

ASAv in GoTo (L3) Mode met het gebruik van AVS-ACI 1.2(x) release

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Verifiëren](#)

[Probleemoplossing](#)

[Verwante informatie](#)

Inleiding

Dit document beschrijft hoe een AVS-switch (Application Virtual Switch) kan worden ingezet met één firewall voor adaptieve security virtuele applicatie (ASAv) in Routed/GOTO-modus als L4-L7 Service Graph tussen twee End Point-Groepen (EPG's) om client-naar-server communicatie op te zetten met ACI 1.2(x) release.

Voorwaarden

Vereisten

Cisco raadt u aan om kennis te hebben over deze onderwerpen:

- Toegangsbeleid ingesteld en interfaces ingesteld en in bedrijf
- reeds geconfigureerd EPG, Bridge Domain (BD) en Virtual Routing and Forwarding (VRF)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

Hardware en software:

- UCS C220 - 2.0(6d)
- ESXi/vCenter - 5.5
- ASAv - asa-toestel-pkg-1.2.4.8
- AVS - 5.2.1.SV3.1.10
- APIC - 1.2(1i)
- Leaf/Spines - 11.2(1i)
- Apparaatpakketten *.zip al gedownload

Functies:

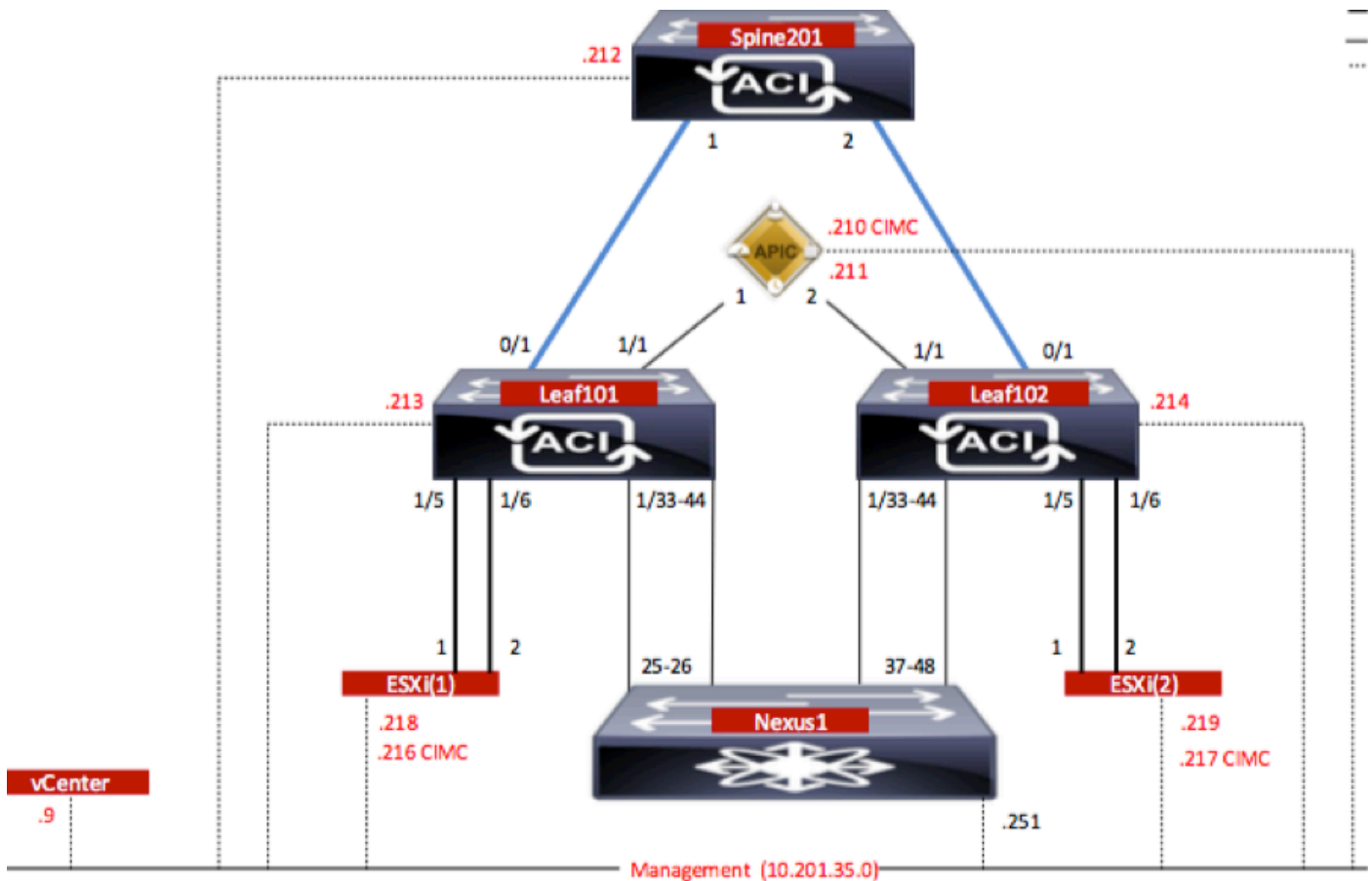
- AVS
- ASAv
- EPG's, BD, VRF
- Toegangscontrolelijst (ACL)
- L4-L7 servicesdiagram
- vCenter

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Netwerkdigram

Zoals in de afbeelding wordt weergegeven,



Configuraties

AVS Initiële Setup maakt een VMware vCenter Domain (VMware-integratie) 2

Opmerking:

- U kunt meerdere datacenters en DVS-items (Distributed Virtual Switch) maken onder één domein. U kunt echter maar één Cisco AVS-account voor elk datacenter hebben.

- De plaatsing van het servicesdiagram met Cisco AVS wordt ondersteund van Cisco ACI release 1.2(1i) met Cisco AVS release 5.2(1)SV3(1.10). De volledige configuratie van de servicesgrafiek wordt uitgevoerd op de Cisco Application Policy Infrastructuur Controller (Cisco APIC).
- De implementatie van Service Virtual Machine (VM) met Cisco AVS wordt alleen ondersteund op Virtual Machine Manager (VM)-domeinen met Virtual Local Area Networks (VLAN's) insluitingsmodus. De berekende VM's (de leverancier en de gebruiker VM's) kunnen echter deel uitmaken van VM-domeinen met Virtual Extensible LAN (VXLAN) of VLAN-insluiting.
- Let er ook op dat als een lokale switching wordt gebruikt, het Multicastadres en de pool niet nodig zijn. Als er geen lokale switching is geselecteerd, moet Multicast pool worden geconfigureerd en het multicast adres van AVS moet geen deel uitmaken van de multicast pool. Al het verkeer dat van de AVS afkomstig is, wordt VLAN of VXLAN ingekapseld.

Navigeren in naar **VM Network > VMWare > vCenter Domain**, zoals in de afbeelding wordt getoond:

Create vCenter Domain

Specify vCenter domain users and controllers

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: × +

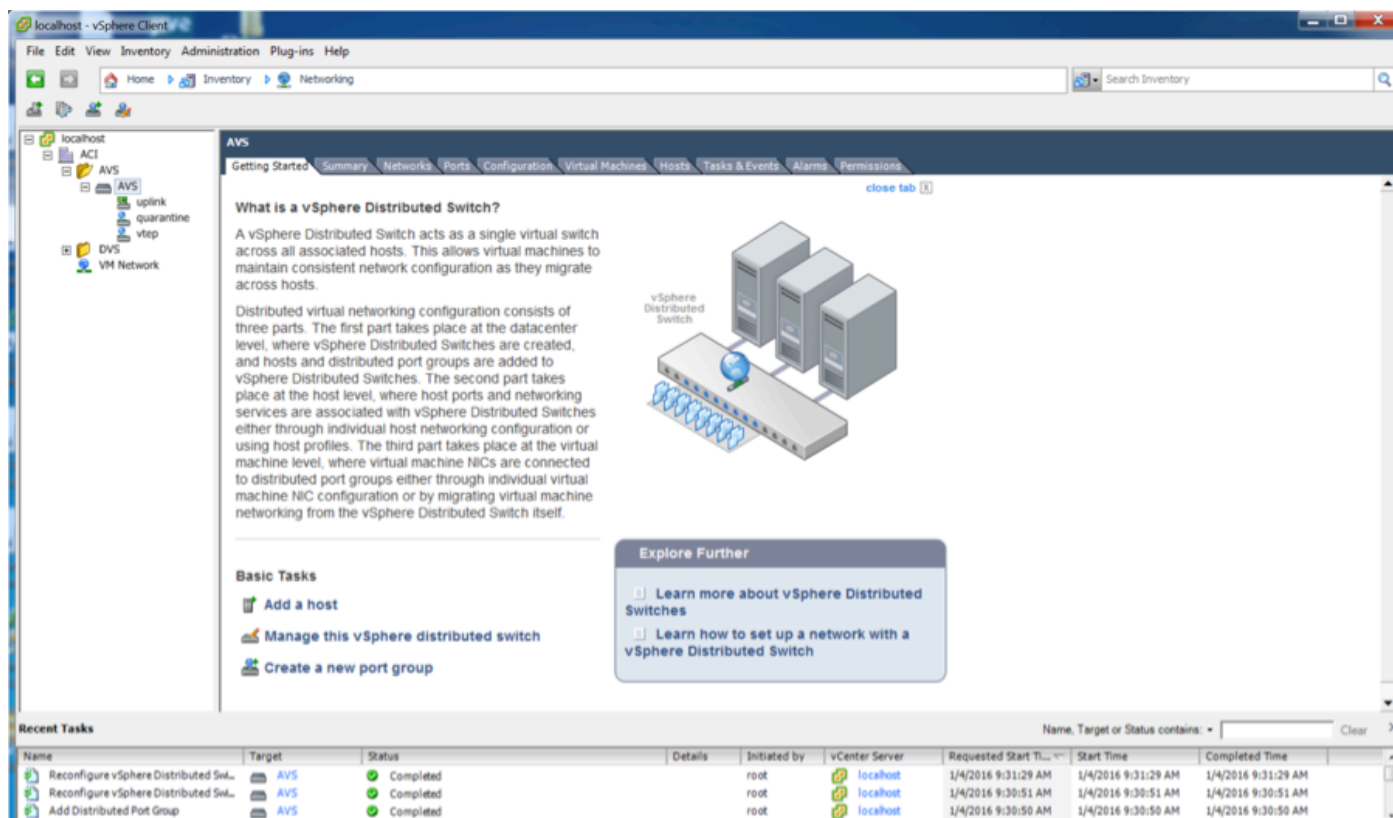
Profile Name	Username	Description
vCenterCredentials	root	

