使用AVS-ACI 1.2(x)版本的GoTo(L3)模式的ASAv

目錄

簡介

本文說明如何使用ACI 1.2(x)版本在兩個端點組(EPG)之間將應用虛擬交換機(AVS)交換機與採用路由/轉至模式的自適應安全虛擬裝置(ASAv)單防火牆部署為第4-7層服務圖，以建立客戶端到伺服器的通訊。

必要條件

需求

思科建議您瞭解以下主題：

- 已配置訪問策略，介面處於啟用狀態並處於服務狀態
- 已配置EPG、橋接域(BD)和虛擬路由和轉發(VRF)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

硬體和軟體：

- 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)
- 分葉/主幹 — 11.2(1i)
- 已下載裝置軟體包*.zip

功能：

- AVS

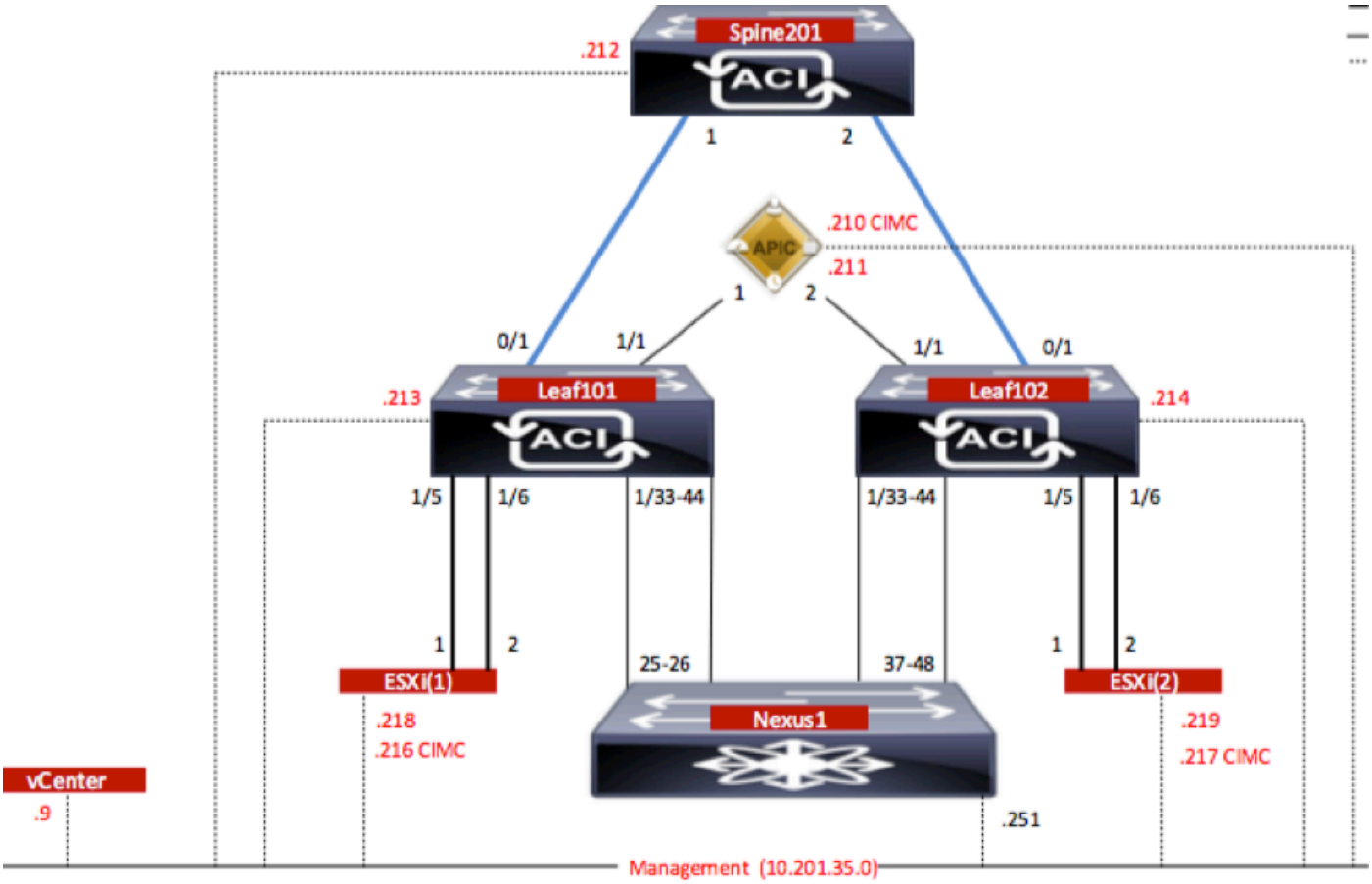
- ASAv
- EPG、BD、VRF
- 存取控制清單(ACL)
- L4-L7服務圖
- vCenter

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

網路圖表

如圖所示，



組態

AVS初始設定建立VMware vCenter域（VMM整合）2

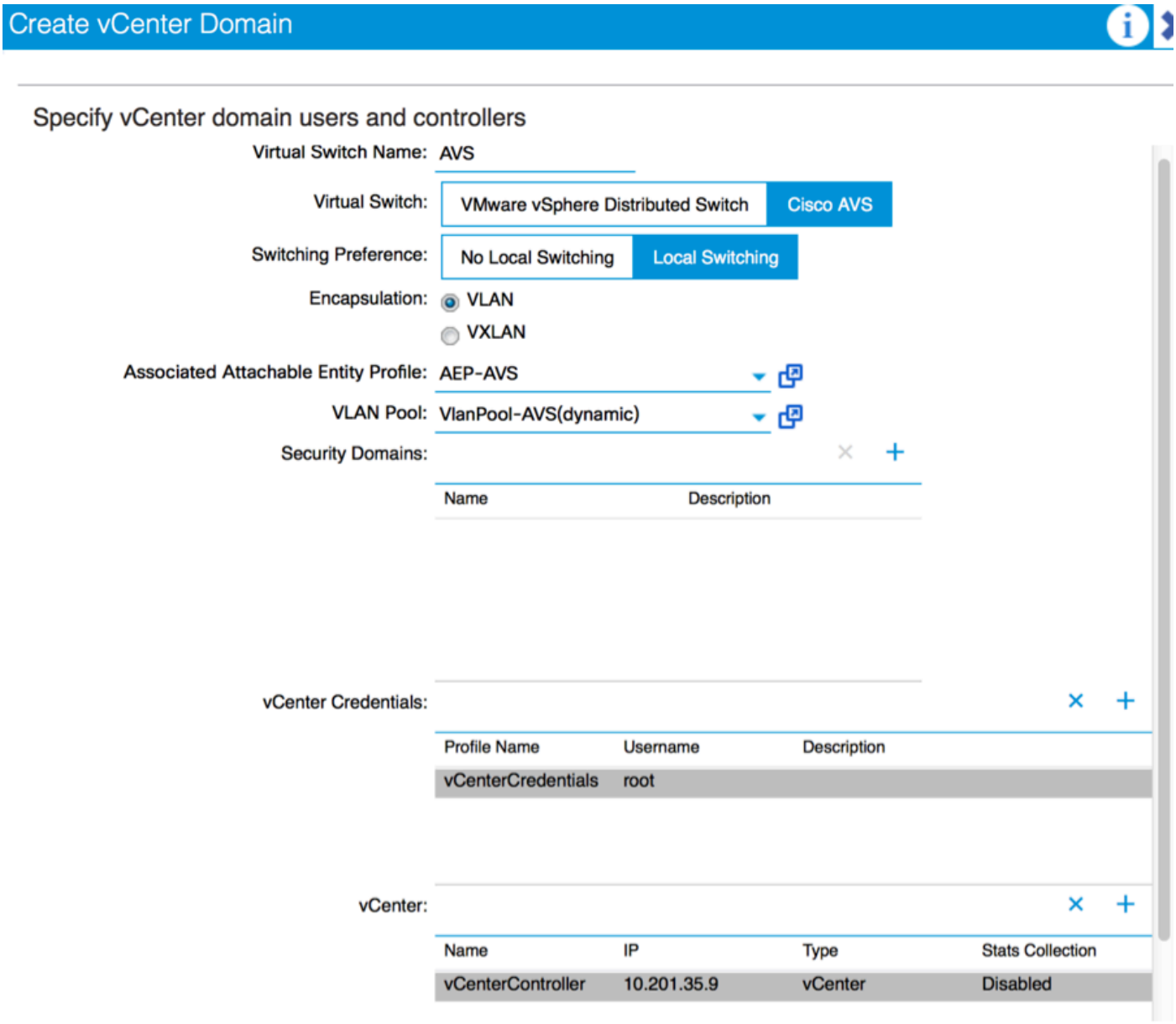
附註：

- 您可以在單個域下建立多個資料中心和分散式虛擬交換機(DVS)條目。但是，您只能為每個資料中心分配一個Cisco AVS。
- Cisco ACI版本1.2(1i)和Cisco AVS版本5.2(1)SV3(1.10)支援使用Cisco AVS部署服務圖。 整個服務圖配置是在思科應用策略基礎架構控制器(思科APIC)上執行的。

- 僅在具有虛擬區域網(VLAN)封裝模式的虛擬機器管理器(VMM)域上支援使用Cisco AVS的服務虛擬機器(VM)部署。但是，計算VM（提供者和使用者VM）可以是具有虛擬可擴展LAN(VXLAN)或VLAN封裝的VMM域的一部分。

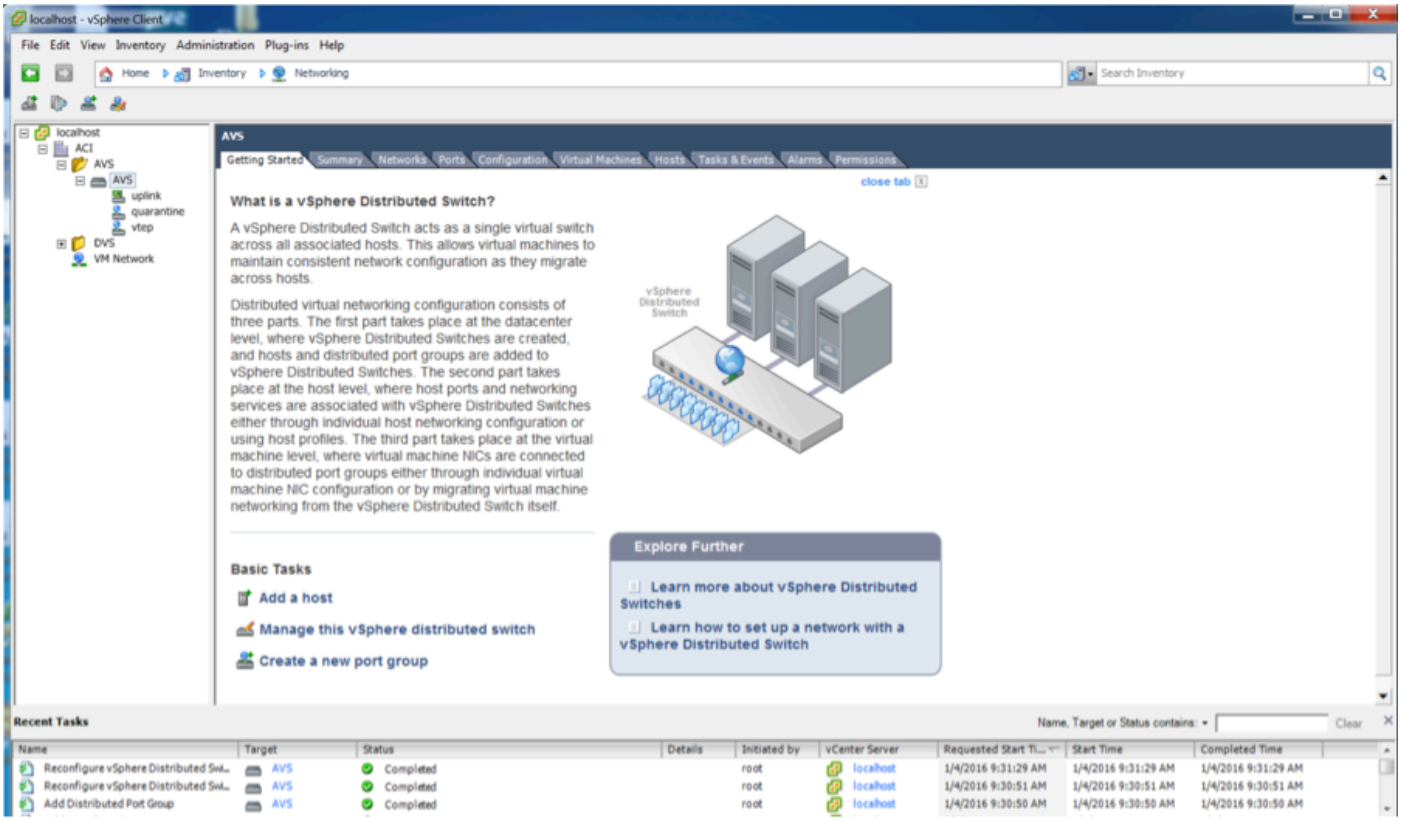
- 另請注意，如果使用本地交換，則不需要組播地址和池。如果未選擇本地交換，則必須配置組播池，並且AVS交換矩陣範圍組播地址不應是組播池的一部分。源自AVS的所有流量將採用VLAN或VXLAN封裝。

導覽至**VM Networking > VMWare > Create vCenter Domain**，如下圖所示：

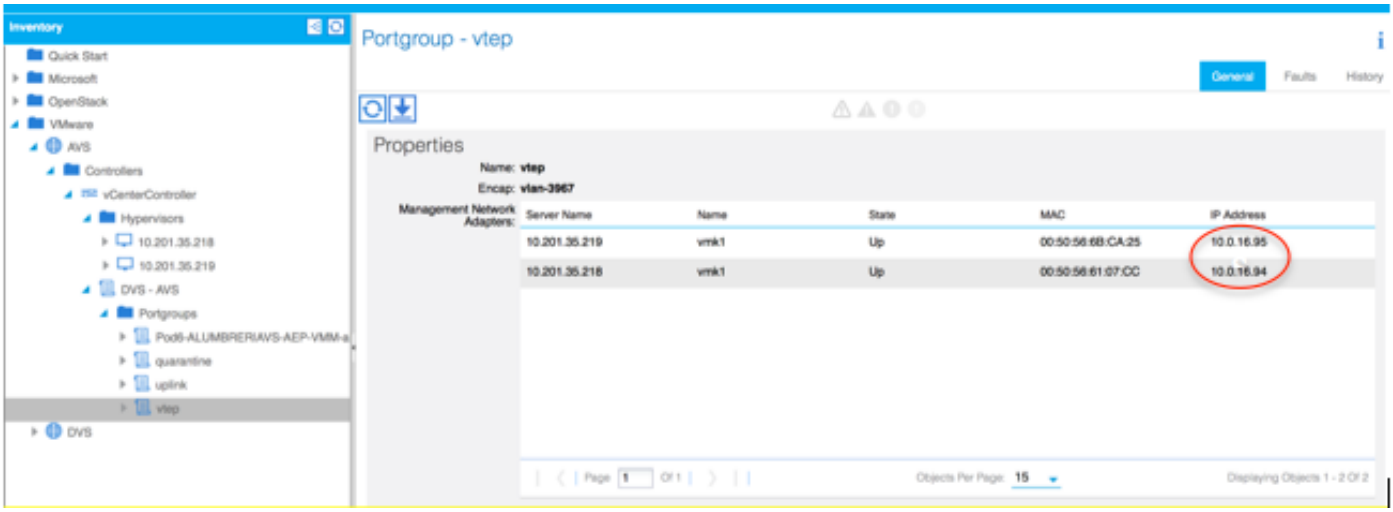


如果您使用埠通道或VPC（虛擬埠通道），建議將vSwitch策略設定為使用Mac固定。

之後，APIC應將AVS交換機配置推送到vCenter，如下圖所示：



在APIC上，您可以注意到VXLAN通道端點(VTEP)位址已指派給AVS的VTEP連線埠群組。無論使用哪種連線模式（VLAN或VXLAN），都會分配此地址



在vCenter中安裝Cisco AVS軟體

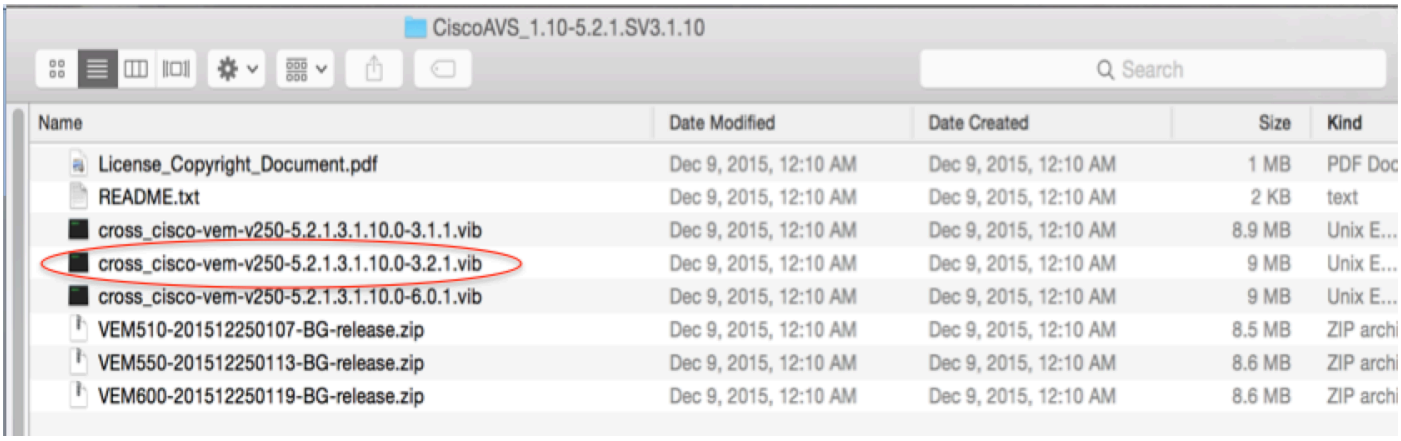
- 使用此連結從CCO下載vSphere安裝套件(VIB)

