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

# Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren Netwerkdiagram 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

## Netwerkdiagram

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 verbruiker 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					i
Specify vCenter domain users and co	ontrollers				
Virtual Switch Name:	AVS				
Virtual Switch:	VMware vSphere D	istributed Switch	Cisco AVS		
Switching Preference:	No Local Switching	Local Switching			
Encapsulation:	● VLAN ● VXLAN		-		
Associated Attachable Entity Profile:	AEP-AVS	•	P		
VLAN Pool:	VlanPool-AVS(dynam	nic) 🗸	Ð		
Security Domains:			× +		
	Name	Description			
vCenter Credentials:				~	-
	Profile Name	Username	Description		_
vCenter:	venteroredentials	1001		×	+
	Name	IP	Туре	Stats Collection	
	vCenterController	10.201.35.9	vCenter	Disabled	

Als u Port-Channel of VPC (Virtual Port-Channel) gebruikt, wordt aanbevolen om het vSwitchbeleid 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)

Inventory Start	Portgroup - vtep					One of the local	i
Microsoft     Microsoft	Properties	vtep		A A O O			matery
	Management Network Adapters:	Server Name 10.201.35.219 10.201.35.218	Nama vrsk1 vrsk1	Stans Up Up	MAC 00:50:56:68:CA:25 00:50:56:61:07:CC	IP Address 10.0.16.95 10.0.76.94	
		(   Page 1	011   )	Objects Per	Prox 15 -	Displaying Objects 1	- 2 Of 2

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

and a parate release reactifier and excession excession excession.					
	VMware 1	V18 2	VEM Bundle 2	Windows VC Installer	Linux vCenter Server Appliance
	ESXI6.0	cross_cisco-vem- x250-5.2.1.3.1.10.0-6.0.1.vib	VEM600-201512250119-8G- release zip (Offine) VEM600-201512250119-8G (Online)	6.0	6.0
<	ESX 5.5	cross_cisco-vem- x250-5.2.1.3.1.10.0-3.2.1.vib	VEM550-201512250113-BG- release zip (Offine) VEM550-201512250113-BG (Online)	5.5	5.5
	ESXI5.1	cross_cisco-vem- x250-5.2.1.3.1.10.0-3.1.1.vib	VEM510-201512250107-8G- release.zip (Offine) VEM510-201512250107-8G (Online)	5.1	5.1
	ESXI 5.0	cross_cisco-vem- x250-5.2.1.3.1.10.0-3.0.1.vib	VEM500-201512250101-8G- release.zip (Offline) VEM500-201512250101-8G (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:

CiscoAVS_1.10-5	i.2.1.SV3.1.10			
		Q Searc	h	
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 arch
VEM550-201512250113-BG-release.zip	Dec 9, 2015, 12:10 AM	Dec 9, 2015, 12:10 AM	8.6 MB	ZIP arch
VEM600-201512250119-BG-release.zip	Dec 9, 2015, 12:10 AM	Dec 9, 2015, 12:10 AM	8.6 MB	ZIP arch

 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** 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

<pre>~ # esxcli software vib install -v /vmfs/volumes/datastore1/cross_cisco-vem-v250-5.2.1.3.1.10.0-3.2.1.vibmaintenance-modeno-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</pre>						
VEM modules are	loaded					
Switch Name vSwitchØ DVS Name DVS	Num Ports 5632 Num Ports 5632	Used Ports 8 Used Ports 10	Configured Ports 128 Configured Ports 512	MTU 1500 MTU 9000	Uplinks vmnic0 Uplinks 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:

dd Host to vSphere Distributed Swite	h			
Select Hosts and Physical Adapter Select hosts and physical adapters	s to add to this vSphere distributed switc	h.		
elect Host and Physical Adapters			Settings.	View Incompatible Hos
etwork Connectivity	Host/Physical adapters	In use by switch	Settings	Uplink port group
ual Machine Networking	E I 10.201.35.218		View Details	
by to Complete	Select physical adapters			
	vmnic0	vSwitch0	View Details	uplink
	vmnic1		View Details	uplink
	vmnic10		View Details	uplink
	vmnic11		View Details	uplink
	vmnic2		View Details	uplink
	vmnic3		View Details	uplink
	vmnic4	DVS	View Details	uplink
	vmnic5	DVS	View Details	uplink
	Vmnic6		View Details	uplink
	vmnic7		View Details	uplink
	vmnic8		View Details	uplink
	vmnic9	**	View Details	uplink
ielp	1		< Back	Next > Cancel

- 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:

Fabric	VM Networking	L4-L7 Services	Admin	Operations	
		Inventory   Packages			
Quick S	tart				
HELP					
The <b>Pac</b> balancer, and netw	cages menu allows you to in context switch, SSL termin ork connectivity information	nport L4-L7 device par ation device, or intrusio for each function. A ne	ckages, which are use on prevention system etwork service device	ed to define, configure, and mo (IPS). Device packages contai b is deployed in the network by	nitor a network service n descriptions of the ft adding it to a service g
You can configuri	use the <b>Import a Device P</b> a	ckage wizard to impor	rt a device package fo	or a function that you want to m	anage with APIC. We
oornigun	lr	nport Device Pa	ackage	i	×
Qui	ck Start ort a Device Package	File Name:		BROWSE	Device Types

• Als alles goed werkt, kunt u het geïmporteerde apparaatpakket zien, waarmee de map L4-L7servicetypen wordt uitgebreid, zoals in de afbeelding:

SUBMIT

CLOSE

i

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

				General	Operational	Faults	History
						ACT	TIONS -
Properties							
Vendor:	CISCO AITATA						
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:	1						
Interface Labels:	<ul> <li>Name</li> </ul>						
	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 ASAv, Loadbalances, enz. zouden omvatten.