vCenter: × +

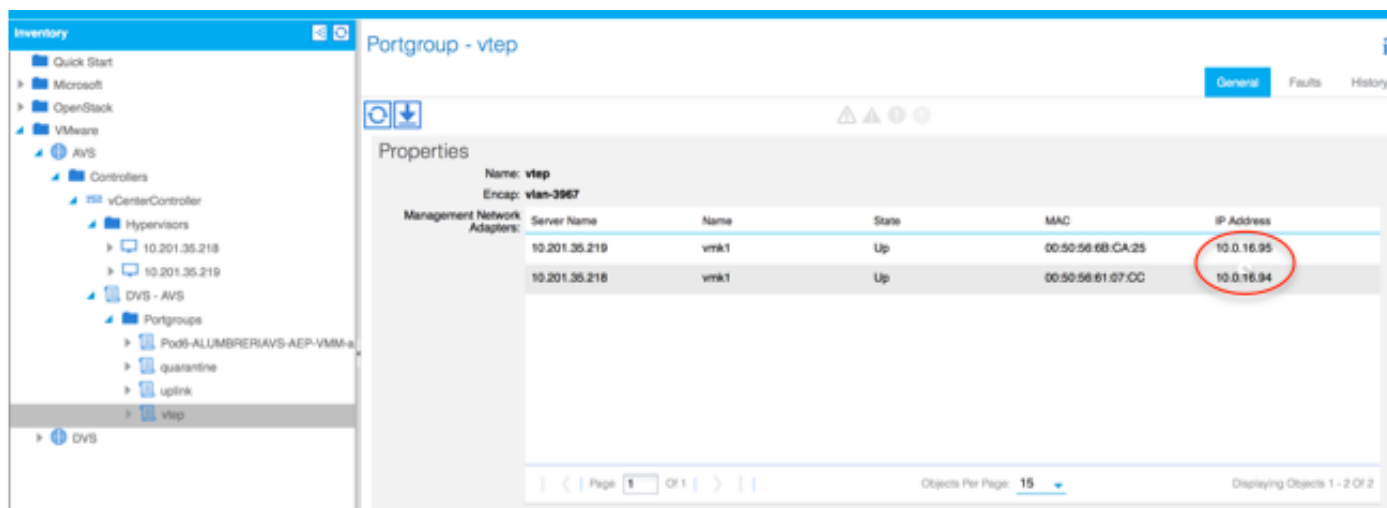
Name	IP	Type	Stats Collection
vCenterController	10.201.35.9	vCenter	Disabled

Als u Port-Channel of VPC (Virtual Port-Channel) gebruikt, wordt aanbevolen om het vSwitch-beleid in te stellen voor het gebruik van Mac-centrifugeren.

Daarna moet APIC de AVS switch configuratie naar vCenter duwen, zoals in de afbeelding wordt getoond:



Op APIC kunt u opmerken dat een VXLAN Tunnel Endpoint (VTEP) adres is toegewezen aan de VTEP poortgroep voor AVS. Dit adres wordt toegewezen ongeacht welke Connectivity-modus wordt gebruikt (VLAN of VXLAN)



Installeer de Cisco AVS-software in vCenter.

- Download vSphere Installatie Bundle (VIB) vanuit CCO door deze [link](#) te gebruiken

Opmerking: in dit geval gebruiken we ESX 5.5, tabel 1, geeft de compatibiliteitsmatrix voor ESXi 6.0, 5.5, 5.1 en 5.0 weer

Tabel 1 - host-softwareversie en compatibiliteit voor ESXi 6.0, 5.5, 5.1 en 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

In het ZIP-bestand zijn er 3 VIB-bestanden, één voor elk van de ESXi-hostversies, selecteer de bestanden die geschikt zijn voor ESX 5.5, zoals in de afbeelding:

Name	Date Modified	Date Created	Size	Kind
License_Copyright_Document.pdf	Dec 9, 2015, 12:10 AM	Dec 9, 2015, 12:10 AM	1 MB	PDF Doc
README.txt	Dec 9, 2015, 12:10 AM	Dec 9, 2015, 12:10 AM	2 KB	text
cross_cisco-vem-v250-5.2.1.3.1.10.0-3.1.1.vib	Dec 9, 2015, 12:10 AM	Dec 9, 2015, 12:10 AM	8.9 MB	Unix E...
cross_cisco-vem-v250-5.2.1.3.1.10.0-3.2.1.vib	Dec 9, 2015, 12:10 AM	Dec 9, 2015, 12:10 AM	9 MB	Unix E...
cross_cisco-vem-v250-5.2.1.3.1.10.0-6.0.1.vib	Dec 9, 2015, 12:10 AM	Dec 9, 2015, 12:10 AM	9 MB	Unix E...
VEM510-201512250107-BG-release.zip	Dec 9, 2015, 12:10 AM	Dec 9, 2015, 12:10 AM	8.5 MB	ZIP archi
VEM550-201512250113-BG-release.zip	Dec 9, 2015, 12:10 AM	Dec 9, 2015, 12:10 AM	8.6 MB	ZIP archi
VEM600-201512250119-BG-release.zip	Dec 9, 2015, 12:10 AM	Dec 9, 2015, 12:10 AM	8.6 MB	ZIP archi

- Kopieer het VIB-bestand naar ESX Datastore - dit kan via CLI of rechtstreeks vanaf vCenter worden gedaan

Opmerking: Als er een VIB-bestand op de host bestaat, verwijdert u het bestand door de opdracht **esxcli software vib** te gebruiken.

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

of door rechtstreeks door te bladeren in de Datastore.

- Installeer de AVS-software met de volgende opdracht op de ESXi-host:

esxcli software vib install -v /vmfs/Volume/datastore1/cross_cisco-vem-v250-5.2.1.3.1.10.0-3.2.1.vib —onderhoudsmodus —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

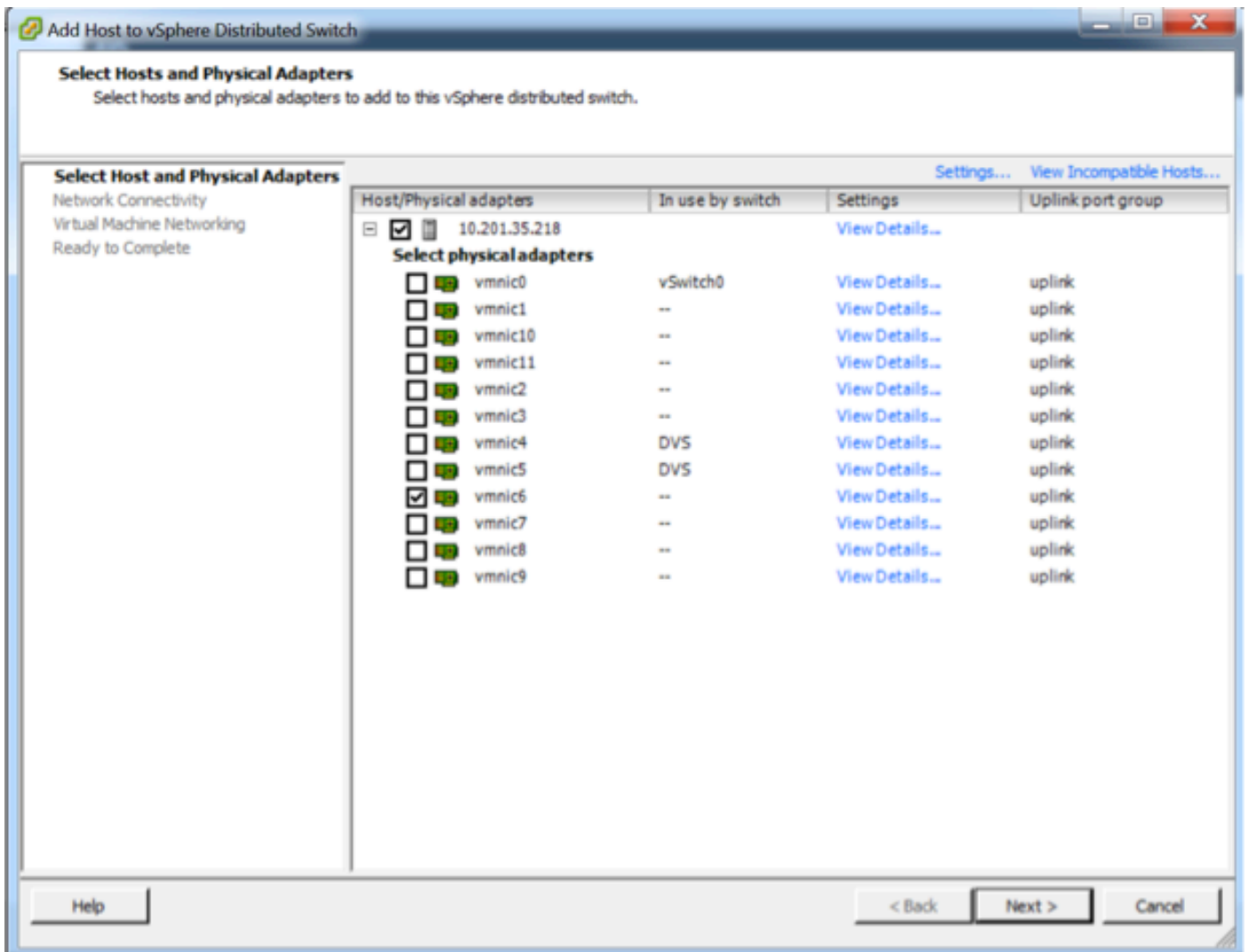
Switch Name    Num Ports  Used Ports  Configured Ports  MTU    Uplinks
vSwitch0      5632       8           128              1500   vmnic0
DVS Name       Num Ports  Used Ports  Configured Ports  MTU    Uplinks
DVS            5632       10          512              9000   vmnic5,vmnic4

