ASAv en mode GoTo (L3) avec AVS- ACI 1.2(x) version

Contenu

Introduction

Ce document décrit comment déployer un commutateur AVS (Application Virtual Switch) avec un pare-feu ASAv (Adaptive Security Virtual Appliance) unique en mode routé/GOTO en tant que graphique de service L4-L7 entre deux groupes de terminaux (EPG) pour établir une communication client-serveur à l'aide de la version ACI 1.2(x).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Stratégies d'accès configurées et interfaces en service
- EPG, Bridge Domain (BD) et Virtual Routing and Forwarding (VRF) déjà configurés

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

Matériel et logiciels :

- 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)
- Leaf/Spines - 11.2(1i)
- Packages de périphériques *.zip déjà téléchargés

Fonctionnalités :

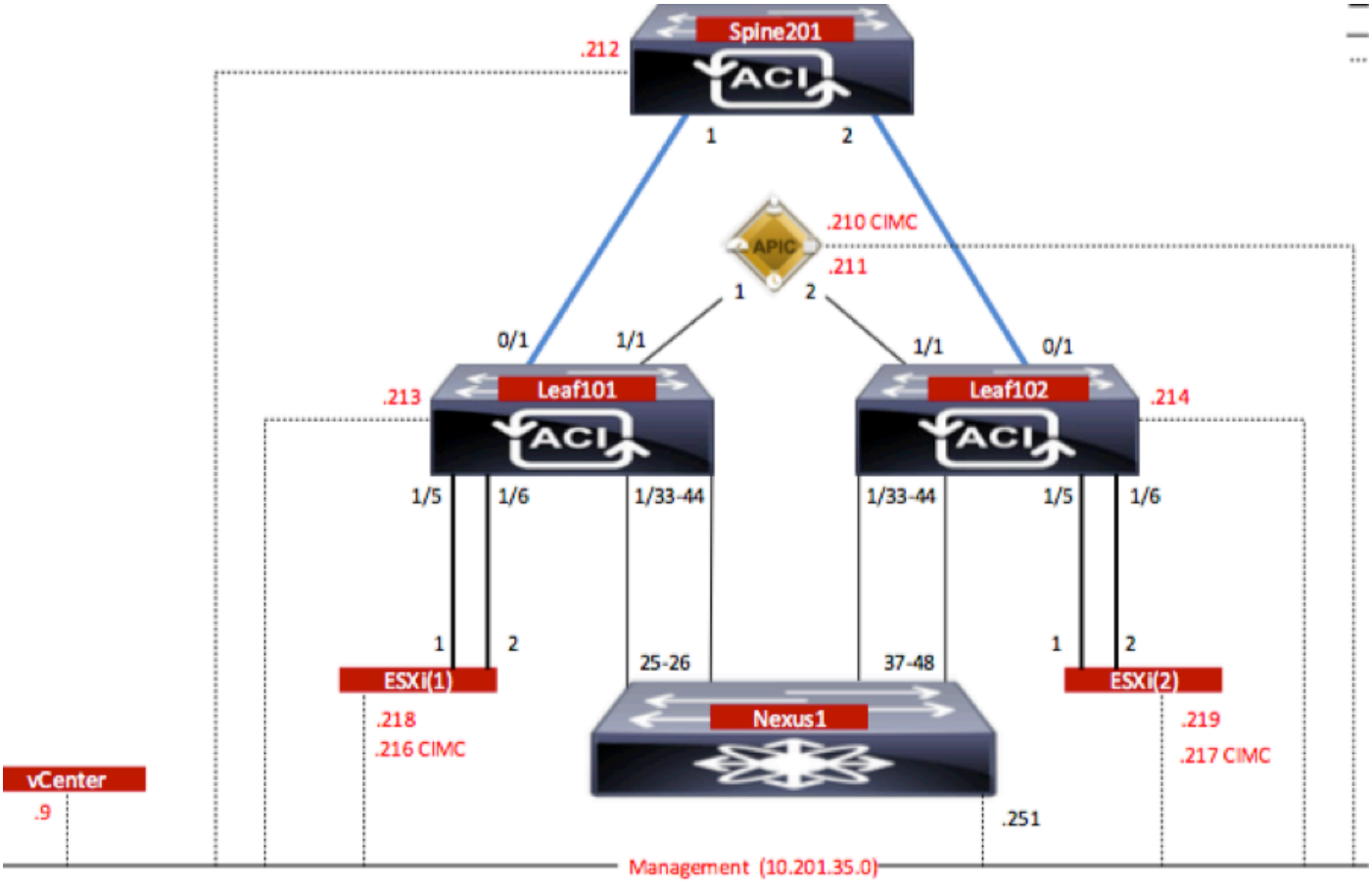
- AVS
- ASAv
- EPG, BD, VRF
- Liste de contrôle d'accès (ACL)
- Graphique des services L4-L7
- vCenter

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.

Configuration

Diagramme du réseau

Comme le montre l'image,



Configurations

La configuration initiale d'AVS crée un domaine VMware vCenter (intégration VMM)2

Note:

- Vous pouvez créer plusieurs data centers et entrées DVS (Distributed Virtual Switch) sous un

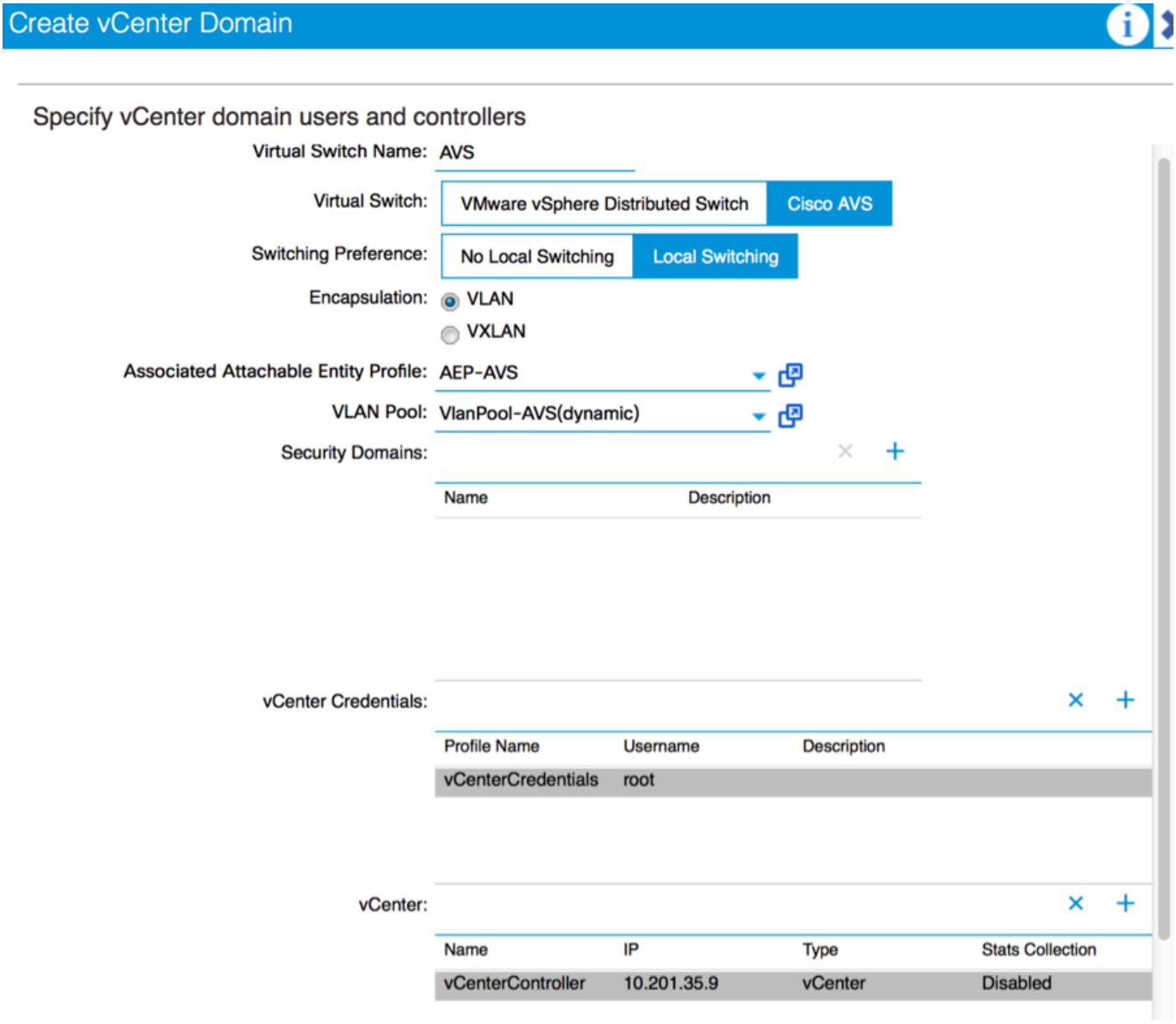
seul domaine. Cependant, un seul AVS Cisco peut être attribué à chaque data center.

- Le déploiement du graphique de services avec Cisco AVS est pris en charge à partir de Cisco ACI version 1.2(1i) avec Cisco AVS version 5.2(1)SV3(1.10). La configuration complète du graphique de service est effectuée sur le contrôleur Cisco APIC (Application Policy Infrastructure Controller).

- Le déploiement de la machine virtuelle de service (VM) avec Cisco AVS est pris en charge uniquement sur les domaines Virtual Machine Manager (VMM) avec le mode d'encapsulation VLAN (Virtual Local Area Networks). Cependant, les machines virtuelles de calcul (les machines virtuelles du fournisseur et du consommateur) peuvent faire partie de domaines VMM avec encapsulation VXLAN (Virtual Extensible LAN) ou VLAN.

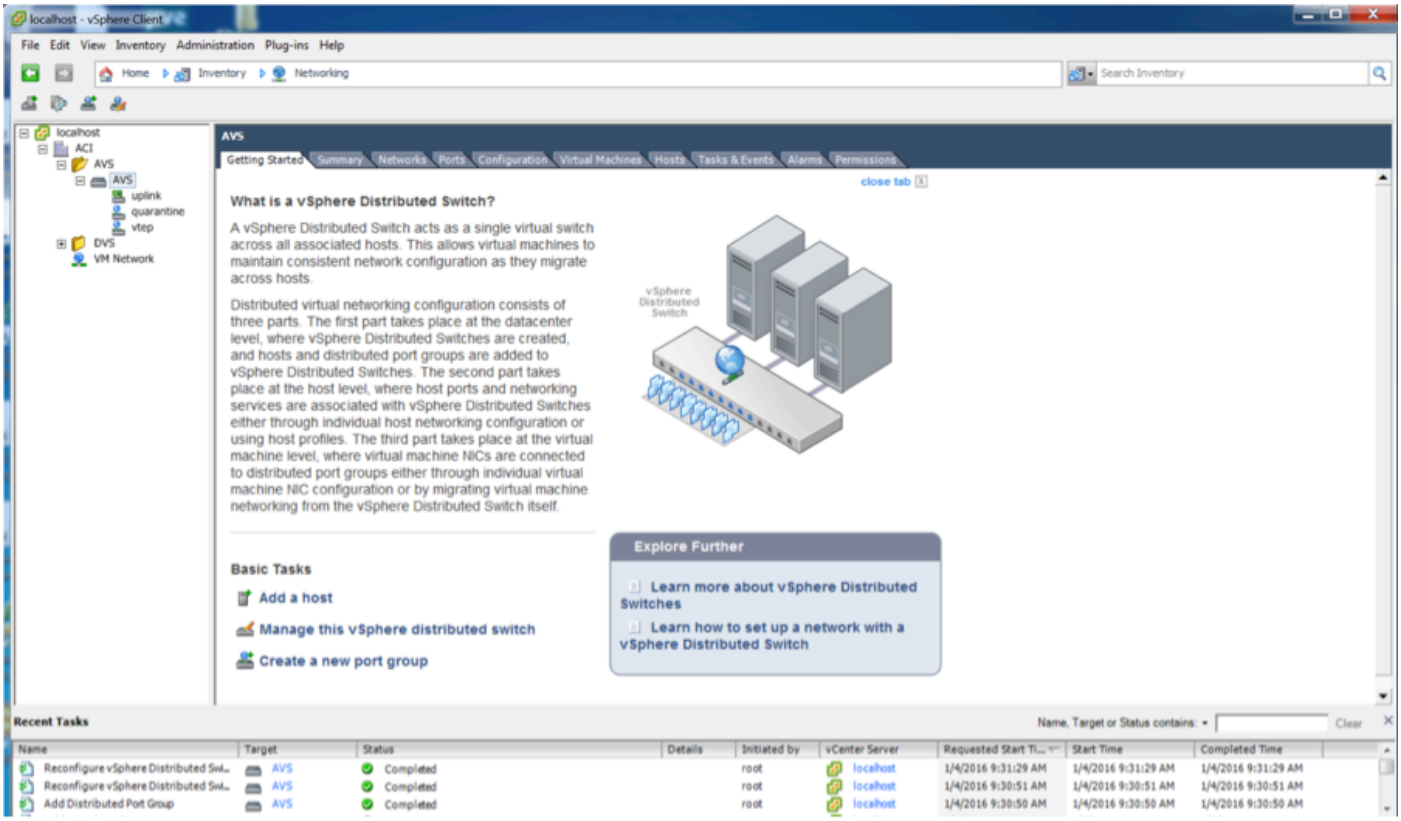
- Notez également que si la commutation locale est utilisée, l'adresse de multidiffusion et le pool ne sont pas requis. Si aucune commutation locale n'est sélectionnée, le pool de multidiffusion doit être configuré et l'adresse de multidiffusion de la structure AVS ne doit pas faire partie du pool de multidiffusion. Tout le trafic provenant de l'AVS sera encapsulé VLAN ou VXLAN.

Accédez à **Mise en réseau de VM > VMWare > Créer un domaine vCenter,** comme illustré dans l'image :

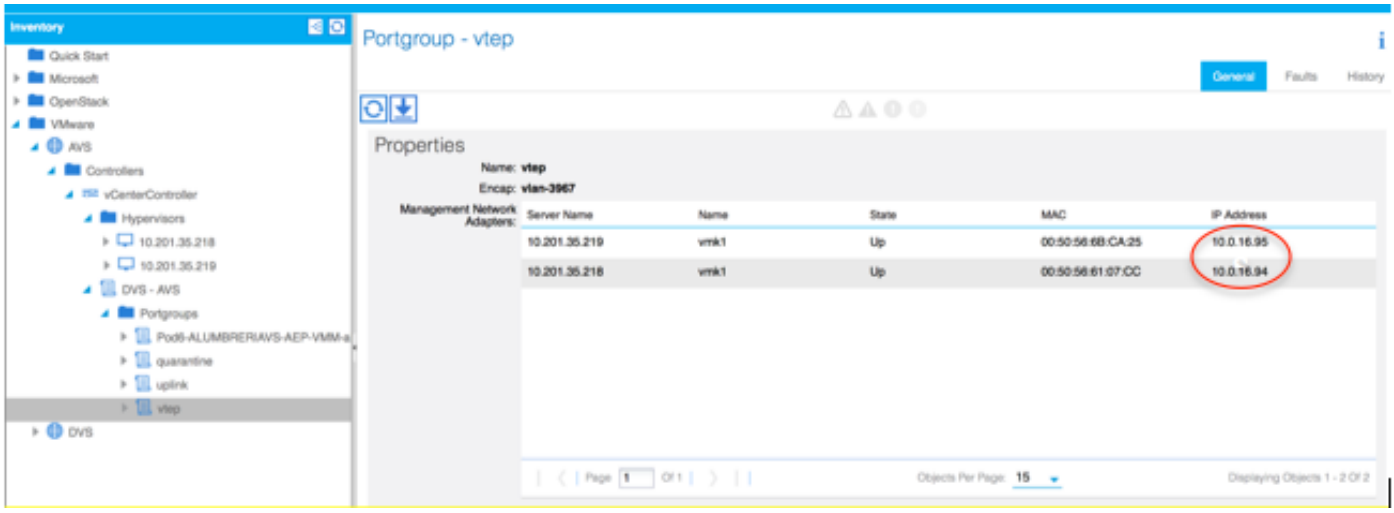


Si vous utilisez Port-Channel ou VPC (Virtual Port-Channel), il est recommandé de définir les stratégies vSwitch pour qu'elles utilisent Mac Pinning.

