Contents

Introduction Prerequisites Requirements Components Used Configure Network Diagram Configurations Verify Troubleshoot Related Information

Introduction

This document decribes how to deploy an Application Virtual Switch (AVS) switch with an Adaptive Security Virtual Appliance (ASAv) single firewall in Routed/GOTO mode as a L4-L7 Service Graph between two End Point Groups (EPGs) to establish client-to-server communication using ACI 1.2(x) Release.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Access Policies configured and interfaces up and in service
- EPG, Bridge Domain (BD) and Virtual Routing and Forwarding (VRF) already configured

Components Used

The information in this document is based on these software and hardware versions:

Hardware & Software:

- UCS C220 2.0(6d)
- ESXi/vCenter 5.5
- ASAv asa-device-pkg-1.2.4.8
- AVS 5.2.1.SV3.1.10
- APIC 1.2(1i)
- Leaf/Spines 11.2(1i)
- Device packages *.zip already downloaded Features:

```
• AVS
```

• ASAv

- EPGs, BD, VRF
- Access Control List (ACL)
- L4-L7 Service Graph
- vCenter

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Network Diagram

As shown in the image,



Configurations

AVS Initial Setup creates a VMware vCenter Domain (VMM integration)2

Note:

- You can create multiple datacenters and Distributed Virtual Switch (DVS) entries under a single domain. However, you can have only one Cisco AVS assigned to each datacenter.
- Service graph deployment with Cisco AVS is supported from Cisco ACI Release 1.2(1i) with Cisco AVS Release 5.2(1)SV3(1.10). The entire service graph configuration is performed on

the (Cisco APIC).

- Service Virtual Machine (VM) deployment with Cisco AVS is supported only on Virtual Machine Manager (VMM) domains with Virtual Local Area Networks (VLAN) encapsulation mode. However, the compute VMs (the provider and consumer VMs) can be part of VMM domains with Virtual Extensible LAN (VXLAN) or VLAN encapsulation.
- Also note that if local switching is used, Multicast address and pool are not required. If no local switching is selected, then Multicast pool has to be configured and the AVS Fabric-wide multicast address should not part of the Multicast pool. All traffic originated from the AVS will be either VLAN or VXLAN encapsulated.

G 1

Navigate to VM Networking > VMWare > Create vCenter Domain, as shown in the image:

reate 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	3		
Encapsulation:	VLAN				
	O VXLAN				
Associated Attachable Entity Profile:	AEP-AVS	-	Ø		
VLAN Pool:	VlanPool-AVS(dynam	ic) 🗸	Ø		
Security Domains:			× +		
	Name	Description		-	
vCenter Credentials:				×	+
	Profile Name	Username	Description		
	vCenterCredentials	root			
				×	
vCenter:				6	+
vCenter:	Name	IP	Туре	Stats Collection	+

If you're using Port-channel or VPC (Virtual Port-channel) it is recommended to set the vSwitch policies to use Mac Pinning.

After this, APIC should push AVS switch configuration to vCenter, as shown in the image:



On APIC you can notice that a VXLAN Tunnel Endpoint (VTEP) address is assigned to the VTEP port-group for AVS. This address is assigned no matter what Connectivity mode is used (VLAN or VXLAN)

Inventory S 🖸	Portgroup - vtep						i
Microsoft CoenStack						Ceneral Faults	History
VMware							
AVS	Properties						
Controllers	Encap:	vtep vlan-3967					
Hypervisors	Management Network	Server Name	Name	State	MAC	IP Address	
▶ □ 10.201.35.218	, and the second s	10.201.35.219	vmk1	Up	00:50:56:68:CA:25	10.0.16.95	
▶ □ 10.201.35.219		10.201.35.218	vmk1	Up	00:50:56:61:07:CC	10.0.18.94	
DVS - AVS							
Pod6-ALUMBRERIAVS-AEP-VMM-a							
► 🛄 quarantine							
▶ 1 uplink							
M Mep							
		(Page 1 Of		Objects Per Page: 1	5 🗸	Displaying Objects 1	- 2 Of 2

Install the Cisco AVS software in vCenter

• Download (VIB) from CCO using this link

Note: In this case we are using ESX 5.5, Table 1, shows the Compatibility matrix for ESXi 6.0, 5.5, 5.1, and 5.0