VEM Agent (vemdpa) is running
~ #

```

- Nadat de Virtual Ethernet-module (VEM) is geïnstalleerd, kunt u hosts aan uw AVS toevoegen:

In het dialoogvenster Add Host to vSphere Distributed Switch kiest u de virtuele NIC-poorten die worden aangesloten op de bladswitch (In dit voorbeeld verplaatst u alleen vmnic6), zoals in de afbeelding:



- Klik op **Volgende**
- Klik in het dialoogvenster Network Connectivity op **Volgende**
- Klik in het dialoogvenster Virtual Machine Network op **Volgende**
- Klik in het dialoogvenster Klaar om te voltooien op **Voltooien**

Opmerking: Als er meerdere ESXi-hosts gebruikt worden, moeten al deze hosts gebruik worden gemaakt van de AVS/VEM zodat zij kunnen worden bestuurd van de standaard switch tot DVS of AVS.

Hierdoor is de integratie van AVS voltooid en zijn we klaar om door te gaan met de inzet van L4-L7 ASAv:

ASAv eerste instelling

- Cisco ASAv-apparaatpakket downloaden en in APIC importeren:

Navigeren in op **L4-L7 Services > Packages > het apparaatpakket importeren**, zoals in de afbeelding wordt getoond:

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.

Quick Start

[Import a Device Package](#)

Import Device Package
i
X

File Name: BROWSE...

SUBMIT
CLOSE

Device Types

- Als alles goed werkt, kunt u het geïmporteerde apparaatpakket zien, waarmee de map L4-L7-servicetypen wordt uitgebreid, zoals in de afbeelding:

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: |

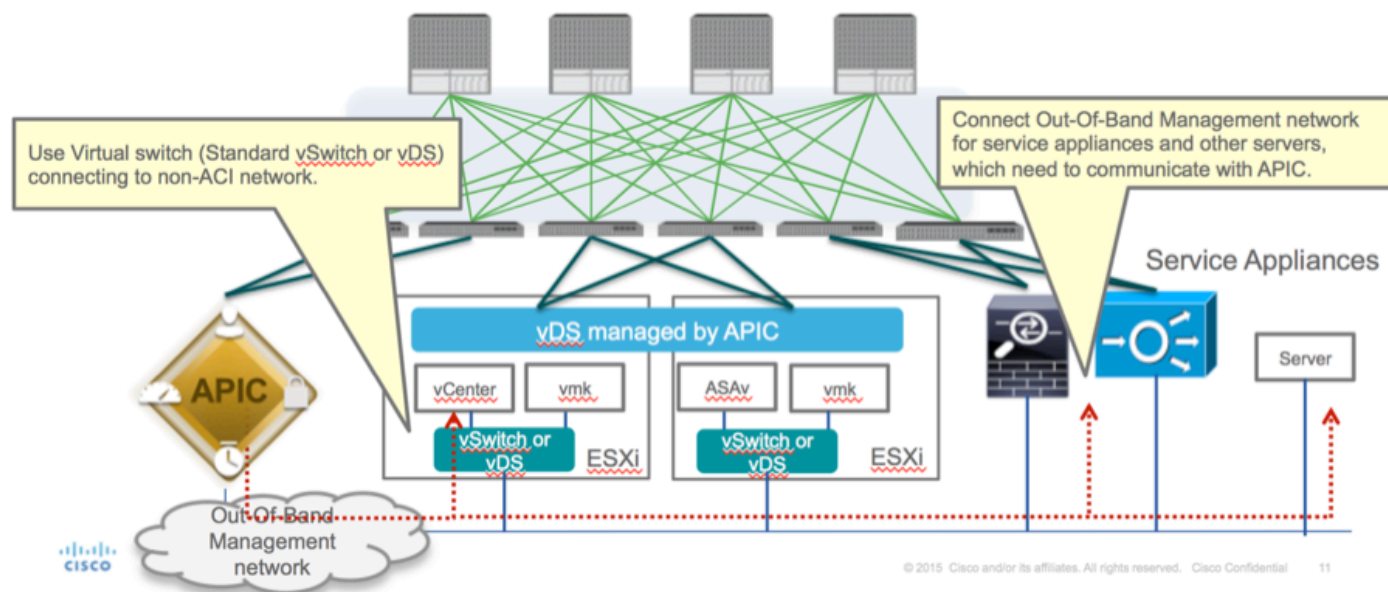
Interface Labels:

Name
cluster_ctrl_lk
external
failover_lan
failover_link
internal
mgmt
utility

Voordat u verdergaat, zijn er weinig aspecten van de installatie die moeten worden bepaald voordat de echte L4-L7 integratie wordt uitgevoerd:

Er zijn twee soorten beheernetwerken: In-Band Management en Out-Band (OB); deze kunnen worden gebruikt voor het beheer van apparaten die geen deel uitmaken van de basis-Application Centric Infrastructure (ACI) (blad, stekels of apic controller) die ASA's, Loadbalancers, enz. zouden omvatten.

In dit geval wordt OB voor ASA's ingezet met behulp van de standaard vSwitch. Voor niet-metalen ASA of andere serviceapparatuur en/of servers sluit u de OB Management-poort aan op de OB-switch of het OB-netwerk, zoals in de afbeelding wordt getoond.



ASA's OB MGMT-poortverbinding moet ESXi-uplinks gebruiken om te communiceren met APIC via OOB. Wanneer u vNIC-interfaces in kaart brengt, komt netwerkadapter1 altijd overeen met de Management0/0-interface in de ASA's en de rest van de datacommunicatie wordt gestart vanaf Network adapter2.

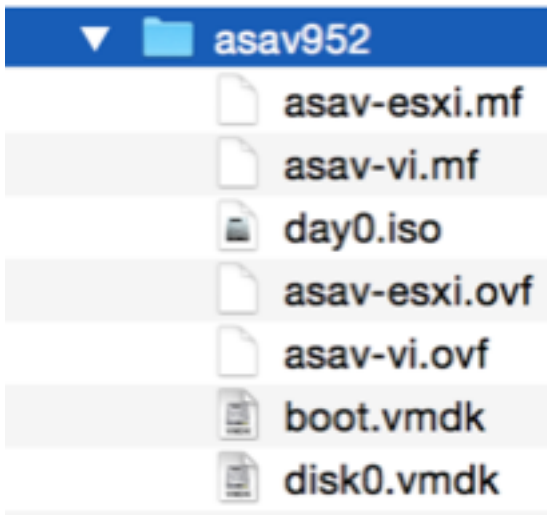
Tabel 2 toont de overeenstemming van netwerkadapter-ID's en ASA's-interface-ID's:

Tabel 2

Network Adapter ID	ASA's 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

- De ASA's VM implementeren via de wizard van **File>OVF (Open Virtualization Format)-sjabloon implementeren**
- Selecteer **asav-esxi** als u standalone ESX Server of **asav-vi** voor vCenter wilt gebruiken. In dit

geval wordt vCenter gebruikt.



- Ga door de installatiewizard, accepteer bepalingen en voorwaarden. Midden in de wizard kunt verschillende opties bepalen, zoals hostname, beheer, ip-adres, firewallmodus en andere specifieke informatie over ASAv. Denk eraan om OB-beheer voor ASAv te gebruiken, zoals in dit geval u interfacebeheer0/0 moet bewaren terwijl u het VM Network (Standard Switch) gebruikt en de interface Gigabit Ethernet0-8 de standaardnetwerkpoorten is.

Source

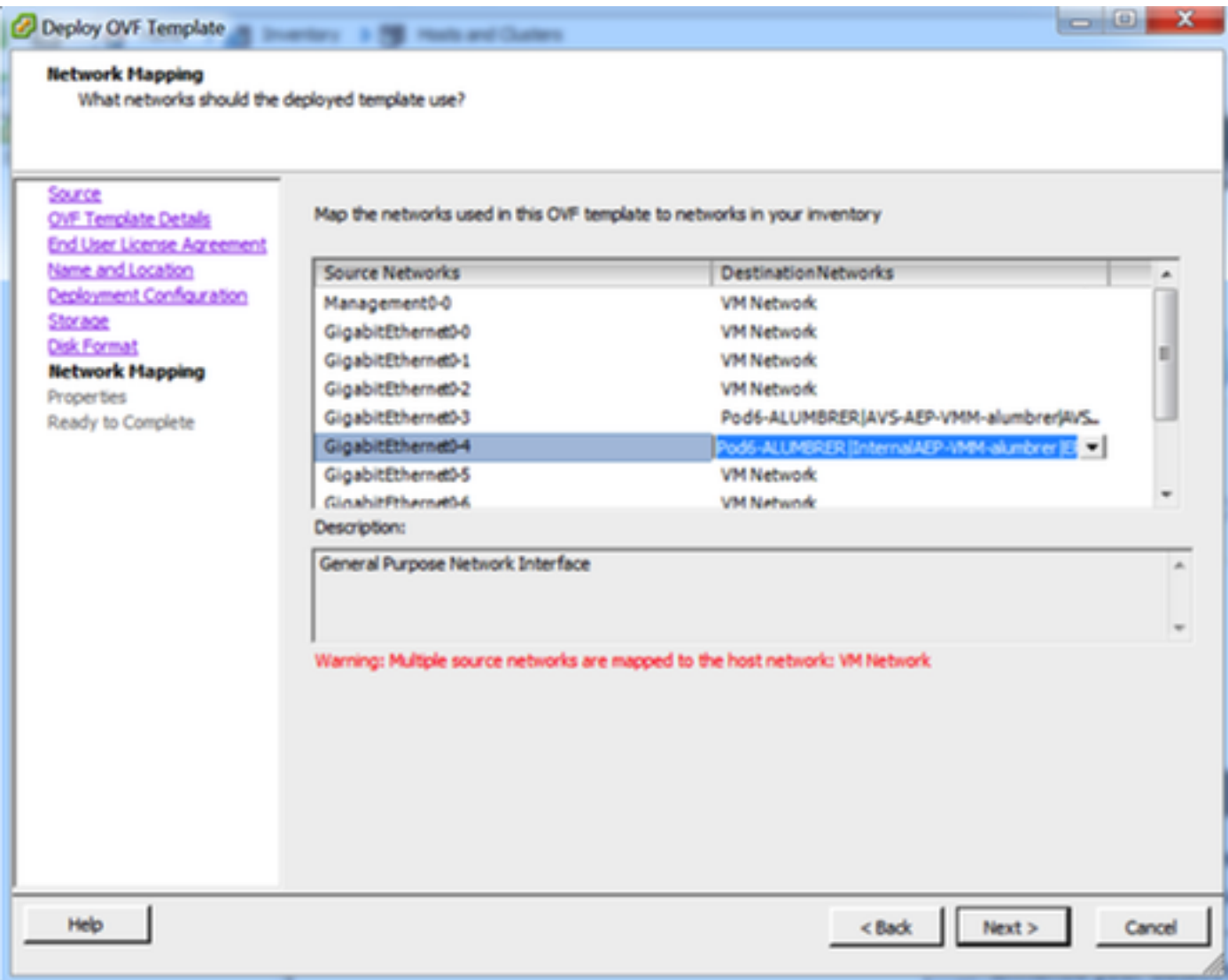
Select the source location.

Source

OVF Template Details
Name and Location
Storage
Disk Format
Ready to Complete

Deploy from a file or URL

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.



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

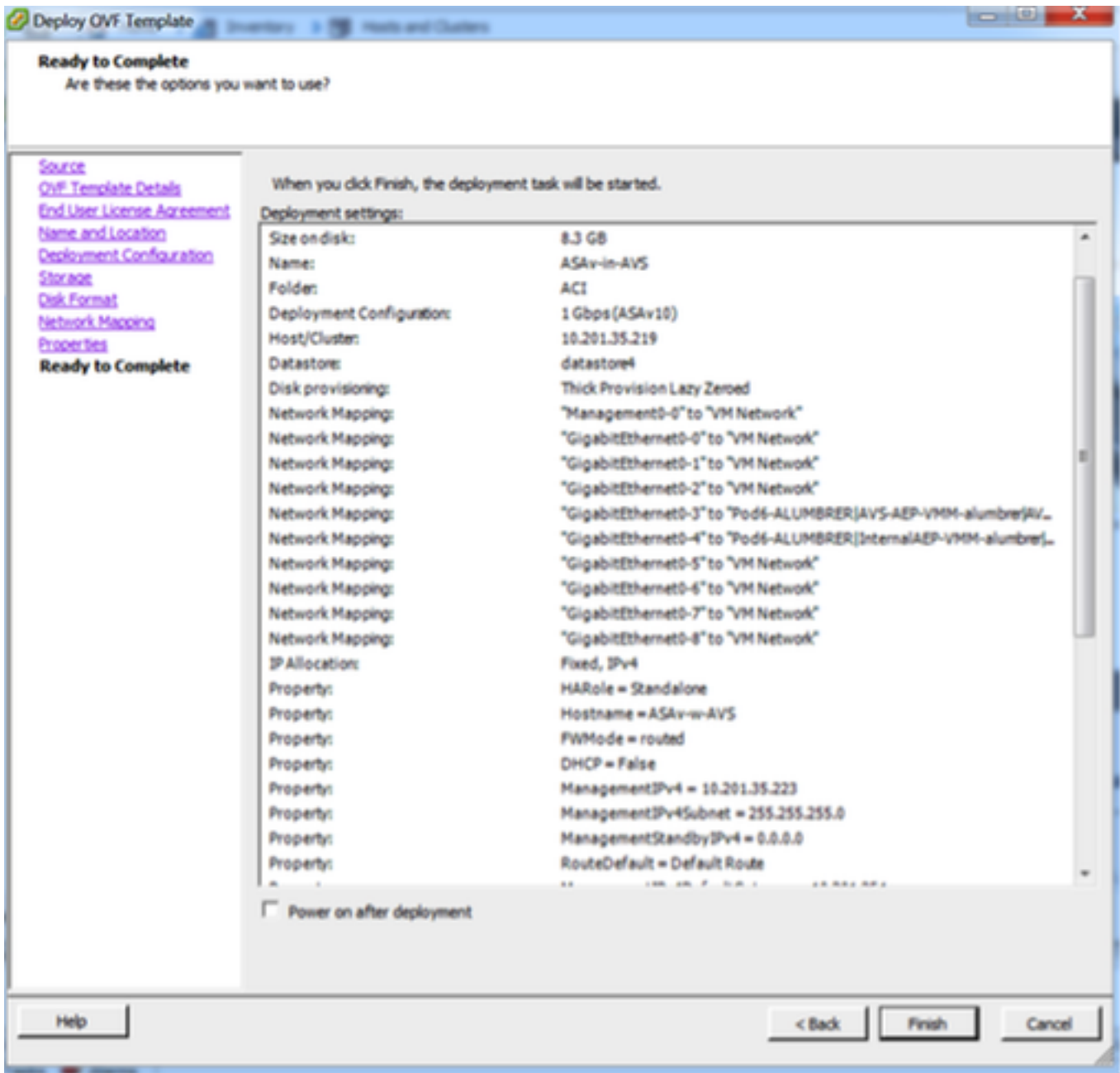
Firewall Properties
Firewall Mode
Select the Firewall Mode
routed

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

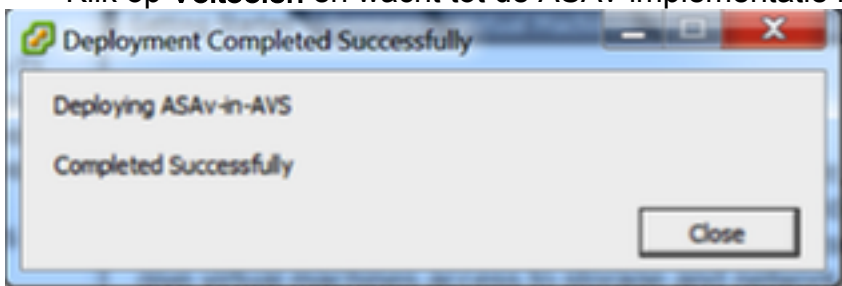
Management IP Address
Enter the Management IPv4 Address. For HA-type deployments, this property specifies the Management IPv4 address of the Active HA host.
10 . 201 . 35 . 223

Management IP Subnet Mask

Help < Back Next > Cancel



- Klik op **Voltoeien** en wacht tot de ASAv-implementatie is voltooid



- Power On uw ASA VM en log in via console om eerste configuratie te verifiëren