Après cela, APIC doit pousser la configuration du commutateur AVS vers vCenter, comme l'illustre l'image :



Sur APIC, vous pouvez remarquer qu'une adresse VTEP (VXLAN Tunnel Endpoint) est attribuée au groupe de ports VTEP pour AVS. Cette adresse est attribuée quel que soit le mode de connectivité utilisé (VLAN ou VXLAN)



Installer le logiciel Cisco AVS dans vCenter

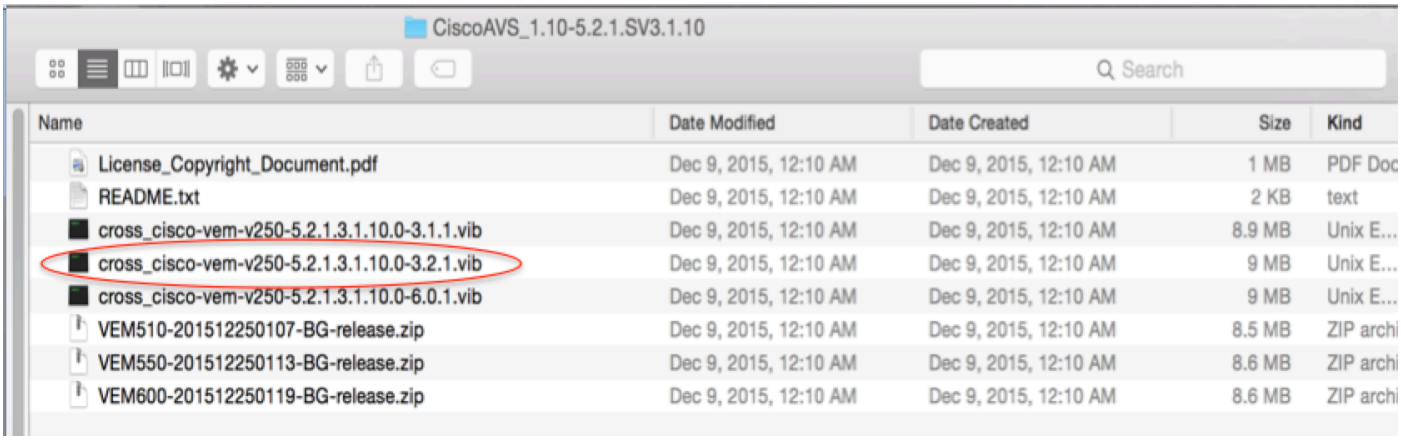
- Télécharger l'offre groupée d'installation vSphere (VIB) depuis CCO à l'aide de ce lien

  Remarque : dans ce cas, nous utilisons ESX 5.5, Tableau 1, qui présente la matrice de compatibilité pour ESXi 6.0, 5.5, 5.1 et 5.0

Tableau 1 - Compatibilité des versions du logiciel hôte pour ESXi 6.0, 5.5, 5.1 et 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

Dans le fichier ZIP, il y a 3 fichiers VIB, un pour chaque version d'hôte ESXi, sélectionnez celui qui convient à ESX 5.5, comme l'illustre l'image :



- Copier le fichier VIB dans le data store ESX - cela peut être fait via l'interface de ligne de commande ou directement à partir de vCenter

  Note: Si un fichier VIB existe sur l'hôte, supprimez-le à l'aide de la commande **esxcli software vib** remove.

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

ou en naviguant directement dans le Datastore.

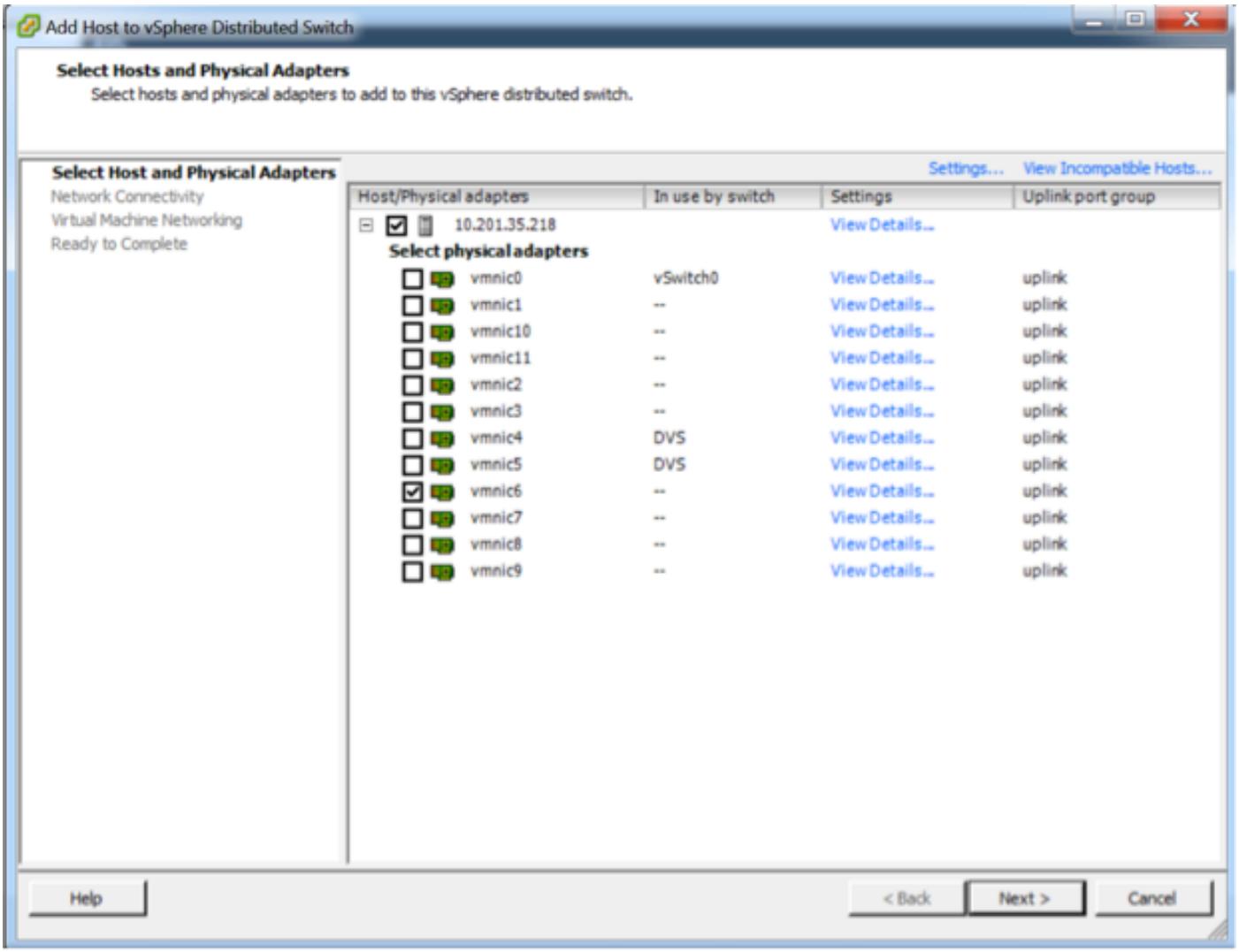
- Installez le logiciel AVS à l'aide de la commande suivante sur l'hôte ESXi :

esxcli software vib install -v /vmfs/volumes/datastore1/cross_cisco-vem-v250-5.2.1.3.1.10.0-3.2.1.vib —mode maintenance —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