In dit geval wordt OB voor ASAv 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.



ASAv 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 ASAv en de rest van de datacommunicatie wordt gestart vanaf Network adapter2.

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

#### Tabel 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

- De ASAv 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 2:1/Documents/GSP/ACTI/IMAGE/asav/952/asav-vi.ovf      rowse Enter a URL to download and install the OVF package from the Internet, or social hard drive, a network share, or a CD/DVD drive.
Нер	< Back Next > Cancel

ource VF Template Details nd User License Agreement	Map the networks used in this OVF to	emplate to networks in your inventory	
ame and Location	Source Networks	DestinationNetworks	
eployment Configuration	Management0-0	VM Network	
lor age	GigabitEthernet0-0	VM Network	
etwork Happing	GigabitEthernet0-1	VM Network	1
roperties	GigabitEthernet0-2	VM Network	
eady to Complete	GigabitEthernet0-3	Pod6-ALUMBRERJAVS-AEP-VMM-alumbrerJAVS	
	GigabitEthernet0-4	Pod6-ALUMERER [InternalAEP-VMM-alumbrer  E	
	GigabitEthernet0-5	VM Network	
	GinabitPthemet0-6	VM Network	٠
	Description:		
	General Purpose Network Interface		^
	1		Ŧ
	menning: mangate source methodika a		

#### Properties

Customize the software solution for this deployment.