  注意：在本例中，我們使用ESX 5.5，表1 ，顯示了ESXi 6.0、5.5、5.1和5.0的相容性表

表1 - ESXi 6.0、5.5、5.1和5.0的主機軟體版本相容性

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

在ZIP檔案中，有3個VIB檔案（每個ESXi主機版本各一個），請選擇一個適用於ESX 5.5的檔案，如下圖所示：



- 將VIB檔案複製到ESX Datastore — 這可以通過CLI完成，也可以直接從vCenter完成

  附註：如果主機上存在VIB檔案，請使用**esxcli software vib** remove命令將其刪除。

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

或者直接瀏覽Datastore。

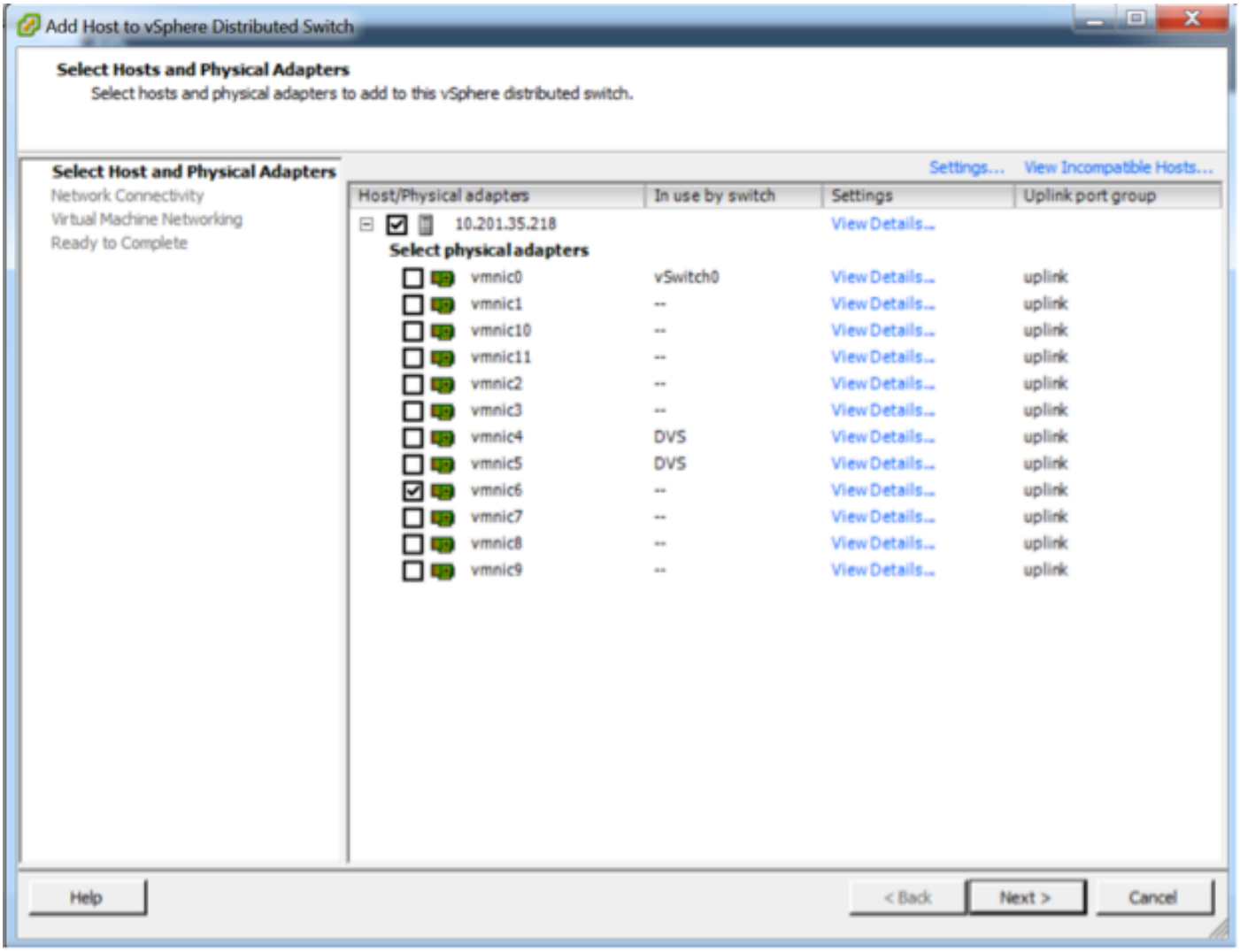
- 在ESXi主機上使用以下命令安裝AVS軟體：

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

```
~ # 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

~ #
```

- 虛擬乙太網路模組(VEM)啟動後，可以將主機新增到AVS中：

在Add Host to vSphere Distributed Switch對話方塊中，選擇連線到枝葉交換機的虛擬NIC埠（在本示例中，僅移動vmnic6），如下圖所示：



- 按一下**下一步**
- 在「網路連線」對話方塊中，按一下**下一步**
- 在「虛擬機器網路」對話方塊中，按一下「下一**步」**
- 在「準備完成」對話方塊中，按一下「完**成」**

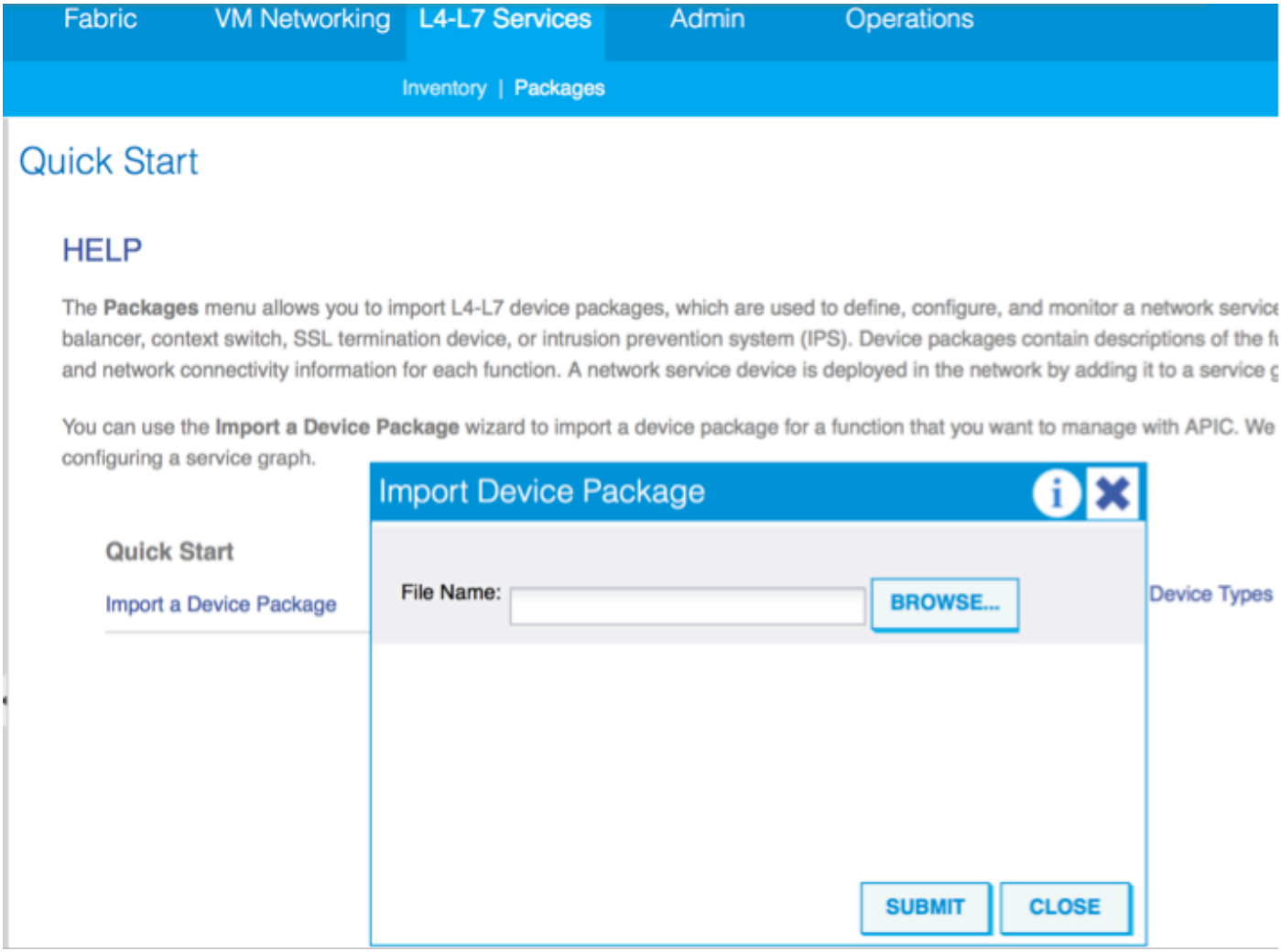
附註：如果使用多個ESXi主機，所有主機都需要運行AVS/VEM，以便它們可以從標準交換機管理到DVS或AVS。

這樣，AVS整合已經完成，我們可以繼續部署L4-L7 ASAv:

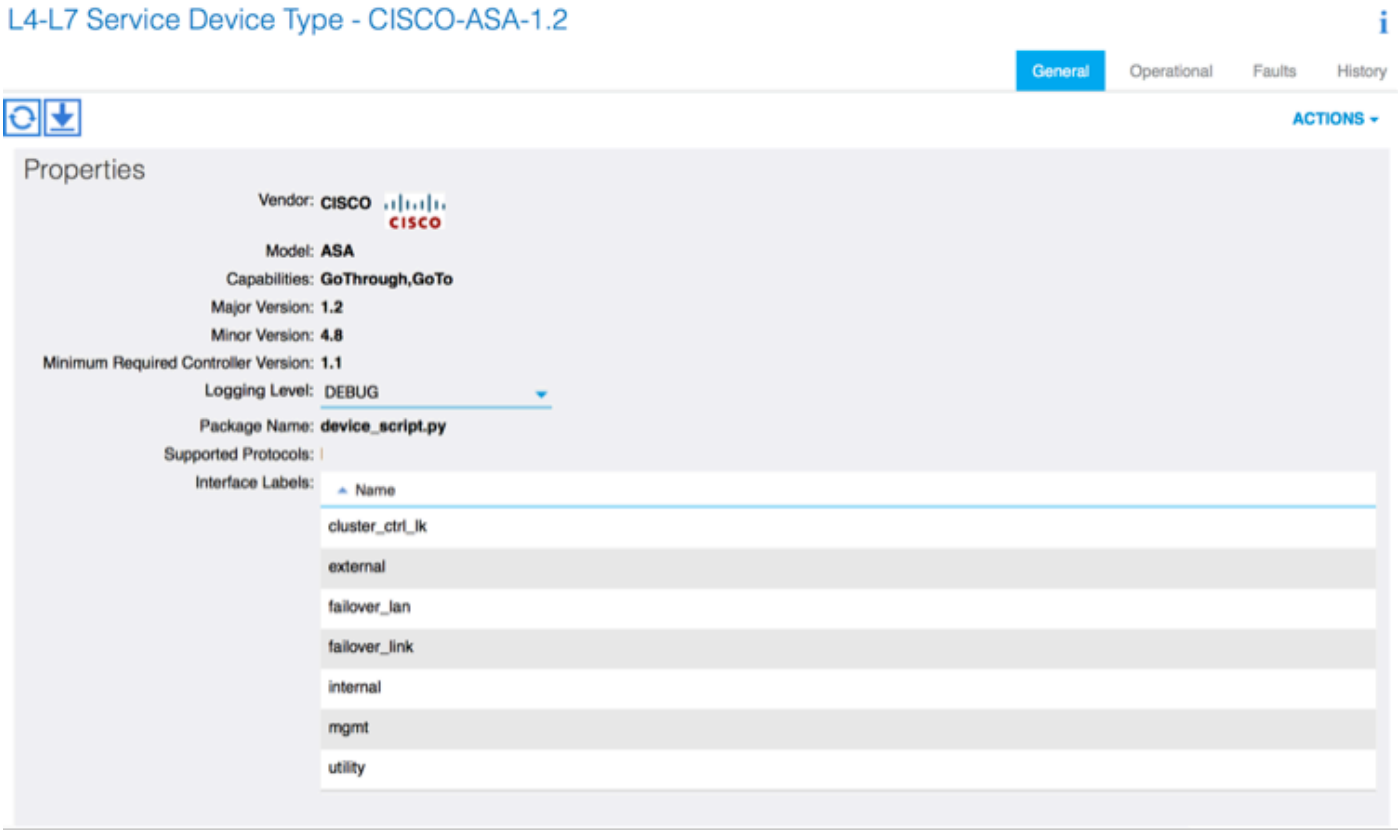
ASAv初始設定

- 下載Cisco ASAv裝置包並將其匯入APIC:

導覽至**L4-L7 Services > Packages > Import Device Package**，如下圖所示：



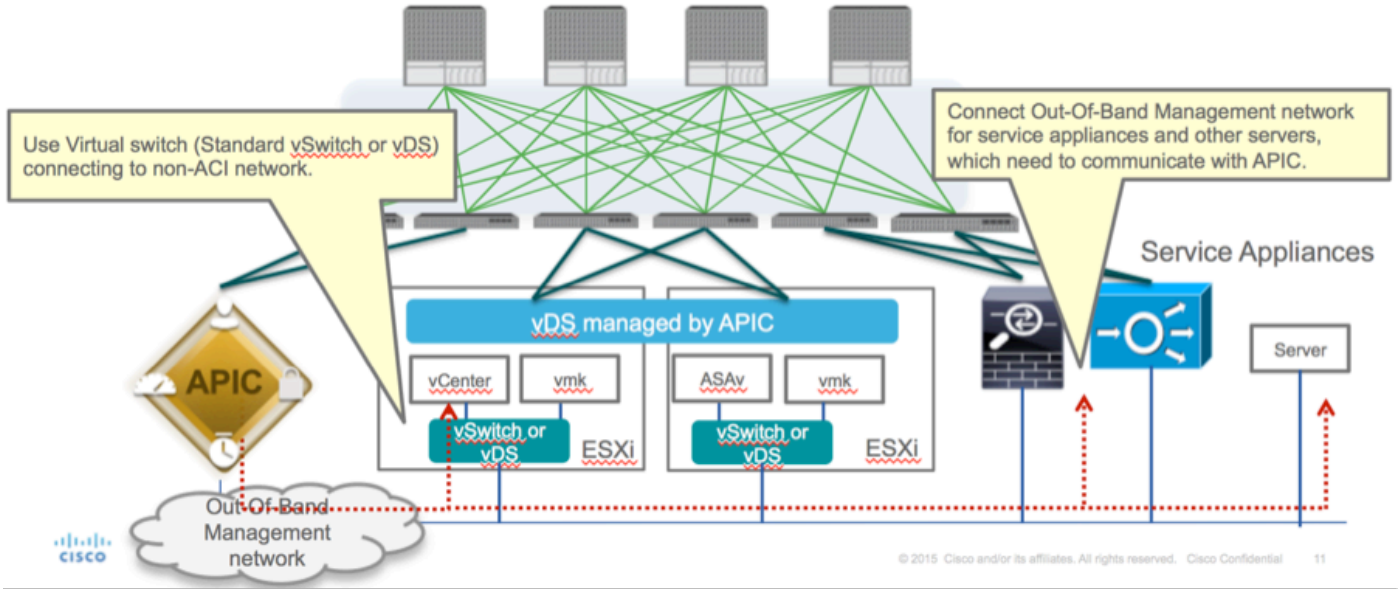
- 如果一切正常，您可以看到匯入的裝置包正在展開L4-L7 Service Device Types資料夾，如下圖所示：