~ #
```

- Une fois le module Virtual Ethernet (VEM) activé, vous pouvez ajouter des hôtes à votre AVS :

Dans la boîte de dialogue Ajouter un hôte au commutateur distribué vSphere, sélectionnez les ports de la carte réseau virtuelle connectés au commutateur Leaf (dans cet exemple, vous déplacez uniquement vmnic6), comme illustré dans l'image :



- Cliquez sur **Suivant**
- Dans la boîte de dialogue Connectivité réseau, cliquez sur **Suivant**
- Dans la boîte de dialogue Mise en réseau de machines virtuelles, cliquez sur **Suivant**
- Dans la boîte de dialogue Prêt à terminer, cliquez sur **Terminer**

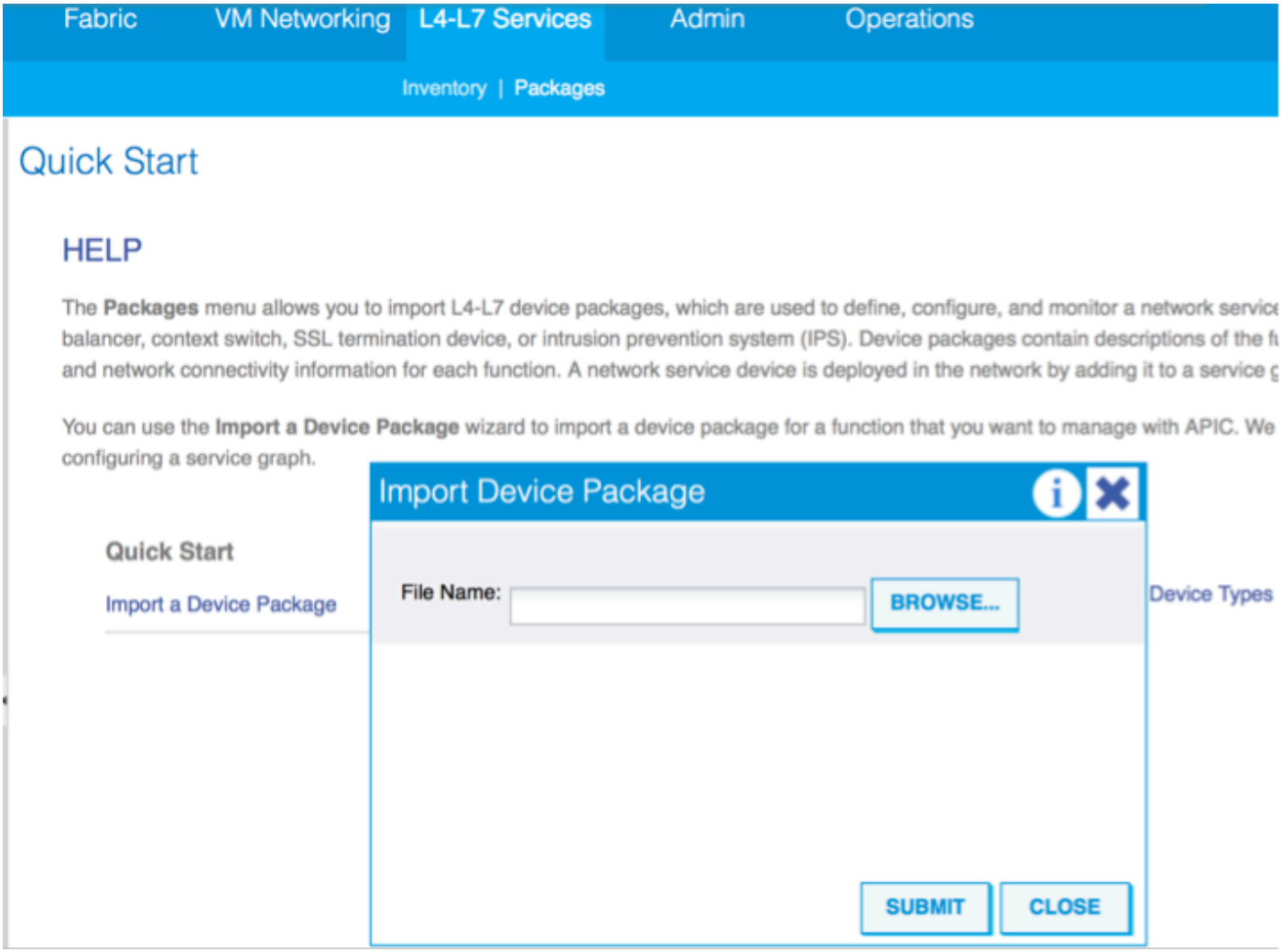
Note: Si plusieurs hôtes ESXi sont utilisés, tous doivent exécuter AVS/VEM pour pouvoir les gérer du commutateur standard au DVS ou AVS.

Avec cela, l'intégration AVS est terminée et nous sommes prêts à poursuivre le déploiement ASAv de couche 4-7 :

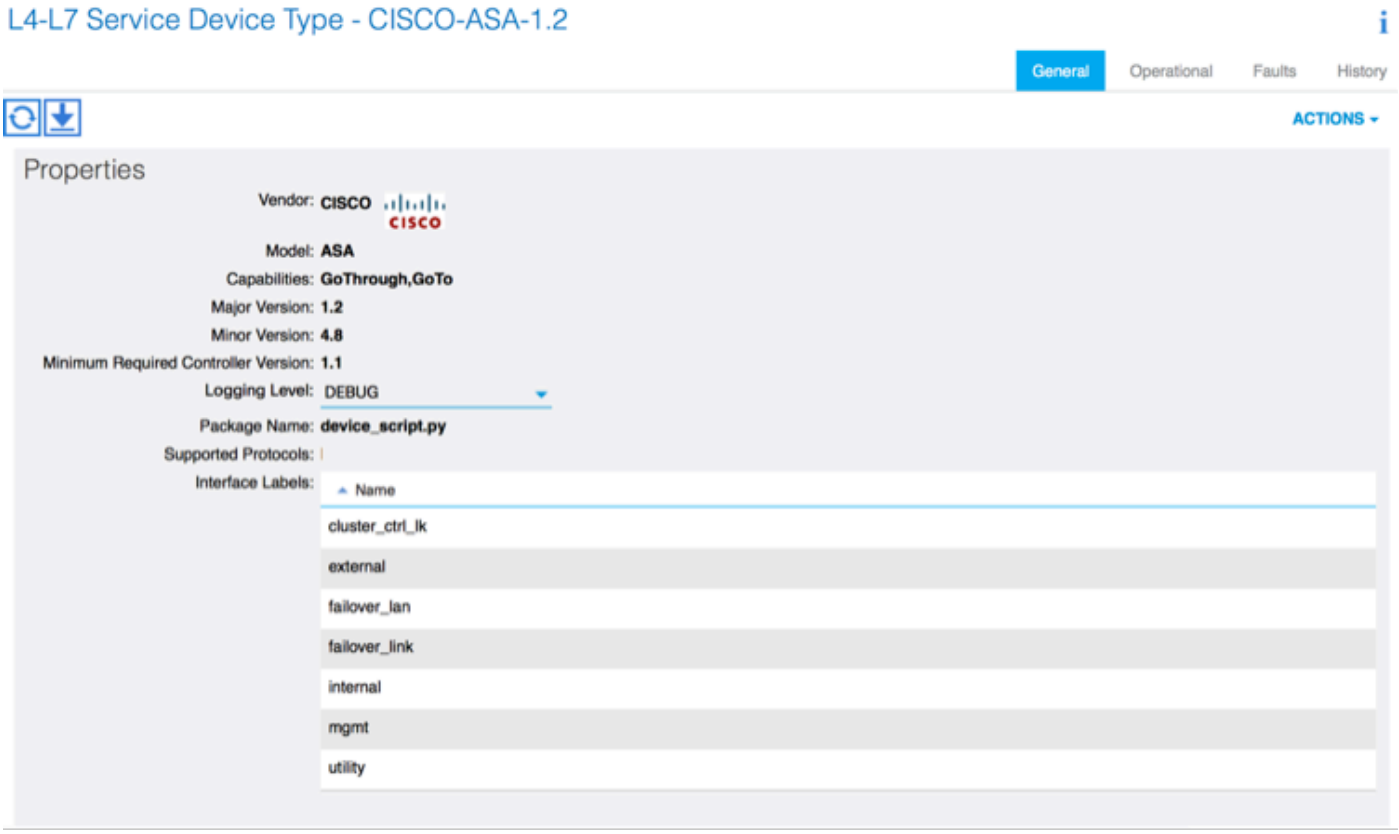
Configuration initiale d'ASAv

- Téléchargez le package de périphériques Cisco ASAv et importez-le dans APIC :

Accédez à **Services L4-L7 > Packages > Import Device Package,** comme indiqué dans l'image :



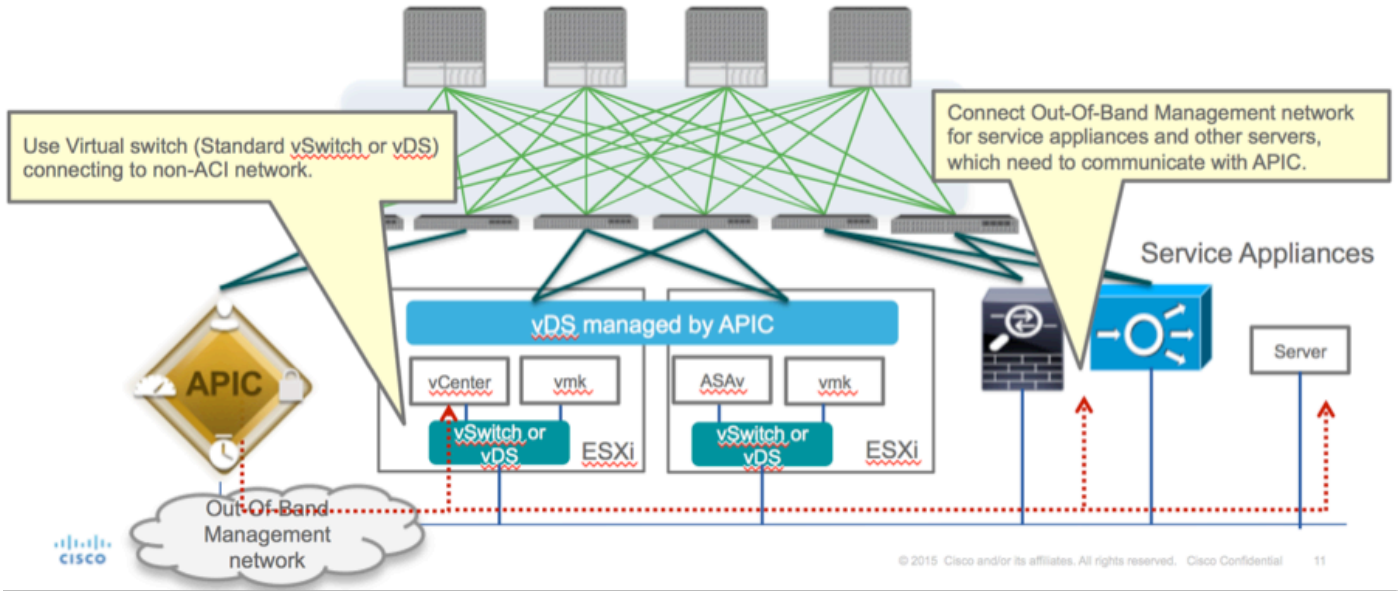
- Si tout fonctionne bien, vous pouvez voir le package de périphérique importé développant le dossier Types de périphérique de service L4-L7, comme illustré dans l'image :



Avant de continuer, il y a peu d'aspects de l'installation qui doivent être déterminés avant que l'intégration L4-L7 réelle soit effectuée :

Il existe deux types de réseaux de gestion, la gestion intrabande et la gestion hors bande (OOB), qui peuvent être utilisés pour gérer les périphériques qui ne font pas partie de l'infrastructure ACI (ACI) de base (leaf, spines ou contrôleur apic) et qui incluent ASAv, les répartiteurs de charge, etc.

Dans ce cas, OOB pour ASAv est déployé avec l'utilisation d'un vSwitch standard. Pour les appliances ASA sans système d'exploitation ou d'autres appareils et/ou serveurs de service, connectez le port de gestion OOB au commutateur ou au réseau OOB, comme illustré sur l'image.



La connexion de gestion des ports OOB ASAv doit utiliser les ports de liaison ascendante ESXi pour communiquer avec APIC via OOB. Lors du mappage des interfaces vNIC, la carte réseau 1 correspond toujours à l'interface Management0/0 sur l'ASAv et les autres interfaces du plan de données sont démarrées à partir de la carte réseau 2.

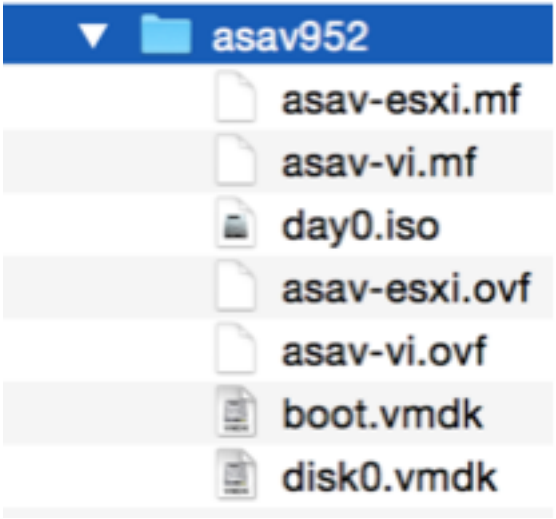
Le tableau 2 présente la concordance des ID d'adaptateur réseau et des ID d'interface ASAv :

Tableau 2

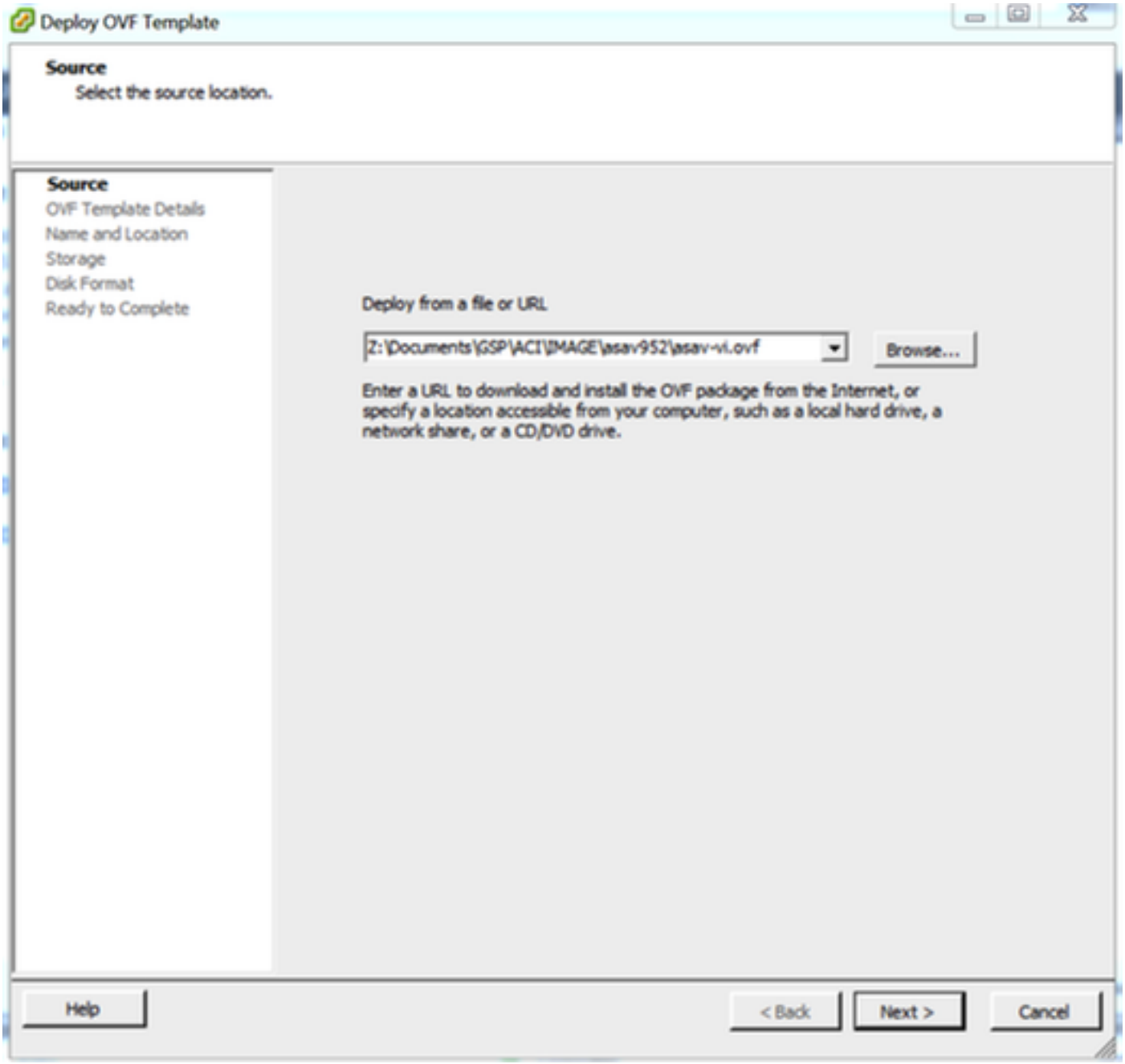
Network Adapter ID	ASAv Interface ID
Network Adapter 1	Management0/0
Network Adapter 2	GigabitEthernet0/0
Network Adapter 3	GigabitEthernet0/1
Network Adapter 4	GigabitEthernet0/2
Network Adapter 5	GigabitEthernet0/3
Network Adapter 6	GigabitEthernet0/4
Network Adapter 7	GigabitEthernet0/5
Network Adapter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

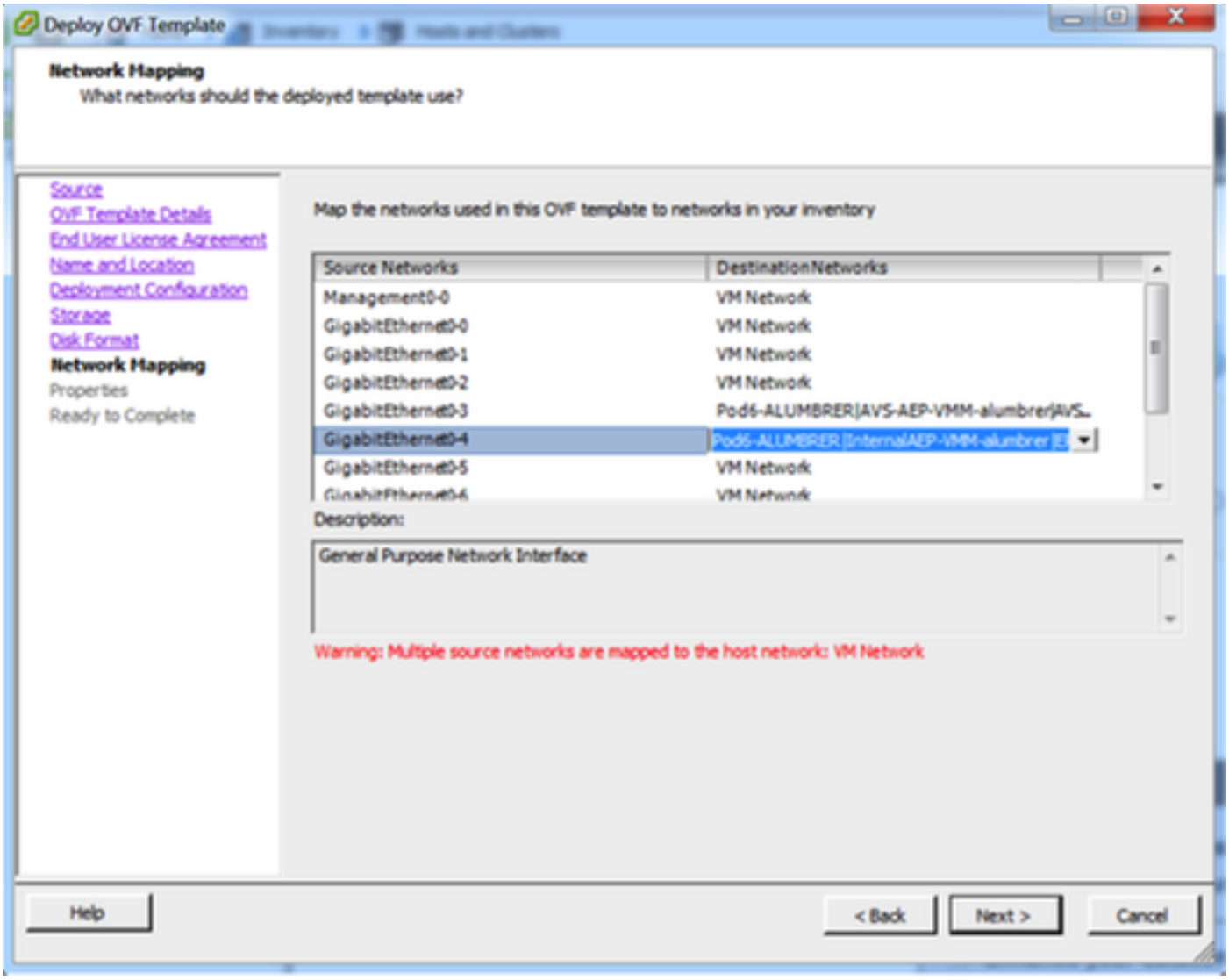
- Déployez la machine virtuelle ASAv via l'Assistant à partir de **Fichier>Déployer le modèle OVF (Open Virtualization Format)**
- Sélectionnez **asav-esxi** si vous souhaitez utiliser ESX Server autonome ou **asav-vi** pour

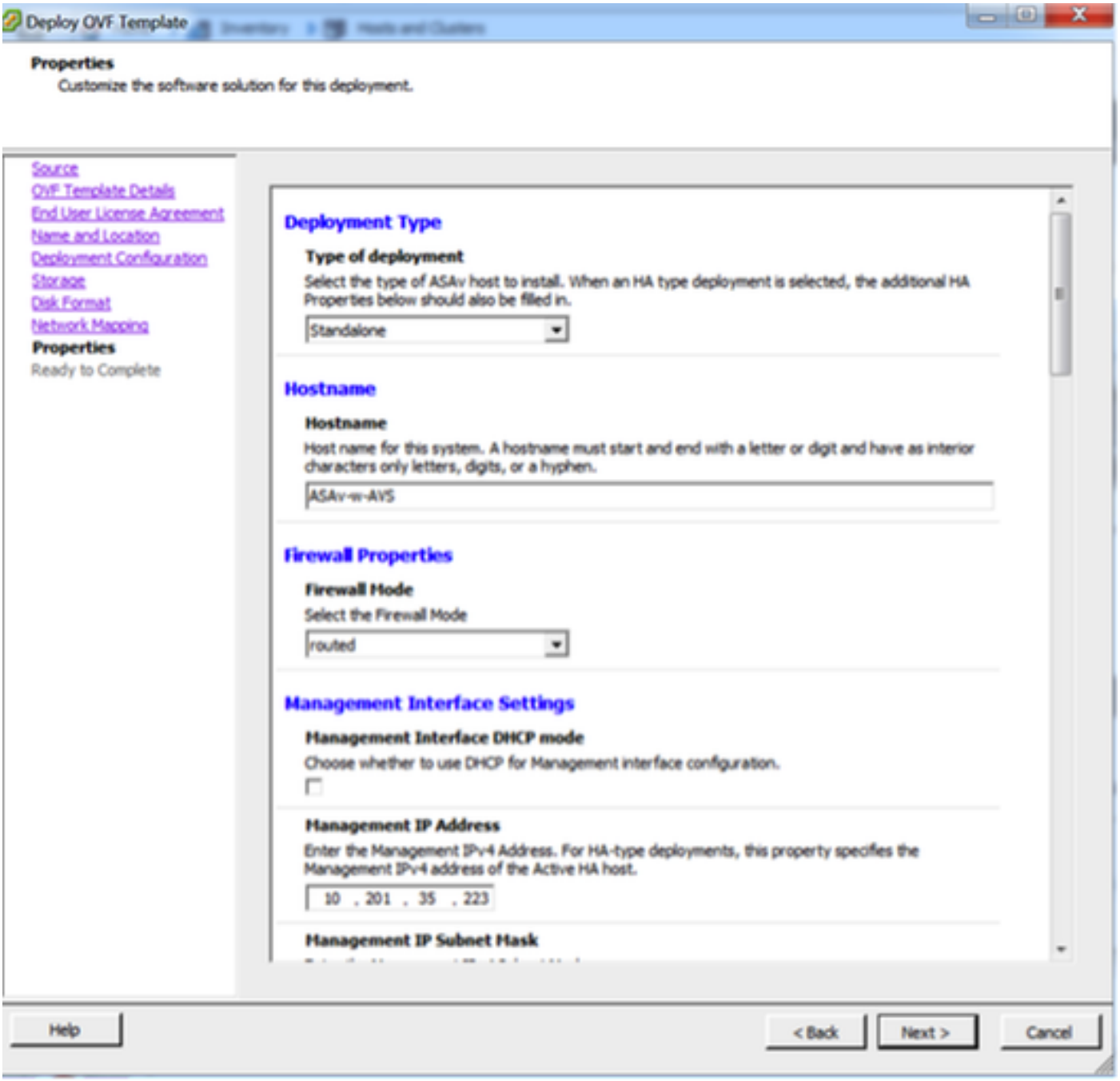
vCenter. Dans ce cas, vCenter est utilisé.

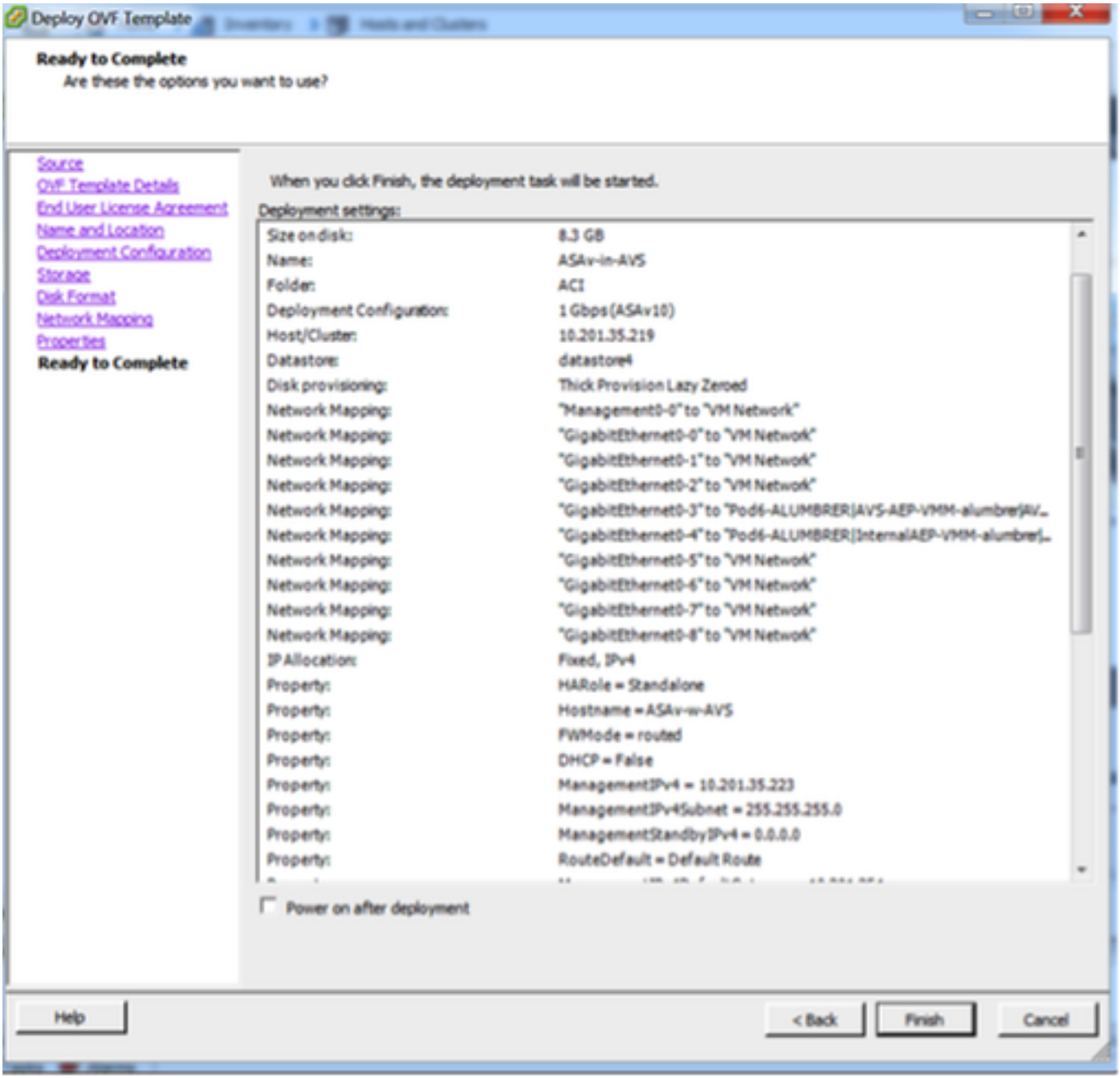


- Accédez à l'assistant d'installation, acceptez les conditions générales. Au milieu de l'assistant, vous pouvez déterminer plusieurs options telles que nom d'hôte, gestion, adresse IP, mode pare-feu et d'autres informations spécifiques relatives à ASAv. N'oubliez pas d'utiliser la gestion OOB pour ASAv, car dans ce cas, vous devez conserver l'interface Management0/0 pendant que vous utilisez le réseau de machines virtuelles (commutateur standard) et l'interface GigabitEthernet0-8 est les ports réseau par défaut.

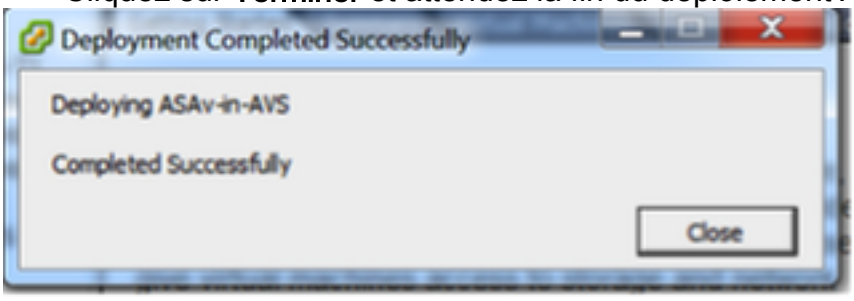

Deploy OVF Template
Source
Select the source location.
Source
OVF Template Details
Name and Location
Storage
Disk Format
Ready to Complete
Deploy from a file or URL
Z:\Documents\GSP\ACI\IMAGE\asav952\asav-vi.ovf
Browse...
Enter a URL to download and install the OVF package from the Internet, or specify 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

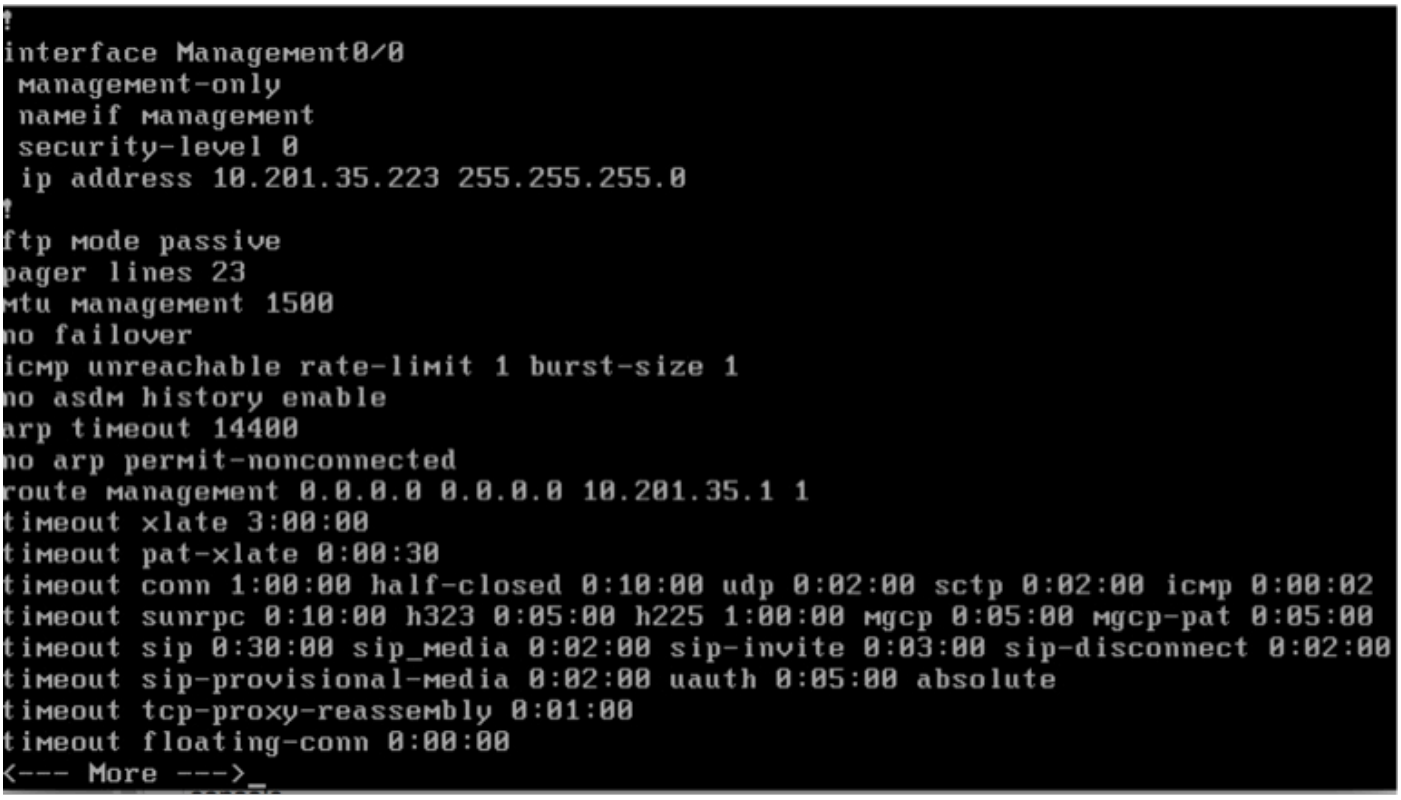

