod6-ALUMBRER/ExtBD-alubr

Cluster Interface: ClientInt

Provider Connector

Type: General Route Peering

BD: Pod6-ALUMBRER/IntBD-alubr

Cluster Interface: ServerInt

PREVIOUS

NEXT

CANCEL

- 在“配置参数”部分，单击“所有参数”，并验证是否有需要更新/配置红色指示灯。在如图所示的输出中，可以注意到访问列表上的顺序丢失。这相当于您在show ip access-list X中看到的行顺

序。

config parameters for the selected device

Profile Name: FunPro-ASA

Features: Interfaces, AccessLists, NAT, TrafficSelectorObjects, All

Required Parameters All Parameters

Folder/Param	Name	Value	Write Domain
Access List	access-list-inbound		
Access Control Entry	ICMP		
Access Control Entry	SSH		
Access Control Entry	SSH		
Destination Address			
Destination Service	destination_service		
ICMP			
Logging			
Protocol	protocol		
Source Address			
Source Service			
Action	action	permit	
Order	order	30	select asa domain
Access Control Entry			
Access Control Entry			

UPDATE RESET CANCEL

RED indicators parameters needed to be updated and GREEN indicates parameters will be submitted to the provider EPG.

PREVIOUS FINISH CANCEL

- 您还可以验证从前面定义的功能配置文件分配的IP编址，如果需要，此处是更改信息的良机。设置所有参数后，单击**完成**，如图所示：

config parameters for the selected device

Profile Name: FunProf-ASA

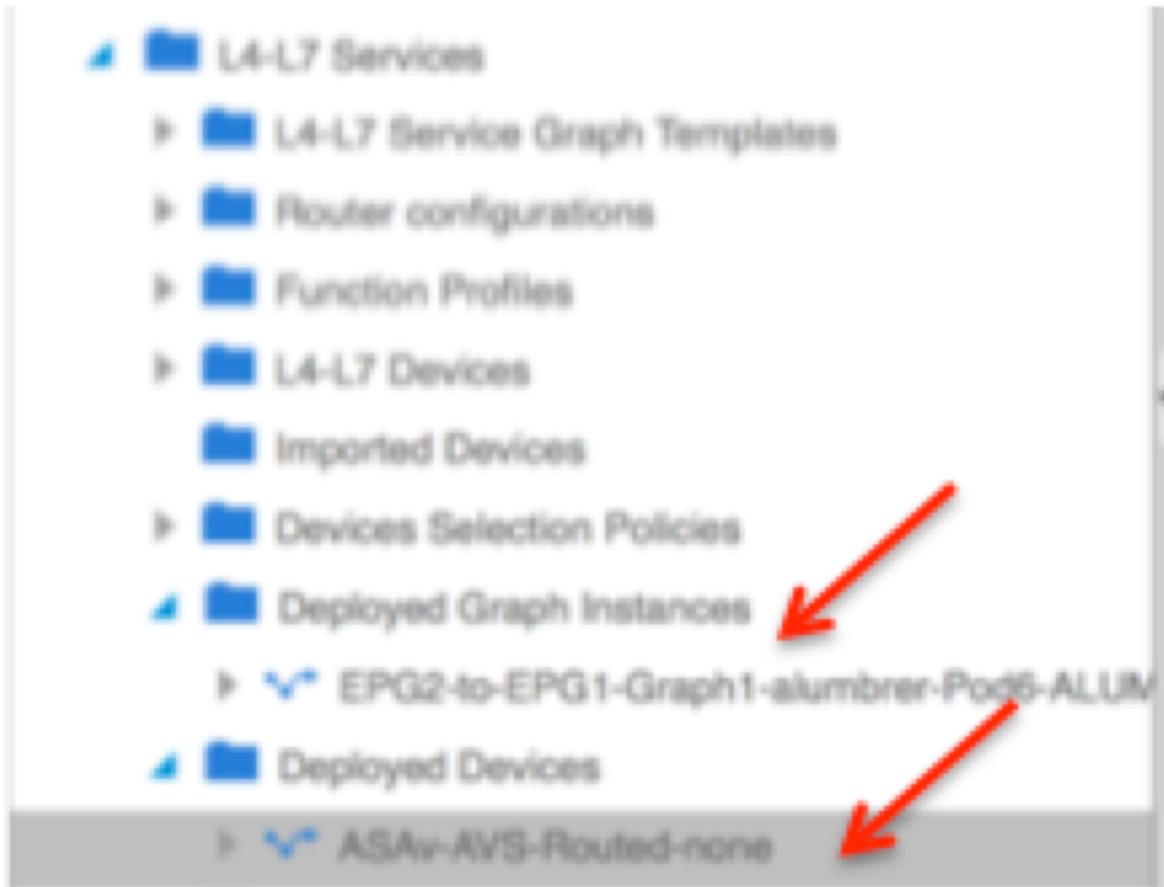
Features: Interfaces, AccessLists, NAT, TrafficSelectorObjects, All