```

?
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 --->_

```

- Zoals in de afbeelding wordt getoond, wordt sommige beheerconfiguratie al naar de ASA firewall geduwd. Configureer de gebruikersnaam en het wachtwoord voor de beheerder. Deze gebruikersnaam en het wachtwoord worden door APIC gebruikt om in te loggen en de ASA te configureren. De ASA zou connectiviteit moeten hebben aan het OB netwerk en APIC moeten kunnen bereiken.

wachtwoord voor gebruikersnaam <device_password> gecodeerd recht 15

```

ASA-v-w-AUS(config)# username admin password C1sc0123 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)# _

```

Daarnaast schakelt u http server in vanaf de Global Configuration-modus:

http-server

http 0.0.0.0.0.0.0

L4-L7 voor ASA-v-integratie in APIC:

- Meld u aan bij de ACI GUI, klik op de aanbesteding waar het servicesdiagram wordt ingezet. L4-L7-services uitvouwen onder in het navigatiedeelvenster en met de rechtermuisknop op L4-L7-apparaten en op L4-L7-apparaten maken om de wizard te openen

- Voor deze implementatie worden de volgende instellingen toegepast:

Beheerde modus

Firewallservice

-virtueel apparaat

-Verbonden met een AVS-domein met één knooppunt

ASA 5500-V model

Routed Mode (GoTo)

-Management Address (moet het eerder toegewezen adres aan de MGMT0/0 interface aanpassen)

- Gebruik HTTPS als APIC standaard het best beveiligde protocol om met ASAv te communiceren

Create L4-L7 Devices i x

STEP 1 > General 1. General 2. Device Configuration

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

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

Connectivity

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

Credentials

Username: admin

Password:

Confirm Password:

- De juiste definitie van de apparaatinterfaces en de clusterinterfaces is van cruciaal belang voor een succesvolle implementatie

Voor het eerste deel, gebruik tabel 2 in de vorige sectie om de IDs van de Netwerkadapter goed aan te passen aan de ASAv interface-IDs die u wilt gebruiken. Het pad verwijst naar de fysieke poort of poortkanaal of VPC die de weg in en uit de firewallinterfaces mogelijk maakt. In dit geval, is ASA gevestigd in een ESX host, waar in en uit hetzelfde zijn voor beide interfaces. In een fysiek apparaat zouden binnen en buiten de firewall (FW) verschillende fysieke poorten zijn.

Voor het tweede deel moeten de Cluster interfaces altijd worden gedefinieerd zonder uitzonderingen (zelfs als Cluster HA niet wordt gebruikt), dit is omdat het Objectmodel een

associatie heeft tussen de **mAs**-interface (meta-interface op het Apparaatpakket), de **Lif**-interface (bladinterface zoals bijvoorbeeld, extern, intern, binnen, enz.) en de **Cif** (beton) . De L4-L7 betonapparaten moeten worden geconfigureerd in een apparaatclusterconfiguratie en deze abstractie wordt een logisch apparaat genoemd. Het logische apparaat heeft logische interfaces die in kaart worden gebracht aan concrete interfaces op het betonnen apparaat.

Voor dit voorbeeld zal de volgende vereniging worden gebruikt:

Gi0/0 = Vmnic2 = serverInt/provider/server > EPG1

Gi0/1 = Vmnic3 = clientInt/consument/cliënt > EPG2

L4-L7 Devices - ASAv-AVS-Routed

The screenshot displays the configuration page for 'L4-L7 Devices - ASAv-AVS-Routed'. It is divided into several sections:

- General:** Managed (checked), Name: ASAv-AVS-Routed, Device Package: CISCO-ASA-1.2, Service Type: Firewall, Device Type: VIRTUAL, VMM Domain: AVS, Context Aware: Single, Function Type: GoThrough (selected), Cluster Mode: Single Node.
- Credentials:** Username: admin, Password: [redacted], Confirm Password: [redacted].
- Configuration State:** Configuration Issues: [redacted], Devices State: **stable** (circled in red).
- Device 1:** Management IP Address: 10.201.35.223, Management Port: 443, vCenter Name: vCenterController, VM Name: **ASAv-in-AVS** (circled in red). Interfaces table:

Name	VMC	Path (Only For Route Peering)
GigabitEthernet0/1	Network adapter 3	Node-102/MAC_Pinning, Nod...
GigabitEthernet0/2	Network adapter 4	Node-102/MAC_Pinning
- Cluster:** Management IP Address: 10.201.35.223, Management Port: 443. Cluster Interfaces table:

Type	Name	Concrete Interfaces
consumer	ClientInt	ASAv-AVS-Routed_Device_1[GigabitEthernet0/2]
provider	ServerInt	ASAv-AVS-Routed_Device_1[GigabitEthernet0/1]

Opmerking: Voor failover/HA-implementaties wordt Gigabit Ethernet 0/8 vooraf geconfigureerd als de failover-interface.

De status van het apparaat moet stabiel zijn en u dient bereid te zijn om het sjabloon van het functieprofiel en de servicesdiagram in te voeren

Servicecamera

Om te beginnen, om een Functieprofiel voor ASAv te maken maar daarvoor moet u Functie Profile Group en dan L4-L7 Services Functie Profile onder deze map maken, zoals in de afbeelding te zien is:

Create L4-L7 Services Function Profile Group

Specify the information about the Function Profile Group

Name: FunProfGroup

Description:

SUBMIT CANCEL

Tenant Pod9-ALUMBRER

L4-L7 Services Function Profile Group - FunProfGroup

General Faults History

Properties

Name: FunProfGroup

Description:

Service Function Profiles:

Name	Associated Function	Description
No items have been found. Select Actions to create a new item.		

Delete
 Create L4-L7 Services Function Profile
 Save as ...
 Post ...

- Selecteer het **Webex ProfileForRoutedMode** van het uitrolmenu en ga verder om de interfaces op de firewall te configureren. Vanaf hier zijn de stappen optioneel en kunnen deze later worden geïmplementeerd of aangepast. Deze stappen kunnen in een paar verschillende fasen in de implementatie worden genomen afhankelijk van hoe herbruikbaar of aangepast de Grafiek van de Dienst zou kunnen zijn.

Voor deze oefening vereist een routed Firewall(GoTo Mode) dat elke interface een uniek IP-adres heeft. De standaard ASA-configuratie heeft ook een interface-beveiligingsniveau (externe interface is minder veilig, interne interface is veiliger). U kunt de naam van de interface ook wijzigen volgens uw vereisten. In dit voorbeeld worden de standaardinstellingen gebruikt.

- Uitbreidt de interface-specifieke configuratie, voegt IP-adres en beveiligingsniveau voor ServerInt toe met de volgende indeling voor het IP-adres **x.x.x.x/y.y.y** of **x.x.x.x/yy**. Herhaal het proces voor de ClientInt-interface.

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.

Features:

Interfaces

AccessLists

NAT

TrafficSelectionObjects

All

Basic Parameters

All Parameters

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...	externallICfg			false	
IPv4 Address Configura...					
IPv4 Address	ipv4_address	192.168.10.1/24			
IPv4 Standby Address					
IPv6 Address Configura...					
IPv6 Link Local Address...					

UPDATE

RESET

CANCEL

SUBMIT

CANCEL

Opmerking: U kunt ook de standaardinstellingen voor toegangslijsten wijzigen en uw eigen basissjabloon maken. Standaard zal de RoutedMode-sjabloon regels voor HTTP en HTTPS bevatten. Voor deze oefening zullen SSH en ICMP aan de toegestane buitentoegangslijst worden toegevoegd.

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.

Features:

Interfaces

AccessLists

NAT

TrafficSelectionObjects

All

Basic Parameters

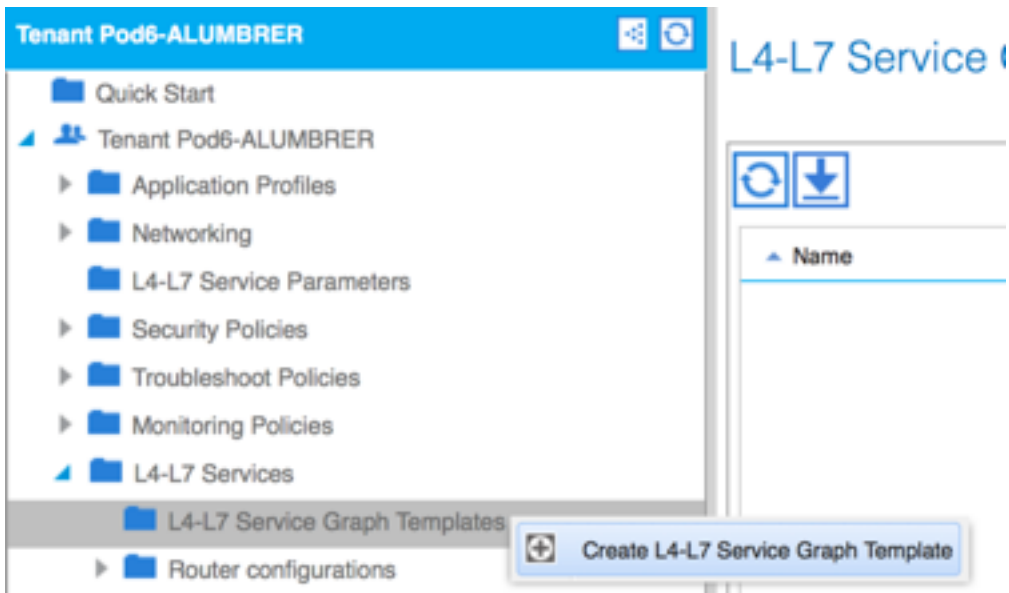
All Parameters

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	

SUBMIT

CANCEL




- Klik vervolgens op **Inzenden**
- Creëer nu de opdracht Grafiek Service



- Sleep de Cluster in het recht om de relatie tussen consument en leverancier te vormen, selecteer Routed Mode en het eerder gemaakte functieprofiel.

Graph Name:


Graph Type: Create A New One Clone An Existing One

Consumer  —  — **Provider** 

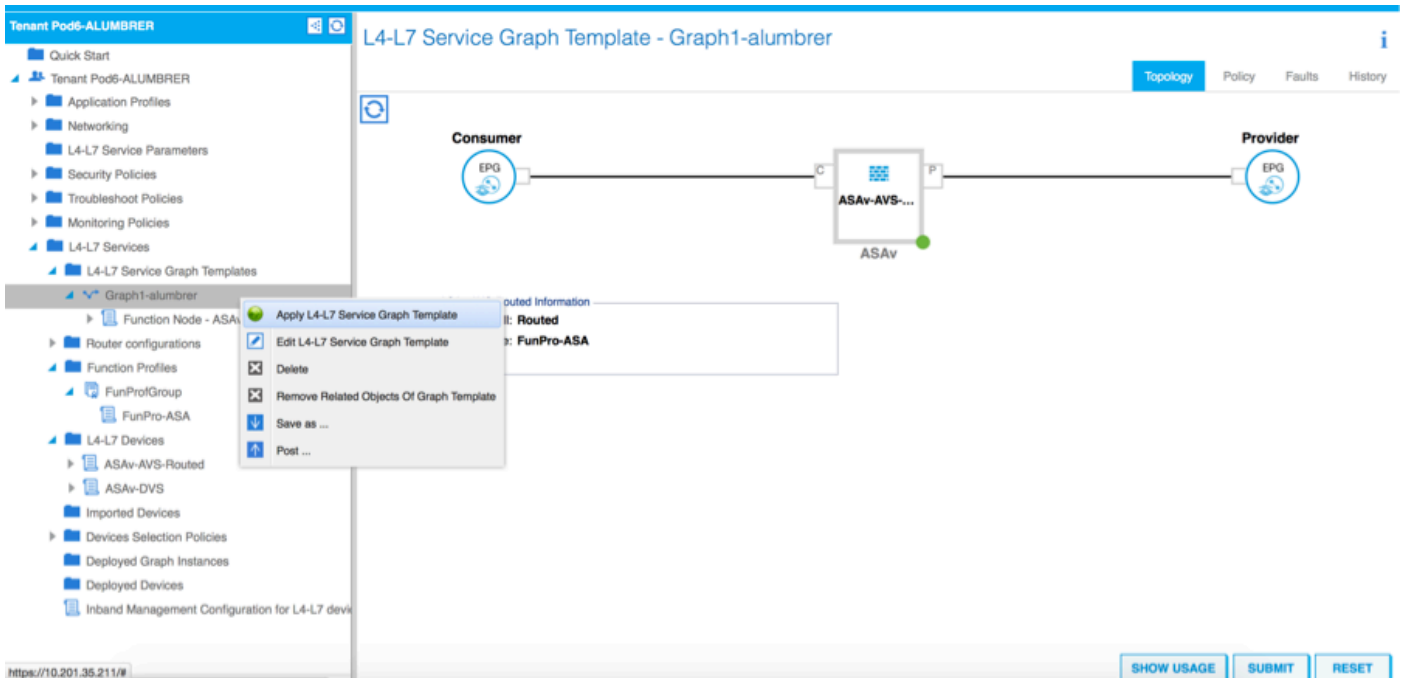