Deploy OVF Template
Properties
Customize the software solution for this deployment.
Source
OVF Template Details
End User License Agreement
Name and Location
Deployment Configuration
Storage
Disk Format
Network Mapping
Properties
Ready to Complete
Deployment Type
Type of deployment
Select the type of 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



- Cliquez sur **Terminer** et attendez la fin du déploiement ASAv.

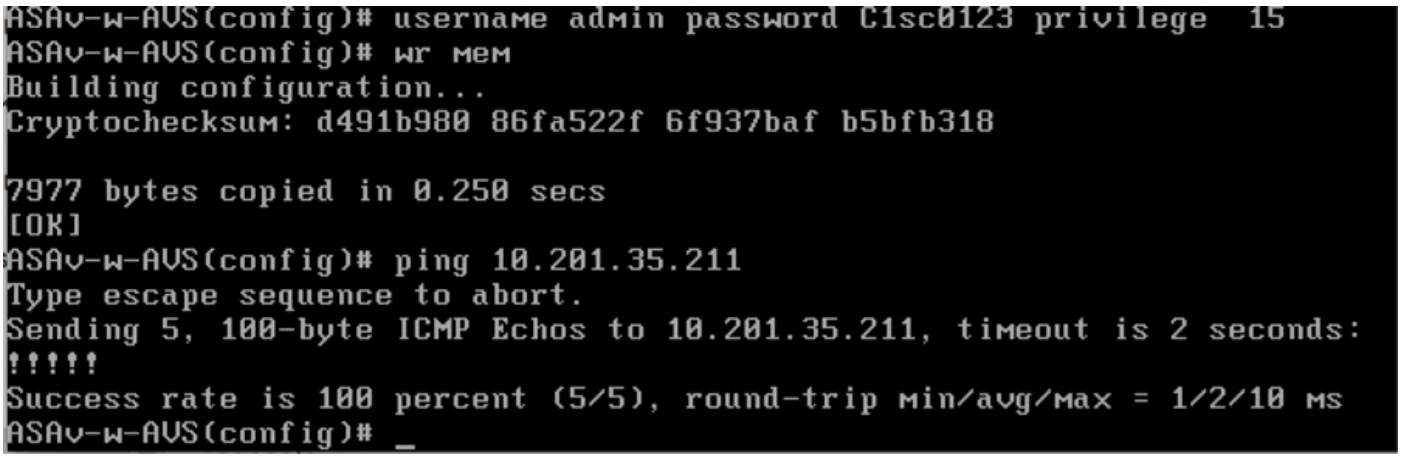


- Mettez sous tension votre machine virtuelle ASAv et connectez-vous via la console pour vérifier la configuration initiale



- Comme l'illustre l'image, certaines configurations de gestion sont déjà transmises au pare-feu ASAv. Configurez le nom d'utilisateur et le mot de passe admin. Ce nom d'utilisateur et ce mot de passe sont utilisés par l'APIC pour se connecter et configurer l'ASA. L'ASA doit être connecté au réseau OOB et être en mesure d'atteindre le contrôleur APIC.

username admin password <device_password> crypté, privilège 15



En outre, à partir du mode de configuration globale, activez le serveur http :

http server enable

http 0.0.0.0 0.0.0.0 gestion

L4-L7 pour l'intégration ASAv dans APIC :

- Connectez-vous à l'interface utilisateur graphique de l'ACI, cliquez sur le locataire où le graphique de service sera déployé. Développez les services L4-L7 en bas du volet de navigation et cliquez avec le bouton droit sur **Périphériques L4-L7**, puis cliquez sur **Créer des périphériques L4-L7** pour ouvrir l'Assistant

- Pour cette implémentation, les paramètres suivants seront appliqués :
  - Mode géré

  - Service de pare-feu

  -Périphérique virtuel

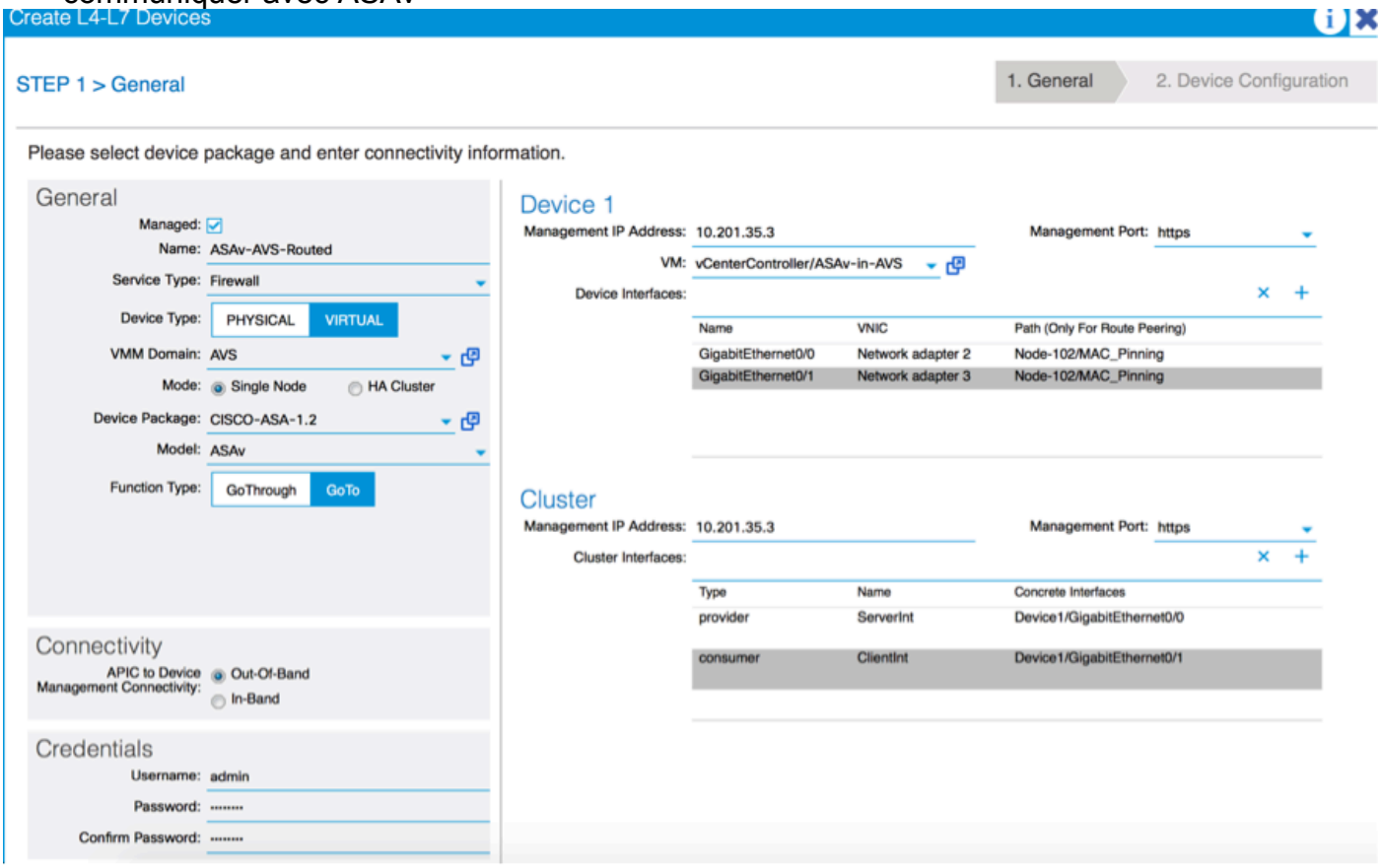
  - Connecté au domaine AVS avec un noeud unique

  -Modèle ASAv

  - Mode routé (GoTo)

  - Adresse de gestion (doit correspondre à l'adresse précédemment attribuée à l'interface Mgmt0/0)

- Utiliser HTTPS comme carte APIC par défaut utilise le protocole le plus sécurisé pour communiquer avec ASAv



- La définition correcte des interfaces de périphérique et des interfaces de cluster est essentielle pour un déploiement réussi

Pour la première partie, utilisez le tableau 2 présenté dans la section précédente pour faire correspondre correctement les ID d'adaptateur réseau aux ID d'interface ASAv que vous souhaitez utiliser. Le chemin fait référence au port physique, au canal de port ou au VPC qui active le chemin d'entrée et de sortie des interfaces du pare-feu. Dans ce cas, ASA est situé dans un hôte ESX, où les entrées et les sorties sont identiques pour les deux interfaces. Dans un appareil physique, les ports physiques internes et externes du pare-feu (FW) sont différents.

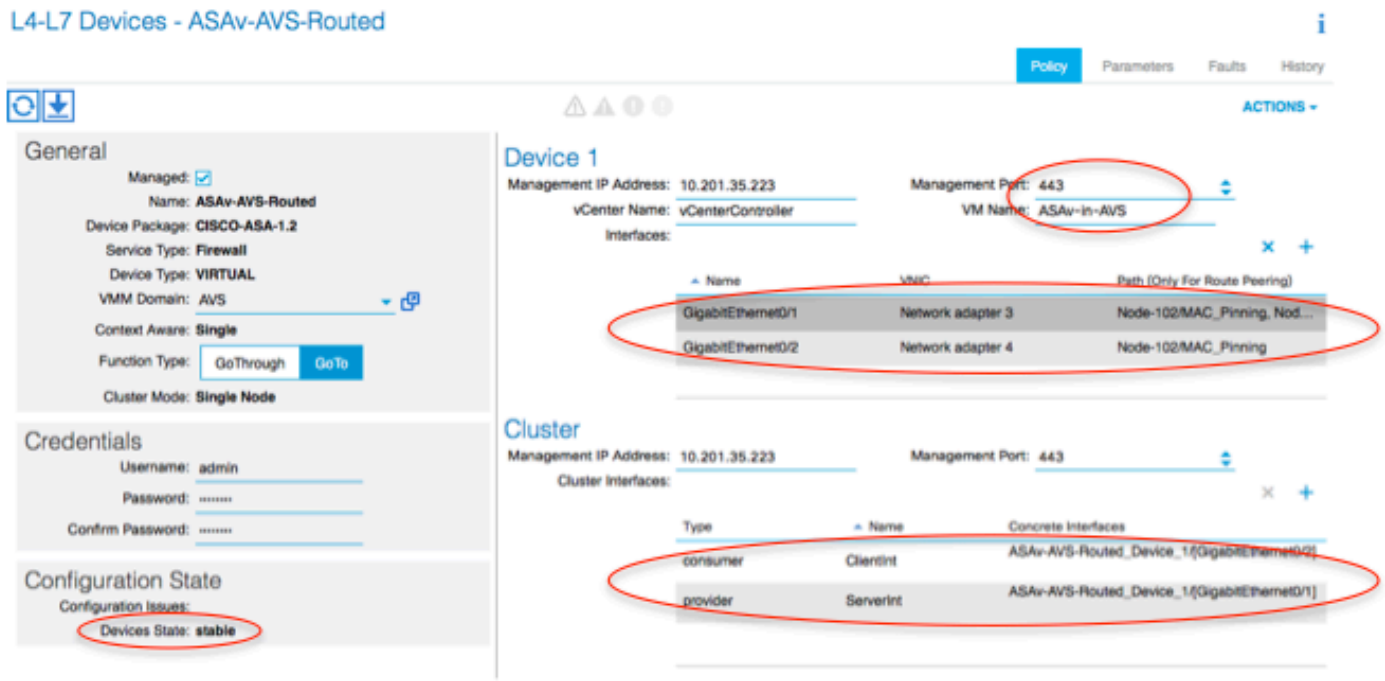
Pour la deuxième partie, les interfaces de cluster doivent être définies toujours sans exception

(même si le cluster HA n'est pas utilisé), car le modèle d'objet a une association entre l'interface **mIf** (méta interface sur le package de périphériques), l'interface **LIf** (interface leaf comme externe, interne, interne, etc.) et l'**CIf** (interface concrète). Les périphériques concrets L4-L7 doivent être configurés dans une configuration de cluster de périphériques et cette abstraction est appelée un périphérique logique. Le périphérique logique possède des interfaces logiques qui sont mappées à des interfaces concrètes sur le périphérique concret.

Dans cet exemple, l'association suivante sera utilisée :

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

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

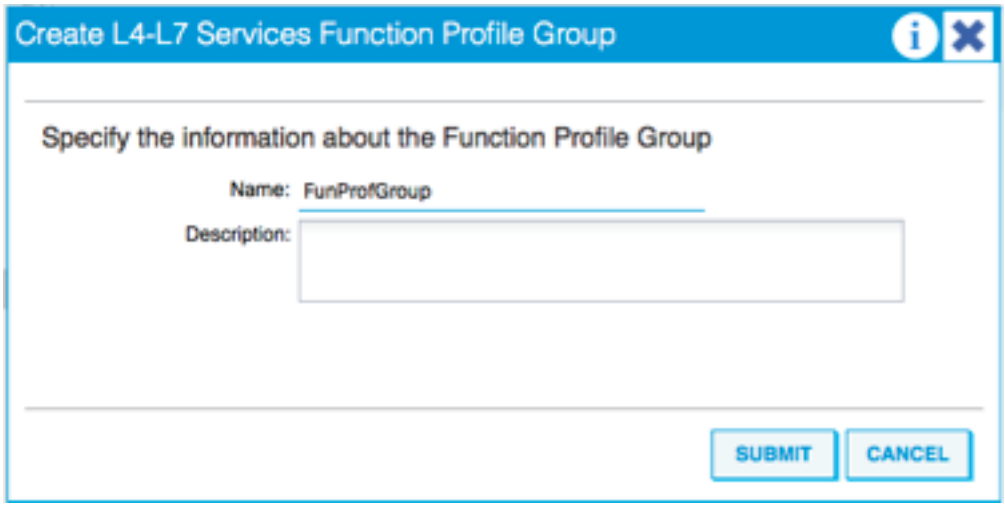


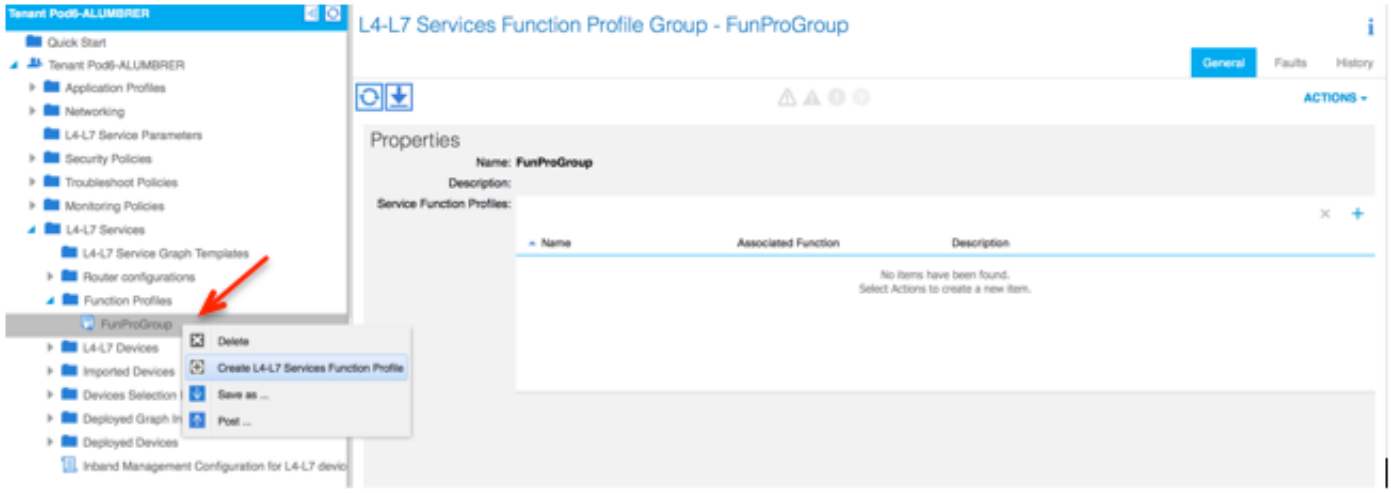
> **Note**: Pour les déploiements de basculement/HA, GigabitEthernet 0/8 est préconfiguré comme interface de basculement.

L'état du périphérique doit être Stable et vous devez être prêt à déployer le profil de fonction et le modèle de graphique de service

Temple du graphique de service

Tout d'abord, créez un profil de fonction pour ASAv, mais avant cela, vous devez créer un groupe de profils de fonction, puis un profil de fonction de services L4-L7 sous ce dossier, comme illustré dans l'image :

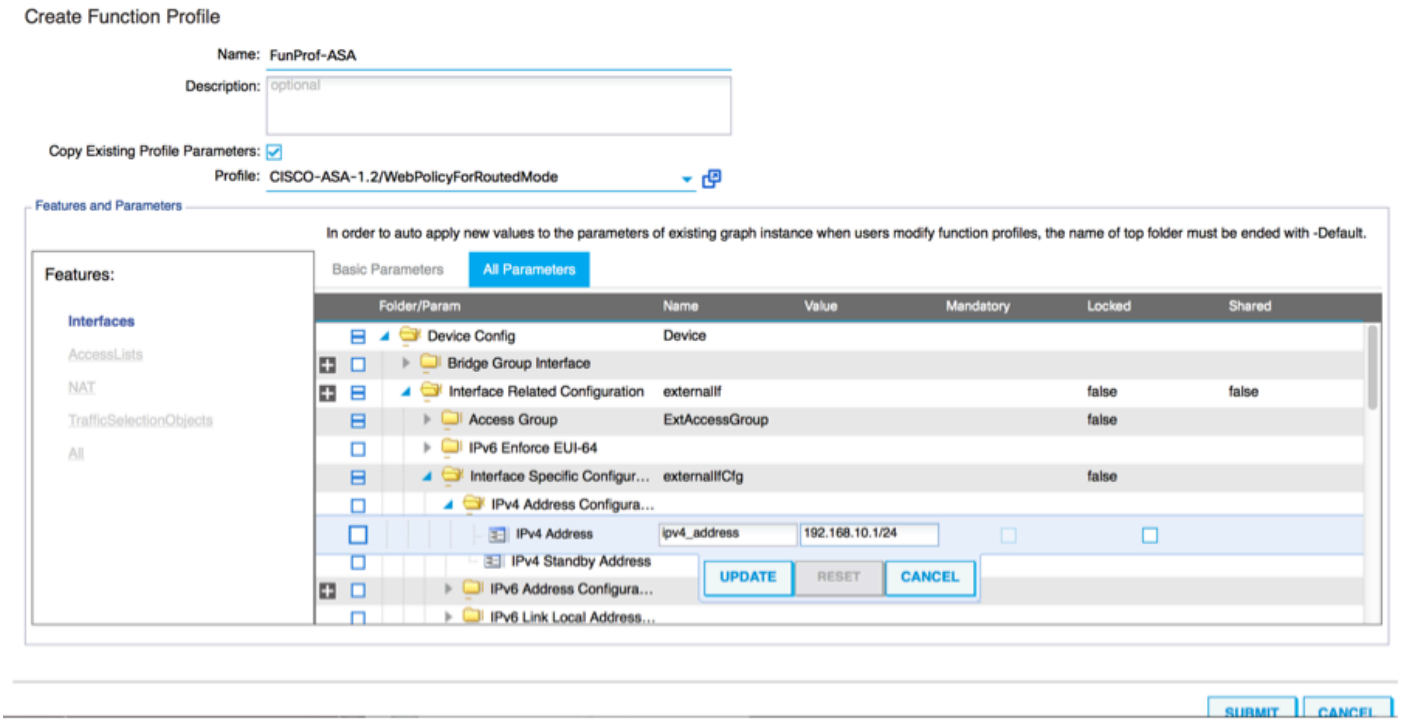




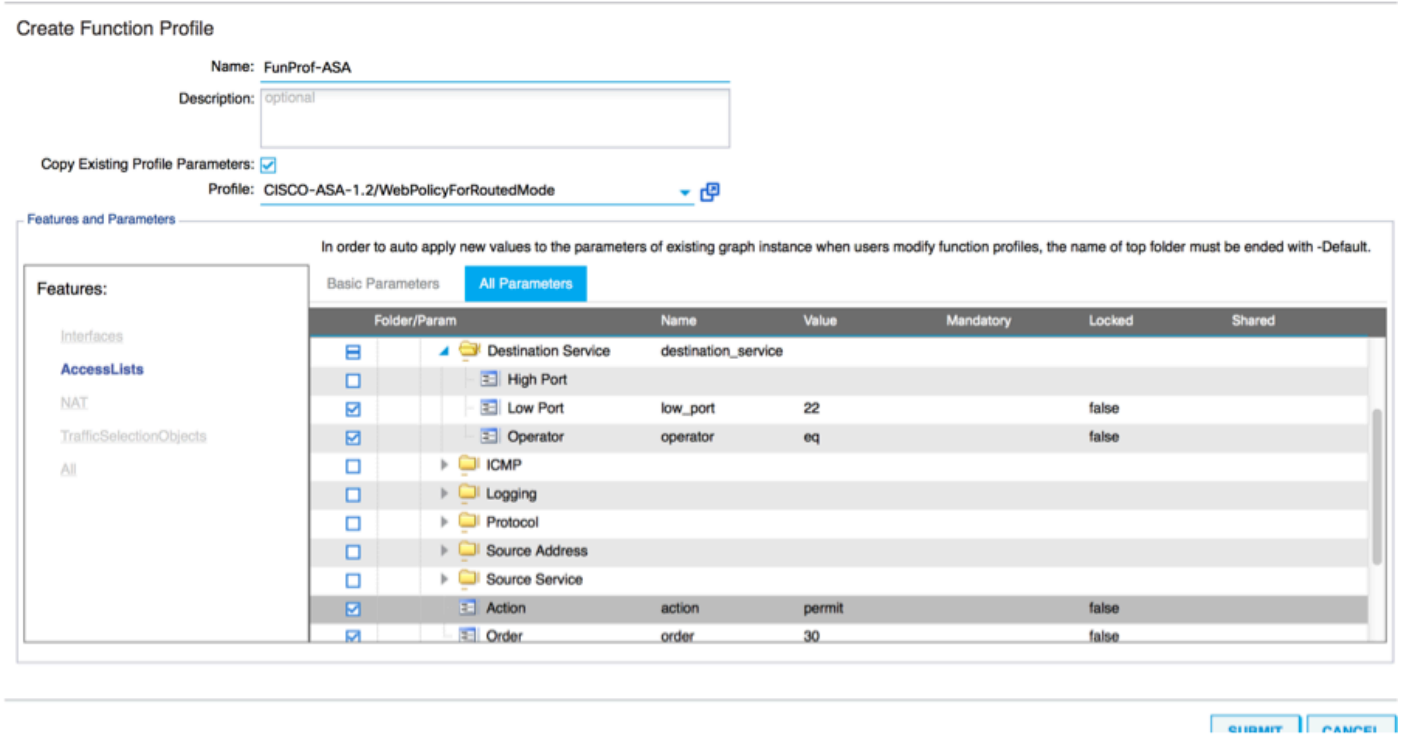