Required Parameters All Parameters

Folder/Param	Name	Value	Write Domain
Device Config	Device		
Access List	access-list-inbound		
Bridge Group Interface			
Interface Related Configuration	externalIf		
Access Group	ExtAccessGroup		
Inbound Access List	name	access-list-inbound	
Outbound Access List			
IPv6 Enforce EUI-64			
Interface Specific Configuration	externalIfCfg		
IPv4 Address Configuration	IPv4Address		
IPv4 Address	ipv4_address	192.168.10.1/24	
IPv4 Standby Address			
IPv6 Address Configuration			
IPv6 Link Local Address Configuration			
IPv6 Router Advertisement			

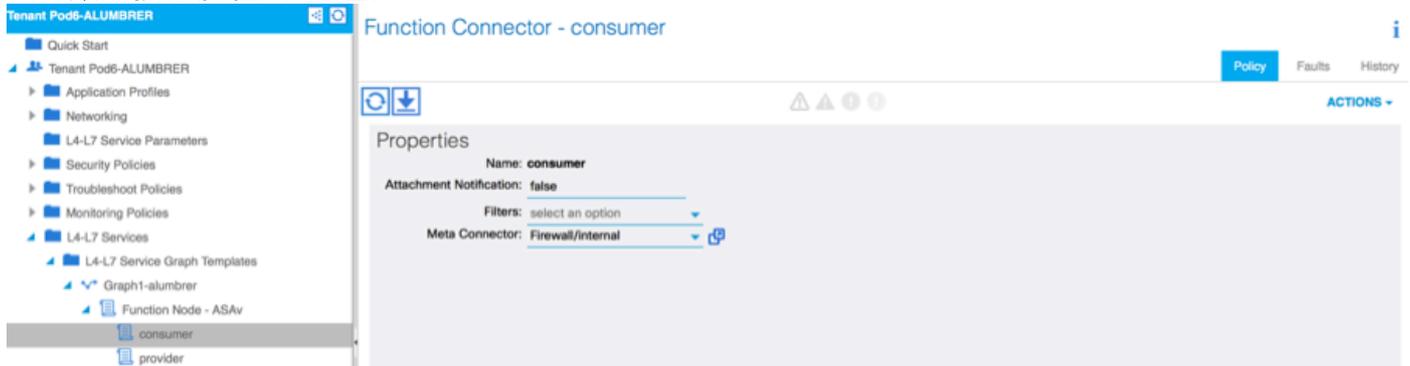
RED indicators parameters needed to be updated and GREEN indicates parameters will be submitted to the provider EPG.