Sizes       Off Tendata Details         Control Meet License Accessences       Type of deployment.         Sizes       Type of deployment.         Sizes       Sectores         Control Meet Conflocation       Select the type of ASA' host to install. When an HA type deployment is selected, the additional HA         Properties       Standatione         Ready to Complete       Mostname         Mostname       Mostname			
Oxf: Tenckate Details         Modules: Location         Management Configuration         Statistic         Statistic         Concomment Configuration         Statistic         Concomment Configuration         Statistic         Ready to Complete         Hostname         <	Source		
Item Litter Location       Deployment Type         Status       Type of deployment         Status       Sector         Sector       Sector         Management       Mathematic Sector         Management       Interface Settings	OVF Template Details		*
Name:       Type of deployment         Status       Select the type of ASAv host to instal. When an HA type deployment is selected, the additional HA Properties below should also be filed in.         Status       Standaione         Properties       Ready to Complete         Hostname       Hostname         Hostname       Hostname (bits, or a hyphen).         Adave::-AVS       Firewall Properties         Firewall Properties       Firewall Properties         Note:       Name(bits)         Management Interface Settings       Hanagement Interface Settings         Hanagement Interface DHCP mode       Choose whether to use CHOP for Management interface configuration.         10       .01       .05       .01         Hanagement Interface DHCP mode       Choose whether to use CHOP for Management interface configuration.       .01         10       .01       .05       .01       .01         Hanagement IP-4 Address.       For HA-type deployments, this property specifies the Management PP-4 Address of the Active HA host.       .00       .01       .01       .01       .01         Heip        Ketz the HA deces.       For HA-type deployments, this property specifies the Management PP-4 Address of the Active HA host.       .00       .01       .01       .01       .01       .01       .01	End User License Agreement	Deployment Type	
Descurators       Type of displayment         Statual       Statual         Oak Format       Second         Properties       Statual         Ready to Complete       Imagement for this system. A hostname must start and end with a letter or dgit and have as interior characters only letters, dgits, or a hyphen.         Addata       Addata         Imagement Interface Settings         Management Interface Settings         Management IP Address         Choose whether to use DHOP for Management interface configuration.         10 , 201 , 35 , 223         Heip         Meter Line Statue	Name and Location		
Select the type of ASAv has to install. When an HA type deployment is selected, the additional HA Properties Biow should also be filed in. Standards Properties Ready to Complete Hostname Hostn	Deployment Configuration	Type of deployment	
Disk format       Properties below should also be filed n.         Standalone       Image: Imag	Storage	Select the type of ASAv host to install. When an HA type deployment is selected, the additional HA	
Metadolice         Standalone         Properties         Ready to Complete         Hostname         Hostname filter         Hostname filter         Hostname filter         Adaracters only letters, digits, or a hyphen.         Management Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Hanagement IP-4 Address.         Enter the Management IP-4 Address. For HA-type deployments, this property specifies the Management IP-4 Address of the Active HA host.         10       201         10       201         Hanagement IP-4 Address.         Hanagement IP-5 Subart Hask	Disk Format	Properties below should also be filled in.	1
Properties         Ready to Complete         Hostname         Hostname         Hostname 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-en-AVS         Firewall Properties         Firewall Mode         Select the Firewall Mode         Foulted         Management Interface Settings         Management Interface Settings         Management Interface Settings         Management Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Imagement IP-4 address         Enter the Management IP-4 address of the Active HA host.         10       .201         Heapement IP Subset Hask	Network Mapping	Standalone •	
Ready to Complete       Hostname         Hostname       Hostname         Hostname       Hostname         Hostname       Hostname must start and end with a letter or digit and have as interior characters only letters, digits, or a hyphen.         ASAvrer-Avis       Firewall Properties         Firewall Properties       Firewall Mode         routed       Imagement Interface Settings         Hanagement Interface Settings       Hanagement Interface DHCP mode         Oncose whether to use DHCP for Management interface configuration.       Imagement IP Address         Enter the Management IP-4 Address of the Active HA host.       10 . 201 . 35 . 223         Hanagement IP Subnet Hask       Imagement IP Subnet Hask	Properties		
Hostname         Host name for this system. A hostname must start and end with a letter or digit and have as interior duracters only letters, digits, or a hyphen.         ASAv-m-AVS         Firewall Properties         Firewall Mode         Select the Firewall Mode         routed         Management Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Hanagement IP-v4 Address         Enter the Management EV-4 Address. For HA-type deployments, this property specifies the Management EV-4 Address for the Active HA host.         10       .201         10       .201         Hanagement IP Subnet Hask	Ready to Complete	Hostname	
Hostname         Hostname for this system. A hostname must start and end with a letter or digit and have as interior divaracters only letters, digits, or a hyphen.         ASAv-m-AVS         Firewall Properties         Firewall Mode         Select the Firewall Mode         routed         Management Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Hanagement IP-v4 Address.         Enter the Management IP-v4 Address. For HA-type deployments, this property specifies the Management IP-v4 address of the Active HA host.         10       .201         10       .201         Hanagement IP-Subnet Hask			
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 Prevail Mode         routed         Management Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Hanagement IP Address         Enter the Management SV-4 Address. For HA-type deployments, this property specifies the Management IP-4 Address of the Active HA host.         10       .01         .01       .021         Help          Help		Hostname	
ASAr-w-AVS         Firewall Properties         Firewall Mode         Select the Firewall Mode         routed         Management Interface Settings         Management Interface OHCP mode         Choose whether to use DHOP for Management interface configuration.         Hanagement IP Address         Enter the Management IP Address.         Enter the Management IP-v4 Address. For HA-type deployments, this property specifies the Management IP-v4 Address of the Active HA host.         10       .201         Management IP Subnet Mask         Memory         Address         Management IP Subnet Mask		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.	
Firewall Properties         Firewall Mode         Select the Prewall Mode         routed         management Interface Settings         Hanagement Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Hanagement IP-4 Address         Enter the Management IP-4 Address. For HA-type deployments, this property specifies the Management IP-4 Address of the Active HA host.         10       .201         Management IP Subnet Hask		ASAv-w-AVS	
Help       < Back			
Help       < Back		Firewall Properties	
Select the Firewall Mode         routed         Management Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Imagement IP Address         Enter the Management IP-v4 Address. For HA-type deployments, this property specifies the Management IP-v4 Address of the Active HA host.         ID       .01         Hanagement IP Subnet Hask         Imagement IP Subnet Hask         Imagement IP Subnet Hask         Imagement IP Subnet Hask		Firewall Mode	
Management Interface Settings         Management Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Imagement IP Address         Enter the Management IPv4 Address. For HA-type deployments, this property specifies the Management IPv4 address of the Active HA host.         Imagement IP Subnet Hask         Help		Select the Firewall Mode	
Imagement Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Imagement IP Address         Enter the Management IP-v4 Address. For HA-type deployments, this property specifies the Management IP-v4 address of the Active HA host.         10       .201         Hanagement IP Subnet Hask         Ket       Cancel			
Hanagement Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Imagement IP Address         Enter the Management IP v4 Address. For HA-type deployments, this property specifies the Management IP v4 address of the Active HA host.         Imagement IP Subnet Hask         Help            Ket >		routed	
Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Hanagement 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         Hanagement IP Subnet Hask		Management Interface Settings	
Help <back< td="">       Next &gt;       Cancel</back<>		Management Interface DHCP mode	
Hanagement IP Address         Enter the Management IP v4 Address. For HA-type deployments, this property specifies the Management IP v4 address of the Active HA host.         10       .201       .35       .223         Hanagement IP Subnet Hask       •              Heip         Cancel		Change whether to use PMCD for Management interface conferenties	
Hanagement 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         Hanagement IP Subnet Hask		Choose whether to use CHCP for Management interface configuration.	
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         Hanagement IP Subnet Hask		Hanagement IP Address	
Hanagement IPv4 address of the Active HA host.       10 , 201 , 35 , 223       Hanagement IP Subnet Hask       Help       < Back		Enter the Management IPv4 Address. For HA-type deployments, this property specifies the	
10         201         35         223           Hanagement IP Subnet Hask         *		Management IPv4 address of the Active HA host.	
Hanagement IP Subnet Hask       Heip <back< td="">     Next &gt;     Cancel</back<>		10 . 201 . 35 . 223	
Help Kext > Cancel		Management IP Subnet Mask	-
Help <back next=""> Cancel</back>		I an and the second sec	
Help < Back Next > Cancel			
	Help	< Back Next >	Cancel