- Sélectionnez le profil **WebPolicyForRoutedMode** dans le menu déroulant et continuez à configurer les interfaces sur le pare-feu. À partir de là, les étapes sont facultatives et peuvent être mises en oeuvre/modifiées ultérieurement. Ces étapes peuvent être effectuées à quelques étapes différentes du déploiement selon la réutilisation ou la personnalisation du graphique de services.

Pour cet exercice, un pare-feu routé (mode Atteindre) nécessite que chaque interface possède une adresse IP unique. La configuration ASA standard a également un niveau de sécurité d'interface (l'interface externe est moins sécurisée, l'interface interne est plus sécurisée). Vous pouvez également modifier le nom de l'interface selon vos besoins. Les valeurs par défaut sont utilisées dans cet exemple.

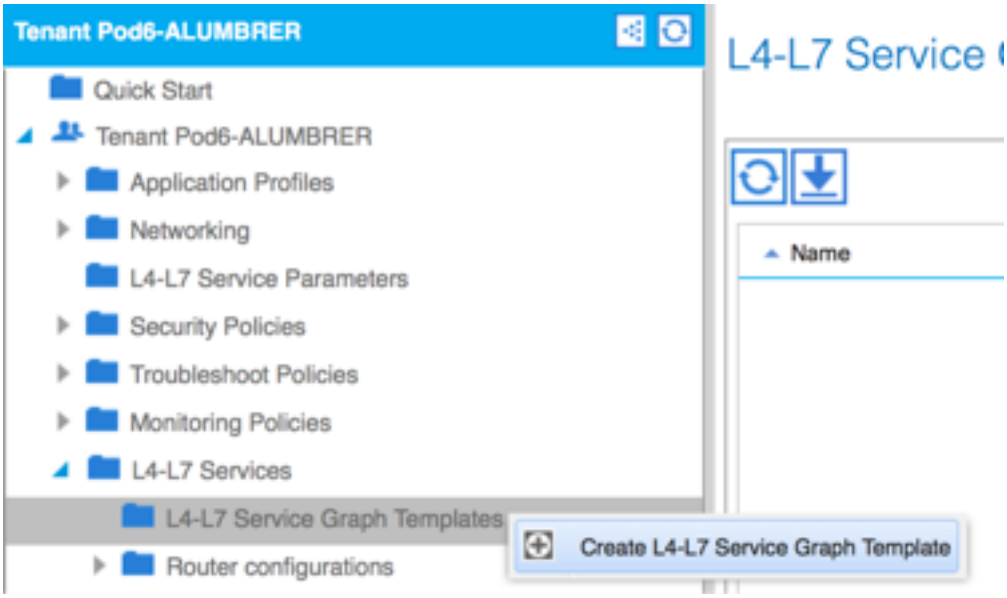
- Développez Configuration spécifique à l'interface, ajoutez l'adresse IP et le niveau de sécurité pour ServerInt avec le format suivant pour l'adresse IP **x.x.x.x/y.y.y.y ou x.x.x.x/yy**. Répétez le processus pour l'interface ClientInt.



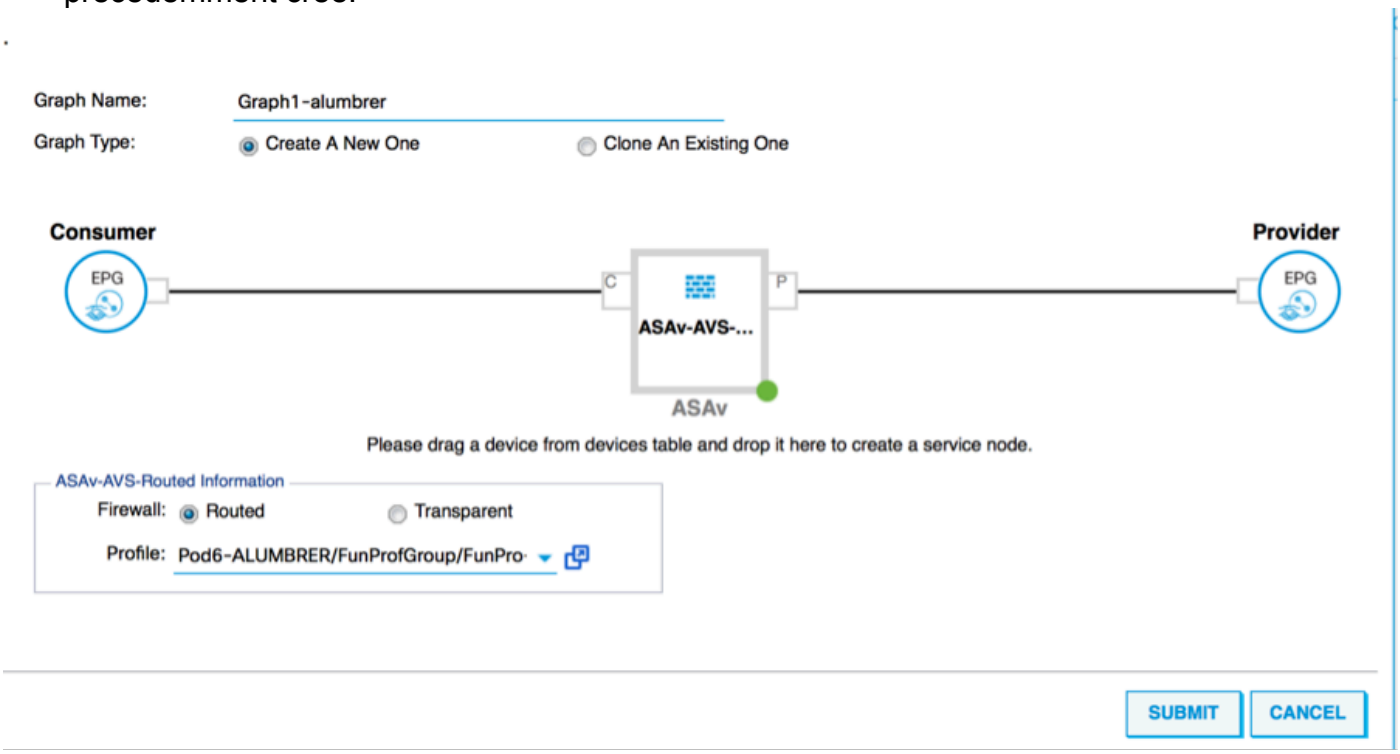
Note: Vous pouvez également modifier les paramètres de liste d'accès par défaut et créer votre propre modèle de base. Par défaut, le modèle RoutedMode inclut des règles pour HTTP et HTTPS. Pour cet exercice, SSH et ICMP seront ajoutés à la liste d'accès externe autorisée.



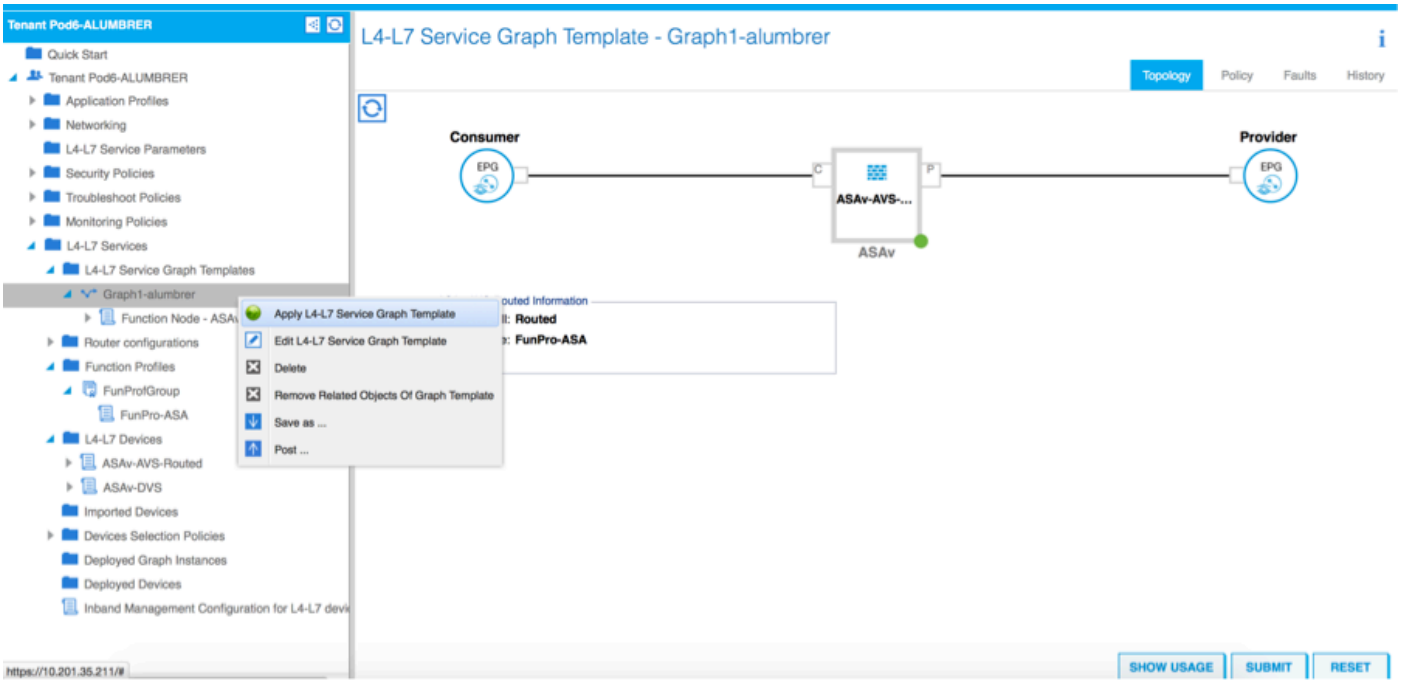
- Cliquez ensuite sur **Envoyer**
- Maintenant, créez le modèle de graphique de service



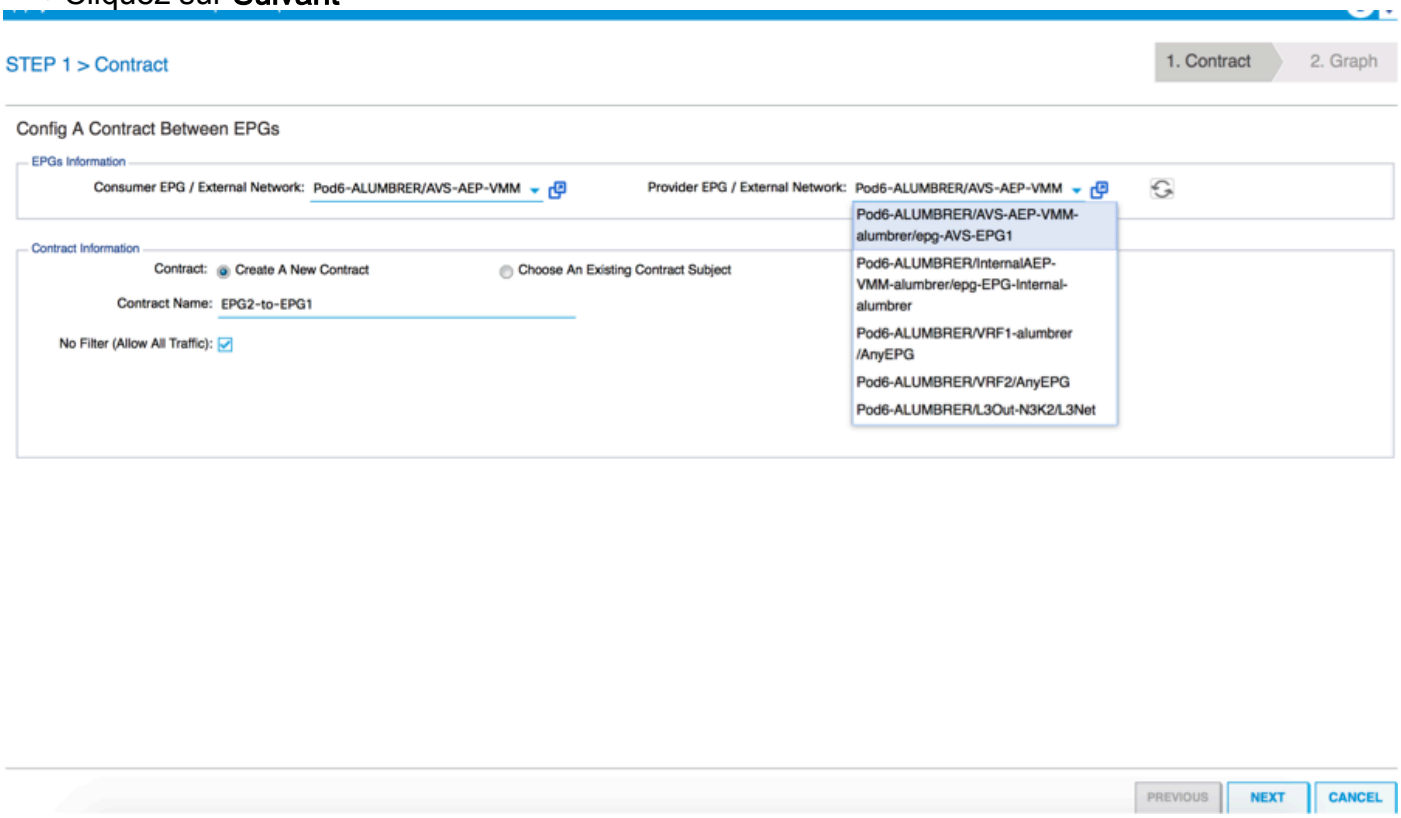
- Faites glisser et déposez le cluster de périphériques vers la droite pour former la relation entre le consommateur et le fournisseur, sélectionnez Mode routé et le profil de fonction précédemment créé.



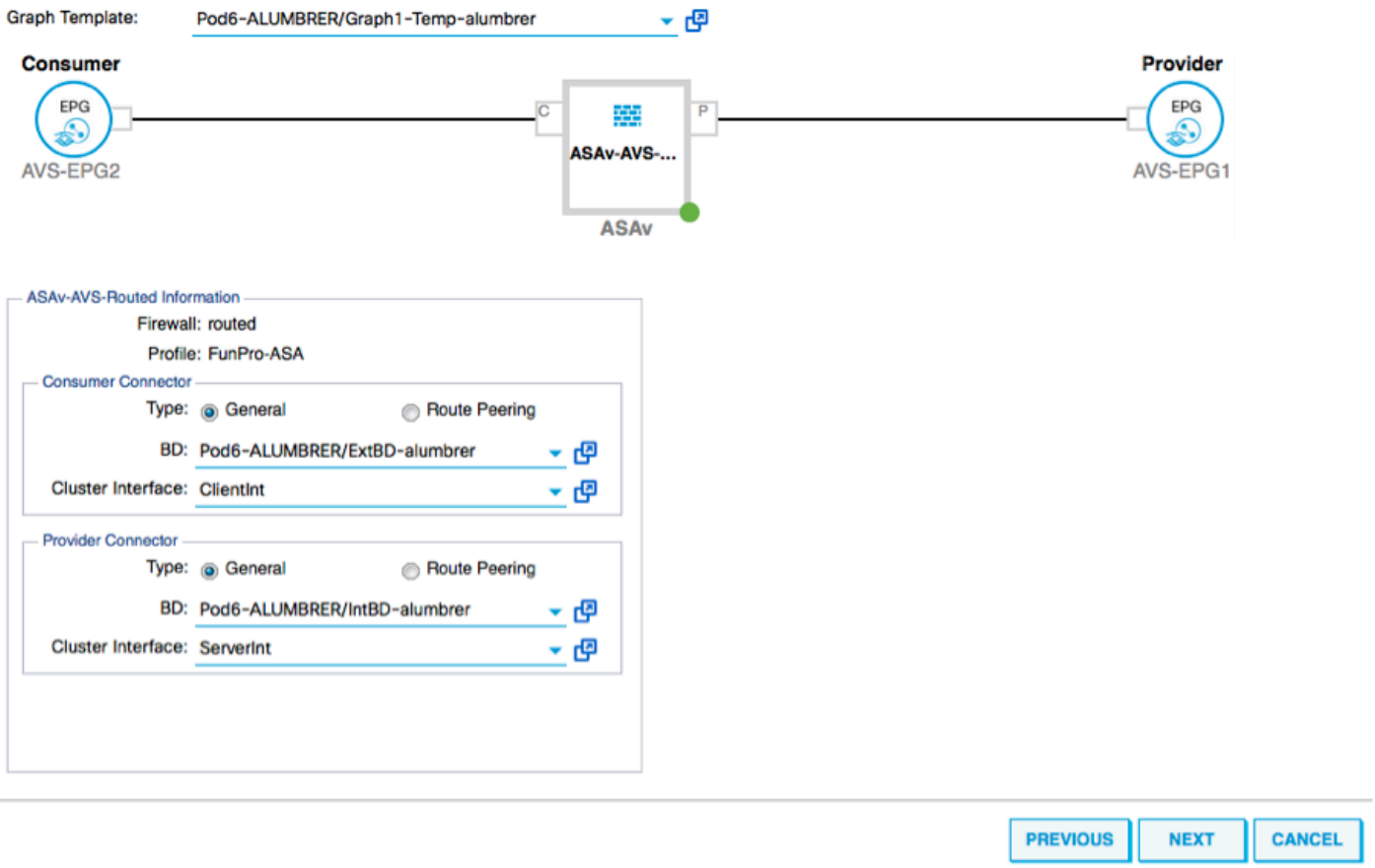
- Vérifier les erreurs dans le modèle. Les modèles sont créés pour être réutilisables, ils doivent ensuite être appliqués à des groupes de terminaux particuliers, etc.
- Pour appliquer un modèle, cliquez avec le bouton droit de la souris et sélectionnez Appliquer le modèle de graphique de service L4-L7



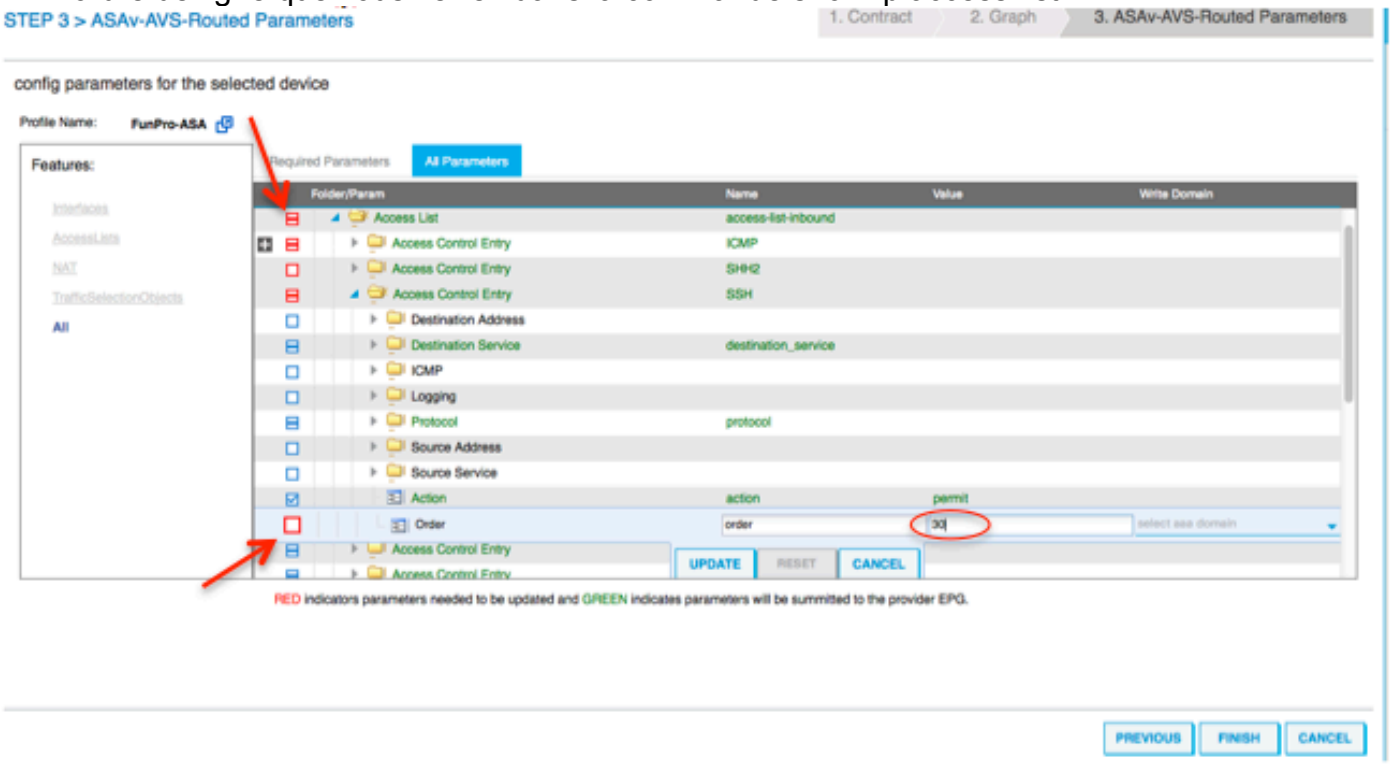
- Définissez quel EPG sera du côté consommateur et du côté fournisseur. Dans cet exercice, AVS-EPG2 est le consommateur (client) et AVS-EPG1 le fournisseur (serveur). N'oubliez pas qu'aucun filtre n'est appliqué, cela permettra au pare-feu d'effectuer tout le filtrage en fonction de la liste d'accès définie dans la dernière section de cet Assistant.
- Cliquez sur **Suivant**



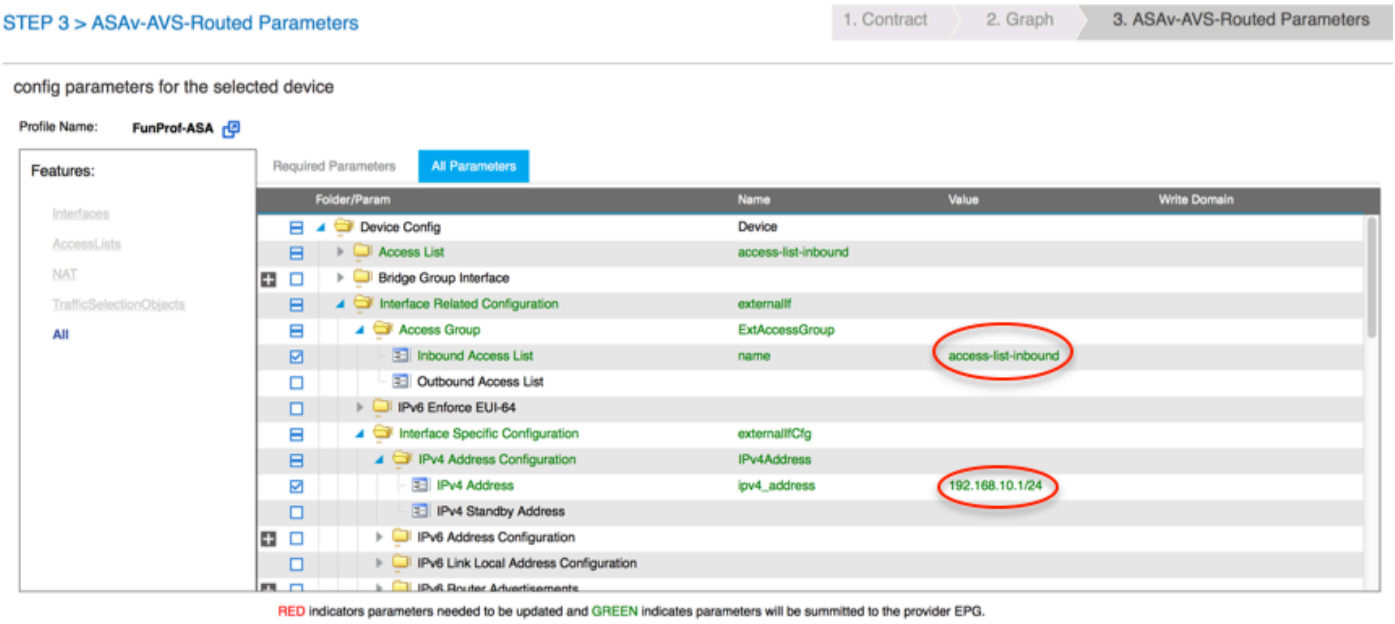
- Vérifiez les informations BD pour chacun des groupes de terminaux. Dans ce cas, EPG1 est le fournisseur sur la base de données IntBD et EPG2 est le consommateur sur BD ExtBD. EPG1 se connectera sur l'interface de pare-feu ServerInt et EPG2 sera connecté sur l'interface ClientInt. Les deux interfaces FW deviendront la DG de chacun des groupes de terminaux, de sorte que le trafic est forcé de traverser le pare-feu à tout moment.
- Cliquez sur **Suivant**



- Dans la section Config Parameters, cliquez sur **All Parameters** et vérifiez s'il existe des indicateurs RED qui doivent être mis à jour/configurés. Dans la sortie comme le montre l'image, il est possible de constater que l'ordre de la liste d'accès est manqué. Cela équivaut à l'ordre de ligne que vous verrez dans la commande show ip access-list X.



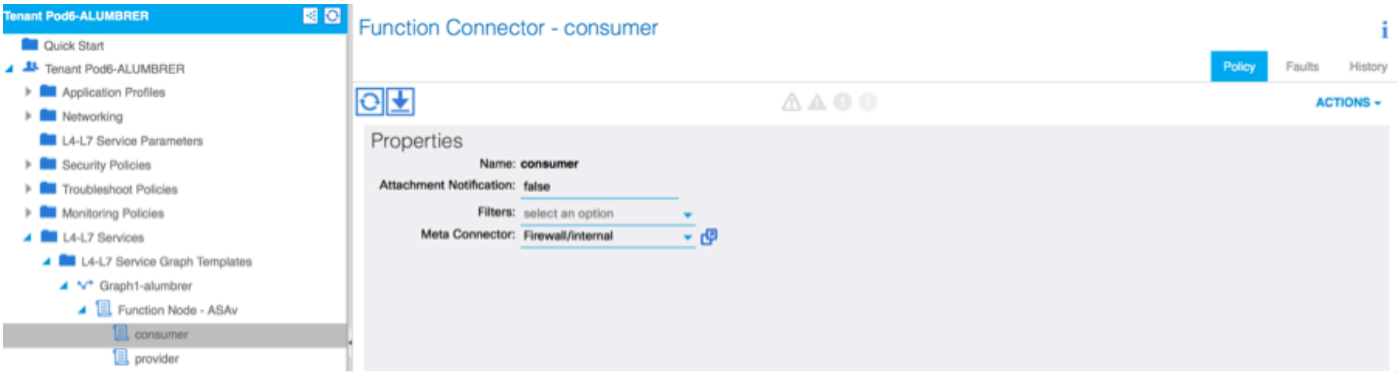
- Vous pouvez également vérifier l'adressage IP attribué à partir du profil de fonction défini précédemment. Il est possible de modifier les informations si nécessaire. Une fois tous les paramètres définis, cliquez sur **Terminer**, comme illustré dans l'image :



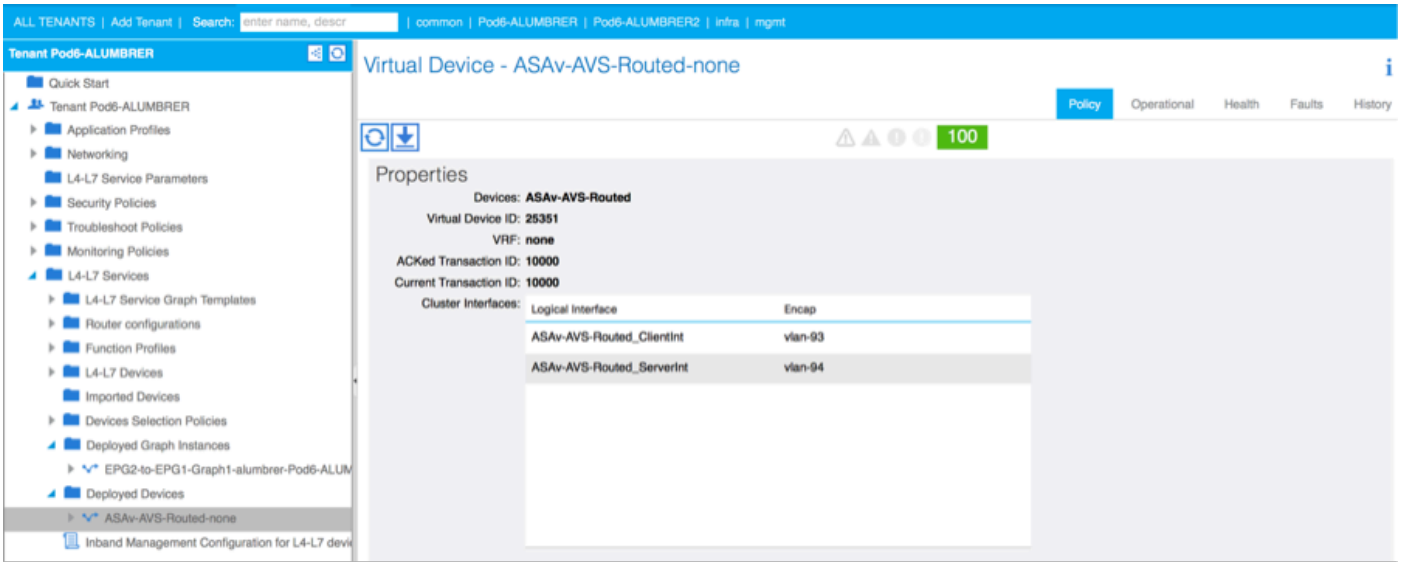
- Si tout va bien, un nouveau périphérique déployé et une nouvelle instance de graphique doivent apparaître.

Vérification

- Une chose importante à vérifier après la création du graphique Service est que la relation Consommateur/Fournisseur a été créée avec le Meta Connector approprié. Vérifiez sous Propriétés du connecteur de fonction.



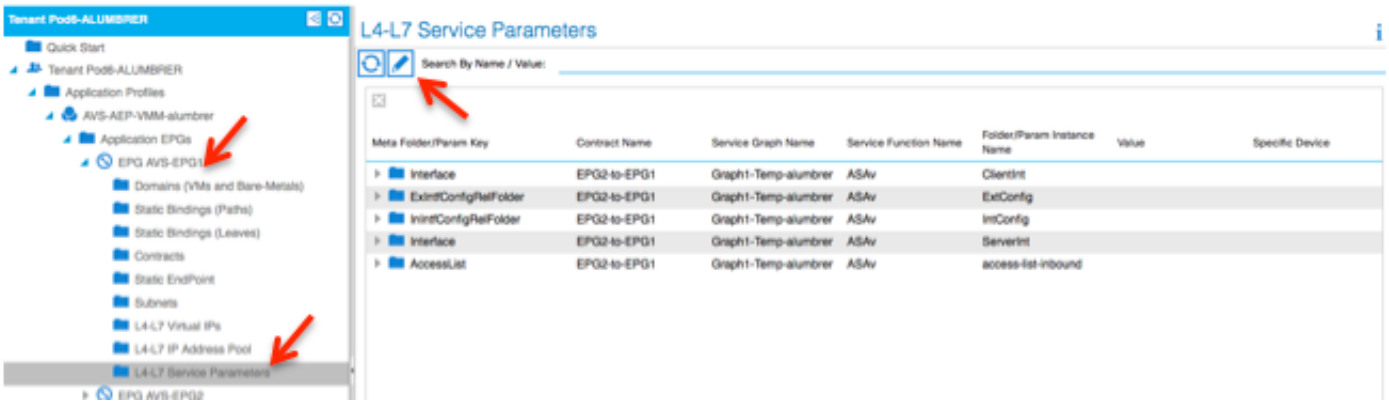
Note: Chaque interface du pare-feu sera affectée avec un encap-vlan du pool dynamique AVS. Vérifiez qu'il n'y a pas de défaillance.



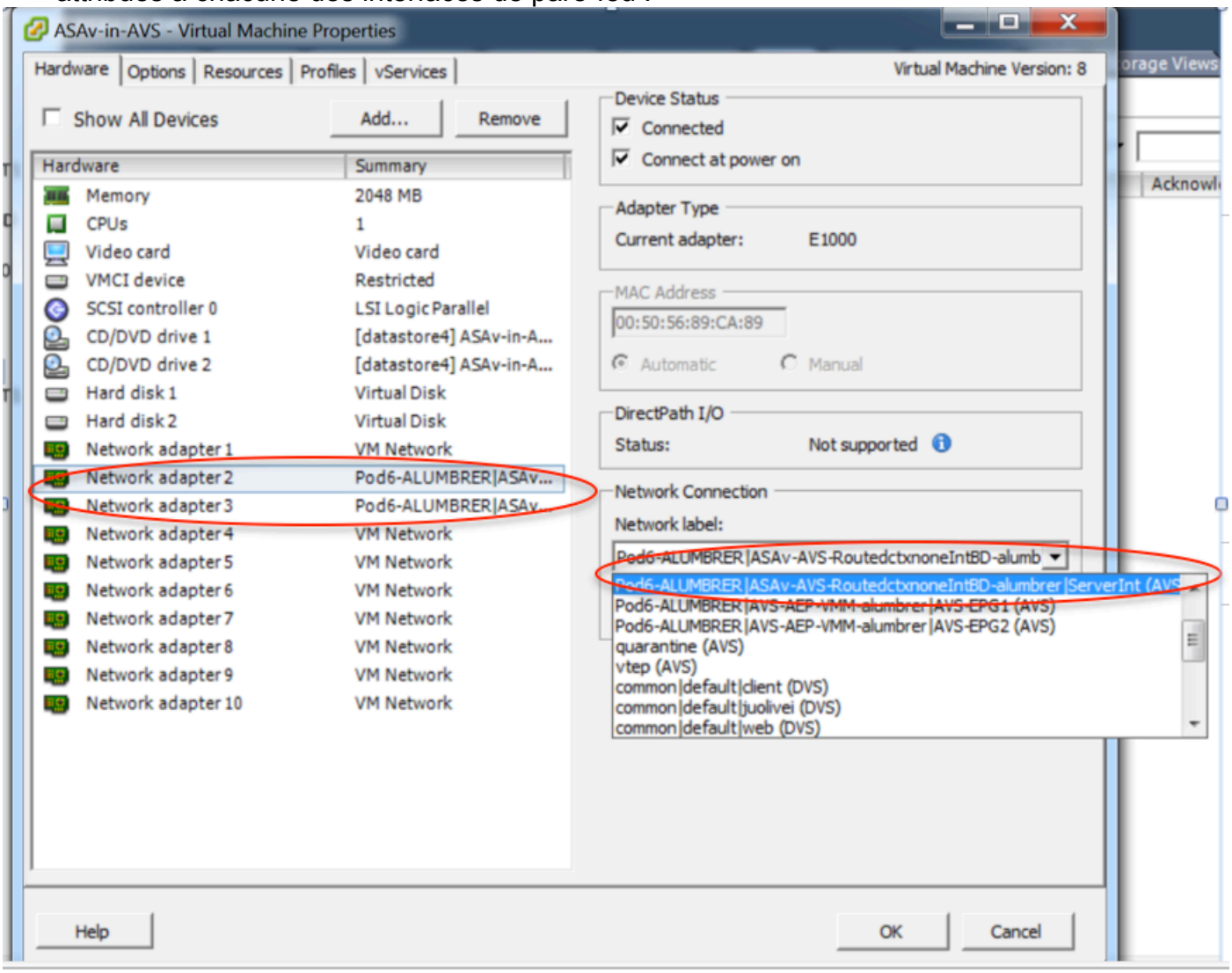
- Maintenant, vous pouvez également vérifier les informations qui ont été transmises à ASAv