繼續之前，在執行實際的L4-L7整合之前，需要確定安裝的幾個方面：

有兩種管理網路：帶內管理和帶外(OOB)，它們可用於管理不屬於基本以應用為中心的基礎設施(ACI)的裝置（枝葉、主幹或apic控制器），包括ASAv、負載均衡器等。

在這種情況下，ASAv的OOB是使用標準vSwitch部署的。對於裸機ASA或其他服務裝置和/或伺服器，請將OOB管理埠連線到OOB交換機或網路，如下圖所示。



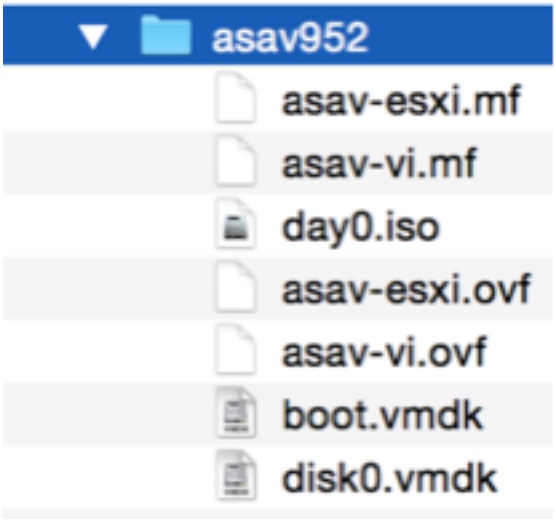
ASAv OOB管理埠管理連線需要使用ESXi上行鏈路埠通過OOB與APIC通訊。在對映vNIC介面時，網路介面卡1始終匹配ASAv上的管理0/0介面，其餘的資料平面介面從網路介面卡2啟動。

表2顯示了網路介面卡ID和ASAv介面ID的一致性：

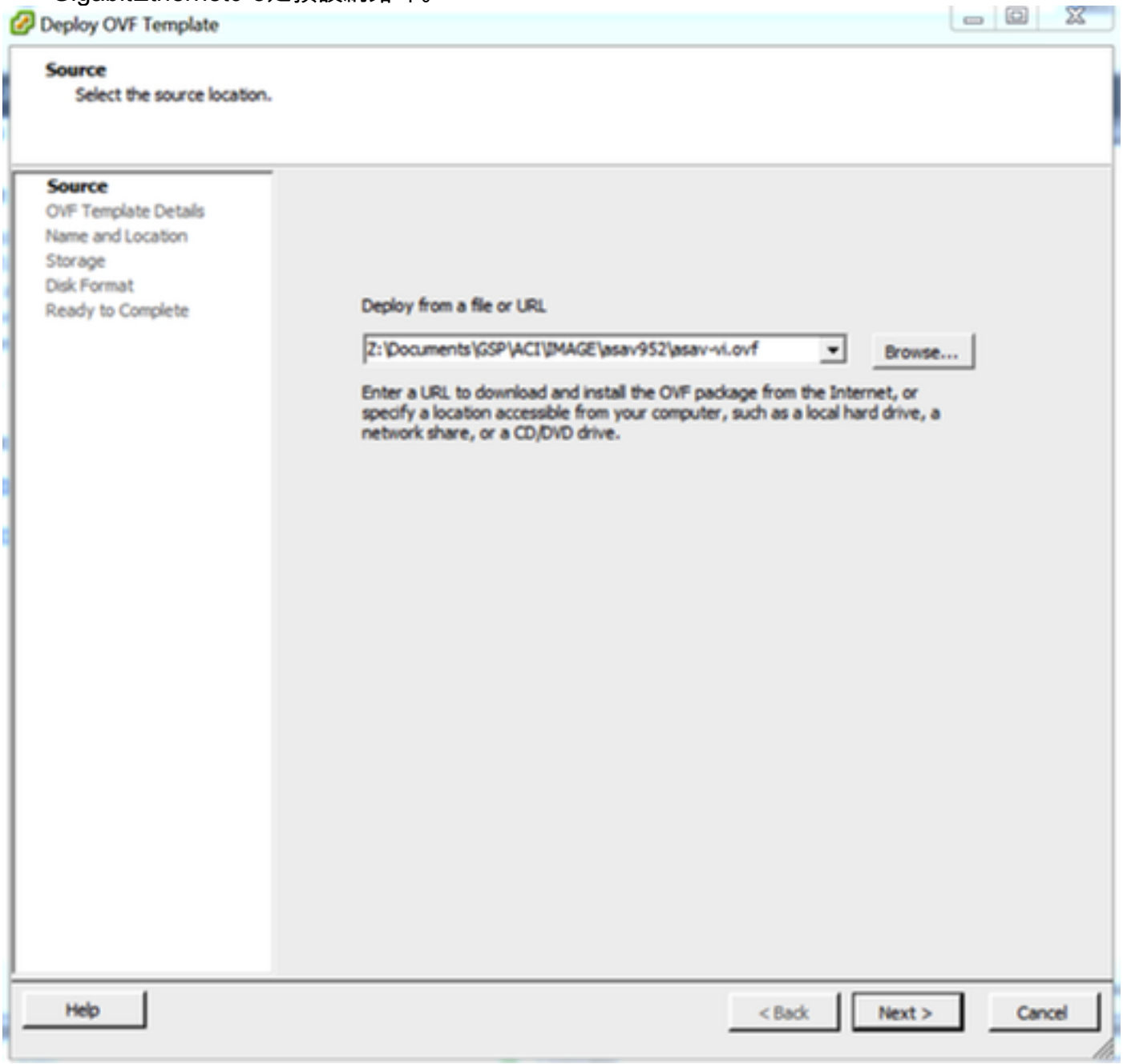
表2

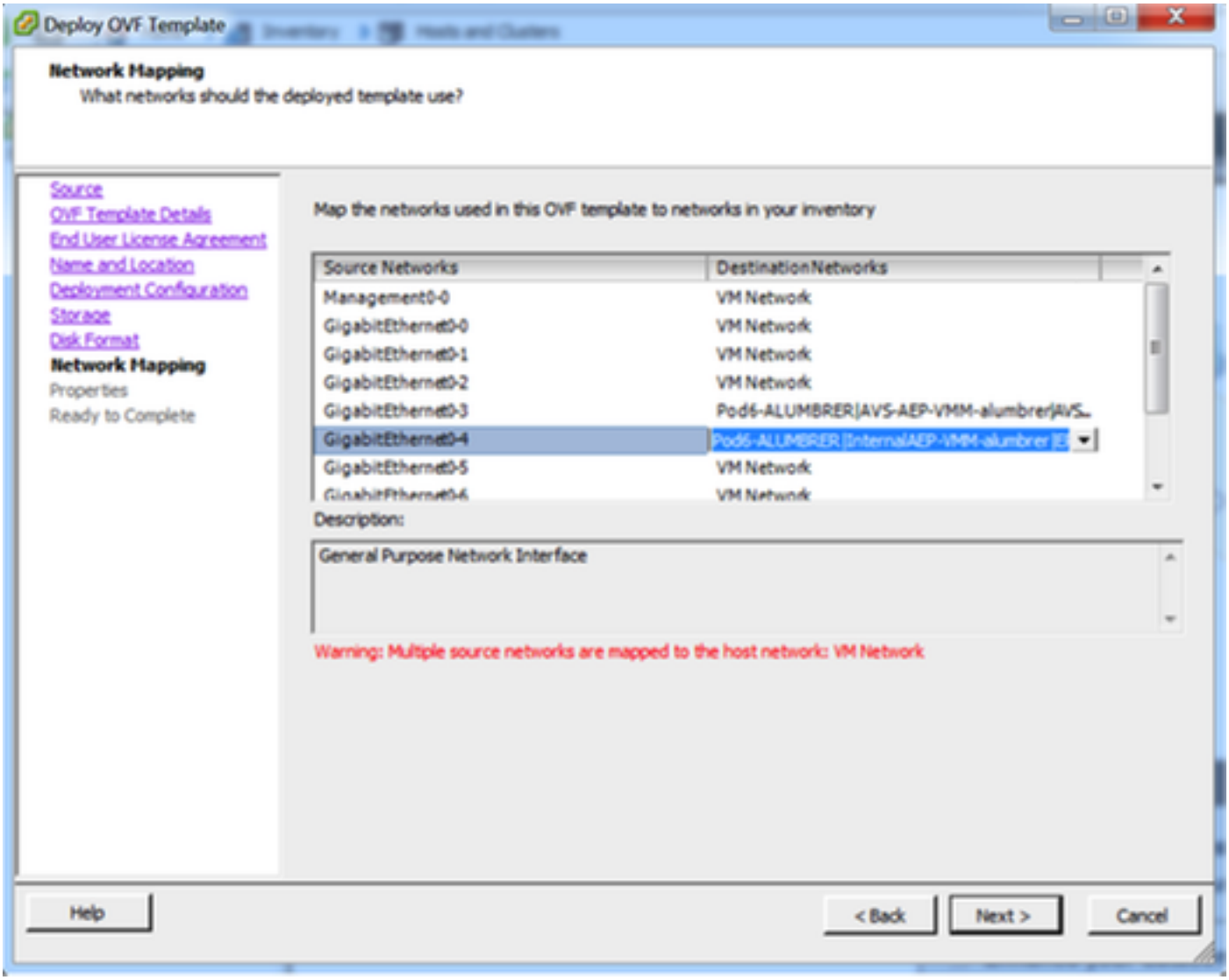
Network Adapter ID	ASAv Interface ID
Network Adapter 1	Management0/0
Network Adapter 2	GigabitEthernet0/0
Network Adapter 3	GigabitEthernet0/1
Network Adapter 4	GigabitEthernet0/2
Network Adapter 5	GigabitEthernet0/3
Network Adapter 6	GigabitEthernet0/4
Network Adapter 7	GigabitEthernet0/5
Network Adapter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

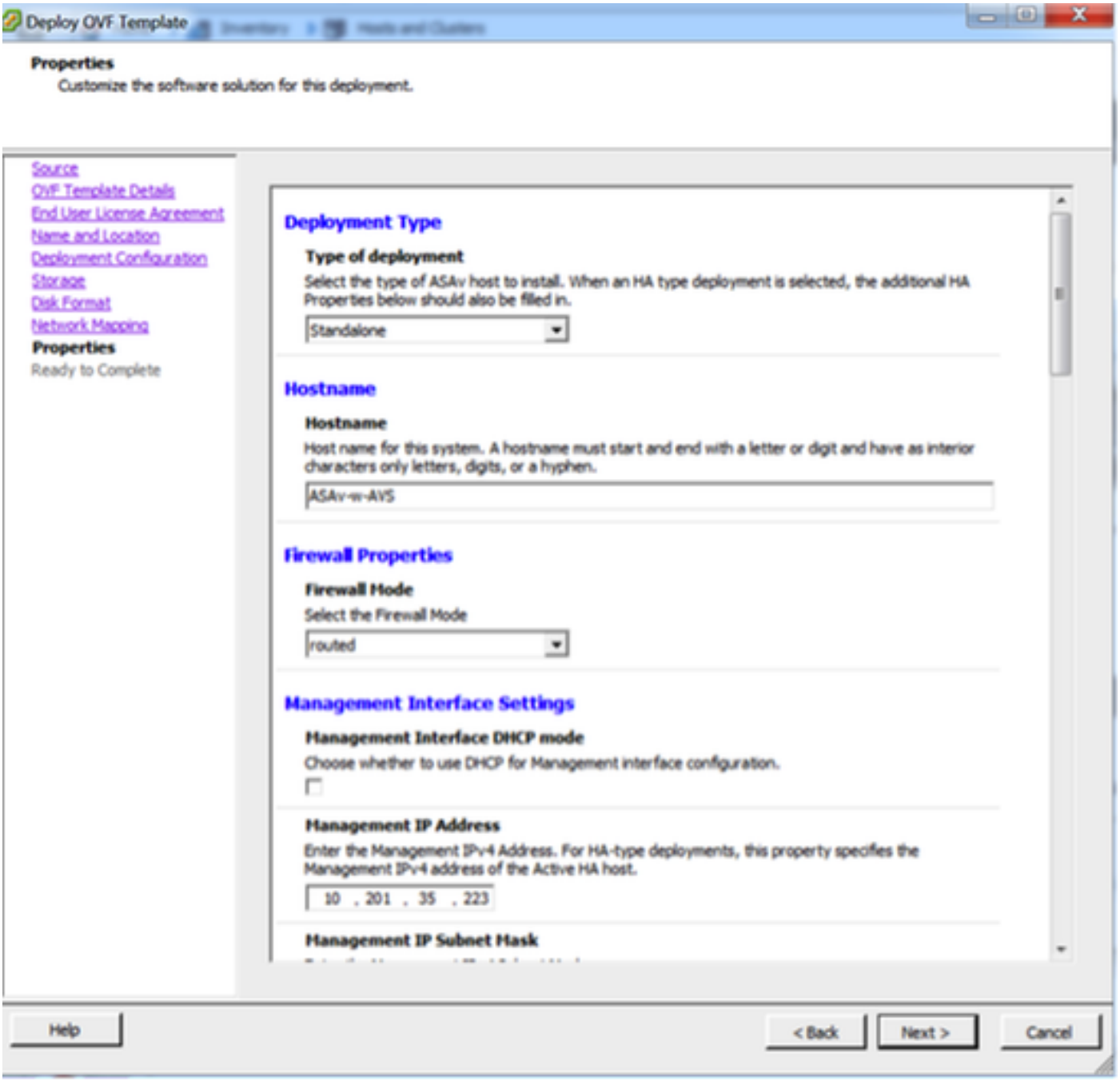
- 通過**File>Deploy OVF(Open Virtualization Format)Template中的嚮導部署ASAv VM**
- 如果要將獨立ESX Server或**asav-vi** for vCenter，請選擇**asav-esxi**。在這種情況下，使用vCenter。