Please drag a device from devices table and drop it here to create a service node.

ASAv-AVS-Routed Information

Firewall: Routed Transparent

Profile: 

- Controleer het sjabloon op fouten. De sjablonen worden gecreëerd om opnieuw te kunnen worden gebruikt, ze moeten dan worden toegepast op specifieke EPG's etc.
- Als u een sjabloon wilt toepassen, klikt u met de rechtermuisknop en vervolgens selecteert u L4-L7 Service Graphsjabloon toepassen



- Stel vast welke EPG aan de zijde van de consument en aan de zijde van de leverancier zal staan. In deze oefening is AVS-EPG2 de Consumentenklant (client) en AVS-EPG1 is de Provider (server). Onthoud dat er geen filter wordt toegepast, zodat de firewall alle filtering kan uitvoeren op basis van de toegangslijst die is gedefinieerd in de laatste sectie van deze wizard.
- Klik op **Volgende**

STEP 1 > Contract

1. Contract 2. Graph

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

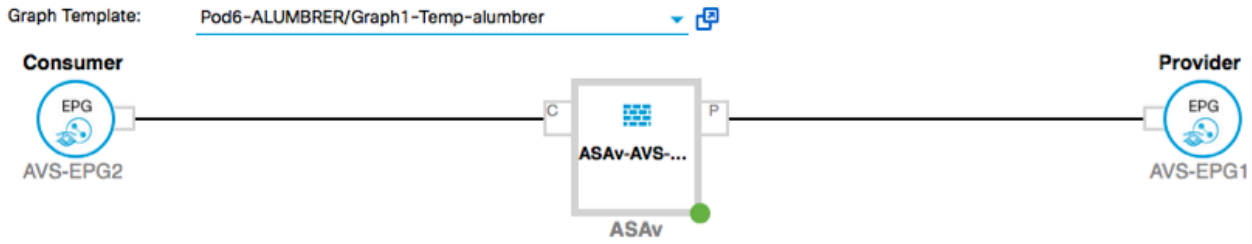
No Filter (Allow All Traffic):

Pod6-ALUMBRER/AVS-AEP-VMM-alumbrer/epg-AVS-EPG1
 Pod6-ALUMBRER/InternalAEP-VMM-alumbrer/epg-EPG-Internal-alumbrer
 Pod6-ALUMBRER/VRF1-alumbrer/AnyEPG
 Pod6-ALUMBRER/VRF2/AnyEPG
 Pod6-ALUMBRER/L3Out-N3K2/L3Net

PREVIOUS NEXT CANCEL

- Controleer de BD - informatie voor elk van de EPG's. In dit geval is EPG1 de leverancier op de IntBD-DB en EPG2 de consument op BD ExtBD. EPG1 sluit een verbinding op een firewallinterface ServerInt en EPG2 wordt aangesloten op een interface-clientInt. Beide interfaces worden het DG voor elk van de EPG's, zodat het verkeer te allen tijde de firewall moet oversteken.

- Klik op **Volgende**



ASAv-AVS-Routed Information

Firewall: routed
Profile: FunPro-ASA

Consumer Connector

Type: General Route Peering

BD: Pod6-ALUMBRER/ExtBD-alubrер

Cluster Interface: ClientInt

Provider Connector

Type: General Route Peering

BD: Pod6-ALUMBRER/IntBD-alubrер

Cluster Interface: ServerInt

PREVIOUS NEXT CANCEL

- Klik in het gedeelte Config op **Alle parameters** en controleer of er RODE indicatoren zijn die moeten worden bijgewerkt/geconfigureerd. In de uitvoer zoals weergegeven in de afbeelding, kan worden opgemerkt dat de volgorde op de toegangslijst is gemist. Dit is gelijk aan de lijnvolgorde die u in een toonip access-list X zult zien.

STEP 3 > ASAv-AVS-Routed Parameters

1. Contract 2. Graph 3. ASAv-AVS-Routed Parameters

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	SSH2		
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

- U kunt ook de IP-adressering controleren die is toegewezen op basis van het functieprofiel dat eerder is gedefinieerd. Hier is een goede kans om informatie indien nodig te wijzigen. Nadat

alle parameters zijn ingesteld, klikt u op **Voltooien**, zoals in de afbeelding:

STEP 3 > ASA-**AVS-Routed Parameters**

1. Contract 2. Graph 3. ASA-**AVS-Routed Parameters**

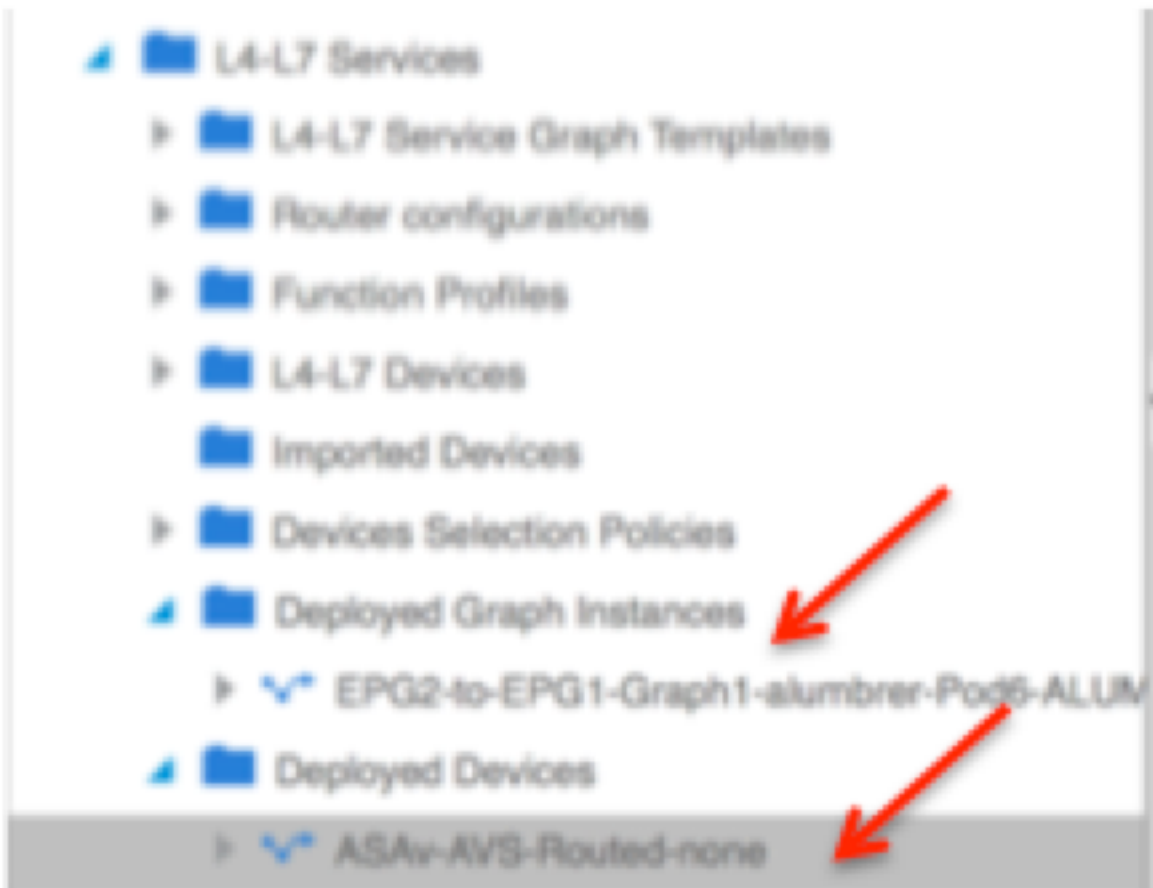
config parameters for the selected device

Profile Name: FunProf-ASA

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			

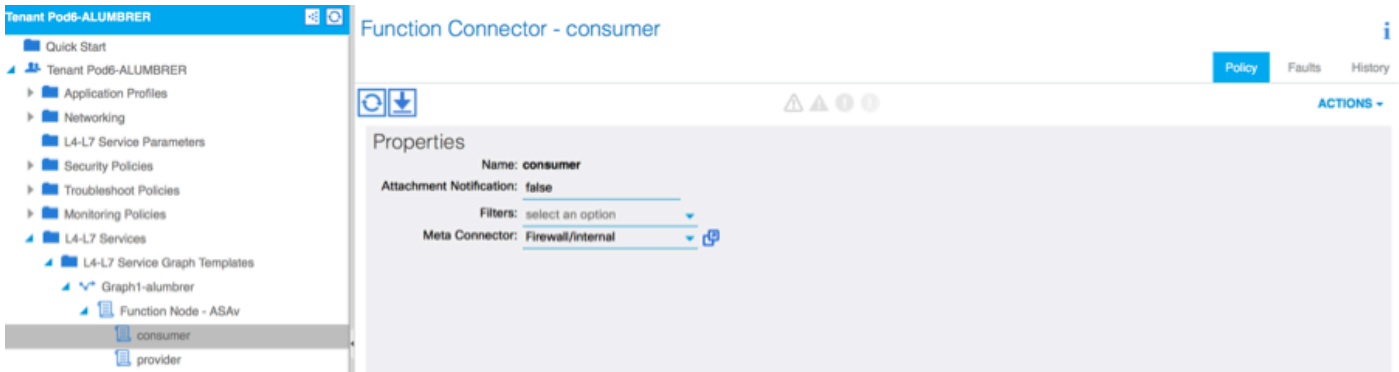
RED indicators parameters needed to be updated and GREEN indicates parameters will be submitted to the provider EPG.

- Als alles goed gaat, moet er een nieuw gebruikt apparaat en een Graph Instance verschijnen.

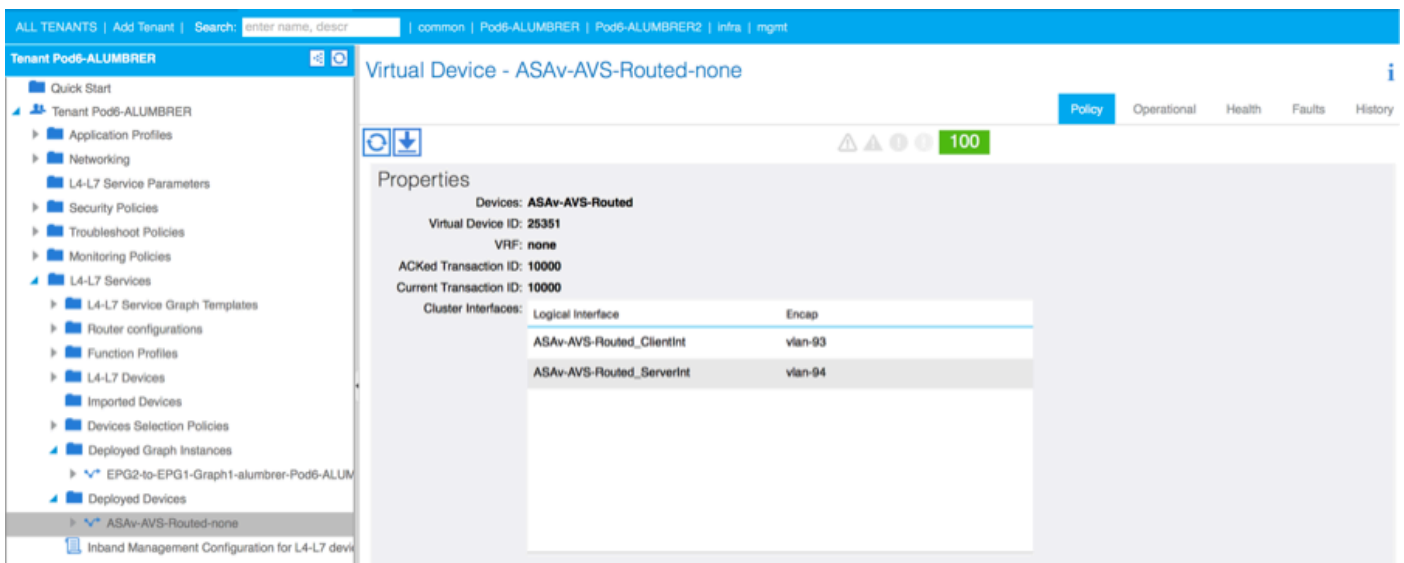


Verifiëren

- Een belangrijk ding om te verifiëren na het creëren van de Servicegrafiek is dat de relatie tussen consument en leverancier met de juiste Meta-connector is gecreëerd. Controleer dit onder de eigenschappen van de functieknoop.



Opmerking: Elke interface van de Firewall wordt toegewezen met een encap-VLAN uit de AVS Dynamic Pool. Controleer of er geen fouten zijn.



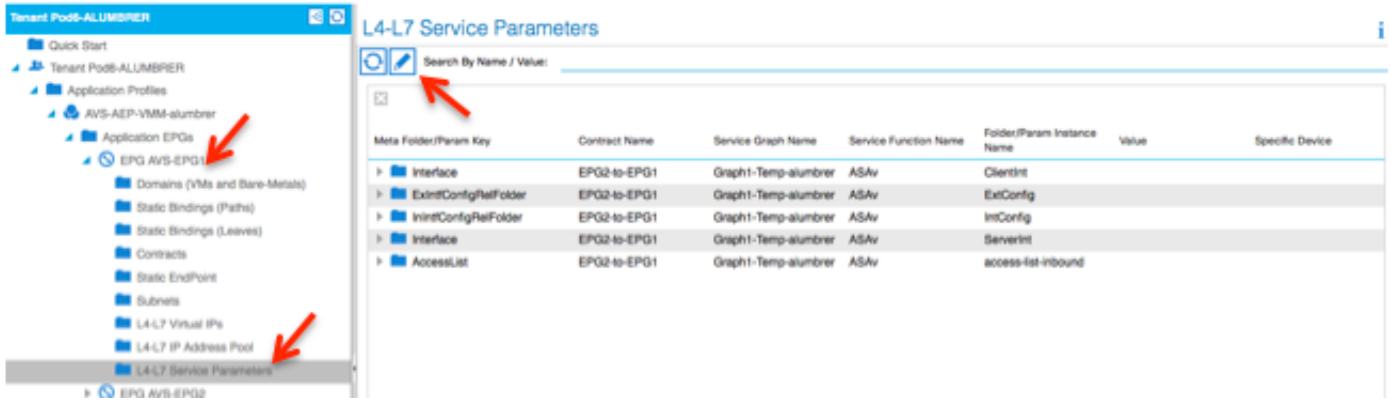
- Nu kan je ook de informatie verifiëren die naar de ASAv is gestuurd