```
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#
```

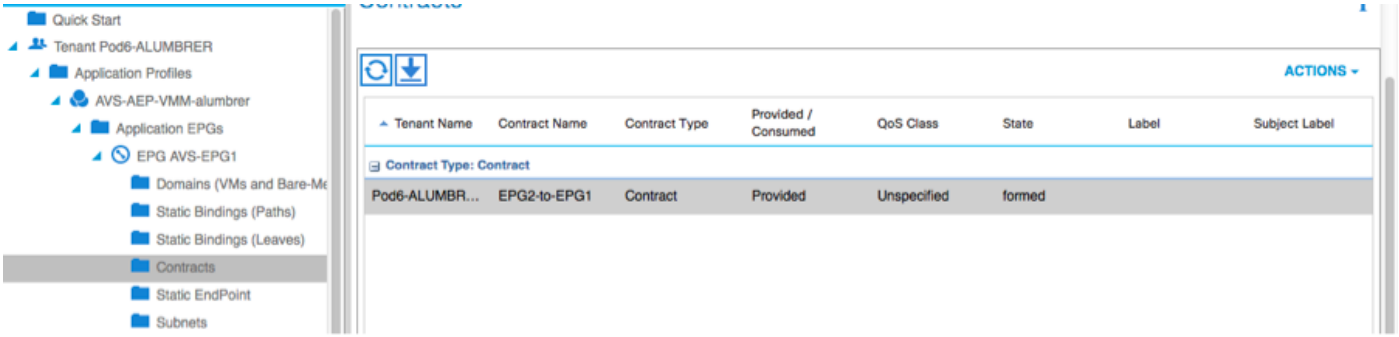
- Un nouveau contrat est attribué en vertu des EPG. À partir de maintenant, si vous devez modifier quoi que ce soit sur la liste d'accès, la modification doit être effectuée à partir des paramètres de service L4-L7 de l'EPG fournisseur.



- Sur vCenter, vous pouvez également vérifier que les groupes de terminaux fantômes sont attribués à chacune des interfaces de pare-feu :



Pour ce test, j'ai eu les 2 EPG communiquant avec les contrats standard, ces 2 EPG sont dans des domaines différents et des VRF différents, de sorte que la fuite de route entre eux a été précédemment configuré. Cela simplifie un peu après l'insertion du graphique de service lorsque le pare-feu configure le routage et le filtrage entre les 2 groupes de terminaux. La DG précédemment configurée sous EPG et BD peut maintenant être supprimée comme les contrats. Seul le contrat poussé par les liaisons L4-L7 doit rester sous les GPE.



Lorsque le contrat standard est supprimé, vous pouvez confirmer que le trafic est maintenant acheminé via l'ASAv, la commande show access-list doit afficher le nombre de résultats de la règle incrémentant chaque fois que le client envoie une requête au serveur.