- 如果一切正常，应显示新的已部署设备和图形实例。

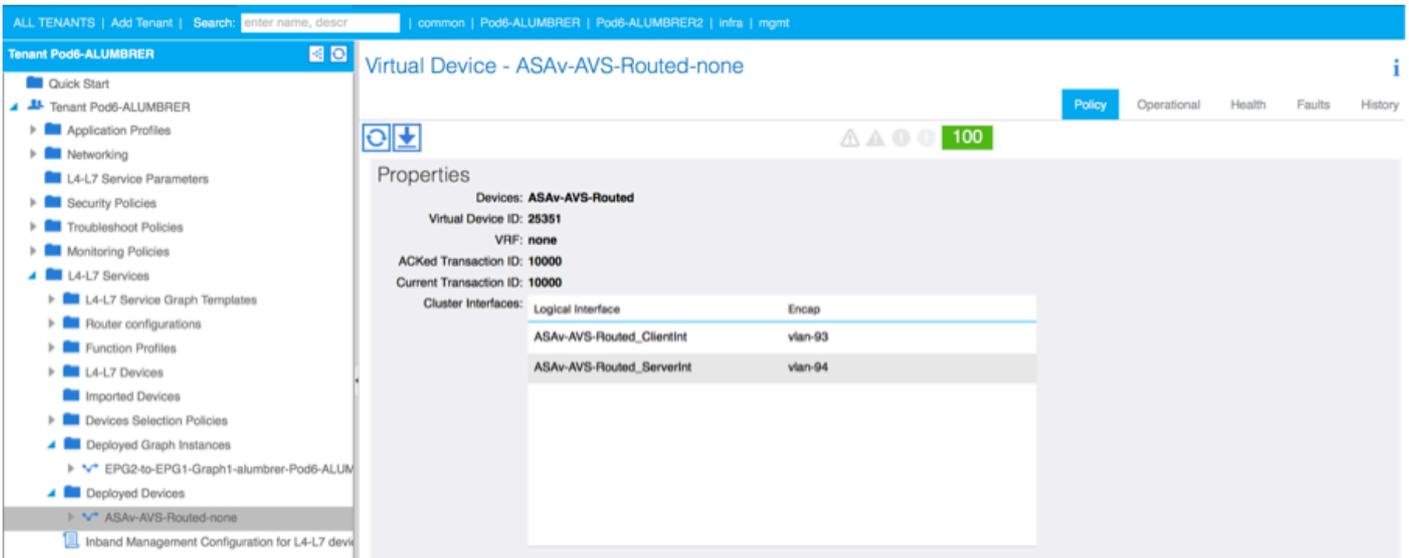


验证

- 创建服务图后需要验证的一件重要事是，使用正确的元连接器创建了消费者/提供商关系。在“函数连接器属性”下验证。



注意：防火墙的每个接口将分配一个来自AVS动态池的encap-vlan。验证是否没有故障。



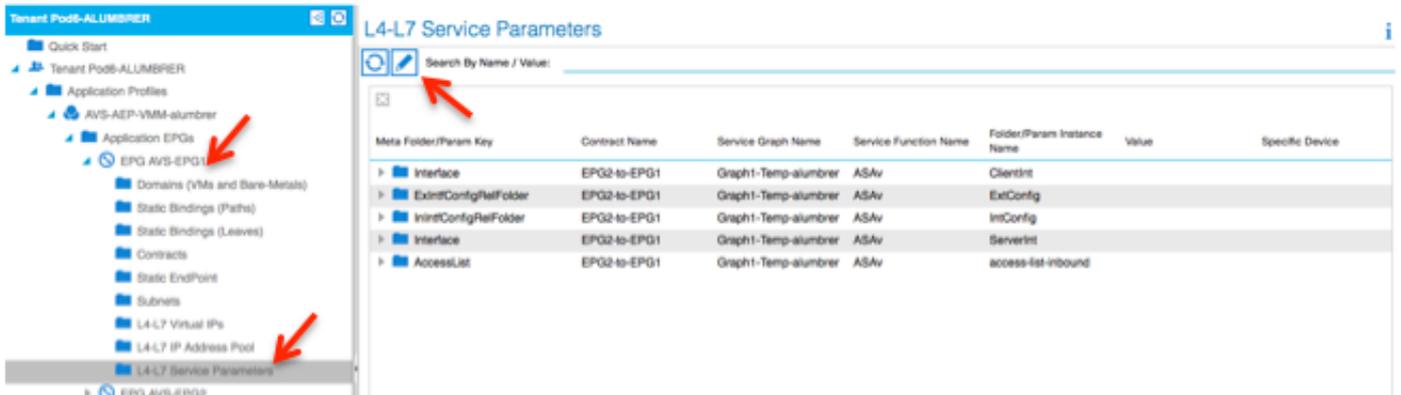
- 现在，您还可以验证推送到ASAv的信息

```

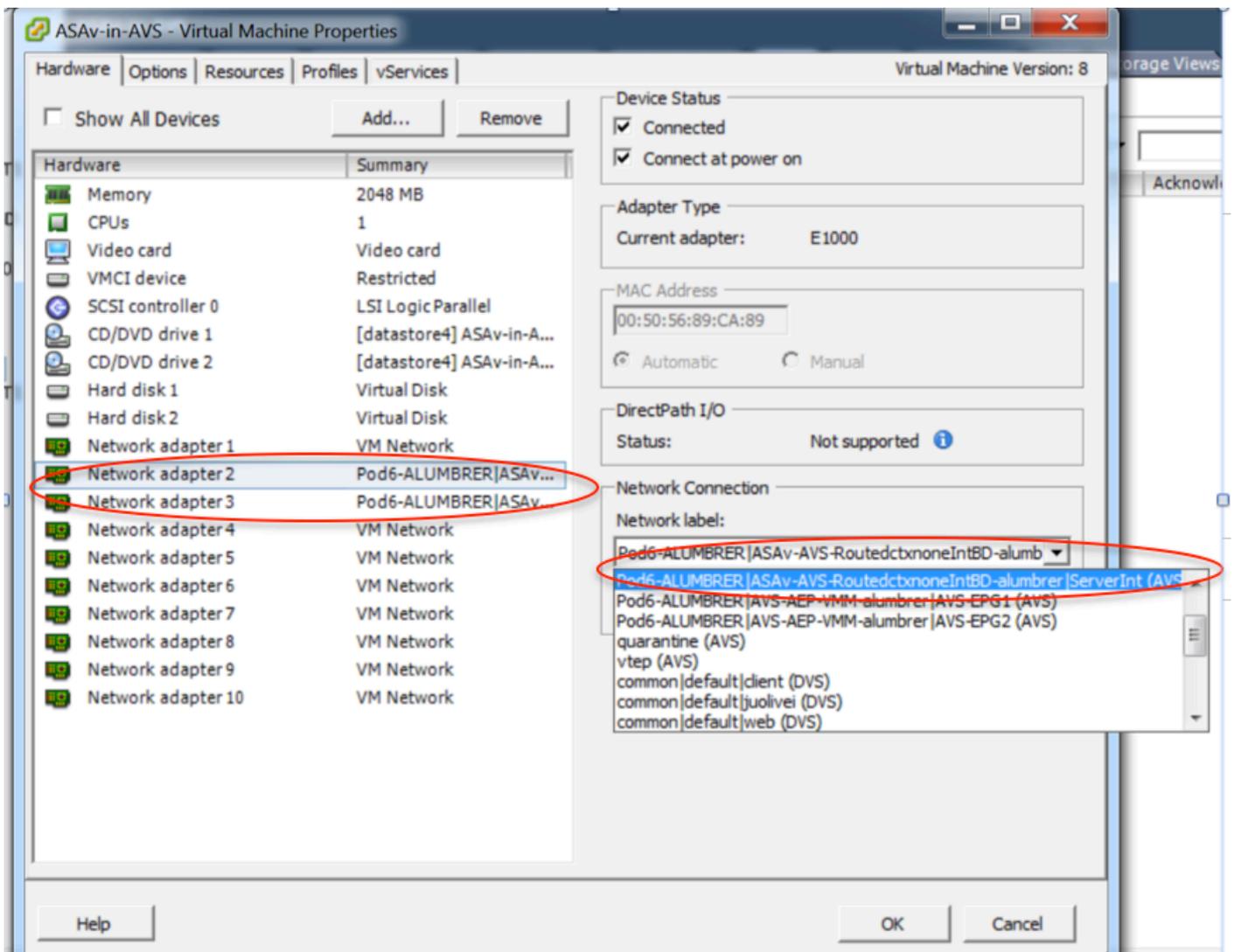
ASAv-W-AUS# show interface ip brief
Interface                               IP-Address      OK? Method Status        Prot