idy to Complete Are these the options you			
	want to use?		
			_
2 Templete Datals	When you click Finish, the deploym	ent task will be started.	
errukase License Acreement	Decloyment settings:		
Location	Sta on disk:	83.68	1
Configuration	Name	ACAuria AVC	
	Ealder	401	h
	Deployment Configuration	1 Chest (ASA-18)	
202	Heat/Cluster	10.001.06.010	
	Datastorr	datastrond	
ompiete	Disk provisioning	Thick Dravision Law Zamad	
	Natural Manajar	"Managements A" to "UM Naturals"	
	Natural Mandian	"CinableDhamath.0"to "VM Naturok"	
	Natural Manajary	"CinabitRhamath, 1"to "UN Naturok"	ji.
	Natural Manajary	"ClashitBharrath," to "Printerrok"	
	Natural Mandian	*CinablePhareath.1*to *Do.46_511MEDED12VC.5ED.VMM.slumburd8V	
	Natural Mandan	"CinabitPhanath.4"to "Dode-Li I IMROFD Internal LED. UMM-alumburd	
	Natural Mancing	"GinabitRhamato.S" to "VM Network"	
	Natural Manding	"GinabitRhamath.6" to "VM Naturok"	
	Natural Manaine	"CinabitPhanath, 7" to "VM Naturd"	
	Natural Manday	"Cinabilithemath.#"to "VM Network"	U
	10 Allocation	Fixed 12v4	
	Printer	HABole - Gandalone	
	Property	Hosteama = 152 com 200	
	Property	Extended a contract	
	Property	DHCP = False	
	Property	Mananamant2bud = 10.201.35.223	
	Property	Mananamani DudGubnat = 265,265,265 A	
	Property	Management Orandhu (Dud = 0.0.0.0	
	Property	PosteDelasit = Delasit Poste	
	Property.		
	Property: Property:	ManagementStandbyIPv4 = 0.0.0.0 RouteDefault = Default Route	

## • Klik op Voltooien 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 ntu management 1500 no failover icmp unreachable rate-limit 1 burst-size 1 no asdm history enable arp timeout 14400 no arp permit-nonconnected oute 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 ASAv 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

ASAv-w-AVS(config)# username admin password C1sc0123 privilege 15 ASAv-w-AVS(config)# wr mem Building configuration... Cryptochecksum: d491b980 86fa522f 6f937baf b5bfb318 7977 bytes copied in 0.250 secs [OK] ASAv-w-AVS(config)# ping 10.201.35.211 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.201.35.211, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip Min/avg/Max = 1/2/10 Ms ASAv-w-AVS(config)# \_\_

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

#### http-server

http 0.0.0.0.0.0.0.0

#### L4-L7 voor ASAv-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

communic	eren					
Create L4-L7 Device:	5					
STEP 1 > General					1. General 2. Device	e Configuration
Please select device	package and enter connectivity info	ormation.				
General		Device 1				
Managed:		Management IP Address:	10.201.35.3		Management Port: https	
Name:	ASAv-AVS-Routed	VM:	vCenterController/AS	Av-in-AVS 🚽 🗗		
Service Type:	Firewall	Device Interfaces:				× +
Device Type:	PHYSICAL VIRTUAL		Name	VNIC	Path (Only For Boute Peering)	
VMM Domain:	AVS T		GigabitEthernet0/0	Network adapter 2	Node-102/MAC_Pinning	
Mode:	Single Node     HA Cluster		GigabitEthernet0/1	Network adapter 3	Node-102/MAC_Pinning	
Device Package:						
Model:						
Function Type:	GoThrough GoTo	Cluster Management IP Address:	10.201.35.3		Management Port: https	
		Cluster Interfaces:				× +
			Туре	Name	Concrete Interfaces	
			provider	ServerInt	Device1/GigabitEthernet0/0	
Connectivity APIC to Device Management Connectivity:	Out-Of-Band In-Band		consumer	ClientInt	Device1/GigabitEthernet0/1	
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 **Clf** (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.

i

Voor dit voorbeeld zal de volgende vereniging worden gebruikt:

- Gi0/0 = Vmnic2 = serverInt/provider/server > EPG1
- Gi0/1 = Vmnic3 = clientInt/consument/client > EPG2

€¥						ACT
General Managed: 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 GoTe Cluster Mode: Single Node	Device 1 Management IP Address: vCenter Name: Interfaces:	10.201.35.223 vCenterController Name GigabitEthemet0/1 GigabitEthemet0/2	Manage Veac Network a	ment Port: 443 VM Name: ASAv-in-v dapter 3 dapter 4	AVS Path (Only For I Node-102/MAC Node-102/MAC	Route Peer D_Pinning. C_Pinning
Credentials Username: admin Password: Confirm Password: Configuration State Configuration Issues: Devices State: stable	Cluster Management IP Address: Cluster Interfaces:	10.201.35.223 Type consumer provider	Nanage Name Clientint Serverint	ment Port: 443 Concrete Interfa ASAv-AVS-Rou ASAv-AVS-Rou	rces rted_Device_1/jG rted_Device_1/jG	¢ igabitEthe