```
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# _
```

Au niveau de la feuille de route, les terminaux doivent être acquis pour les machines virtuelles client et serveur ainsi que pour les 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      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
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)

voir les deux interfaces de pare-feu reliées au VEM.

ESX-1

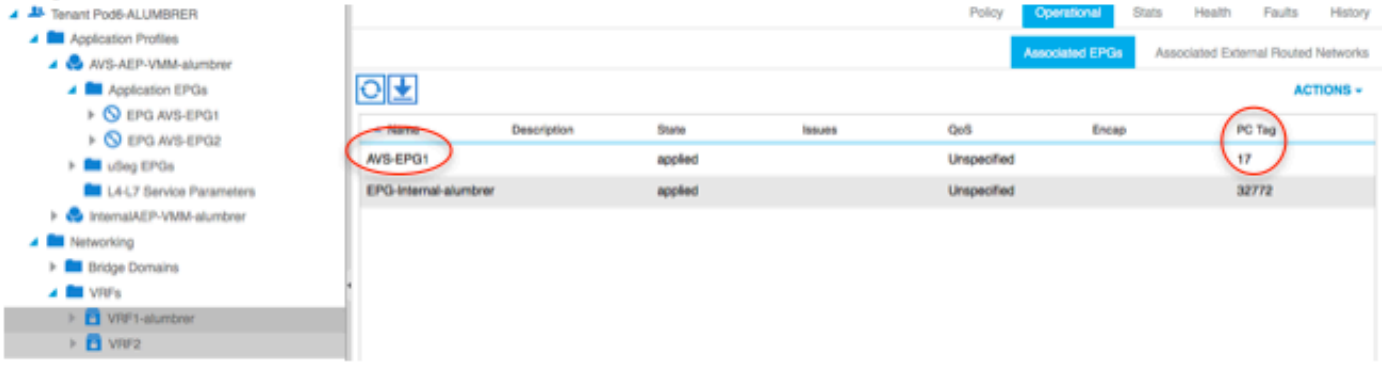
```
~ # vemcmd show port vlan
  LTL   VSM Port  Admin Link  State    Cause  PC-LTL  SGID  ORG  svcpath  Type    Vem Port
   22     Eth1/5     UP   UP    FWD        -    1040     4    0        0                vmnic4
   23     Eth1/6     UP   UP    FWD        -    1040     5    0        0            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