-----                               -
GigabitEthernet0/0                      192.168.10.1   YES manual up            up
GigabitEthernet0/1                      172.16.1.1     YES 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-AUS# 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-AUS#
  
```

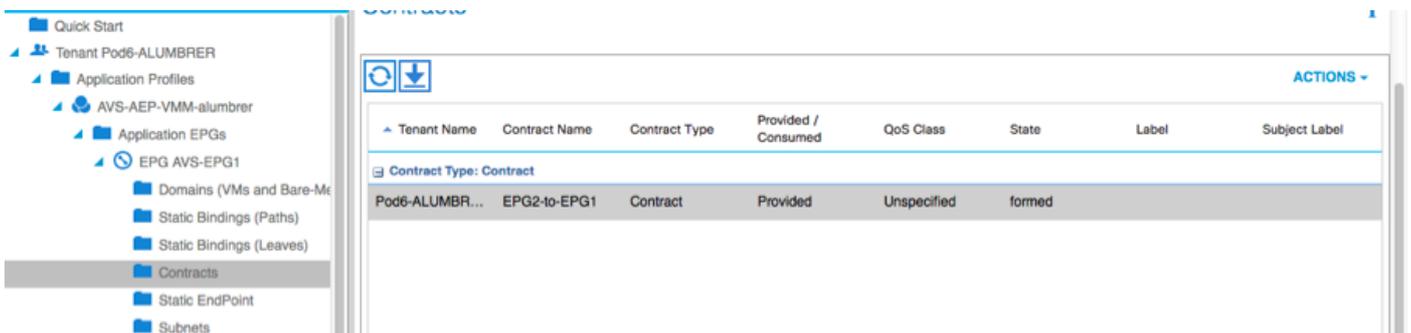
- 在EPG下分配新合同。从现在起，如果您需要修改访问列表上的任何内容，则必须从提供商 EPG的L4-L7服务参数进行更改。