```

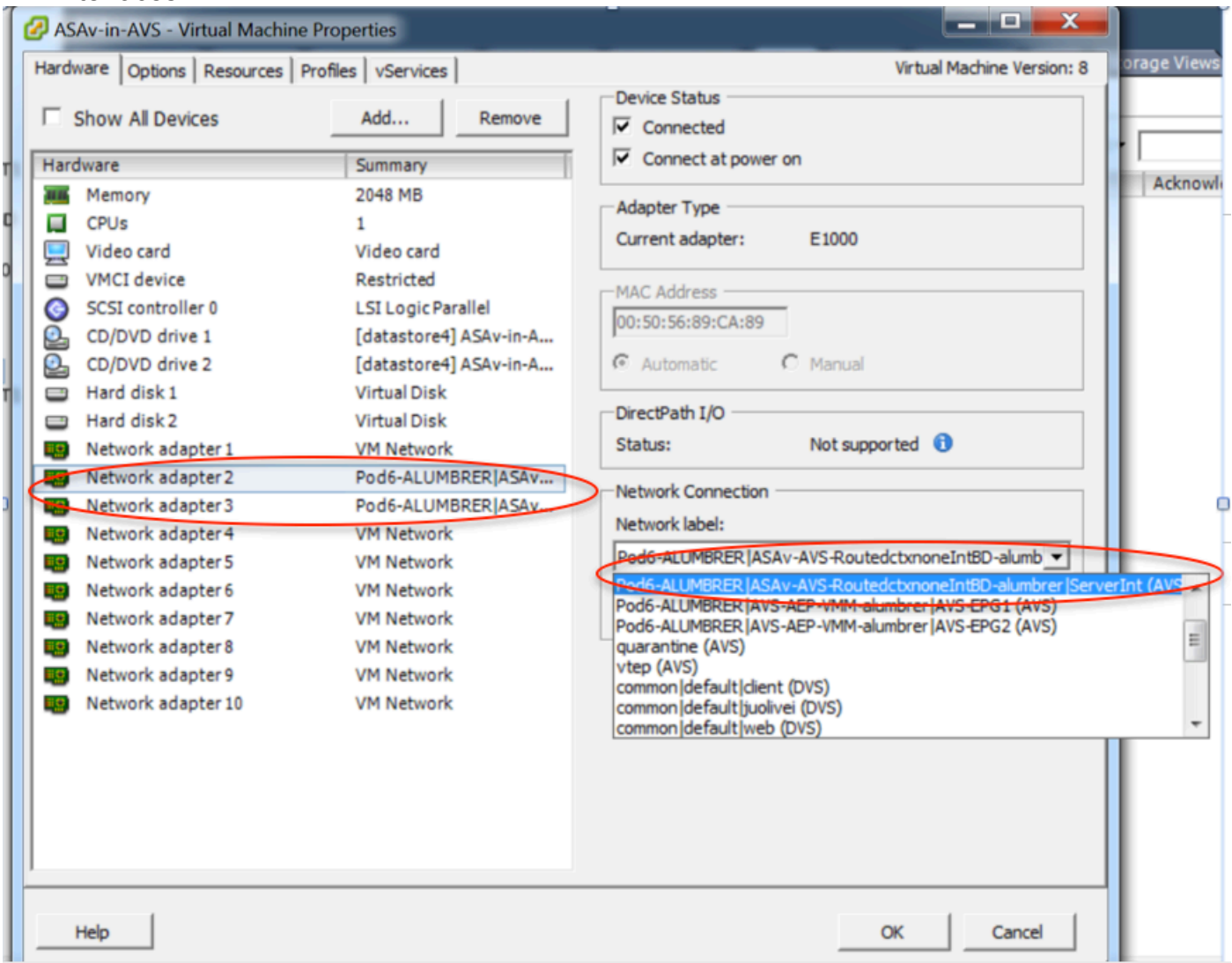
ASA-V-AUS# show interface ip brief
Interface          IP-Address      OK? Method Status      Prot
-----
GigabitEthernet0/0 192.168.10.1    YES manual  up          up
GigabitEthernet0/1 172.16.1.1      YES manual  up          up
GigabitEthernet0/2 unassigned      YES unset   administratively down up
GigabitEthernet0/3 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
ASA-V-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
ASA-V-AUS#

```

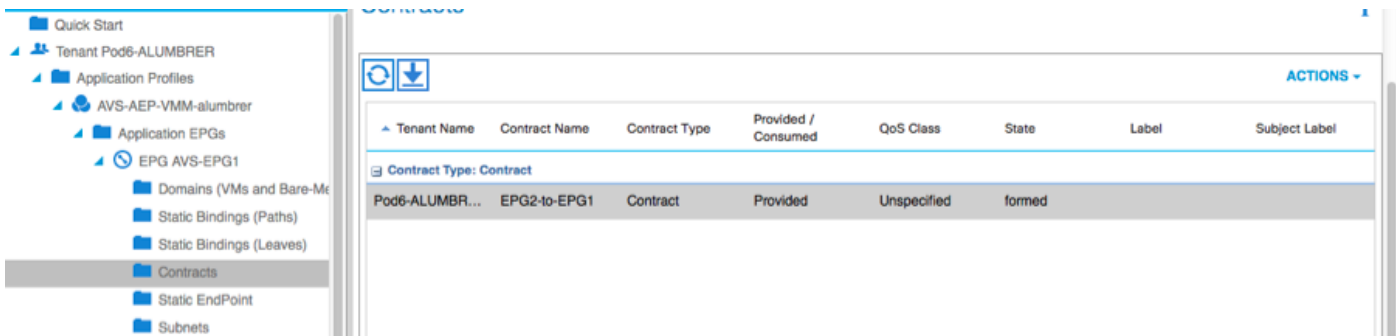
- Een nieuw contract wordt toegewezen onder de EPG's. Als u van nu af aan iets in de toegangslijst wilt wijzigen, moet de wijziging worden doorgevoerd vanuit de L4-L7 Service parameters van de Provider EPG.



- Op vCenter kunt u ook controleren of de schaduwEPG's zijn toegewezen aan elk van de FW-interfaces:



Voor deze test lieten ik de 2 EPG's communiceren met standaardcontracten, deze 2 EPG's zijn in verschillende domeinen en verschillende VRF's, dus was het lekken van de route tussen deze twee eerder geconfigureerd. Dit vereenvoudigt een beetje nadat u de Service Graph hebt ingevoegd aangezien de FW de routing en het filteren tussen de 2 EPG's instelt. Het DG dat voorheen in het kader van de EPG en de BD was ingesteld, kan nu worden afgeschaft, net als de contracten. Alleen het door de L4-L7 aangegane contract dient onder de EPG's te blijven.



Aangezien het standaardcontract wordt verwijderd, kunt u bevestigen dat het verkeer nu door de ASAv stroomt, zou de opdracht toegang-lijst moeten tonen de hit tellen voor de regel die elke keer dat de client een verzoek naar de server verstuurt.

```

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#
  
```

Op het blad moeten endpoints worden geleerd voor VM's van klanten en servers en de ASAv-interfaces

```

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
14/Pod6-ALUMBRER:VRF1-alumbrer
30          vxlan-14778359  50.50.50.50 L
          vxlan-98  5897.bda4.f9bc L
Pod6-ALUMBRER:VRF1-alumbrer  Server IP & MAC  vxlan-98  0050.5689.f008 L
25          vxlan-94  192.168.10.10 L
Pod6-ALUMBRER:VRF1-alumbrer  vxlan-94  0050.5689.ca89 L
mgmt:inb          vxlan-94  192.168.10.1 L
21          vxlan-94  192.168.2.11 S
Pod6-ALUMBRER:VRF2  Client IP & MAC  vxlan-97  0050.5689.3fca L
26          vxlan-97  172.16.1.10 L
Pod6-ALUMBRER:VRF2  vxlan-93  0050.5689.e7dd L
overlay-1          vxlan-93  172.16.1.1 L
overlay-1          vxlan-93  10.0.104.93 L
13          vxlan-93  10.0.96.67 L
overlay-1          vxlan-16777209  0050.5677.18a5 H
13          vxlan-16777209  10.0.32.93 H
overlay-1          vxlan-16777209  0050.5660.ddab H
overlay-1          vxlan-16777209  10.0.32.64 H
  
```

Zie beide firewallinterfaces op de VEM.

ESX-1

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

ESX-2

```
~ # vmmcmd show port vlan
LTL   VSM Port  Admin Link  State  Cause  PC-LTL  SGID  ORG  svcpth  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
~ #
```

Ten slotte kunnen de firewallregels ook op bladniveau worden geverifieerd als we de pc-tags voor bron- en doelgroepen kennen:

EPG1

The screenshot shows the ACI GUI for Tenant Pod6-ALUMBRRER. The left sidebar shows the navigation tree with 'VRF2' selected. The main panel displays the configuration for 'AVS-EPG1'. The 'Associated EPGs' table is as follows:

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

EPG2

The screenshot shows the ACI GUI for Tenant Pod6-ALUMBRRER. The left sidebar shows the navigation tree with 'VRF2' selected. The main panel displays the configuration for 'AVS-EPG2'. The 'Associated EPGs' table is as follows:

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

Filter ID's kunnen worden aangepast met de PC-tags op het blad om de FW-regels te controleren.

```
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#
```

Opmerking: De EPG PCTags/klasse communiceren nooit rechtstreeks. De communicatie wordt onderbroken of samengebonden via de schaduwEPG's die worden gecreëerd door de invoeging van de L4-L7 servicesgrafiek.

En communicatielijn naar server werkt.

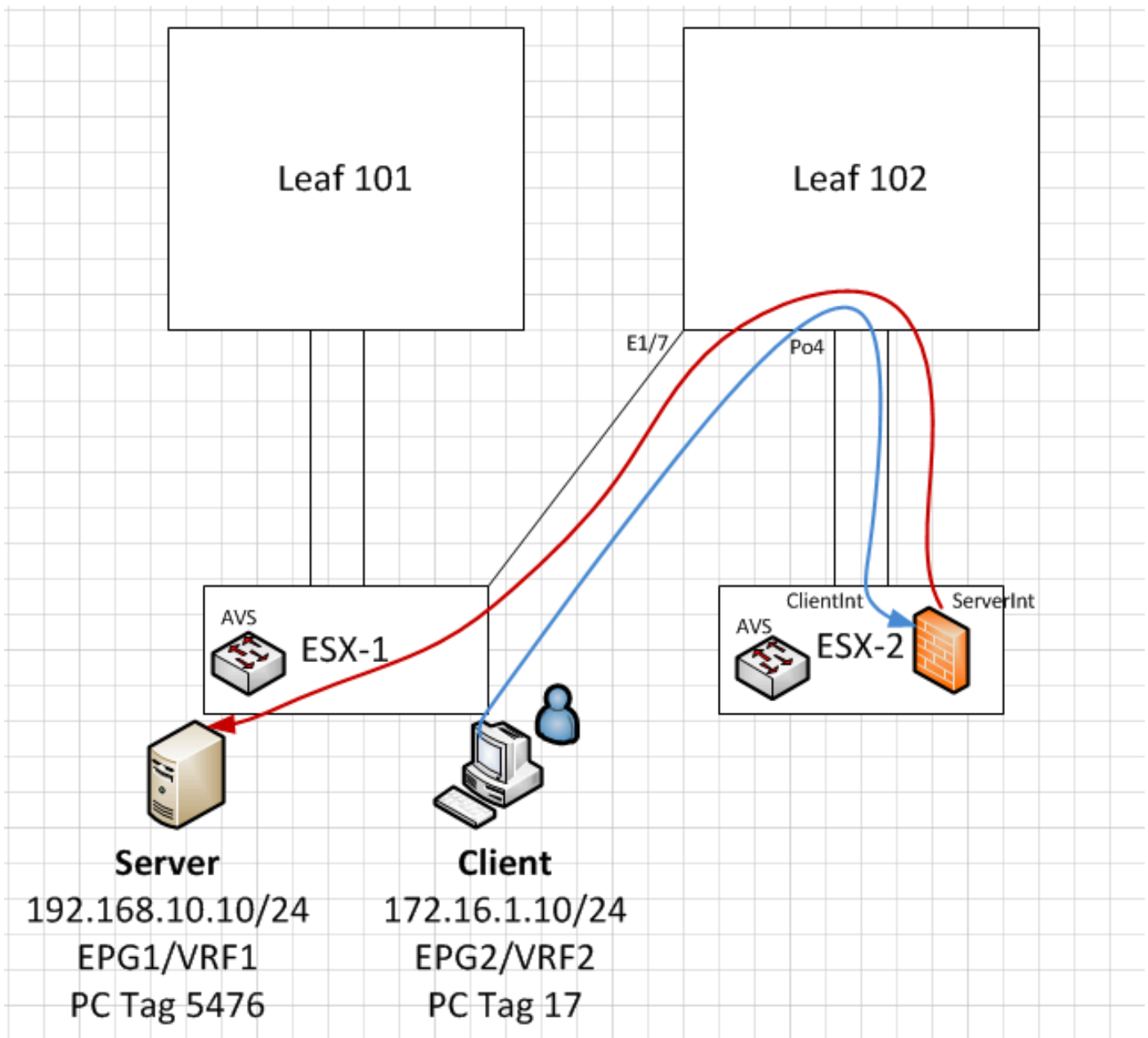
```
cisco@cisco-UbuntuClient:~$ ifconfig
eth1      Link encap:Ethernet  HWaddr 00:50:56:89:3f:ca
          inet addr:172.16.1.10  Bcast:172.16.1.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe89:3fca/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        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