Table 1 - Host Software Version Compatibility for ESXi 6.0, 5.5, 5.1, and 5.0

there is a second to prove the second	The same second second second second			
Viliware 1	V18 2	VEM Bundle 2	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- misase.zip (Offine) VEM600-201512250119-BG (Online)	6.0	6.0
ESX 5.5	cross_cisco-vem-v250-5.2.1.3.1.10.0-3.2.1.vib	VEM550-201512250113-BG- release.zip (Offine) VEM550-201512250113-BG (Online)	5.5	5.5
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	VEM500-201512250101-8G- release.zip (Offline) VEM500-201512250101-8G (Online)	5.0	5.0

Within the ZIP file there are 3 VIB files, one for each of the ESXi host versions, select the one appropriate for ESX 5.5, as shown in the image:

CiscoAVS_1.10-5.2	.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 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

• Copy the VIB file to ESX Datastore - this can be done via CLI or directly from vCenter

Note: If a VIB file exists on the host, remove it by using the esxcli software vib remove

command.

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

or by browsing the Datastore directly.

• Install the AVS software using the following command on the ESXi host:

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

<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					1	
Switch Name vSwitch0 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							
~ #						0	

• Once the Virtual Ethernet module (VEM) is up, you can add Hosts to your AVS:

In the Add Host to vSphere Distributed Switch dialog box, choose the virtual NIC ports that are connected to the leaf switch (In this example you move only vmnic6), as shown in the image:

Add Host to vSphere Distributed Switch	h			_ 🗆 🗾 📈
Select Hosts and Physical Adapter Select hosts and physical adapters	s to add to this vSphere distributed switch			
Select Host and Physical Adapters			Settings	View Incompatible Hosts
Network Connectivity	Host/Physical adapters	In use by switch	Settings	Uplink port group
Virtual Machine Networking	E I 10.201.35.218		View Details	
Ready 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
Help			< Back N	lext > Cancel

- Click Next
- In the Network Connectivity dialog box, click Next
- In the Virtual Machine Networking dialog box, click Next
- In the Ready to Complete dialog box, click Finish

Note: If multiple ESXi hosts are used, all of them need to run the AVS/VEM so they can be managed from Standard switch to DVS or AVS.

With this, AVS integration has been completed and we are ready to continue with L4-L7 ASAv deployment:

ASAv Initial Setup

• Download Cisco ASAv Device Package and import it into APIC:

Navigate to L4-L7 Services > Packages > Import Device Package, as shown in the image:

Fabric	VM Networking	L4-L7 Services	Admin	Operations	
		Inventory Packages			
Quick Star	t				
HELP					
The Package balancer, cont and network c	s menu allows you to in ext switch, SSL termina onnectivity information	nport L4-L7 device pao ttion device, or intrusio for each function. A ne	ckages, which are used on prevention system (atwork service device i	d to define, configure, and monito (IPS). Device packages contain d is deployed in the network by add	or a network service lescriptions of the fu ding it to a service g
You can use the configuring as	ne Import a Device Pa	ckage wizard to impor	t a device package for	r a function that you want to man	age with APIC. We
ostrigunig ut	In	nport Device Pa	ackage	i	×
Quick S	Start				
Import a	Device Package	File Name:		BROWSE	Device Types
					_
				SUBMIT CLOSE	

• If everything works well, you can see the imported device package expanding L4-L7 Service Device Types folder, as shown in the image:



Before you continue, there are few aspects of the installation that need to be determined before the actual L4-L7 integration is performed:

There are two types of Management networks, In-Band Management and Out-Of-Band (OOB), these can be used to manage devices that are not part of the basic Application Centric Infrastructure (ACI) (leaf, spines nor apic controller) which would include ASAv, Loadbalancers, etc.

In this case, OOB for ASAv is deployed with the use of Standard vSwitch. For bare metal ASA or other service appliances and/or servers, connect the OOB Management port to the OOB switch or Network, as shown in the image.



ASAv OOB Mgmt Port management connection needs to use ESXi uplink ports to communicate with APIC via OOB. When mapping vNIC interfaces, Network adapter1 always matches the Management0/0 interface on the ASAv, and the rest of the data plane interfaces are started from Network adapter2.