**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:

#### L

Create L4-L7 Services Fu	nction Profile	Group		0×			
Specify the information ab	out the Function	on Profile Group					
Name: FunP Description:	rofGroup						
Tenant Pod6-ALLMORER	L4-L7 Services F	unction Profile Group	- FunProGroup	CANCEL			i
Tenant Pod6-ALUMBRER     E Application Profiles	⊙±					General Fax	ACTIONS -
L4-L7 Service Parameters     Security Policies     Troubleshoot Policies	Properties Name: Description:	FunProGroup					
Monitoring Policies     Monitoring Policies     L4-L7 Services     L4-L7 Service Graph Templates	service Function Provies:	- Name	Associated Function	Description	n		× +
Pouter configurations     Prunction Profiles     Punction Profiles     Delete     L4-L7 Devices     Devices Selection     Devices Selection     Save as	iction Profile		5	No items have been four idelect Actions to create a new	d. 1809.		
Deployed Graph In     Deployed Devices     Inband Management Configuration for L4-L7 devices							

 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	
eatures and Parameters		
	In order to auto apply new values to the parameters of existing graph instance when users modify function pr	rofiles, the name of top folder must be ended with -Default
Features:	Basic Parameters All Parameters	
Interfaces	Folder/Param Name Value Mandator	ry Locked Shared
interlaces	E 🖌 🍽 Device Config Device	
AccessLists	Bridge Group Interface	
NAT	📰 😑 🔺 🎯 Interface Related Configuration external If	false false
TrafficSelectionObjects	E Access Group ExtAccessGroup	false
All	IPv6 Enforce EUI-64	
	Interface Specific Configur externalIfCfg	false
	IPv4 Address Configura	
	IPv4 Address     Ipv4_address     192.168.10.1/24	
	IPv4 Standby Address UPDATE RESET CANCEL	
	IPv6 Link Local Address	
		SUBMIT

**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: FunP	Prof-ASA						
Description: Optio	nal						
Copy Existing Profile Parameters: 🛃							
Profile: CISC	O-ASA-1.2/WebPolicy	ForRoutedMode	<u> </u>				
Features and Parameters							
	In order to auto apply	new values to the parameter	ers of existing graph in	stance when users	modify function profiles, th	ne name of top folder	r must be ended with -Default.
Features:	Basic Parameters	All Parameters					
Interference	Folder/Param	1	Name	Value	Mandatory	Locked	Shared
Internaces	8 4	Destination Service	destination_servi	се			
AccessLists		High Port					
NAT		Low Port	low_port	22		false	
TrafficSelectionObjects		Operator	operator	eq		false	
All							
		Logging					
		Source Address					
		Source Service					
		Action	action	permit		false	
	M	Crder	order	30		false	

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

Tenant Pod6-ALUMBRER	<ul> <li>O</li> </ul>	1 4-1 7 Service (
Quick Start		
Tenant Pod6-ALUMBRER		
Application Profiles		⊖±
Networking		Neme
L4-L7 Service Parameters		<ul> <li>Name</li> </ul>
Security Policies		
Troubleshoot Policies		
Monitoring Policies		
🔺 💼 L4-L7 Services		
L4-L7 Service Graph Templates		
Router configurations	Create L4-L7	Service Graph Template

• 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:	Graph1-alumbrer		
Graph Type:	Create A New One	Clone An Existing One	
Consumer		C ASAv-AVS	Provider EPG
	Please drag a dev	ice from devices table and drop it here to create a service node.	
ASAv-AVS-Routed	Information		
Firewall: 🧿	Routed   Transparent		
Profile: Po	d6-ALUMBRER/FunProfGroup/FunPr	o. 🚽 🗗	
			CANCEL

- 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

Tenant Pod6-ALUMBRER		⊴ ⊙	1 4-1 7 Service (	Graph Templa	ate - Graph1-alum	brer					
Cuick Start			21 21 0011100		ato orapiti atom	0.01					
Tenant Pod6-ALUMBRER								Topology	Policy F	aults	History
Application Profiles			Ð								
Networking			Concur						Browlete		
L4-L7 Service Parameters			Consum	ier			1		Provide		
Security Policies			( EPG	D		C	P			)	
Troubleshoot Policies						ASAv-AVS			0		
Monitoring Policies											
L4-L7 Services						ASAv	•				
🔺 🚞 L4-L7 Service Graph Templa	ates										
4 💙 Graph1-alumbrer				outed Information							
Function Node - ASA	•	Apply L4-L7 Ser	vice Graph Template	I: Routed							
Router configurations		Edit L4-L7 Servi	ce Graph Template	E FunPro-ASA							
Function Profiles	×	Delete									
🔺 🕎 FunProtGroup	×	Remove Related	d Objects Of Graph Template								
FunPro-ASA	Ψ	Save as									
L4-L7 Devices		Doet									
ASAv-AVS-Routed		r oat									
ASAV-DVS											
Imported Devices											
Devices Selection Policies											
💼 Deployed Graph Instances											
Deployed Devices											
📃 Inband Management Configu	uration	for L4-L7 devi									
https://10.201.35.211/#								SHOW USAGE	SUBMI		RESET