- 在vCenter上，您还可以验证影子EPG是否已分配给每个防火墙接口：



在本测试中，我让2个EPG与标准合同通信，这2个EPG位于不同的域和不同的VRF中，因此它们之间的路由泄漏已预先配置。当防火墙在2个EPG之间设置路由和过滤时，这样在插入服务图后会简化一点。EPG和BD下之前配置的DG现在可以与合同一样删除。只有L4-L7推送的合同应保留在EPG下。



在删除标准合同后，您可以确认流量现在是否流经ASAv，命令show access-list应显示每次客户端向服务器发送请求时递增的规则的命中计数。

```

ASA-V-W-AUS#
ASA-V-W-AUS# 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 (hitcnt=0) 0xc873a747
access-list access-list-inbound line 2 extended permit tcp any any eq https (hitcnt=0) 0x48bedbdd
access-list access-list-inbound line 3 extended permit tcp any any eq ssh (hitcnt=4) 0x532fd57a
access-list access-list-inbound line 4 extended permit icmp any any (hitcnt=4) 0xe4b5a75d
ASA-V-W-AUS#

```

在枝叶上，应为客户端和服务端虚拟机以及ASAv接口学习终端

```

leaf2# show endpoint
Legend:
  0 - 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 | vxlan-98 | 0050.5689.fa08 | L | eth1/7 |
Pod6-ALUMBRER:VRF1-alumbrer | Server IP & MAC | vxlan-98 | 192.168.10.10 | L | |
25 | vxlan-94 | 0050.5689.ca89 | L | po4 |
Pod6-ALUMBRER:VRF1-alumbrer | vxlan-94 | 192.168.10.1 | L | |
mgmt:inb | 192.168.2.11 | S | | |
21 | vxlan-97 | 0050.5689.3fca | L | eth1/7 |
Pod6-ALUMBRER:VRF2 | Client IP & MAC | vxlan-97 | 172.16.1.10 | L | |
26 | vxlan-93 | 0050.5689.e7dd | L | po4 |
Pod6-ALUMBRER:VRF2 | vxlan-93 | 172.16.1.1 | L | |
overlay-1 | 10.0.104.93 | L | | |
overlay-1 | 10.0.96.67 | L | | |
13 | vxlan-16777209 | 0050.5677.18a5 | H | FW interface (ServerInt) | unspecified |
overlay-1 | vxlan-16777209 | 10.0.32.93 | H | | unspecified |
13 | vxlan-16777209 | 0050.5660.ddab | H | | unspecified |
overlay-1 | vxlan-16777209 | 10.0.32.64 | H | | unspecified |

```

参见连接到VEM的两个防火墙接口。

ESX-1

```

~ # vmemcmd 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    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      0      vmnic6
 50                               UP    UP    FWD    -     0     6    0      0      0      vmk1
 51                               UP    UP    FWD    -     0     6    0      0      0      Client1-AVS.eth0
 52                               UP    UP    FWD    -     0     6    0      0      0      Server1-AVS.eth0
1040   Po1     UP    UP    FWD    -     0     0    0      0      0
~ #

```

最后，如果我们知道源和目标EPG的PC标记，也可以在枝叶级别验证防火墙规则：

EPG1

Name	Description	State	Issues	QoS	Encap	PC Tag
AVS-EPG1		applied		Unspecified		17
EPG-internal-almubrer		applied		Unspecified		32772

EPG2

Name	Description	State	Issues	QoS	Encap	PC Tag
AVS-EPG2		applied		Unspecified		5476

过滤器ID可以与枝叶上的PC标记匹配，以验证防火墙规则。

```

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#