The Table 2 shows the concordance of Network Adapter IDs and ASAv interface IDs:

Table 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

- Deploy the ASAv VM through the wizard from File>Deploy OVF (Open Virtualization Format) Template
- Select asav-esxi if you want to use standalone ESX Server or asav-vi for vCenter. In this

case, vCenter is used.



 Go through the installation wizard, accept terms and conditions. In the middle of the wizard you can determine several options like hostname, management, ip address, firewall mode and other specific information related to ASAv. Remember to use OOB management for ASAv, as in this case you need to keep interface Management0/0 while you use the VM Network (Standard Switch) and interface GigabitEthernet0-8 is the default network ports.

Deploy OVF Template	
Source Select the source location.	
Source OVF Template Details Name and Location Storage Disk Format Ready to Complete	Deploy from a file or URL 2: 'Documents'(SSP WCTUPMAGE'ssav952'ssav-vi.ovf
Help	< Back Next > Cancel

• Booke 5 White State and the Assace and password. This username and password is used by

username admin password <device_password> encrypted privilege 15

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

Additionally, from Global configuration mode enable http server:

http server enable

http 0.0.0.0 0.0.0.0 management

L4-L7 for ASAv Integration in APIC:

- Log in to the ACI GUI, click on the Tenant where the service graph will be deployed. Expand L4-L7 services at the bottom of the navigation pane and right click on L4-L7 Devices and click on Create L4-L7 devices to open the wizard
- For this implementation, following settings will be applied: -Managed Mode
- -Firewall Service
- -Virtual Device
- -Connected to AVS domain with a Single Node
- -ASAv Model
- -Routed mode (GoTo)
- -Management Address (has to match the previously address assigned to Mgmt0/0 interface)
- Use HTTPS as APIC by default uses the most secure protocol to communicate with ASAv

TEP 1 > General 1. General 2. Dord Configural Tesses select device package and enter connectivity information. Image: [2] Image: [2] Image: [2] Swint Try Tesses Image: [2] Image:	eate L4-L7 Device	S					
Neese solect device package and enter connectivity information. General Manager & Man	TEP 1 > General					1. General 2. Device	Configura
General Measure of Advancement of Advance (Advance) (Advancement of Advance (Advance) (Advancement of Advance (Advance) (Advance) (Advancement of Advance (Advance) (Advance) (Advancement of Advance (Advance) (Please select device	package and enter connectivity info	rmation.				
Manipulsion Machadis Round Bencing Tipe Time: Chan Add Round Bencing Tipe Time: Chan Add Round Bencing Tipe Time: Chan Add Round Unit Operating Tipe Time: Chan Add Round Unit Operating Tipe Time: Chan Add Round Device Previage Global Add Round Connectivity Chan Add Round Preview Time:	General	a	Device 1				
Service Type: Immediation Mode Cancer Develop(Mode - Mode	Name	ASAv-AVS-Routed	Management IP Address:	10.201.35.3		Management Port: https	*
Dever type Investor type Investo	Service Type	Finwal	VM:	vCenterController/AS	Av-in-AVS 🚽 付		
Device free Marcack, withing Widd Dearter, Marcack, Withing → M Claser Mote: # Singe Note: → M Claser → M Claser Device Privace, Close 3.04: 12 → Ø Mone: Kalw → Ø Function Type: Classification → Ø Connectivity - Ø Marcark Closer - Ø Connectivity - Ø Dealer Breiker, Classification - Ø Connectivity - Ø Bits Breiker - Ø Dealer -			Device Interfaces:				× +
Wide Duraits: KS • ØF Mode: Statute:	Device Type	PHYSICAL VIRTUAL		Name	VNIC	Path (Only For Route Peering)	
Mote::::::::::::::::::::::::::::::::::::	VMM Domain:	AVS 🗸 🖓		GigabitEthernet0/0	Network adapter 2	Node-102/MAC_Pinning	
Objecto Prolonger: GEOD ASS-12 • @B Model:: Xdow • @B Function Type:: Contract_Conttact_Conttact_Contract_Contract_Contract_Contract_Contract_Contr	Mode	Single Node O HA Cluster		GigabitEthernet0/1	Network adapter 3	Node-102/MAC_Pinning	
Mode: Xdor Cluster Pureton Type: Custor Science(Vit) Custor Micro Editores: Custor Connectivity: Science: Micro Editores: Custor Micro Editores: Custores	Device Package:	CISCO-ASA-1.2					
Rundon Type: Optimum: Optimum: Texts Management Pixt Stripts	Model	ASAv					
Processing Control of Charter Classifier Connectivity Connectivity Connectivity Control of Read Contr	Duration Trans						
Management PActives 15 323 33 Management PActives 15 323 33 Management PActive tags - Claster Instruction Xet -	Punceon Type.	Gothrough Goto	Cluster				
Connectivity Conne			Management IP Address:	10.201.35.3		Management Port: https	-
Type Name Convektive Donnectivity Braviniti Devisit SignificitiumedDi AMD to Devis Quel Collaud Braviniti Devisit SignificitiumedDi Interactivity In Brandi Devisit SignificitiumedDi Devisit SignificitiumedDi Credentialis Userance Immunor Immunor Immunor Prodentianises Immunor Immunor Immunor Immunor			Cluster Interfaces:				× +
Connectivity				Туре	Name	Concrete Interfaces	
APC & Devis & Out Read APC & Devis & Out Read APC & Devis & Out Read Devis &				provider	Serverint	Device1/GigabitEthernet0/0	
Control Texas and the second sec	Connectivity			0004118947	Cleatiat	Device (RisshitEthernet)/1	
Zredenlais burrent with paramoti	APIC to Device	Out-Of-Band		consoliter	Congritteria	Dense in against the local i	
Credentizers white Prevent	varagement Corriboraty	In-Band					
Userane: admin Pessoot Postoot	Credentials						
Password:	Username	admin					
Confirm Passaurot:	Password:						
	Confirm Password						