Enfin, les règles de pare-feu peuvent également être vérifiées au niveau de la feuille si nous connaissons les balises PC pour les groupes de terminaux source et de destination :

EPG1



EPG2

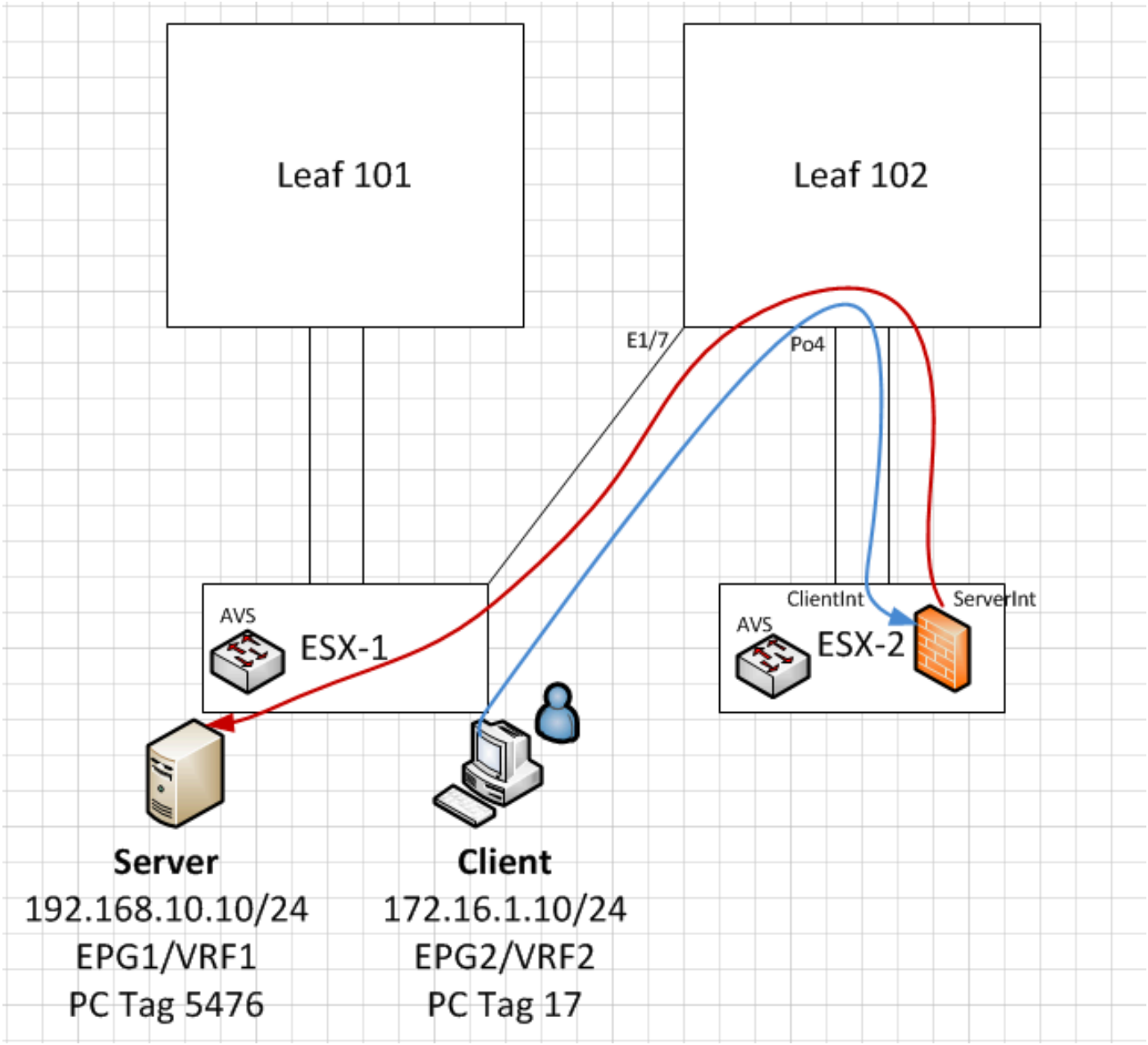
Les ID de filtre peuvent être associés aux balises PC de la feuille pour vérifier les règles de pare-feu.

```
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: L'EPG PCTags/Sclass ne communique jamais directement. La communication est interrompue ou liée par les EPG fantômes créés par l'insertion du graphique de service L4-L7.

Et communication entre le client et le serveur fonctionne.

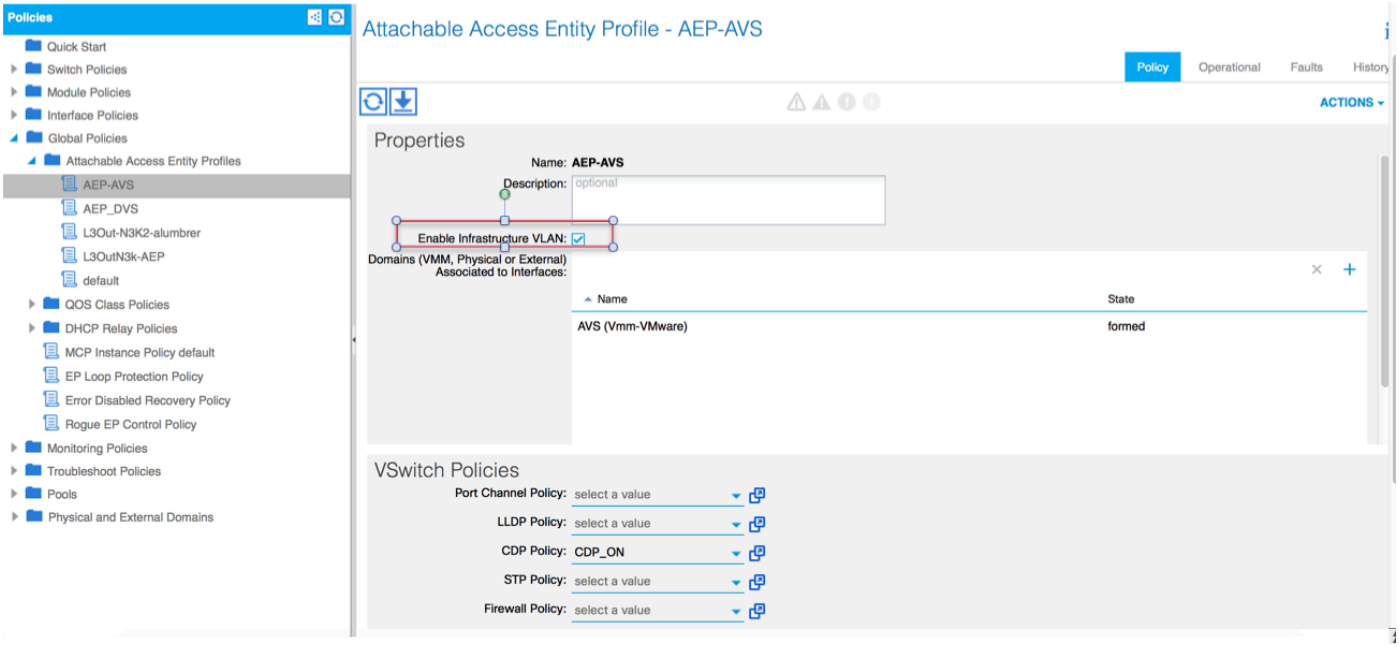
```
cisco@cisco-UbuntuClient:~$ ifconfig
eth1      Link encap:Ethernet  HWaddr 00:50:56:89:3f:ca
          inet addr:172.16.1.10  Bcast:172.16.1.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe89:3fca/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         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



Dépannage

L'adresse VTEP n'est pas attribuée

Vérifiez que le VLAN d'infrastructure est vérifié sous AEP :



Version non prise en charge

Vérifiez que la version VEM est correcte et prenez en charge le système VMWare ESXi approprié.

```
~ # 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
```

La communication VEM et Fabric ne fonctionne pas

```
- 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
```

À ce stade, il est possible de déterminer que la communication de fabric entre l'hôte ESXi et le leaf ne fonctionne pas correctement. Certaines commandes de vérification peuvent être vérifiées au niveau de la feuille pour déterminer la cause première.

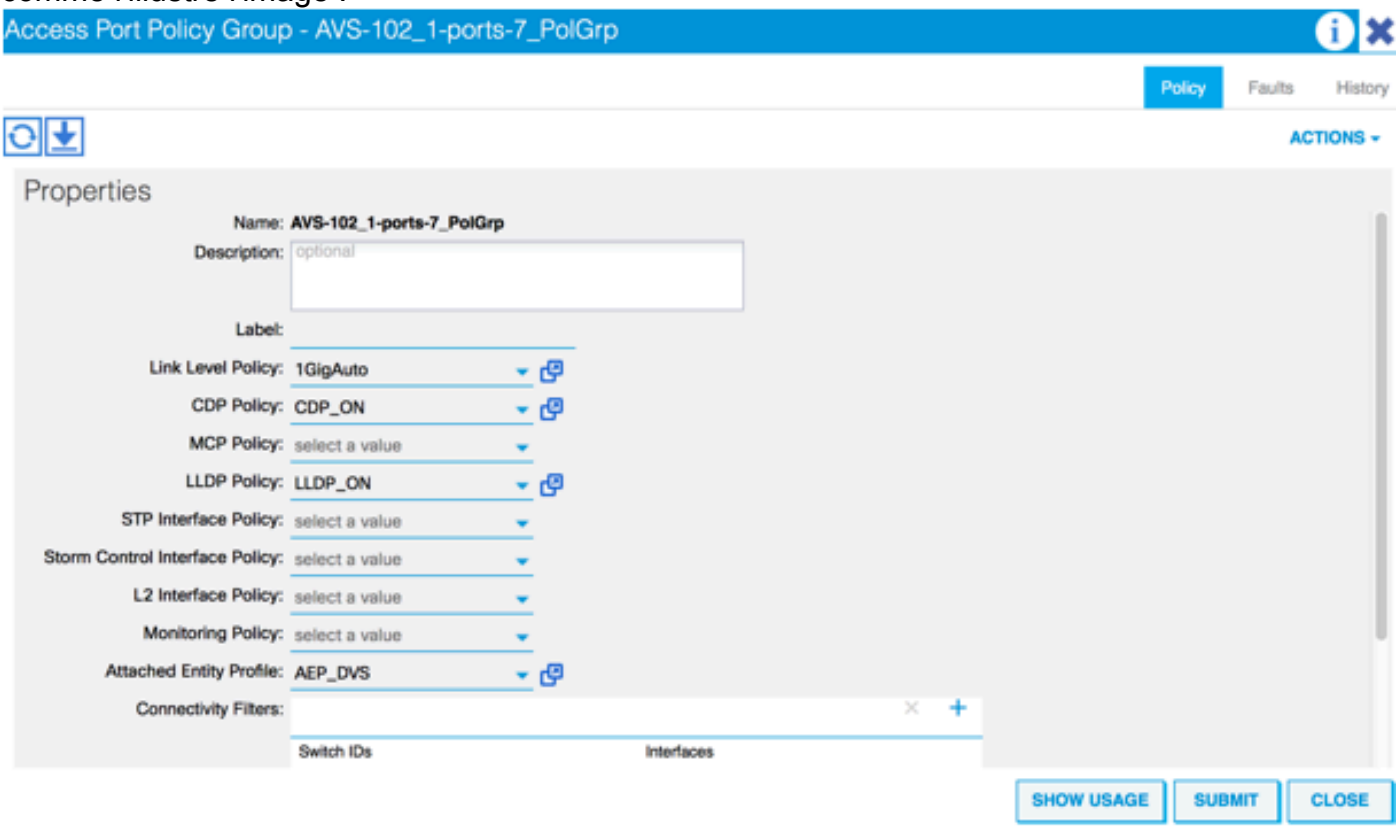
```
leaf2# show cdp ne

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)
```

Deux ports sont utilisés dans l'ESXi connecté via un 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
```

D'après le résultat ci-dessus, il est possible de constater que le VLAN Infra n'est pas autorisé ou ne passe pas par les ports de liaisons ascendantes qui vont à l'hôte ESXi (1/5-6). Ceci indique une mauvaise configuration avec la stratégie d'interface ou de commutateur configurée sur APIC. Cochez les deux :
Stratégies d'accès > Stratégies d'interface > Profils Stratégies d'accès > Stratégies de commutateur > Profils
Dans ce cas, les profils d'interface sont attachés au mauvais AEP (ancien AEP utilisé pour DVS), comme l'illustre l'image :



Après avoir configuré l'AEP correct pour AVS, nous pouvons maintenant voir que le VLAN Infra est vu à travers les Unlinks appropriés au niveau de la feuille :

```
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
```

Informations connexes

Installation du commutateur virtuel d'application

Cisco Systems, Inc. Guide d'installation du commutateur virtuel d'application Cisco, version 5.2(1)SV3(1.2)

Déployer ASAv à l'aide de VMware

Guide de démarrage rapide de Cisco Systems, Inc. Cisco Adaptive Security Virtual Appliance (ASAv), 9.4

Cisco ACI et Cisco AVS

Cisco Systems, Inc. Guide de virtualisation de l'ACI Cisco, version 1.2(1i)

Livre blanc sur la conception du graphique de services avec l'infrastructure axée sur les

applications Cisco

Livre blanc sur la conception du graphique de services avec l'infrastructure axée sur les applications Cisco

Support et documentation techniques - Cisco Systems