```

注意：EPG PCTags/Sclass从不直接通信。通信通过L4-L7服务图插入创建的影子EPG被中断或绑定在一起。

通信客户端到服务器工作正常。

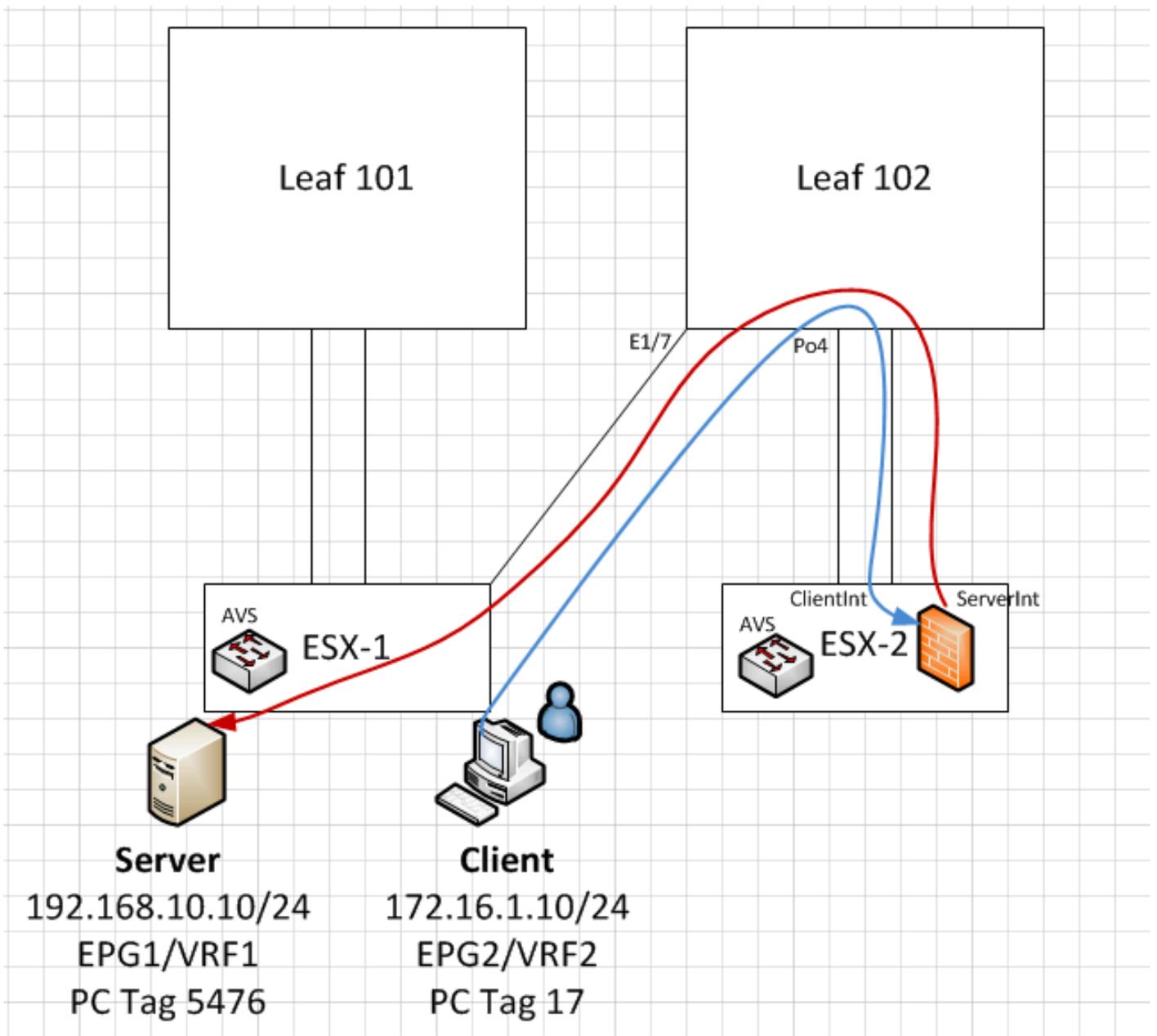
```
cisco@cisco-UbuntuClient:~$ ifconfig
eth1      Link encap:Ethernet  HWaddr 00:50:56:89:3f:ca
          inet addr:172.16.1.10  Bcast:172.16.1.