• The correct definition of the Device Interfaces and the Cluster Interfaces is critical for a successful deployment

For the first part, use Table 2 showed in the previous section to properly match the Network Adapter IDs with the ASAv interface IDs that you'd like to use. The Path refers to the physical Port or Port-channel or VPC that enables the way in and out of the Firewall interfaces. In this case, ASA is located in an ESX host, where in and out are same for both interfaces. In a Physical appliance, Inside and Outside of the Firewall (FW) would be different physical ports.

For the second part, the Cluster interfaces have to be defined always with not exceptions (even if Cluster HA is not used), this is because the Object Model has an association between the **mlf** interface (meta interface on the Device Package), the **Llf** interface (leaf interface such as e.g., external, internal, inside, etc.) and the **Clf** (concrete interface). The L4-L7 concrete devices have to be configured in a device cluster configuration and this abstraction is called a logical device. The logical device has logical interfaces that are mapped to concrete interfaces on the concrete device.

For this example, the following association will be used:

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

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

LATER AND ADD AND DOUBLE

L4-L7 Devices - ASAV-AVS-Houted				1
				Policy Parameters Faults History
⊙₹				ACTIONS -
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: QoThrough CoTo Cluster Mode: Single Node	Device 1 Management IP Address: vCenter Name: Interfaces:	10.201.35.223 vCenterController Name GigabitEthemet0/1 GigabitEthemet0/2	Management Po VM Nart VNIC Network adapter 4	R: 443 ASAv-in-AVS X + Path [Only For Route Peering] Node-102/MAC_Pinning, Nod Node-102/MAC_Pinning
Credentials Username: admin Password: Confirm Password: Configuration State	Cluster Management IP Address: Cluster Interfaces:	10.201.35.223 Type Consumer	Management Po	rf: 443
Configuration Issues: Devices State: stable		provider	Serverins	

Note: For failover/HA deployments, GigabitEthernet 0/8 is pre-configured as the failover interface.