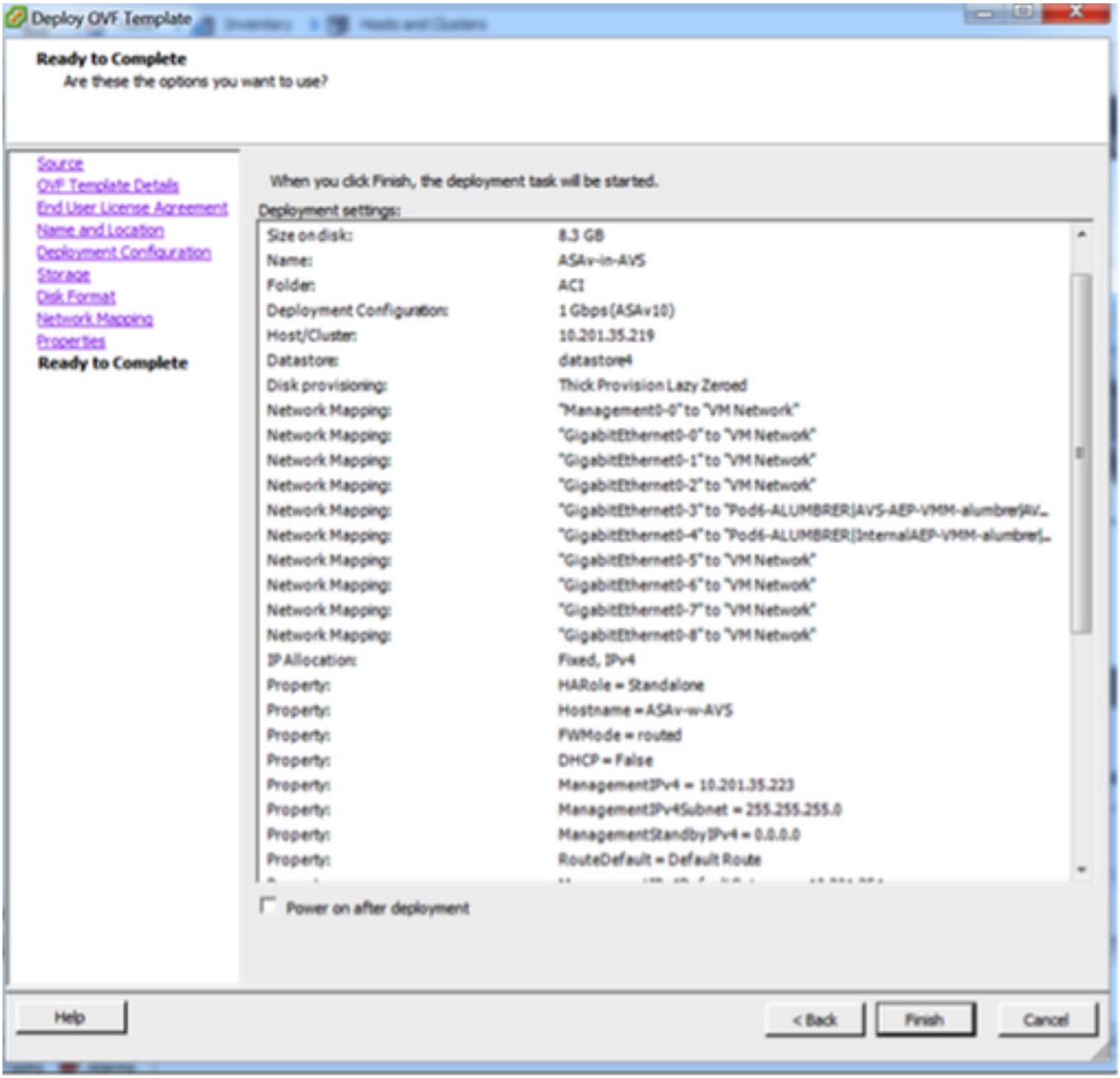


- 通過安裝嚮導，接受條款和條件。在嚮導的中間，您可以確定多個選項，如主機名、管理、ip地址、防火牆模式和其他與ASAv相關的特定資訊。請記住對ASAv使用OOB管理，因為在這種情況下，在使用VM網路（標準交換機）時，您需要保持介面管理0/0，而介面GigabitEthernet0-8是預設網路埠。

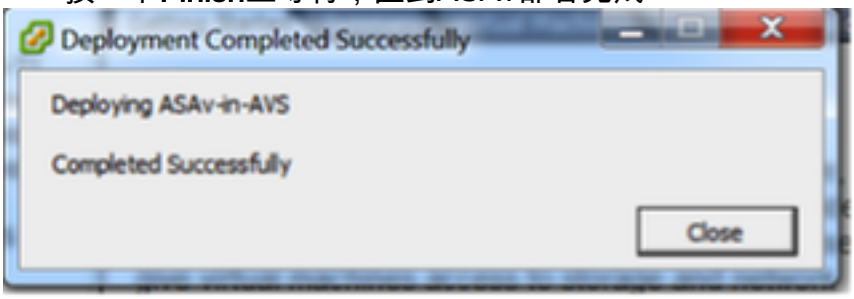



Deploy OVF Template
Network Mapping
What networks should the deployed template use?
Source
OVF Template Details
End User License Agreement
Name and Location
Deployment Configuration
Storage
Disk Format
Network Mapping
Properties
Ready to Complete
Map the networks used in this OVF template to networks 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



- 按一下**Finish**並等待，直到ASAv部署完成



- 開啟ASAv VM並通過控制檯登入以驗證初始配置

```
!
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 --->_
```

- 如圖所示，某些管理配置已推送到ASAv防火牆。配置管理員使用者名稱和密碼。APIC使用此使用者名稱和密碼登入並配置ASA。ASA應能連線到OOB網路，並能夠訪問APIC。

username admin password <device_password> encrypted privilege 15

```
ASAv-w-AVS(config)# username admin password C1sc0123 privilege  15
ASAv-w-AVS(config)# wr mem
Building configuration...
Cryptochecksum: d491b980 86fa522f 6f937baf b5bfb318

7977 bytes copied in 0.250 secs
[OK]
ASAv-w-AVS(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
ASAv-w-AVS(config)# _
```

此外，從全域性配置模式啟用http伺服器：

http server enable

http 0.0.0.0 0.0.0.0管理

L4-L7，用於APIC中的ASAv整合:

- 登入到ACI GUI，點選將部署服務圖的租戶。展開導航窗格底部的L4-L7服務，按一下右鍵**L4-L7裝置**，然後按一下**Create L4-L7裝置**開啟嚮導
- 對於此實施，將應用以下設定：
  — 託管模式

— 防火牆服務

— 虛擬裝置

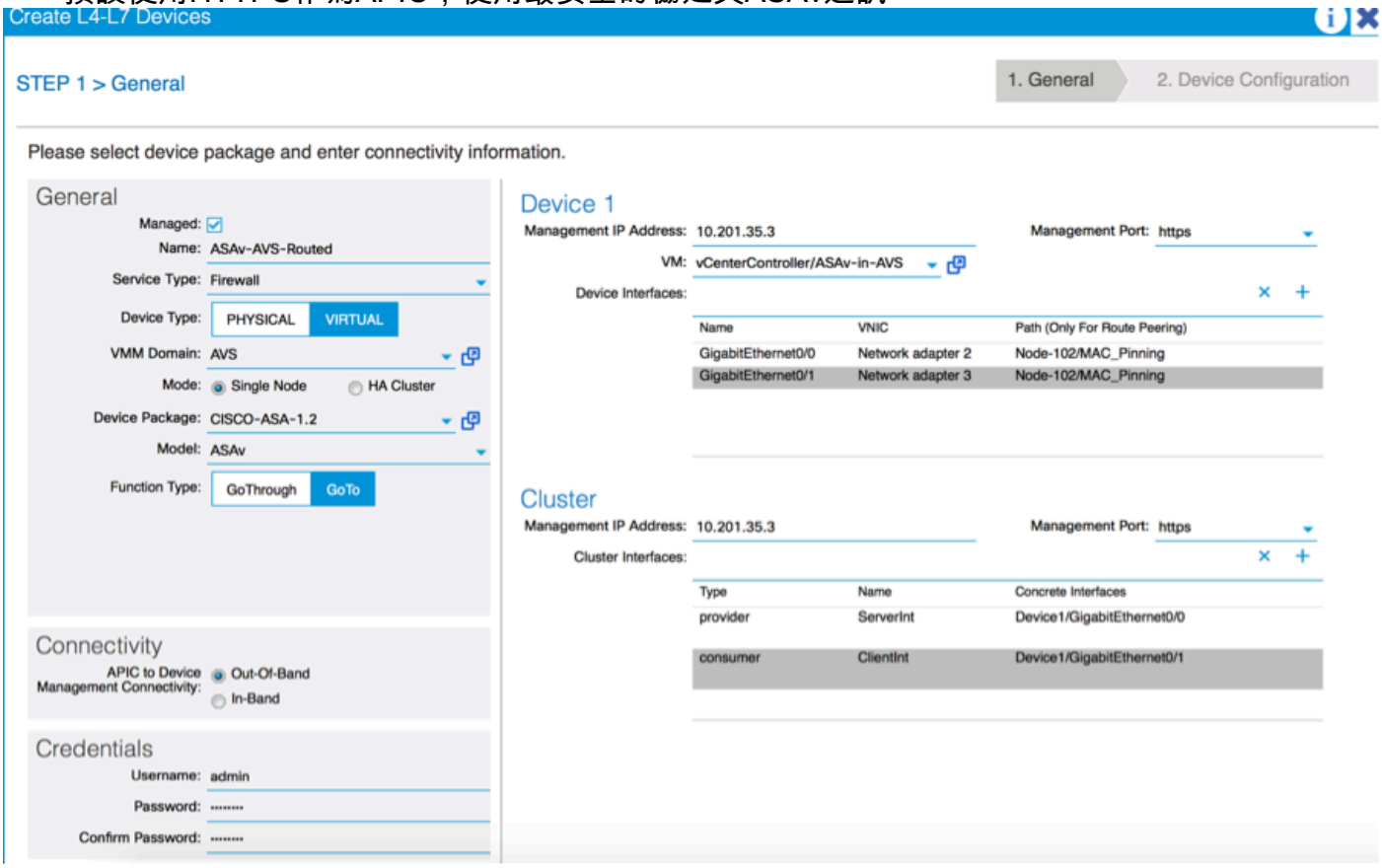
— 通過單個節點連線到AVS域

-ASAv型號

— 路由模式(GoTo)

— 管理地址（必須與之前分配給Mgmt0/0介面的地址匹配）

- 預設使用HTTPS作為APIC，使用最安全的協定與ASAv通訊



- 正確定義裝置介面和集群介面對於成功部署至關重要

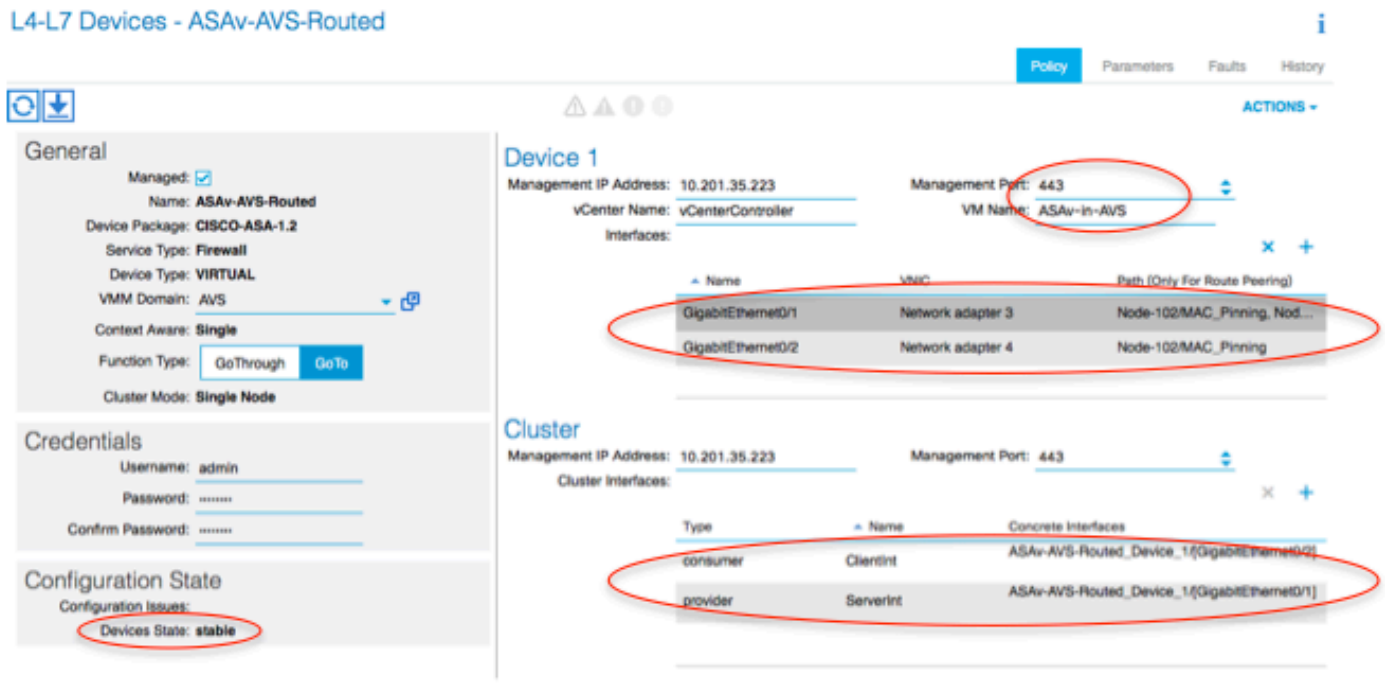
對於第一部分，使用前面部分中顯示的表2，將網路介面卡ID與您要使用的ASAv介面ID正確匹配。路徑是指允許進出防火牆介面的物理埠、埠通道或VPC。在這種情況下，ASA位於ESX主機中，其中兩個介面的傳入和傳出相同。在物理裝置中，防火牆(FW)的內部和外部將是不同的物理埠。

在第二部分中，必須始終定義群集介面（即使未使用群集HA），這是因為，對象模型在**mIf介面（裝置包上的元介面）、LIf**介面（葉介面，如外部、內部、內部等）和**CIf**（具體介面）之間存在關聯。 必須在裝置集群配置中配置L4-L7具體裝置，該抽象稱為邏輯裝置。邏輯裝置具有對映到具體裝置上的具體介面的邏輯介面。

在本示例中，將使用以下關聯：

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

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

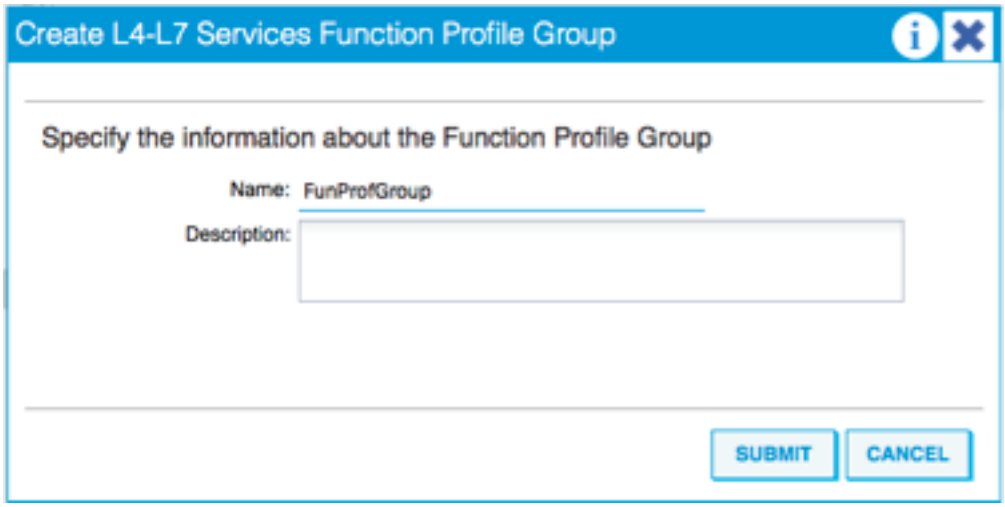


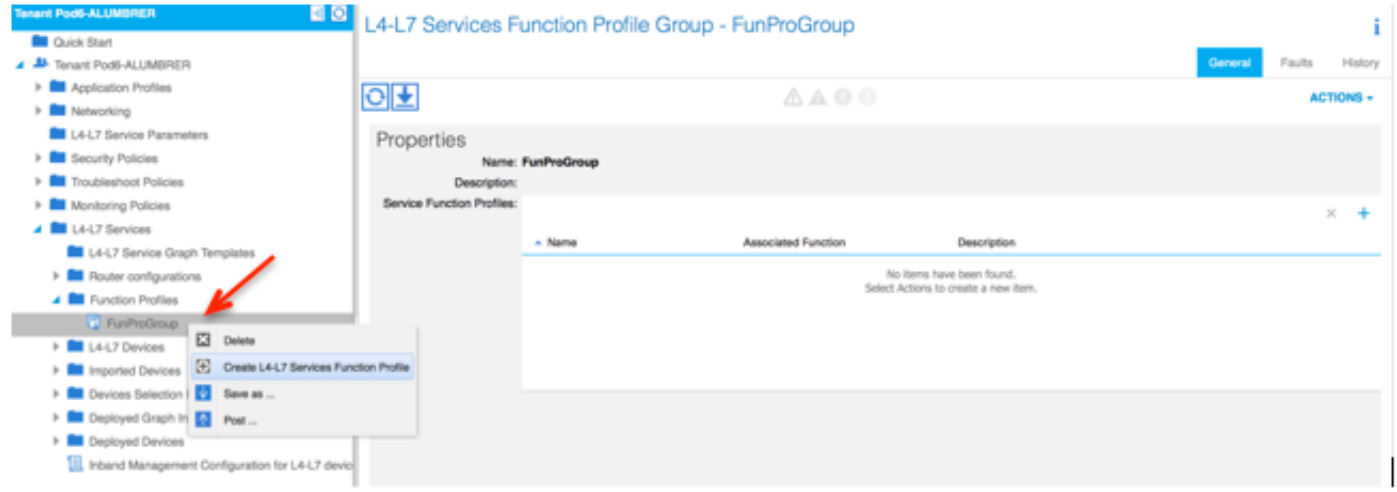
附註：對於故障切換/HA部署，GigabitEthernet 0/8已預配置為故障切換介面。