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe89:3fca/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          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/

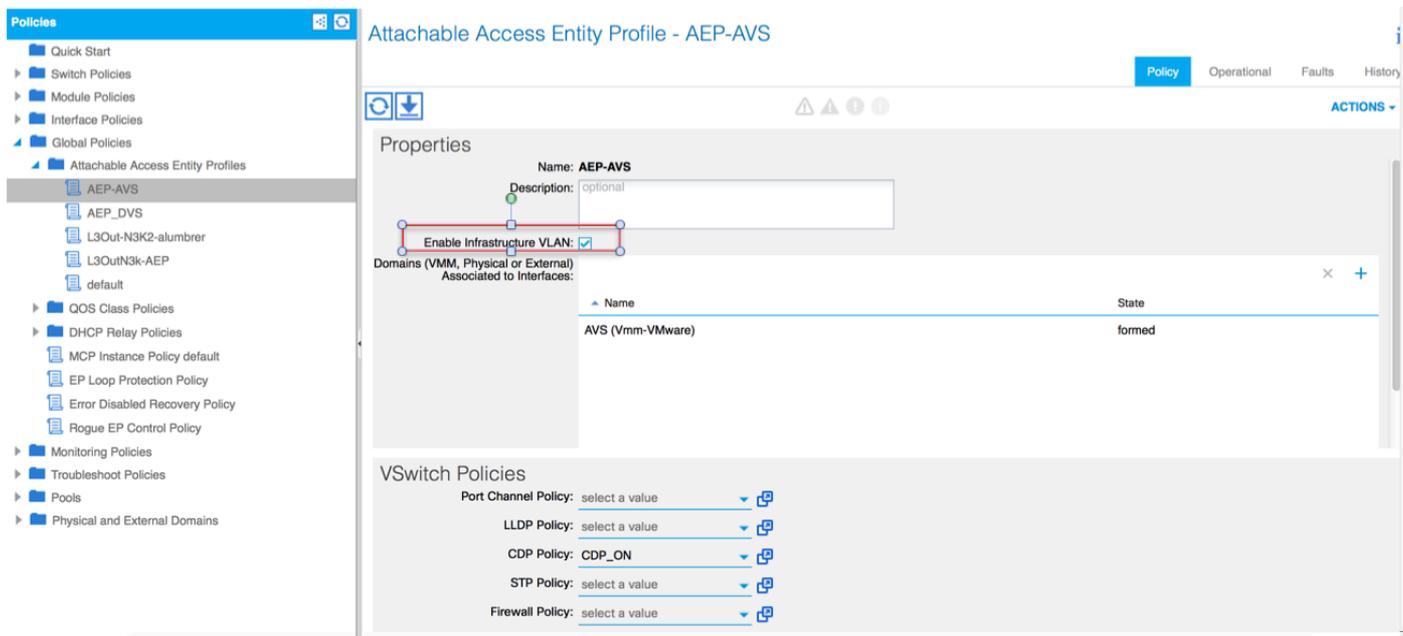
Last login: Mon Feb  1 10:14:11 2016 from 172.16.1.10
cisco@cisco-UbuntuClient:~$ $
```