Device state should be Stable and you should be ready to deploy the Function Profile and Service Graph Template

Service Graph Temple

The second

Firstly, create a Function Profile for ASAv but before that you need to create Function Profile Group and then L4-L7 Services Function Profile under that folder, as shown in the image:

Create L4-L7 Services Fu	nction Profile	Group		i ×			
Specify the information ab	out the Function	on Profile Group					
Name: FunPr Description:	rofGroup						
		[SUBMIT	ANCEL			
Tenant Pod5-ALUMERER	L4-L7 Services Fi	unction Profile Group	- FunProGroup			General Faults	i Hatory
Application Profiles	⊙±		AAOO				CTIONS -
L4-L7 Service Parameters Security Policies M Troubleshoot Policies	Properties Name: Description:	FunProGroup					
Monitoring Policies L4-L7 Services	Service Function Profiles:	• Name	Associated Function	Descriptio			× +
L4-L7 Service Graph Templates Router configurations Encircle Profiles			5	No items have been found dect Actions to create a new	f. Rem.		
FunProGroup Eulote L4-L7 Devices Imported Devices Create L4-L7 Services Fun	ction Pholie						
Devices Selection Save as Deployed Graph In Post							
Deployed Devices Inband Management Configuration for L4-L7 device							

• Select the **WebPolicyForRoutedMode** Profile from the drop down menu and proceed to configure the interfaces on the firewall. From here on, the steps are optional and can be implemented/modified later. These steps can be taken at a few different stages in the deployment depending on how reusable or custom the Service Graph could be.

For this exercise, a routed firewall (GoTo mode) requires that each interface has a unique IP address. Standard ASA configuration also has a interface security level (external interface is less secure, internal interface is more secure). You can also change the name of the interface as per your requirement. Defaults are used in this example.

• Expand Interface Specific Configuration, add IP address and security level for ServerInt with the following format for the IP address **x.x.x.x/y.y.y.y or x.x.x.x/yy**. Repeat the process for the ClientInt interface.

Note: You can also modify the default Access-List settings and create your own base

template. By default, the RoutedMode template will include rules for HTTP & HTTPS. For this exercise, SSH and ICMP will be added to the allowed outside access-list.

Name: FunF	rof-ASA						
Description: optio	nal						
Copy Existing Profile Parameters: 🔽							
Profile: CISC	O-ASA-1.2/WebPolic	yForRoutedMode	- CP				
atures and Parameters							
	In order to auto ap	ply new values to the paramete	rs of existing graph in	stance when users r	modify function profiles, t	he name of top folder	must be ended with -Defa
Features:	Basic Parameters	All Parameters					
	Folder/Par	am	Name	Value	Mandatory	Locked	Shared
Interfaces	В	Destination Service	destination serv	ce			
AccessLists		- 📃 High Port					
NAT		E Low Port	low_port	22		false	
TrafficSelectionObjects		- E Operator	operator	eq		false	
TrafficSelectionObjects All		Operator ICMP	operator	eq		false	
TrafficSelectionObjects		Operator Operator Operator Operator Operator Operator Operator Operator Operator Operator	operator	eq		false	
TrafficSelectionObjects All			operator	eq		false	
TrafficSelectionObjects All		CMP CMP Cogging Protocol Source Address	operator	eq		false	
TrafficSelectionObjecta All			operator	eq		false	
TrafficSelectionObjecta All			operator	eq permit		false false	

Then click Submit

• Now, create the Service Graph Template

Tenant Pod6-ALUMBRER 🛃 🖸	1 4-1 7 Service (
Quick Start	
Tenant Pod6-ALUMBRER	
Application Profiles	⊖±
Networking	hiere
L4-L7 Service Parameters	 Name
Security Policies	
Troubleshoot Policies	
Monitoring Policies	
L4-L7 Services	
L4-L7 Service Graph Templates	
Router configurations	Service Graph Template

• Drag and Drop the Device Cluster to the right to form the relationship between Consumer and Provider, select Routed Mode and the previously created Function Profile.

iraph Name:	Graph1-alumbrer		
iraph Type:	Create A New One	Clone An Existing One	
Consumer		C 555 P	Provide Pro
	Please drag a de	wice from devices table and drop it here to create a service node.	
ASAv-AVS-Routed	Information		
Firewall: 💿	Routed Transparer	nt	
Profile: Po	d6-ALUMBRER/FunProfGroup/FunF	Pro 👻 🗗	
			SUBMIT CANCE

• Check template for faults. The templates are created to be reusable, they must then be applied to particular EPGs etc.