裝置狀態應為「穩定」，並且您應準備好部署功能配置檔案和服務圖模板

服務圖廊

首先，為ASAv建立功能配置檔案，但在此之前，您需要在該資料夾下建立功能配置檔案組，然後建立L4-L7服務功能配置檔案，如下圖所示：

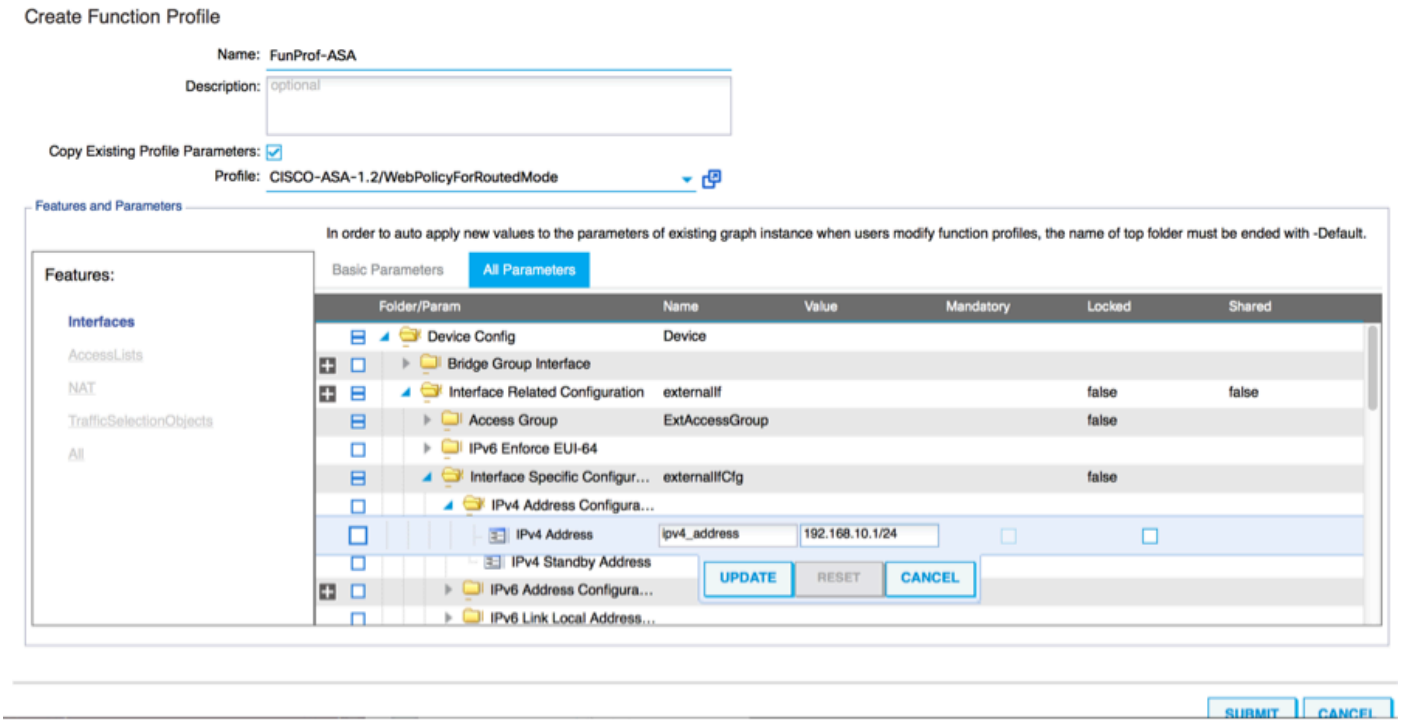




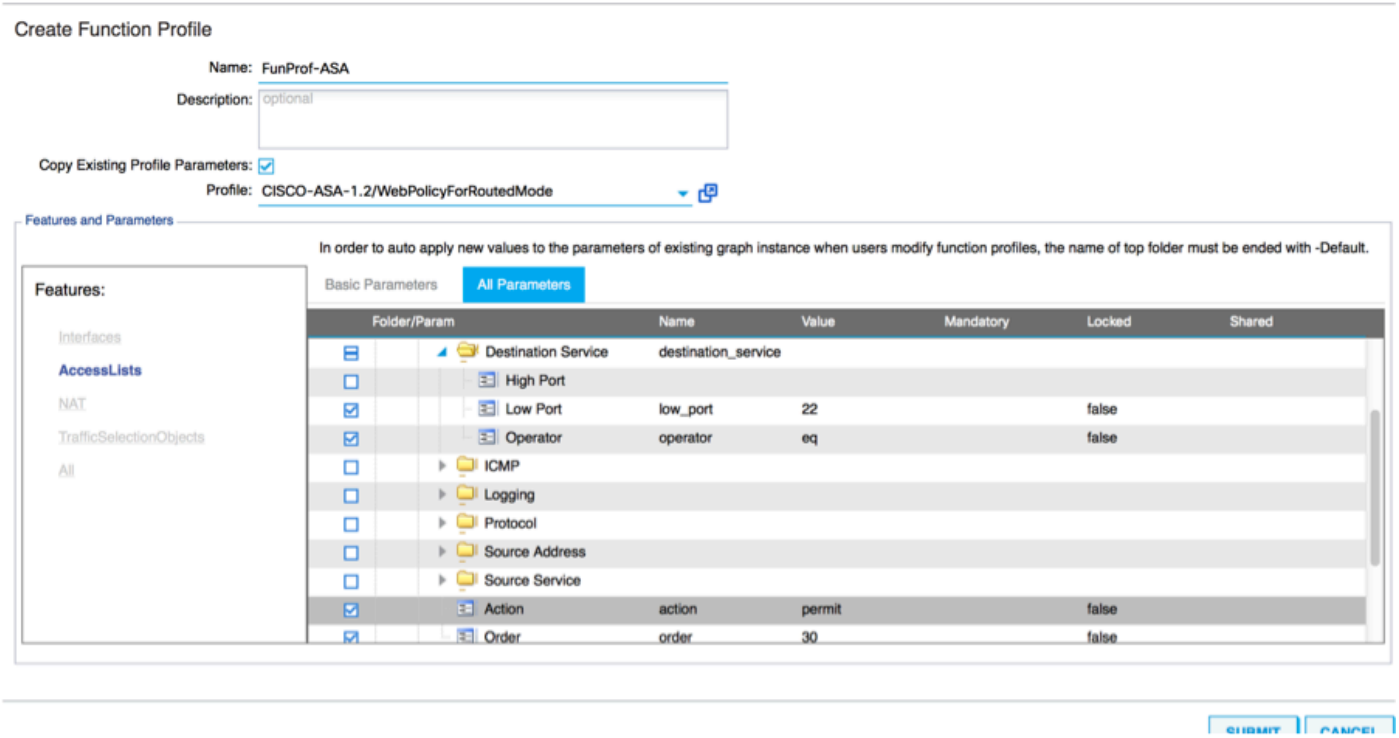
- 從下拉選單中選擇**WebPolicyForRoutedMode** Profile，然後繼續配置防火牆上的介面。從現在起，這些步驟是可選的，以後可以實施/修改。這些步驟可以在部署的幾個不同階段執行，具體取決於服務圖的可重複使用或自定義方式。

在本練習中，路由防火牆（轉到模式）要求每個介面都有一個唯一的IP地址。標準ASA配置還具有介面安全級別（外部介面不太安全，內部介面更安全）。 您也可以根據需要更改介面名稱。本示例中使用預設值。

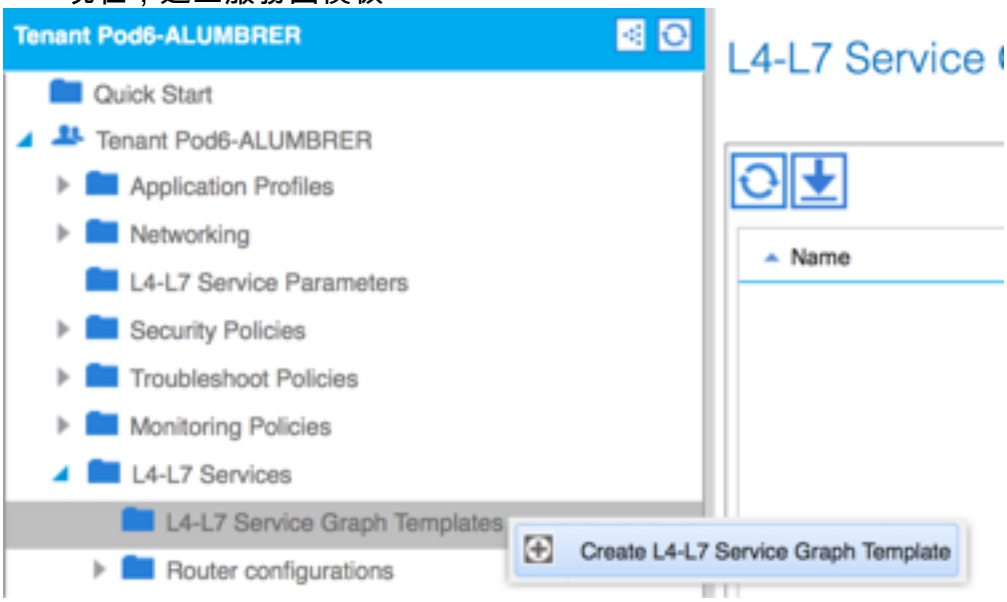
- 展開Interface Specific Configuration，為ServerInt新增IP地址和安全級別，對於IP地址**x.x.x.x/y.y.y.y或x.x.x.x/yy，格式如下**。對ClientInt介面重複此過程。



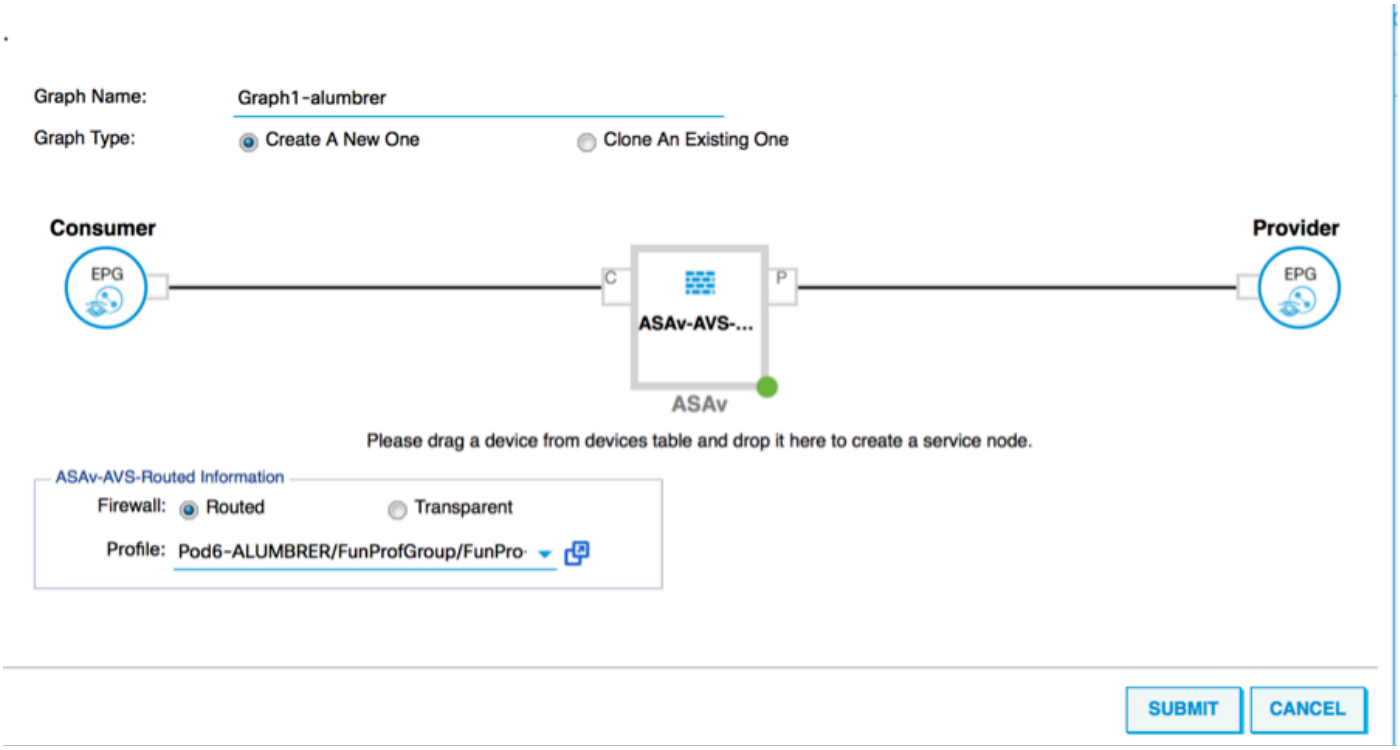
附註：您還可以修改預設訪問清單設定並建立自己的基本模板。預設情況下，RoutedMode模板將包含HTTP和HTTPS規則。在本練習中，SSH和ICMP將新增到允許的外部訪問清單。