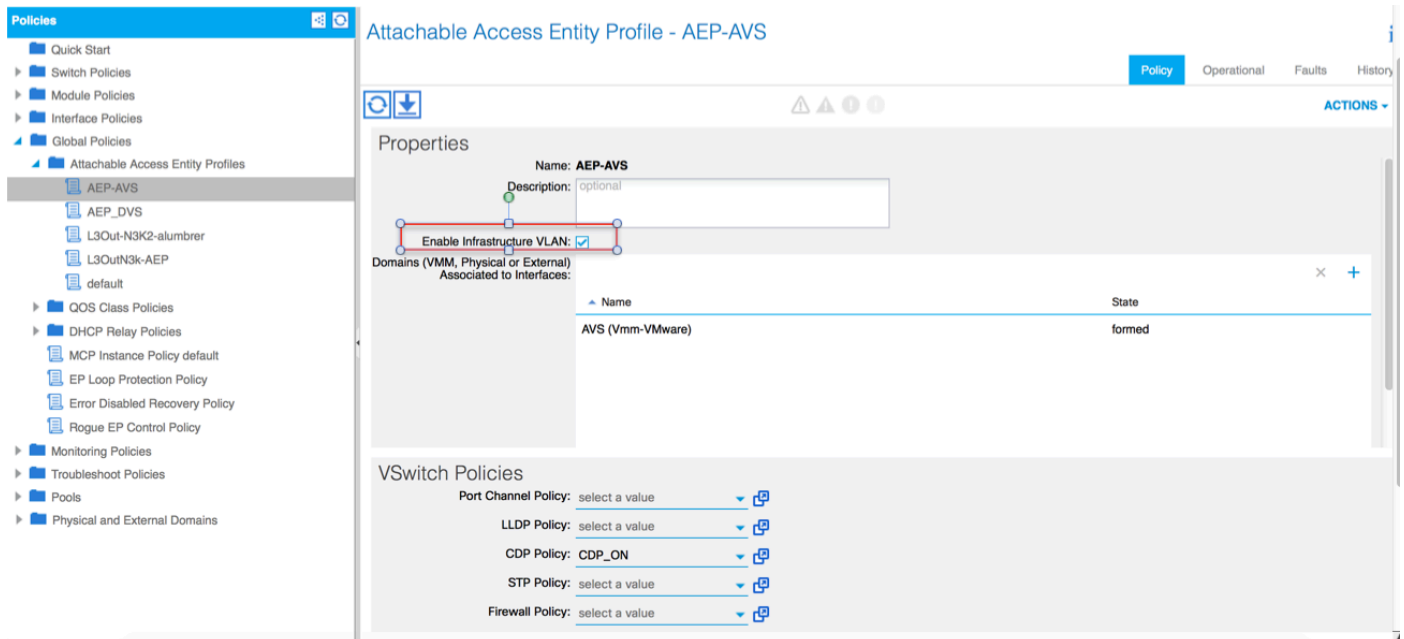
Last login: Mon Feb  1 10:14:11 2016 from 172.16.1.10
cisco@cisco-UbuntuClient:~$
```



Problemen oplossen

VTEP-adres is niet toegewezen

Controleer of het Infrastructuur VLAN is ingeschakeld onder het AEP:



Niet ondersteunde versie

Controleer of de VEM-versie correct is en ondersteuning biedt voor een geschikt ESXi VMWare-systemem.

```

~ # 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- en fabriccommunicatie niet werkend

- 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 IPv4 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

```

Op dit punt kan worden vastgesteld dat de communicatie van de fabric tussen de ESXi-host en de Leaf niet goed werkt. Sommige verificatieopdrachten kunnen aan de linkerkant worden gecontroleerd om de oorzaak van de wortel te bepalen.

```
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)

```

Er zijn 2 poorten die gebruikt worden in de ESXi en die aangesloten zijn via een 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
```

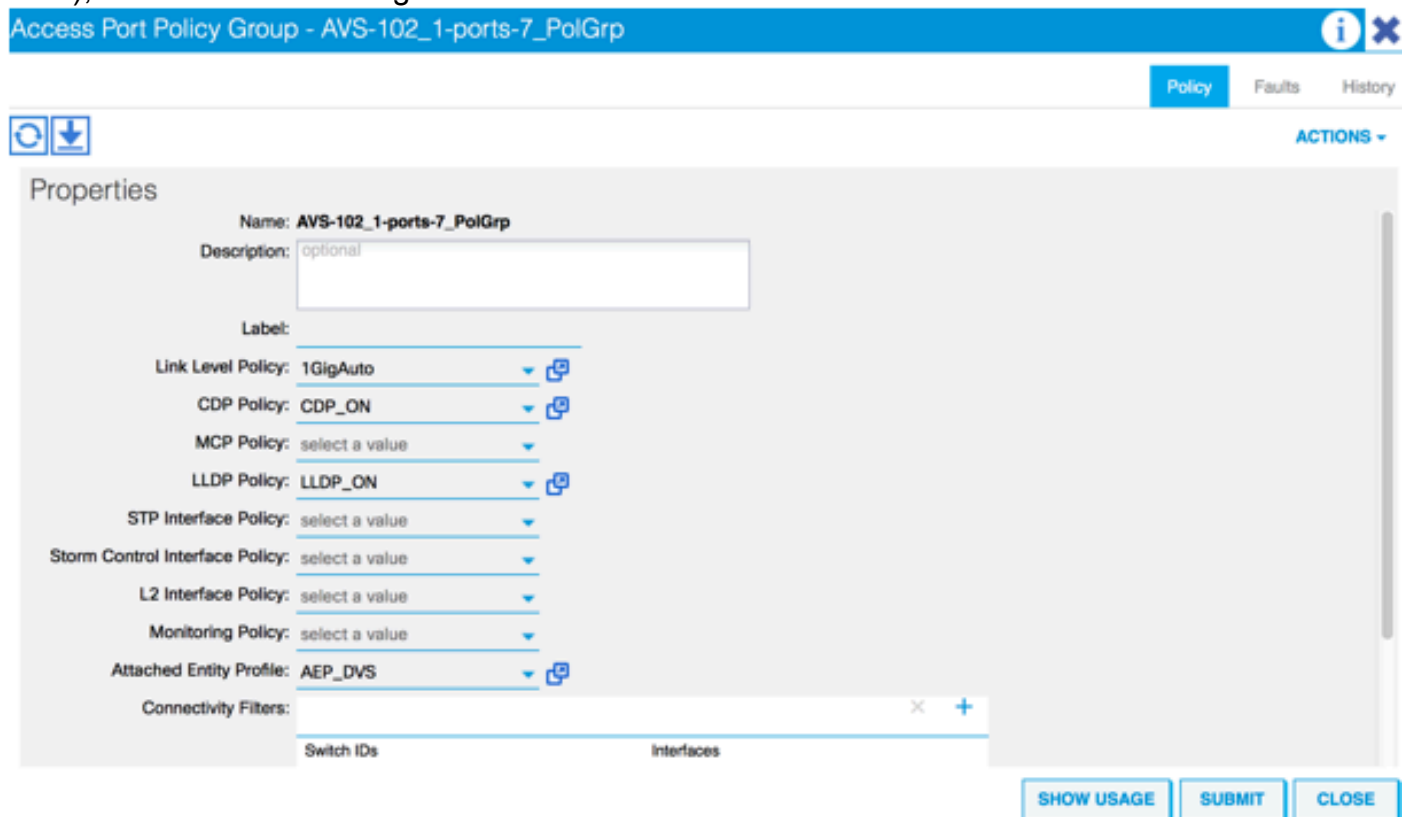
VLAN	Type	Vlan-mode	Encap
13	enet	CE	vxlan-16777209, vlan-3967
19	enet	CE	vxlan-14680064, vlan-150
22	enet	CE	vxlan-16383902
26	enet	CE	vxlan-15531929, vlan-200
27	enet	CE	vlan-11
28	enet	CE	vlan-14
36	enet	CE	vxlan-15662984

Op basis van de bovenstaande output kan worden waargenomen dat het Inra VLAN niet is toegestaan of door de Uplinks poorten loopt die naar de ESXi host gaan (1/5-6). Dit duidt op een verkeerde configuratie met het interfacebeleid of het Switch-beleid dat op APIC is ingesteld.

Controleer beide:

Toegangsbeleid > Interfacebeleid > Bewerkingen > Toegangsbeleid > Switch > profielen

In dit geval zijn de interfaceprofielen gekoppeld aan de verkeerde AEP (oude AEP gebruikt voor DVS), zoals in de afbeelding:



Nadat we de juiste AEP voor AVS hebben ingesteld, kunnen we nu zien dat de Inra Vlan is gezien door de juiste Unlinks op het Leaf:

```
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

```

Gerelateerde informatie

Installatie van virtuele Switch voor toepassingen

[Cisco Systems, Inc. Cisco Application Virtual Switch Installatie-gids, release 5.2\(1\)SV3\(1.2\)](#)

De ASAv implementeren met VMware

[Cisco Systems, Inc. Cisco adaptieve security virtuele applicatie \(ASAv\) Quick Start-gids, 9.4](#)

Cisco ACI en Cisco AVS

[Cisco Systems, Inc. Cisco ACI-virtualisatiegids, release 1.2\(1i\)](#)

Service Graph Design met Cisco Application Centraal Infrastructuur Witboek

[Service Graph Design met Cisco Application Centraal Infrastructuur Witboek](#)