故障排除

未分配VTEP地址

验证是否在AEP下检查了Infrastructure Vlan:



不支持的版本

验证VEM版本是否正确，并支持适当的ESXi VMWare系统。

```

~ # 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

```

VEM和交换矩阵通信不工作

- 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

```

此时可以确定ESXi主机和枝叶之间的交换矩阵通信无法正常工作。可以在枝叶端检查某些验证命令以确定根本原因。

```
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)

```

通过Po5连接的ESXi中有2个端口

```
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

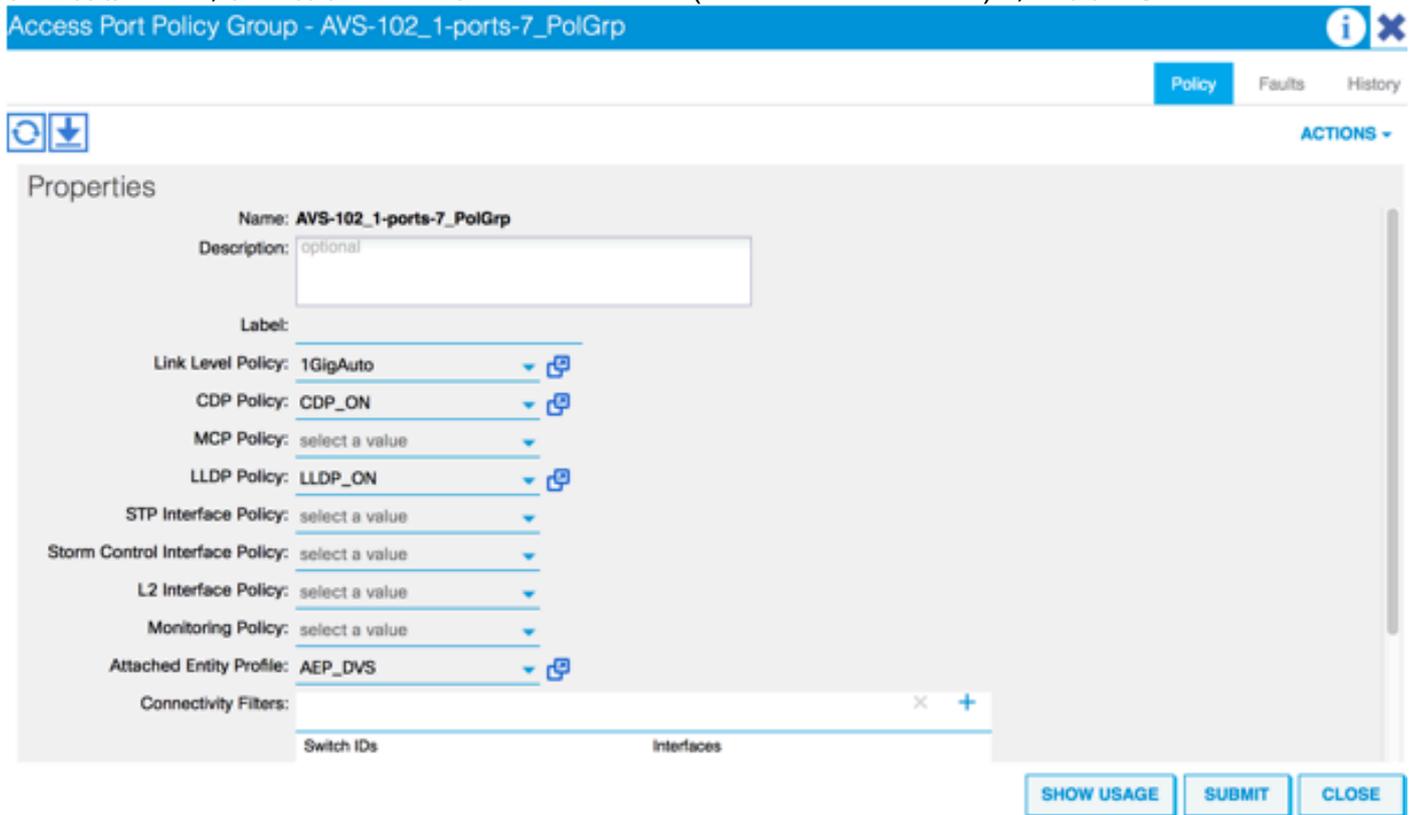
VLAN	Type	Vlan-mode	Encap
13	enet	CE	vxlan-16777209, vlan-3967
19	enet	CE	vxlan-14680064, vlan-150
22	enet	CE	vxlan-16383902
26	enet	CE	vxlan-15531929, vlan-200
27	enet	CE	vlan-11
28	enet	CE	vlan-14
36	enet	CE	vxlan-15662984

从上述输出中可以看到，Infra Vlan不允许或通过通往ESXi主机的上行链路端口(1/5-6)。这表示APIC上配置了接口策略或交换机策略的配置错误。

同时检查：

访问策略>接口策略>配置文件访问策略>交换机策略>配置文件

在这种情况下，接口配置文件连接到错误的AEP（用于DVS的旧AEP），如图所示：



在为AVS设置正确的AEP后，我们现在可以看到，通过枝叶上的正确的取消链路可以看到基础设施VLAN:

```
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 reestablished 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
```

相关信息

应用虚拟交换机安装

[思科系统公司思科应用虚拟交换机安装指南，版本5.2\(1\)SV3\(1.2\)](#)

使用VMware部署ASA v

[思科系统公司思科自适应安全虚拟设备\(ASA v\)快速入门指南，9.4](#)

思科ACI和思科AVS

[思科系统公司思科ACI虚拟化指南，版本1.2\(1i\)](#)

使用思科以应用为中心的基础设施设计服务图白皮书

[使用思科以应用为中心的基础设施设计服务图白皮书](#)

[技术支持和文档 - Cisco Systems](#)