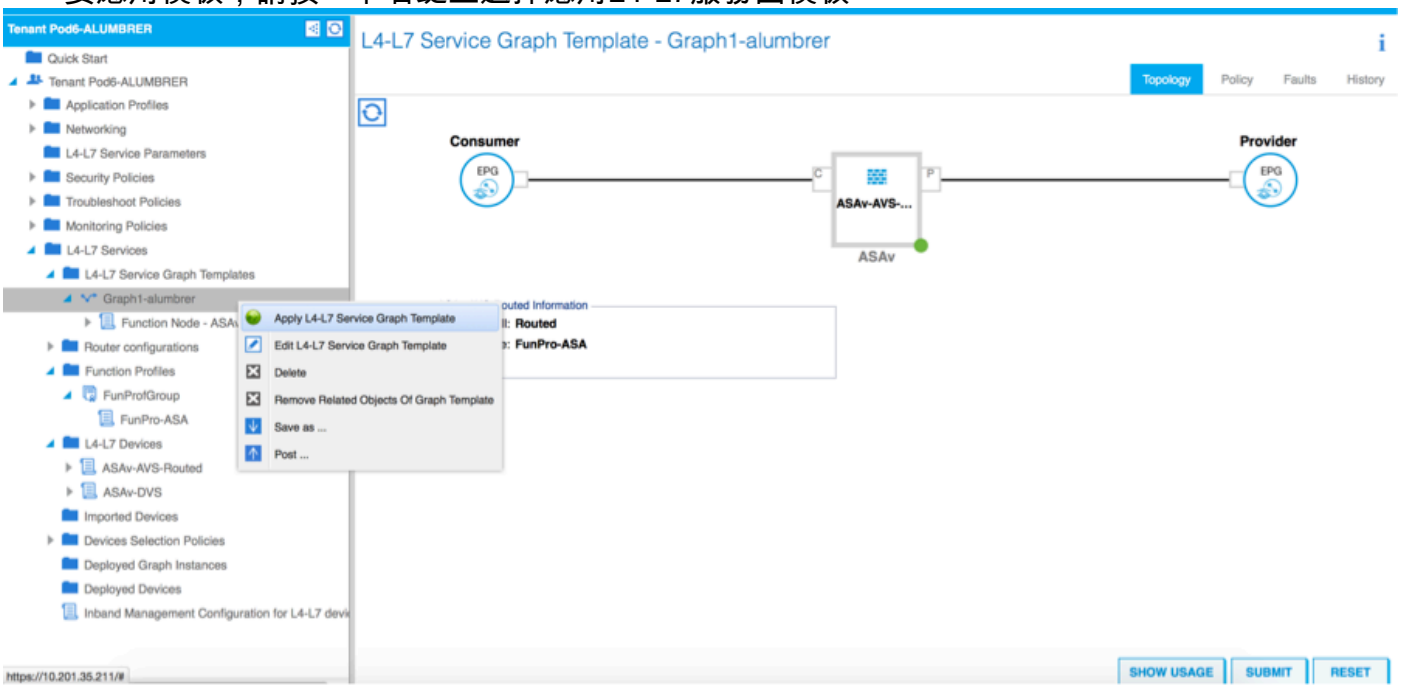
- 然後點選**提交**
- 現在，建立服務圖模板



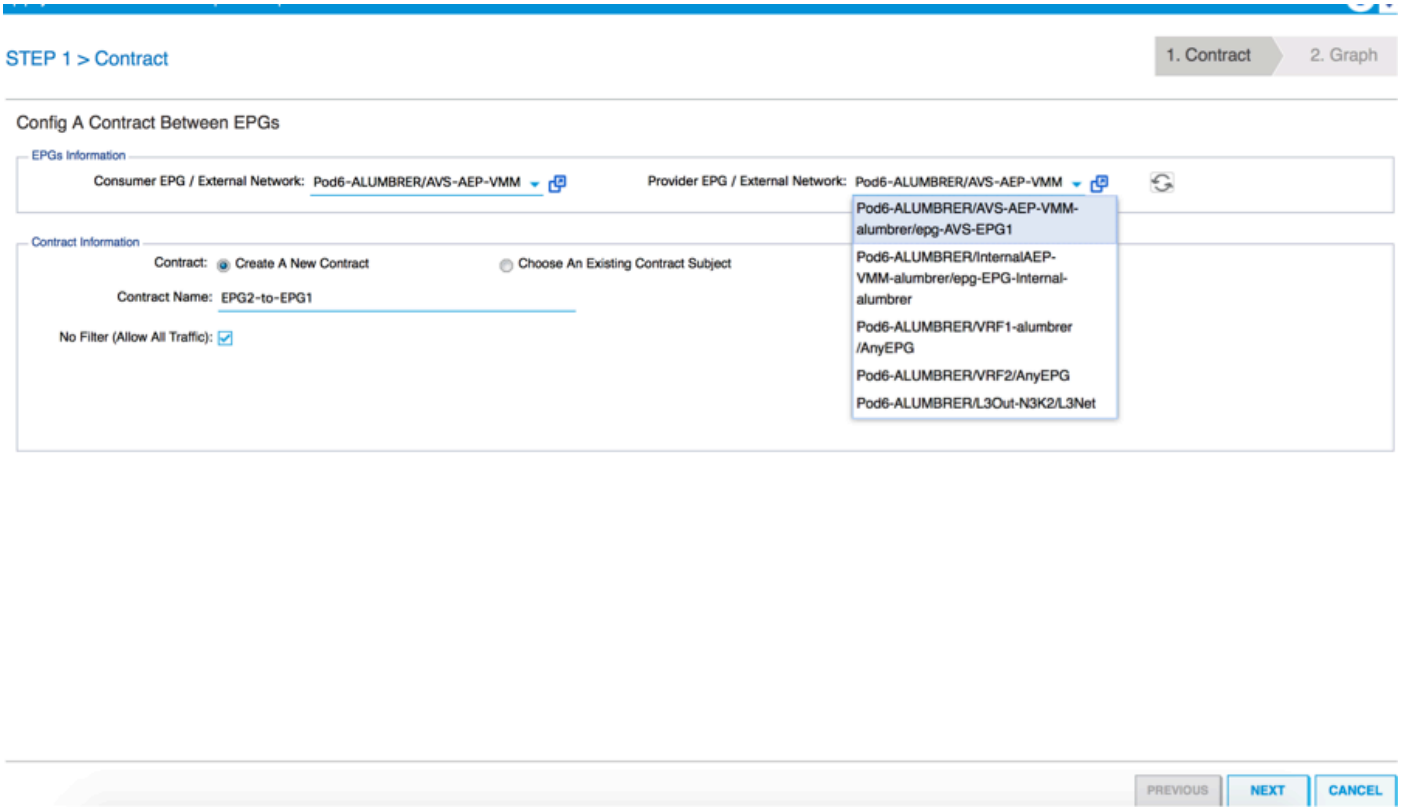
- 將裝置集群拖放到右側，形成消費者和提供商之間的關係，選擇路由模式和先前建立的功能配置檔案。



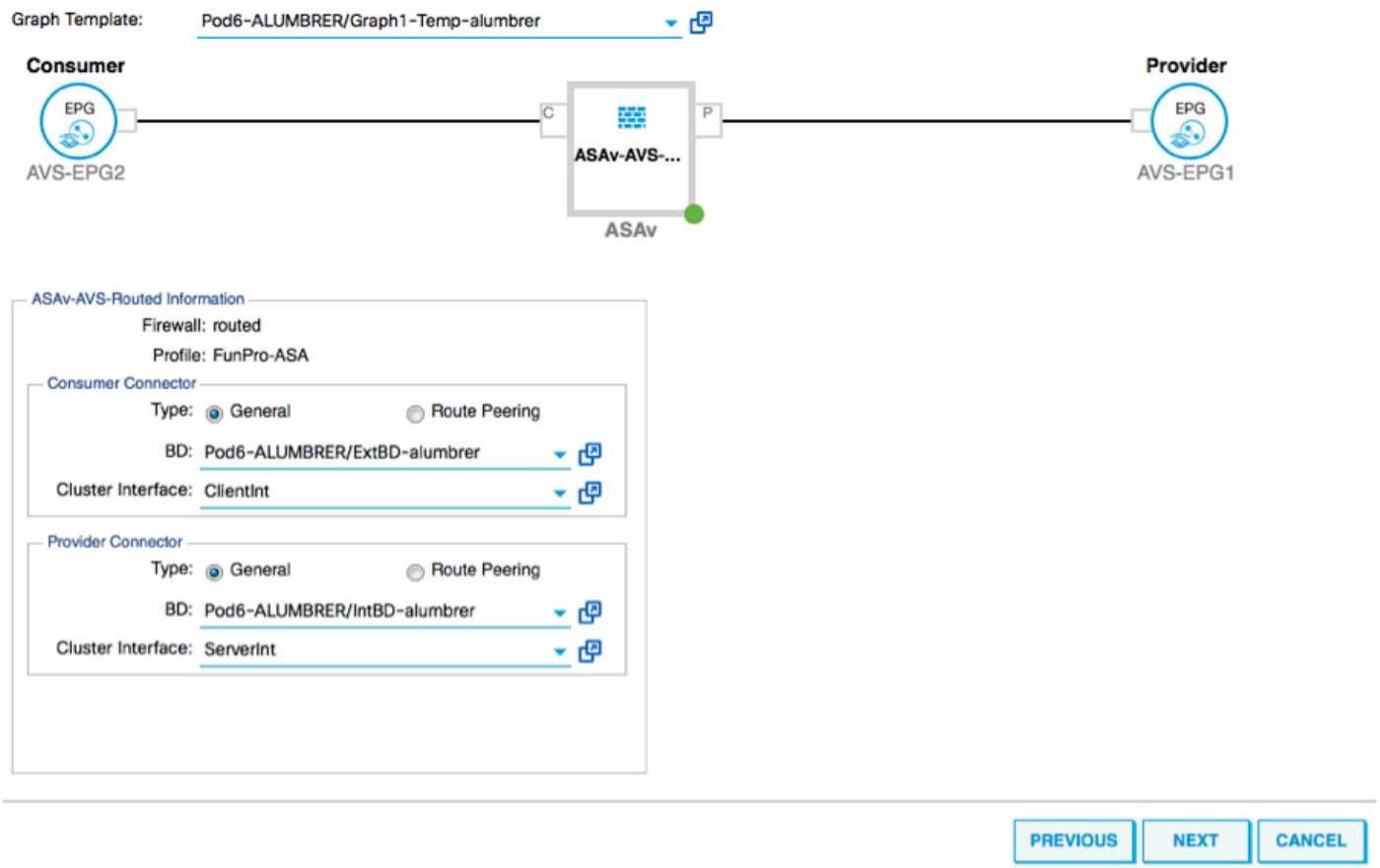
- 檢查模板是否有故障。模板建立為可重複使用，然後必須將其應用於特定EPG等。
- 要應用模板，請按一下右鍵並選擇應用L4-L7服務圖模板



- 定義哪個EPG將位於消費方和提供方側。在本練習中，AVS-EPG2是消費者（客戶端），AVS-EPG1是提供商（伺服器）。 請記住，未應用任何過濾器，這將允許防火牆根據此嚮導的最後一部分中定義的訪問清單執行所有過濾。
- 按一下**下一步**

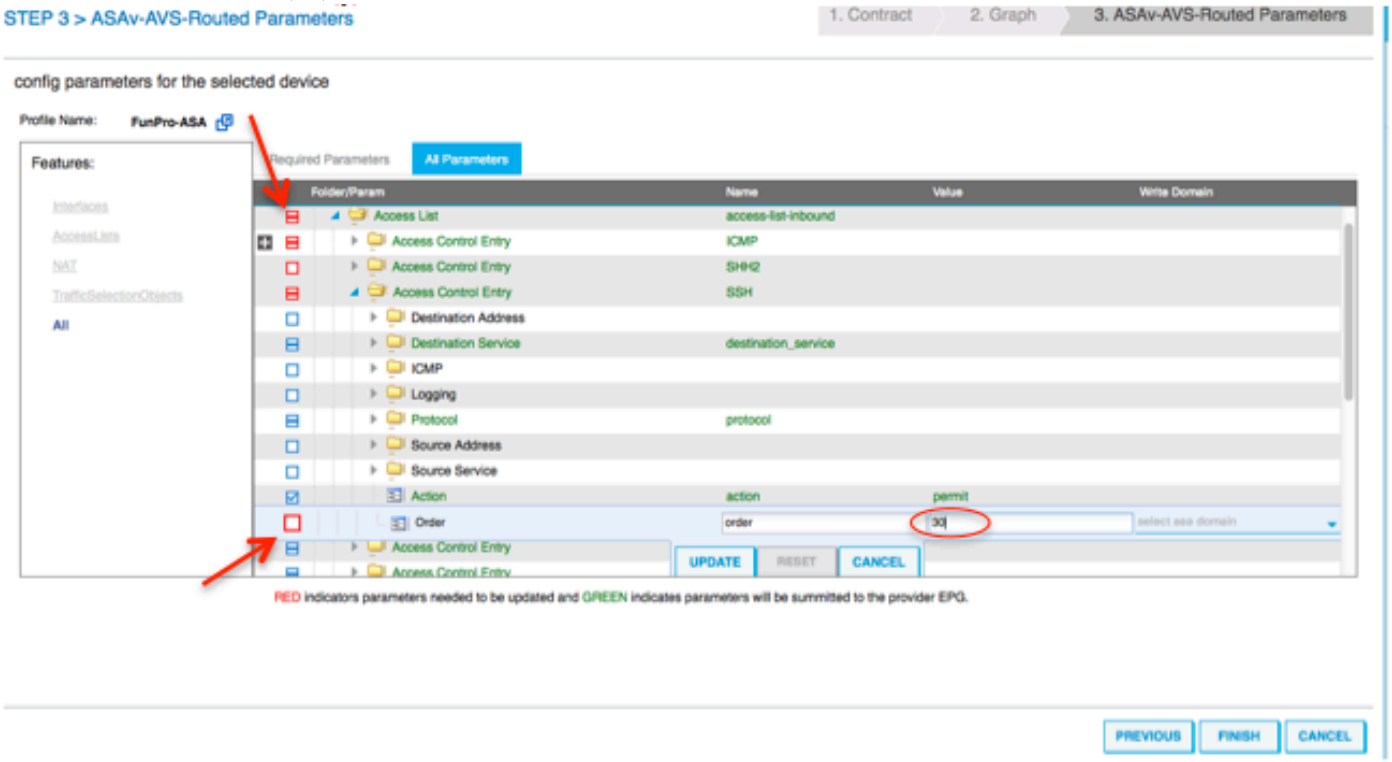


- 驗證每個EPG的BD資訊。在這種情況下，EPG1是IntBD DB上的提供商，EPG2是BD ExtBD上的消費者。EPG1將在防火牆介面ServerInt上連線，EPG2將在介面ClientInt上連線。兩個FW介面將成為每個EPG的DG，因此流量始終被迫通過防火牆。
- 按一下**下一步**

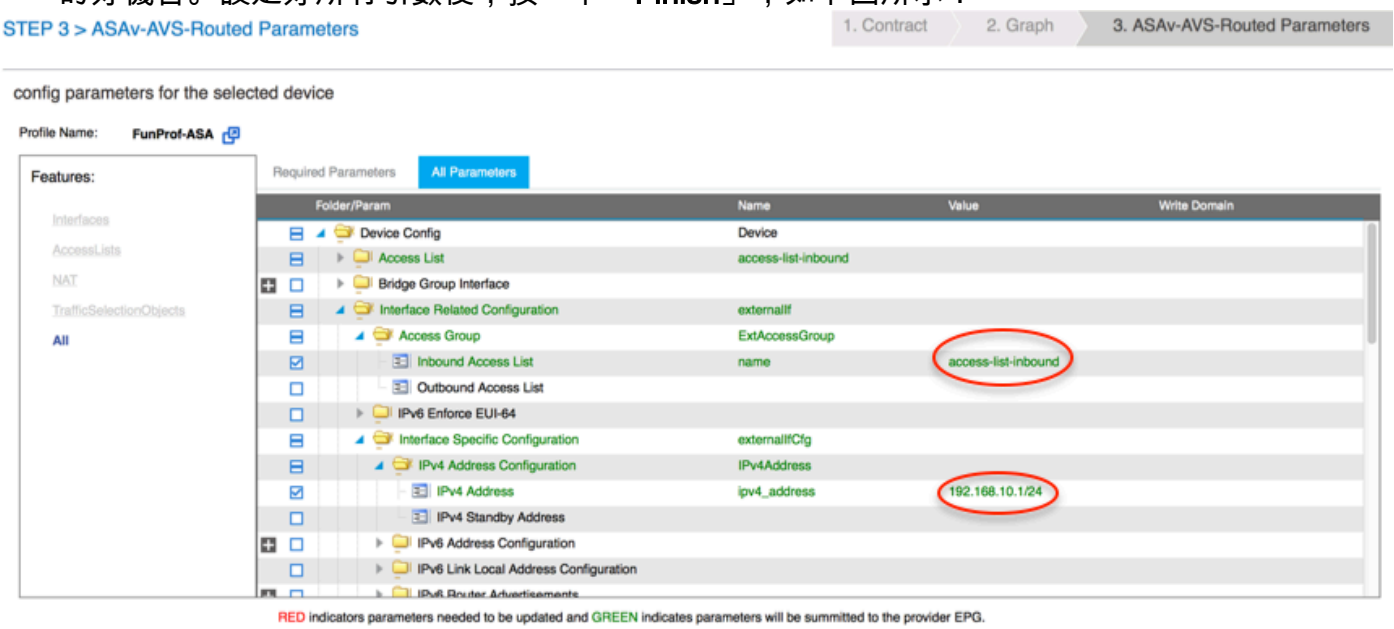


- 在Config Parameters部分，按一下**All Parameters**，並驗證是否有需要更新/配置的RED指示燈。在輸出中（如圖所示），可以看到存取清單上的順序遺漏。這等效於您將在show ip access-

list X中看到的行順序。



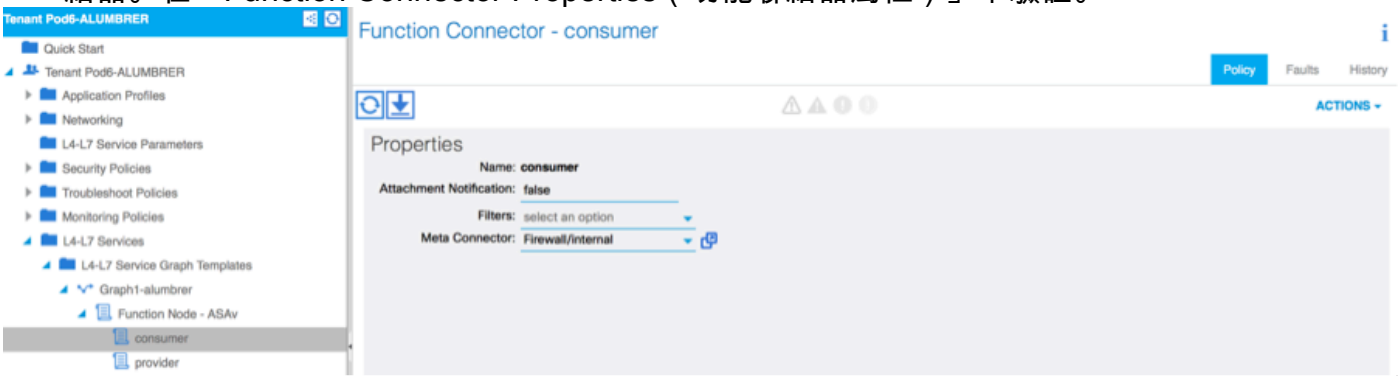
- 您也可以驗證從前面定義的功能配置檔案中分配的IP編址，如果有需要，這裡是一個更改資訊的好機會。設定好所有引數後，按一下「**Finish**」，如下圖所示：