- 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	rork: Pod6-ALUMBRER/AVS-AEP-VMM 👻 📴	\$
	Pod6-ALUMBRER/AVS-AEP-VMM-	
- Contract Information	alumbrer/epg-AVS-EPG1	
Contract:  Contract  Contract Contract	Pod6-ALUMBRER/InternalAEP-	
Contract Name: EPG2-to-EPG1	VMM-alumbrer/epg-EPG-Internal- alumbrer	
No Filter (Allow All Traffic): 🔽	/AnyEPG	
	Pod6-ALUMBRER/VRF2/AnyEPG	
	Pod6-ALUMBRER/L3Out-N3K2/L3Net	

 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.

PREVIOUS NEXT CANCEL

#### • Klik op Volgende

Graph Template:	Pod6-ALUMBRER/Graph1-Temp-alumbre	r		e			
Consumer EPG AVS-EPG2		A	SAV-AVS ASAv	P	 [	Provider EPG AVS-EPG1	
ASAv-AVS-Routed Infor Firewal Profile Consumer Connector Type: BD: Cluster Interface:	in touted     in touted     in FunPro-ASA     in Pro-ASA     in Route Peering     Pod6-ALUMBRER/ExtBD-alumbrer     ClientInt	) 	ም P				
Provider Connector Type: BD: Cluster Interface:	General OROUTE Peering Pod6-ALUMBRER/IntBD-alumbrer ServerInt	) d d	P P				
					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.

in Nama						
e name.	PURPTO-AGA	1				
atures:		Require	ed Parameters Al Parameters			
		1	Folder/Param	Name	Value	Witte Domain
		1	Access List	access-list-inbound		
AccessLists			Access Control Entry	ICMP		
			Access Control Entry	51912		
	onObjects	8	Access Control Entry	SSH		
All			Destination Address			
		8	Destination Service	destination_service		
			▶ □ ICMP			
			Logging			
		8	Protocol	protocol		
			Source Address			
			Source Service			
			Action	action	permit	
			Crder	order	(m)	select asa domain
		78	Access Control Entry	UPDATE RESET CAN	00	
			Access Control Entry	or or other		

• 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 > ASAv-AVS-Routed Parameters

ais		ue	a	ne	eiui	ng.
1.	Cor	tract		2	Graph	

config parameters for the selec	ted device	
Profile Name: FunProf-ASA		
Features:	Required Parameters All Parameters	
Interfaces	Folder/Param	Name Value Write Domain
<u>Internacions</u>	😑 🔺 😅 Device Config	Device
AccessLists	E  Access List	access-list-inbound
NAT	Bridge Group Interface	
TrafficSelectionObjects	Interface Related Configuration	externalIf
All	😑 🔰 🖾 Access Group	ExtAccessGroup
	Inbound Access List	name access-list-inbound
	Outbound Access List	
	IPv6 Enforce EUI-64	
	E 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	
	ITI 🗖 🕨 🕒 IPuß Router Advertisements	

RED indicators parameters needed to be updated and GREEN indicates parameters will be summitted 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 functieknop.



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

ALL TENANTS   Add Tenant   Search: enter name, descr	common   Pod6-AL	UMBRER   Pod6-ALUMBRER2   infra	mgmt					
Tenant Pod6-ALUMBRER	Virtual Device - A	SAv-AVS-Routed-none						i
Cuick Start Cuick	Properties Devices: Virtual Device ID: Vart	ASAv-AVS-Routed 25351 pone	A O O 100	Policy	Operational	Health	Faults	History
Monitoring Policies     Lit-L7 Services     Lit-L7 Service Graph Templates     Declarger Literative Service Complementation	ACKed Transaction ID: Current Transaction ID: Cluster Interfaces:	10000 10000 Logical Interface	Епсар					
Fource computations     Function Profiles     L4-L7 Devices	4	ASAv-AVS-Routed_ClientInt ASAv-AVS-Routed_ServerInt	vlan-93 vlan-94					
Imported Devices  Devices Selection Policies  Deployed Graph Instances  V* EPG2-to-EPG1-Graph 1-alumbrer-Pod6-ALUM  Deployed Devices  V* ASAv-AVS-Routed-none  Inband Management Configuration for L4-L7 devi								