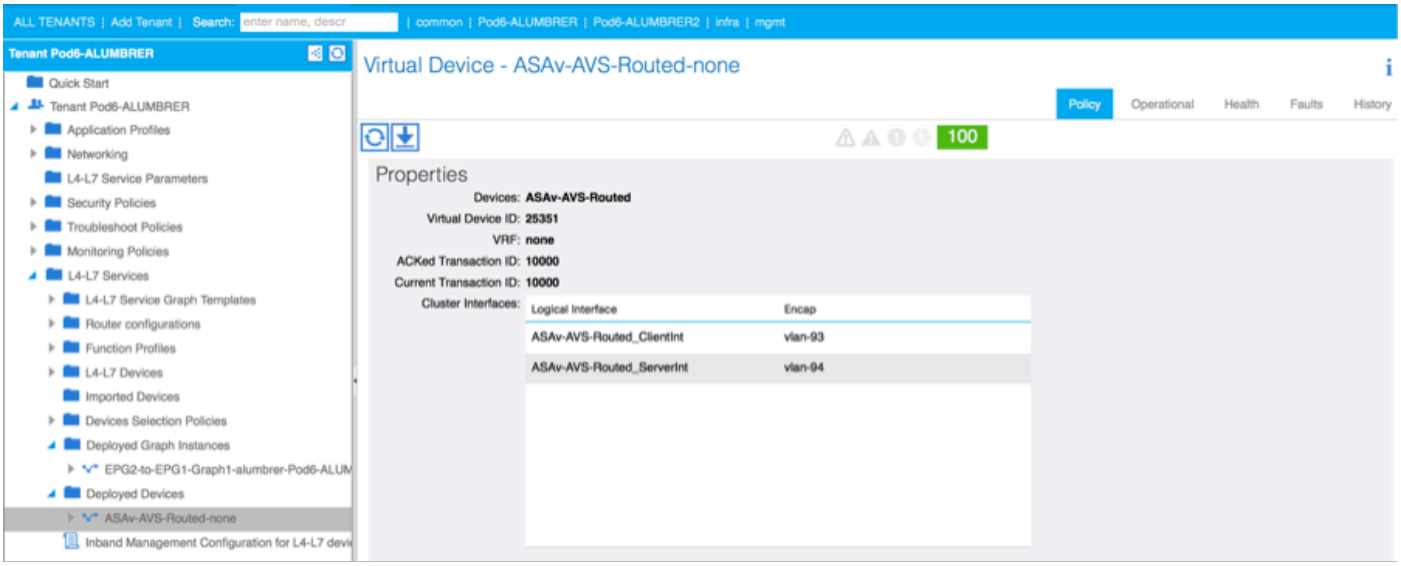
- 如果一切正常，應顯示新的已部署裝置和圖形例項。

驗證

- 建立「服務」圖形後需要驗證的一個重要事項是，建立消費者/提供商關係時使用了正確的元聯結器。在「Function Connector Properties（功能聯結器屬性）」下驗證。



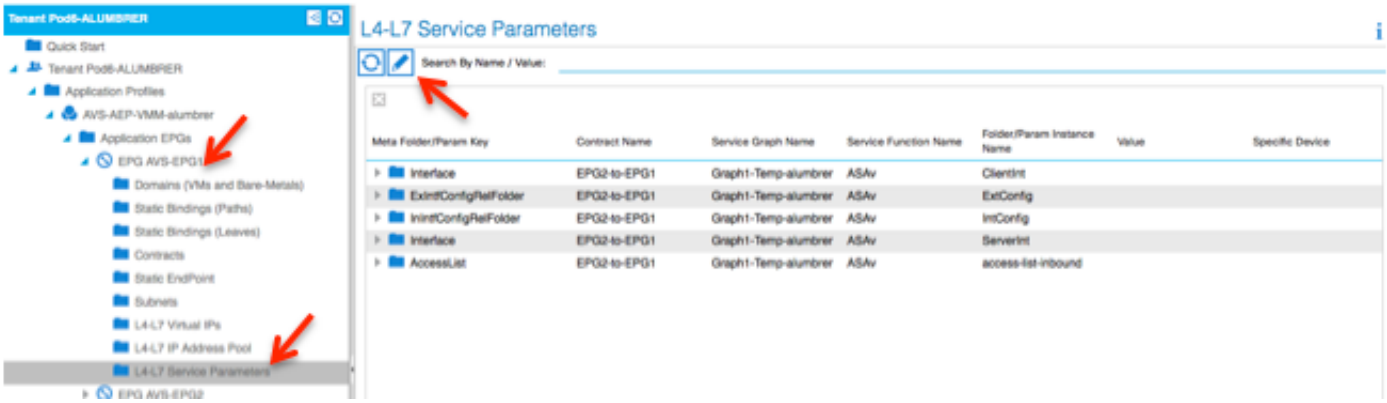
附註：從AVS動態池為防火牆的每個介面分配一個encap-vlan。驗證沒有故障。



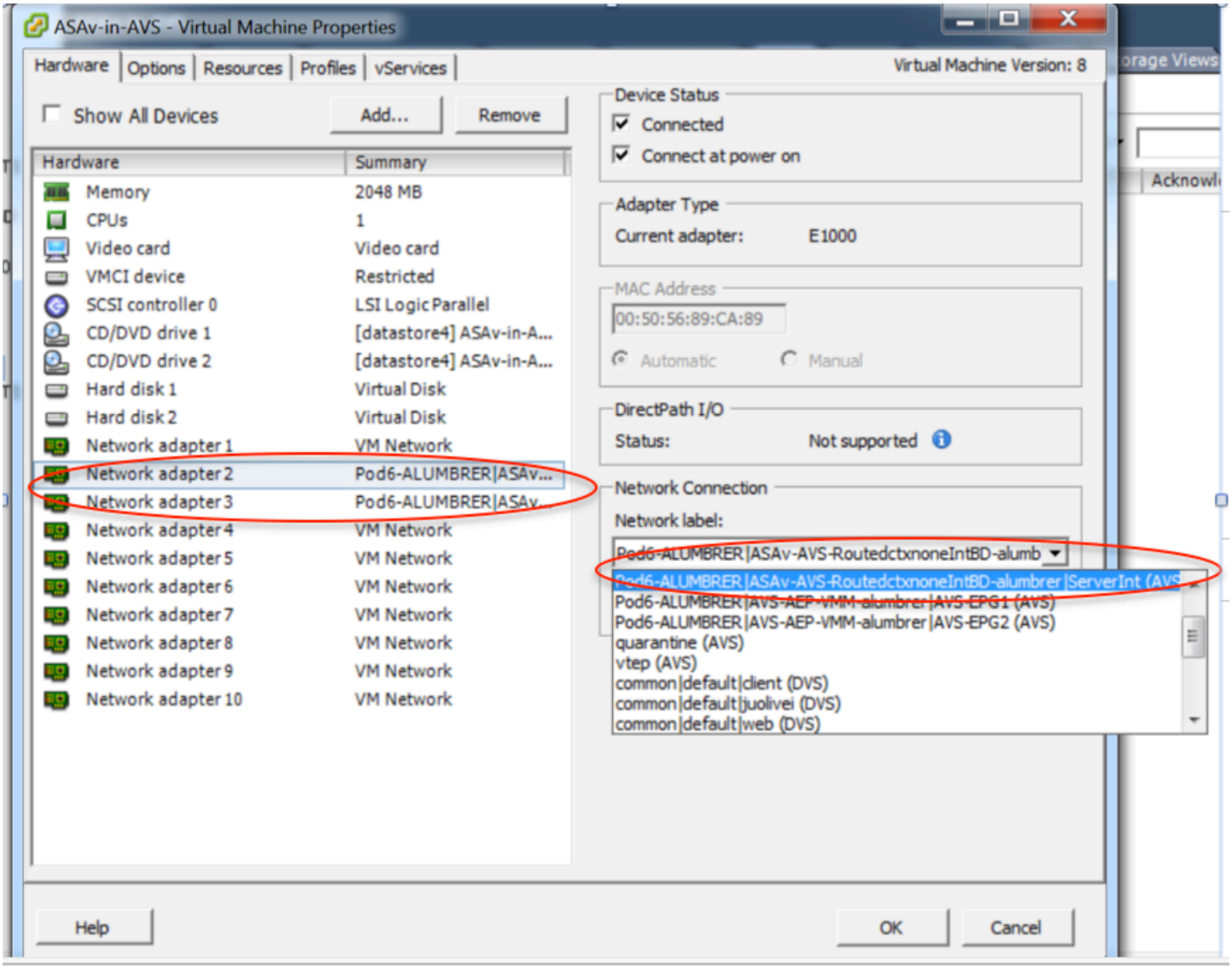
- 現在，您還可以驗證推送到ASAv的資訊

```
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#
```

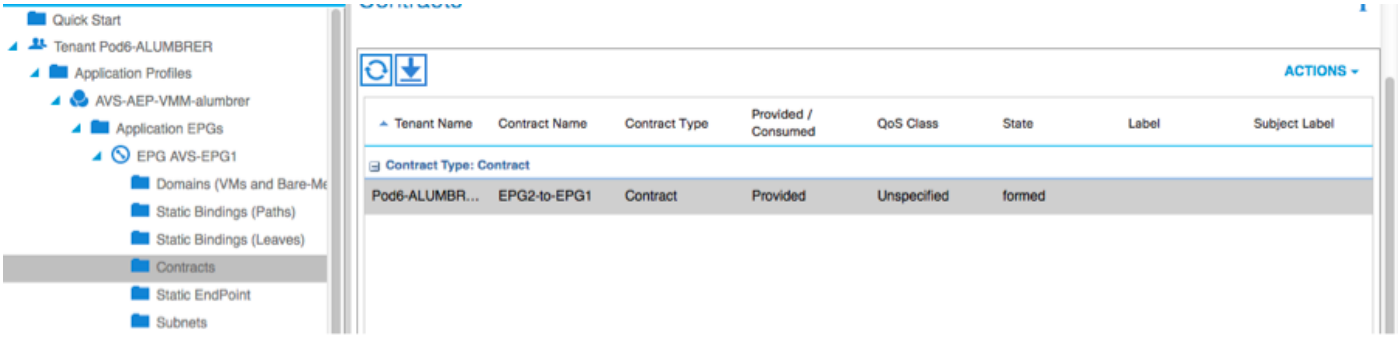
- 新合約在EPG下分配。從現在起，如果您需要修改訪問清單中的任何內容，則必須使用提供程式EPG的第4-7層服務引數完成更改。



- 在vCenter上，您還可以驗證影子EPG已分配到每個防火牆介面：



在本測試中，我讓2個EPG與標準合約進行通訊，這些2個EPG位於不同的域和不同的VRF中，因此先前已配置它們之間的路由洩漏。在插入服務圖後，當防火牆在2個EPG之間設定路由和過濾時，這可以簡化一些操作。以前在EPG和BD下配置的DG現在與合約一樣被刪除。只有L4-L7推行的合約應保留在EPG下。



刪除標準合約後，您可以確認流量現在流經ASAv，每次客戶端向伺服器傳送請求時，命令show access-list應顯示規則的命中計數，該計數將遞增。

```
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# _
```

在枝葉上，應該學習客戶端、伺服器VM以及ASAv介面的終端

```
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                                                      0050.5689.fa08 L                  eth1/7
Pod6-ALUMBRER:VRF1-alumbrer          Server IP          vlan-98        192.168.10.10 L
25                                   & MAC              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                   Client IP &        vlan-97          172.16.1.10 L
26                                   MAC                vlan-93        0050.5689.e7dd L                  po4
Pod6-ALUMBRER:VRF2                                      vlan-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                  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
```

FW interface (ServerInt)

FW interface (ClientInt)

檢視連線到VEM的兩個防火牆介面。

ESX-1

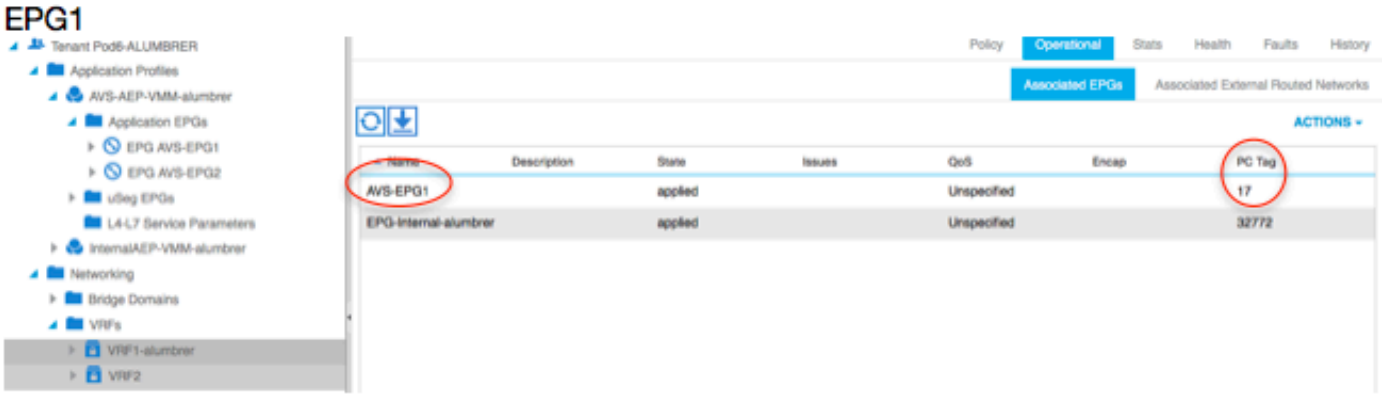
```
~ # vemcmd show port vlan
  LTL   VSM Port  Admin Link  State   Cause  PC-LTL  SGID  ORG  svcpath  Type    Vem Port
   22     Eth1/5     UP   UP    FWD       -    1040     4    0        0               vmnic4
   23     Eth1/6     UP   UP    FWD       -    1040     5    0        0               vmnic5
   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
~ #
```

最後，如果知道源EPG和目標EPG的PC標籤，也可以在枝葉級別驗證防火牆規則：

EPG1



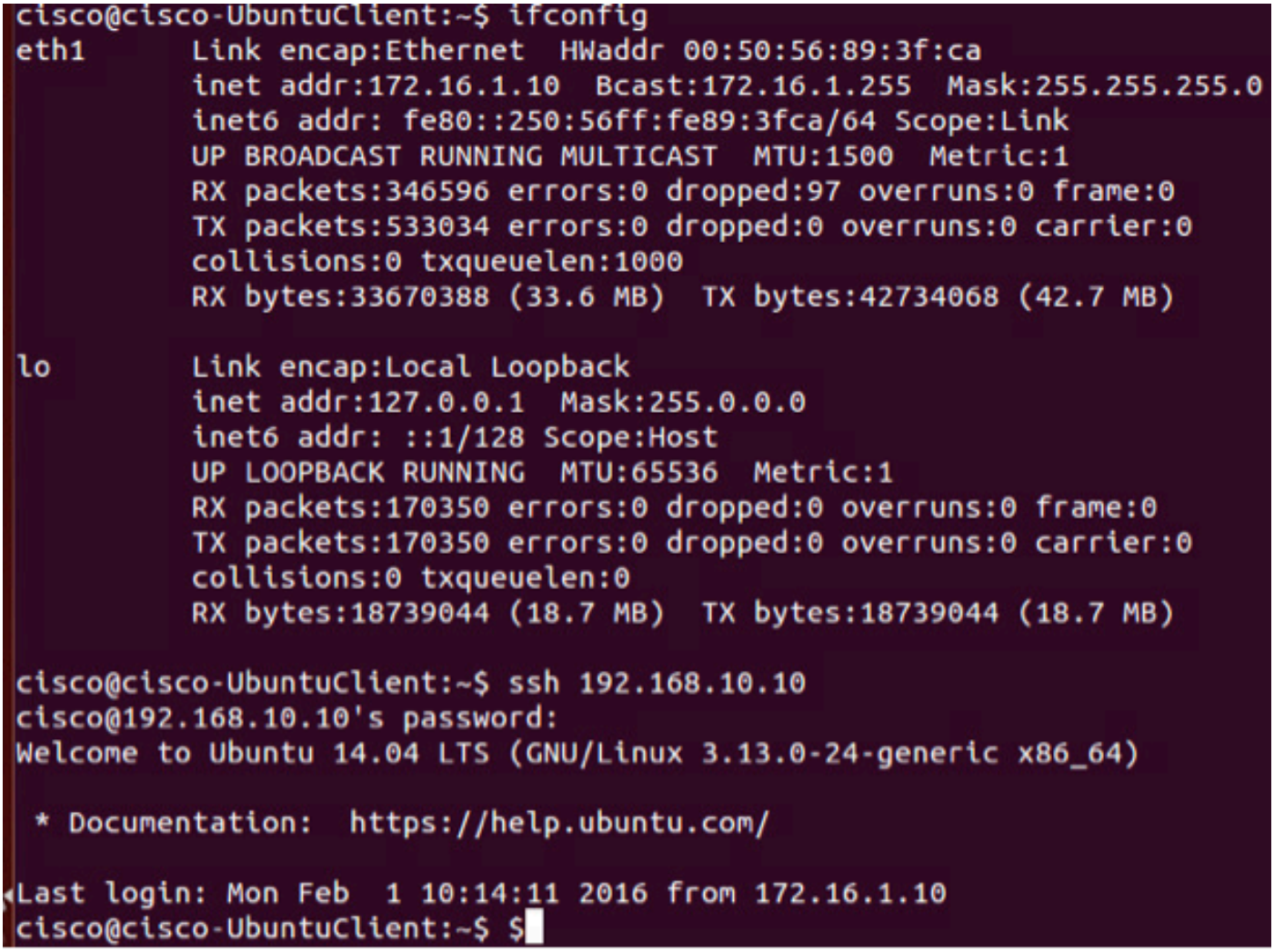
EPG2

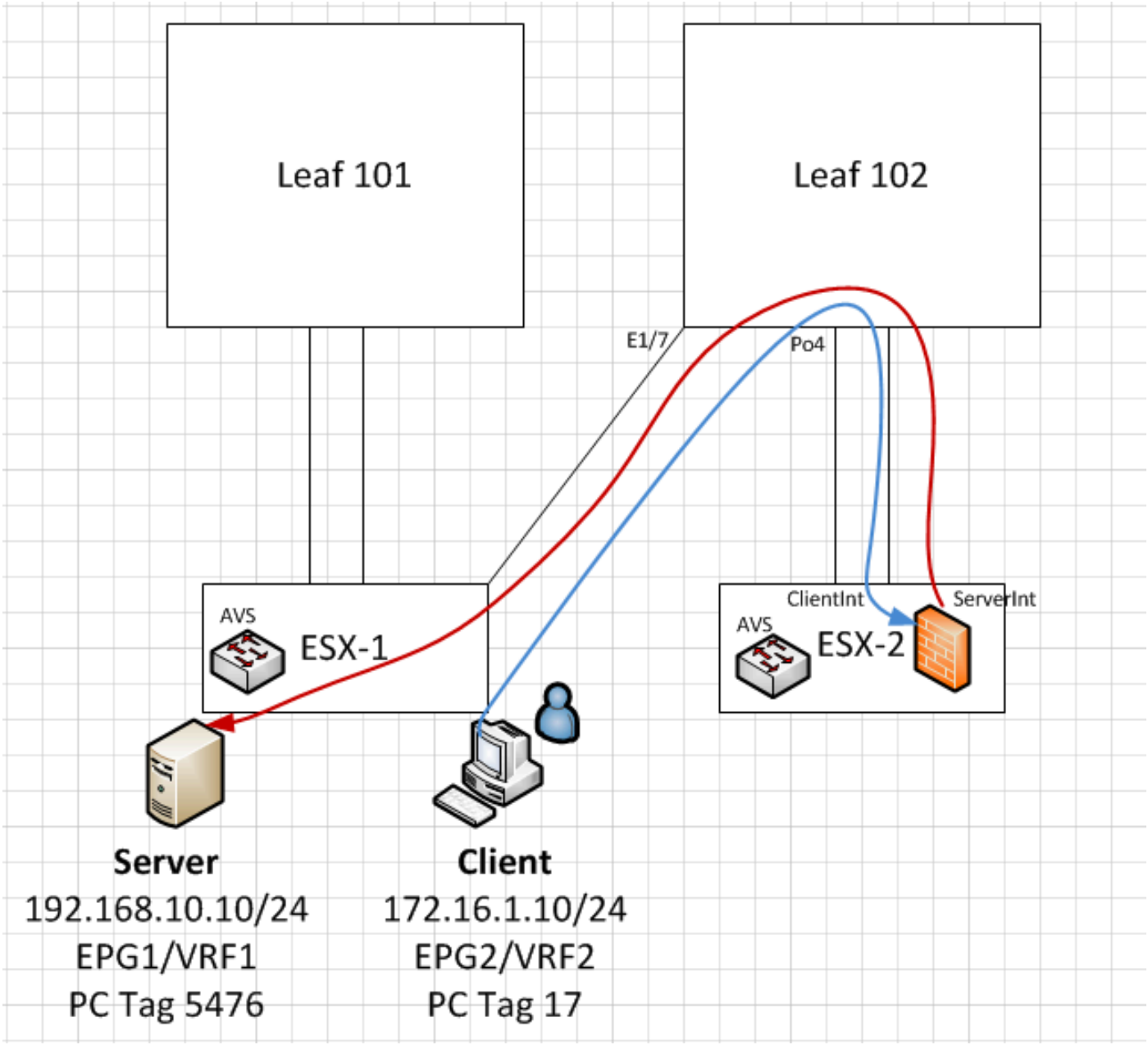
可以將篩選器ID與枝葉上的PC標籤匹配以驗證FW規則。

```
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#
```

> **附註**：EPG PCTags/Sclass從不直接通訊。通過L4-L7服務圖插入建立的影子EPG中斷通訊或將通訊捆綁在一起。

Client to Server通訊正常。

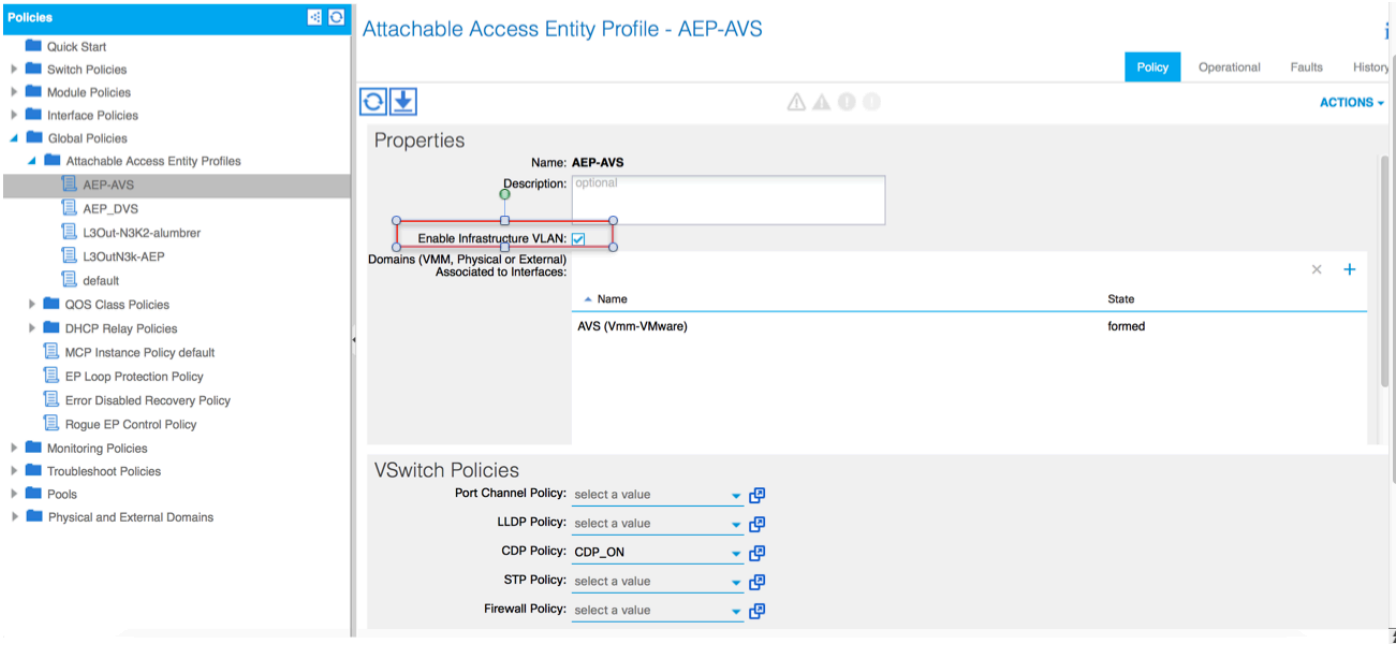

cisco@cisco-UbuntuClient:~$ ifconfig
eth1 Link encap:Ethernet HWaddr 00:50:56:89:3f:ca
inet addr:172.16.1.10 Bcast:172.16.1.255 Mask:255.255.255.0
inet6 addr: fe80::250:56ff:fe89:3fca/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:346596 errors:0 dropped:97 overruns:0 frame:0
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:~$ $



疑難排解

未分配VTEP地址

驗證是否已在AEP下檢查基礎架構VLAN:



不支援的版本

驗證VEM版本是否正確並支援適當的ESXi VMWare系統。

```
~ # 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和交換矩陣通訊不起作用

```
- 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
```

此時，可以確定ESXi主機和枝葉之間的交換矩陣通訊不能正常工作。可以在枝葉端檢查某些驗證命令以確定根本原因。

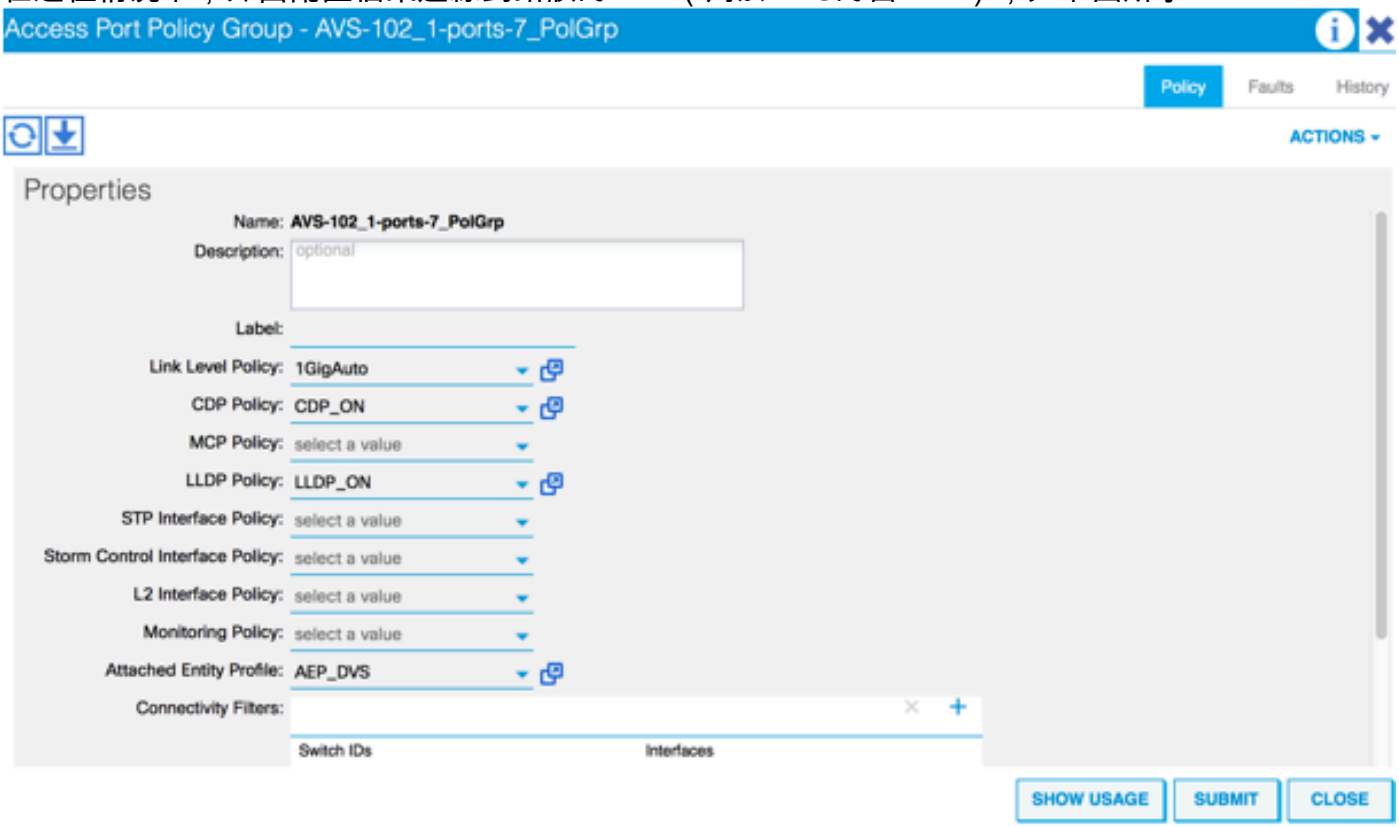
```
leaf2# show cdp ne

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)
```

通過Po5連線的ESXi中使用了2個埠

```
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
```

從上面的輸出中可以看到，Infra Vlan不允許通過，也不通過指向ESXi主機的上行鏈路埠(1/5-6)。這表示在APIC上配置了介面策略或交換機策略的配置錯誤。
檢查兩者：
Access Policies > Interface Policies > Profiles Access Policies > Switch Policies > Profiles
在這種情況下，介面配置檔案連線到錯誤的AEP（用於DVS的舊AEP），如下圖所示：



為AVS設定正確的AEP後，現在我們可以看到通過枝葉上的正確Unlinks（解除連結）可以看到Infra 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 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
```

相關資訊

應用程式虛擬交換機安裝

Cisco Systems， Inc.思科應用虛擬交換機安裝指南5.2(1)SV3(1.2)版
使用VMware部署ASAv

Cisco Systems， Inc.思科自適應安全虛擬裝置(ASAv)快速入門手冊9.4

Cisco ACI和Cisco AVS

Cisco Systems， Inc. Cisco ACI虛擬化指南，版本1.2(1i)

思科以應用為中心的基礎設施服務圖設計白皮書

思科以應用為中心的基礎設施服務圖設計白皮書

技術支援與文件 - Cisco Systems