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

NSAV-W-AVS# show interface	ip brief		
Interface	IP-Address	OK? Method Status	Prot
ocol			
igabitEthernet0/0	192.168.10.1	YES manual up	սք
igabitEthernet0∕1	172.16.1.1	YES manual up	սք
igabitEthernet0/2	unassigned	YES unset administratively dow	ո սք
igabitEthernet0∕3	unassigned	YES unset administratively dow	ո սք
igabitEthernet0∕4	unassigned	YES unset administratively dow	ո սք
igabitEthernet0/5	unassigned	YES unset administratively dow	ո սք
igabitEthernet0/6	unassigned	YES unset administratively dow	ո սք
iigabitEthernet0/7	unassigned	YES unset administratively dow	ո սք
igabitEthernet0/8	unassigned	YES unset administratively dow	ո սք
lanagement0/0	10.201.35.223	YES CONFIG up	սք
ISAv-w-AVS# show run access	s-list		
ccess-list access-list-ind	oound extended	permit tcp any any eq www	
access-list access-list-ind	oound extended	permit tcp any any eq https	
ccess-list access-list-ind	oound extended	permit tcp any any eq ssh	
ccess-list access-list-ind	oound extended	permit icmp any any	
ASAV-M-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 FWinterfaces:

1	🕜 AS	Av-in-AVS - Virtual Machine Pro	perties		
l	Hard	ware Options Resources Profil	es vServices	Virtual Machine Version: 8	orage Views
l	_			Device Status	
l		Show All Devices	Add Remove	Connected	
	Hard	dware	Summary	Connect at power on	
I	-	Memory	2048 MB	- Adapter Tuna	Acknowle
q		CPUs	1	Current adapter E1000	
		Video card	Video card	Current adapter: E 1000	
٩		VMCI device	Restricted	-MAC Address	
I	0	SCSI controller 0	LSI Logic Parallel	00:50:55:89:04:89	
I		CD/DVD drive 1	[datastore4] ASAv-in-A	00.30.30.03.04.03	
l		CD/DVD drive 2	[datastore4] ASAv-in-A	Automatic     C Manual	
T		Hard disk 1	Virtual Disk	DirectDath I/O	
I		Hard disk 2	Virtual Disk	DirectPath 1/0	
I		Network adapter 1	VM Network	Status: Not supported U	
	-	Network adapter 2	Pod6-ALUMBRER ASAv	Network Connection	
1	-	Network adapter 3	Pod6-ALUMBRER ASAv	Network label:	- P
I		Network adapter 4	VM Network	Dade at LIMODED LAS AV, AVS, Davited stypene (at PD, a), mb	
I		Network adapter 5	VM Network	Pad6-ALLIMBRER IASAV-AVS-Routedctynonatot80-alumb	Tot (AVS
I	2	Network adapter 6	VM Network	Pod6-ALUMBRER AVS-AEP-VMM-alumbrer AVS-EPG1 (AVS)	
I	2	Network adapter 7	VM Network	Pod6-ALUMBRER AVS-AEP-VMM-alumbrer AVS-EPG2 (AVS)	=
I		Network adapter 8	VM Network	vtep (AVS)	
I		Network adapter 9	VM Network	common default dient (DVS)	
I		Network adapter 10	VMINELWORK	common (default (juolivei (DVS)	-
I				common de robre (Proy	
I					
I					
I					
	1				
1		Help		OK Cancel	

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.



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

leaf2# show endpoint				
Legend:				
0 - peer-attached H - vtep	a - locall	y-aged S - sta	atic	
V - vpc-attached p - peer-aged	L - local	M - sp	an	
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	vian-98	0050.5689.td08	TW	eth1/7
Pod6-ALUMBRER:VRF1-alumbrer Server	P vlan-98	192.168.10.10	interface	
25 & MAC	vlan-94	0050.5689.ca89	(ServerInt	po4
Pod6-ALUMBRER:VRF1-alumbrer	vlan-94	192,168,10,1		
mgmt:inb		192.168.2.11	S	
21	vlan-97	0050.5689.3fca		eth1/7
Pod6-ALUMBRER:VRF2	P & vlan-97	172.16.1.10		
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	FW	
13	vxlan-16777209	0050.5677.18a5	H interface	unspecified
overlay-1	vxlan-16777209	10.0.32.93	H (ClientInt)	
13	vxlan-16777209	0050.5660.ddab	н	unspecified
overlay-1	vxlan-16777209	10.0.32.64	н	

Zie beide firewallinterfaces op de VEM.

#### ESX-1

~ # V	emcmd show p	ort vl	an								
LTL	VSM Port	Admin	Link	State	Cause	PC-LTL	SGID	ORG	svcpath	Туре	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	Pol	UP	UP	FWD		0		0	0		

ESX-2

	-											
~ # ve	- # vemand show port vlan											
LTL	VSM Port	Admin	Link	State	Cause	PC-LTL	SGID	ORG	svcpath	Туре	Vem Port	
24	Eth1/7	UP	ŲΡ	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	ŲΡ	FWD	-	0	6	0	0		Server1-AVS.eth0	
1040	Po1	UP	UP	FWD	-	0		0	0			
~ #												

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

EPG1								
Tenant Pod6-ALUMBRER	1				Policy Op	erational Stats	Health Faults	History
Application Profiles					1	dated EDCa	section Driver al Davis	of Mathematics
AVS-AEP-VMM-alumbrer					A600	oabbo Erros A	ssocialies External Pious	o nenworks
Application EPGs	⊙₹						^	CTIONS -
	TAUTO	Description	State	issues	QeS	Encep	PC Tag	
Use EPGs	AVS-EPG1		applied		Unspecified		17	
L4-L7 Service Parameters	EPG-Internal-alumbrer		applied		Unspecified		32772	
🕨 🚭 InternalAEP-VMM-alumbrer								
Networking								
Bridge Domains								
VRFs	1							
VRF1-alumbrer								
MB15								



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

leaf2# show zo	<u>ning-rule   g</u>	rep '17\15476'					
4141	17	32775	default	enabled	2916352	permit	<pre>src_dst_any(5)</pre>
4142	32775	17	default	enabled	2916352	permit	<pre>src_dst_any(5)</pre>
4139	5476	49156	14	enabled	2555904	permit	<pre>src_dst_any(5)</pre>
4140	49156	5476	14	enabled	2555904	permit	<pre>src_dst_any(5)</pre>
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 overrups:0 frame:0
TV packets:533034 errors:0 dropped:0 overruns:0 carrier:0
callicience transmolent1000
RX Dytes:330/0388 (33.0 MB) IX Dytes:42/34068 (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 (CNU/Linux 3 13 0-24-generic x86 64)
wetcome to obdited 14.04 LTS (GNO/Lthux 5.15.0-24-generice x80_04)
t Decumentation, https://bolo.ubuptu.com/
* Documentation: https://hetp.ubuntu.com/
Jack Jacker Mar Fab 4 40-44-44 2046 From 472 46 4 40
Last togth: Mon Feb 1 10:14:11 2016 From 1/2.16.1.10
clsco@clsco-ubuntuclient:~\$ \$



# Problemen oplossen

VTEP-adres is niet toegewezen

Controleer of het Infrastructuur VLAN is ingeschakeld onder het AEP:

Policies 🧃 🖸	Attachable Access En	tity Profile - AEP-AVS				ł
Quick Start						
Switch Policies			Policy	Operational	Faults	History
Module Policies		A A O O			A	CTIONS -
Interface Policies		E A C C				
Global Policies	Properties					
Attachable Access Entity Profiles	Name:	AEP-AVS				1
📃 AEP-AVS	Description:	optional				
AEP_DVS	L L					
L3Out-N3K2-alumbrer	Enable Infrastructure VLAN:					
L3OutN3k-AEP	Domains (VMM, Physical or External)	0				
📃 default	Associated to Interfaces:				×	+
QOS Class Policies		<ul> <li>Name</li> </ul>	State			
DHCP Relay Policies		AVS (Vmm-VMware)	formed			
MCP Instance Policy default						
EP Loop Protection Policy						
Error Disabled Recovery Policy						
Rogue EP Control Policy						
Monitoring Policies						
Troubleshoot Policies	VSwitch Policies					
Pools	Port Channel Policy:	select a value 🗸 🗗				
Physical and External Domains	LI DP Policy:					
	LEDF Folicy.					
	CDP Policy:	CDP_ON 👻 🗗				
	STP Policy:	select a value 🗸 🕞				
	Firewall Policy:	select a value 🗸 🛃				

#### Niet ondersteunde versie

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

~ # 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 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.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! 0.0.0.0bootpc > 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 169 SIS VMware ESXi vmnic4 Eth1/5 AVS:localhost.localdomainmain Eth1/6 169 SIS VMware ESXi vmnic5 N3K-2(FOC1938R02L) Eth1/13 166 RSIS 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 \_\_\_\_\_ 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 \_\_\_\_ \_\_\_\_ infra:default active Eth1/1, Eth1/20 13 active Eth1/13 19 \_ \_ 22 mgmt:inb active Eth1/1 26 active Eth1/5, Eth1/6, Po5 active Eth1/1 27 \_\_\_ active Eth1/5, Eth1/6, Po5 28 ::

VLAN	Туре	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:

Access Port Policy Group	- AVS-102_1-ports-7	_PolGrp							<b>i &gt;</b>	ţ
						P	olicy F	aults	Histor	y
⊙±								AC	TIONS -	
Properties										
Name:	AVS-102_1-ports-7_PolGrp								1	l
Description:	optional									
Label:										
Link Lowel Bellevi										
Link Level Policy:	1GigAuto -	C <sup>2</sup>								
CDP Policy:	CDP_ON .	e								
MCP Policy:	select a value									
LLDP Policy:	LLDP_ON	ø								
STP Interface Policy:	select a value									
Storm Control Interface Policy:	select a value									
L2 Interface Policy:	select a value									
Monitoring Policy:	select a value									
Attached Entity Profile:	AEP_DVS	e								
Connectivity Filters:				×	+					
	Switch IDs	In	terfaces							
						SHOW USAGE	SUBMIT		CLOSE	1

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
 _____ _____
    enet CE
13
                    vxlan-16777209, vlan-3967
19 enet CE
                    vxlan-14680064, vlan-150
22 enet CE
                   vxlan-16383902
26 enet CE
                    vxlan-15531929, vlan-200
    enet CE
27
                    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: 10.0.32
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

<u>Cisco Systems, Inc. Cisco Application Virtual Switch Installatie-gids, release 5.2(1)SV3(1.2)</u> 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