• To a	apply a template	right click an	d select Apply L4-L7	Service Graph	Template
--------	------------------	----------------	----------------------	---------------	----------

Tenant Pod6-ALUMBRER S	1 4-1 7 Service Graph Template - Graph1-alumbrer
Cuick Start	
Tenant Pod6-ALUMBRER	Topology Policy Faults History
Application Profiles	
Networking	Consumer Broulder
L4-L7 Service Parameters	Consumer
Security Policies	
Troubleshoot Policies	ASAv-AVS
Monitoring Policies	
L4-L7 Services	ASAy
L4-L7 Service Graph Templates	
Graph1-alumbrer	outed information
🕨 📃 Function Node - ASA 😂 Apply L4-L7 Se	vice Graph Template II: Routed
Router configurations Edit L4-L7 Server	ce Graph Template 1: FunPro-ASA
Function Profiles Delete	
A 🔯 FunProfGroup 🛛 🔀 Remove Relate	d Objects Of Graph Template
📃 FunPro-ASA 🔰 Save as	
L4-L7 Devices	
ASAv-AVS-Routed	
ASAV-DVS	
Imported Devices	
Devices Selection Policies	
Deployed Graph Instances	
Deployed Devices	
🛄 Inband Management Configuration for L4-L7 devi	
https://10.201.35.211/#	SHOW USAGE SUBMIT RESET

Define which EPG will be on the Consumer side and Provider side. In this exercise, AVS-EPG2 is the Consumer (Client) and AVS-EPG1 is the Provider (server). Remember that no Filter is applied, this will allow the firewall to do all the filtering based on the access-list defined in the last section of this wizard.

.

•	C	ic	k	N	ext
•			N I		GAL

STEP 1 > Contract					1. Contract	2. Graph
Config A Contract Betwee	en EPGs					
Consumer EPG / Ext	ternal Network: Pod6-ALUMBRER/AVS	S-AEP-VMM 👻 🗗	Provider EPG / External Netwo	k: Pod6-ALUMBRER/AVS-AEP-VMM -	G	
Contract Information				alumbrer/epg-AVS-EPG1		
Contract: Contract Name:	Create A New Contract EPG2-to-EPG1	Choose Ar	h Existing Contract Subject	Pod6-ALUMBRER/InternalAEP- VMM-alumbrer/epg-EPG-Internal- alumbrer		
No Filter (Allow All Traffic):				Pod6-ALUMBRER/VRF1-alumbrer /AnyEPG		
				Pod6-ALUMBRER/VRF2/AnyEPG		
				Pod6-ALUMBRER/L3Out-N3K2/L3Net		

	PREVIOUS	NEXT	CANCEL	

• Verify the BD information for each of the EPGs. In this case, EPG1 is the Provider on the IntBD DB and EPG2 is the Consumer on BD ExtBD. EPG1 will connect on firewall interface

ServerInt and EPG2 will be connected on interface ClientInt. Both FW interfaces will become the DG for each of the EPGs so traffic is forced to cross the firewall at all times.

Click Next

Consumer		Provider	
ASAv-AVS-Routed Information Firewall: routed Profile: FunPro-ASA Consumer Connector	,	AVS-EPG1	
Type: Ceneral Pauta Pagring			
BD: Pod6-ALUMBRER/ExtBD-alumbrer Cluster Interface: ClientInt ClientInt ClientInt			
Provider Connector Type: ⓐ General ⓑ Route Peering BD: Pod6-ALUMBRER/IntBD-alumbrer ☑ ☑ Cluster Interface: ServerInt ☑			

 In the Config Parameters section, click on All Parameters and verify if there are RED indicators that need to be updated/configured. In the output as shown in the image, it can be noticed that the order on the access-list is missed. This is equivalent to the line order you'll see in a show ip access-list X.

le Name:	FunPro-ASA	g 🐧					
atures:		Require	d Parameters Al Parameters				
		1	Folder/Param	Name		Value	Witte Domain
		8	4 🥩 Access List	access-list-	bound		
AccessLists		E 😑	Access Control Entry	ICMP			
			Access Control Entry	519-2			
	nObjects	8	A 🤿 Access Control Entry	SSH			
All			Destination Address				
		8	Destination Service	destination	ervice		
			ICMP				
			Logging				
		8	Protocol	protocol			
			Source Address				
			Source Service				
			E Action	action		permit	
			Crder	order			select asa domain
		78	Access Control Entry	unnare a			
			Access Control Entry	OPDATE	CANCEL		

• You can also verify the IP addressing assigned from the Function Profile defined earlier, here is a good chance to change information if required. Once all parameters are set, click **Finish**, as shown in the image:

STEP 3 > ASAv-AVS-Rou	uted Parameters	1. Contract 2. Graph 3. ASAv-AVS-Routed P	arameters
config parameters for the se	elected device		
Profile Name: FunProf-ASA	æ		
Features:	Required Parameters All Parameters		
Interfaces	Folder/Param	Name Value Write Domain	
Anneel iste	E 4 🗇 Device Config	Device	
MAT	Access List	access-list-inbound	
DATE OF A LOCAL OF A	Bridge Group Interface		
TrafficSelectionObjects	E Interface Related Configuration	externalif	
All	Access Group	ExtAccessGroup	
	Inbound Access List	name access-list-inbound	
	Outbound Access List		
	IPv6 Enforce EUI-64		
	Interface Specific Configuration	externalIfCfg	
	A Great Pv4 Address Configuration	IPv4Address	
	El IPv4 Address	ipv4_address (192.168.10.1/24)	
	IPv4 Standby Address		
	IPv6 Address Configuration		
	IPv6 Link Local Address Configuration		
	III IPv& Router Advertisemente		

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

• If everything goes fine, a new Deployed device and Graph Instance should appear.

.....

L4-L7 Services
L4-L7 Service Graph Templates
Router configurations
Function Profiles
L4-L7 Devices
Imported Devices
Devices Selection Policies
Deployed Graph Instances
EPG2-to-EPG1-Graph1-alumbrer-Pod6-ALUM
Deployed Devices
* ** ASAv-AVS-Routed-none

Verify

• One important thing to verify after creating the Service graph is that the Consumer/Provider relationship was created with proper Meta Connector. Verify under the Function Connector Properties.

Note: Each interface of the Firewall will be assigned with an encap-vlan from the AVS

Dynamic Pool. Verify there are no faults.

ALL TENANTS Add Tenant Search: enter name, desc	common Pod6-AL	UMBRER Pod6-ALUMBRER2 infra	mgmt					
Tenant Pod6-ALUMBRER	Virtual Device - A	ASAv-AVS-Routed-none						i
Cuick Start	1			_				
Tenant Pod6-ALUMBRER				Policy	Operational	Health	Faults	History
Application Profiles	Ð₩		A A O O 100					
Networking								
L4-L7 Service Parameters	Properties							
Security Policies	Devices:	ASAv-AVS-Routed						
Troubleshoot Policies	Virtual Device ID:	25351						
Monitoring Policies	VHF: ACKed Transaction ID:	10000						
L4-L7 Services	Current Transaction ID:	10000						
L4-L7 Service Graph Templates	Cluster Interfaces:	Logical Interface	Encan					
Router configurations		Logical Interface	cheap	-				
Function Profiles		ASAv-AVS-Routed_ClientInt	vlan-93					
L4-L7 Devices		ASAv-AVS-Routed_ServerInt	vlan-94					
Imported Devices								
Devices Selection Policies								
Deployed Graph Instances								
EPG2-to-EPG1-Graph1-alumbrer-Pod6-ALU	v							
Deployed Devices								
ASAv-AVS-Routed-none								
Internet Management Configuration (eq.) 4.1.7 day								

• Now, you can also verify the information that was pushed to the ASAv

ISAv-w-AVS# show interface	ip brief				
Interface	IP-Address	OK?	Method	Status	Prot
ocol					
igabitEthernet0/0	192.168.10.1	YES	manua l	սք	սք
igabitEthernet0/1	172.16.1.1	YES	manua l	սք	սք
igabitEthernet0/2	unassigned	YES	unset	administratively down	սք
igabitEthernet0/3	unassigned	YES	unset	administratively down	սք
igabitEthernet0/4	unassigned	YES	unset	administratively down	սք
igabitEthernet0/5	unassigned	YES	unset	administratively down	սք
igabitEthernet0/6	unassigned	YES	unset	administratively down	սք
igabitEthernet0/7	unassigned	YES	unset	administratively down	սք
igabitEthernet0/8	unassigned	YES	unset	administratively down	սք
1anagement0/0	10.201.35.223	YES	CONFIG	սք	սք
ISAv-w-AVS# show run access	s-list				
access-list access-list-inl	oound extended	permit	tcp ar	ny any eq ымы	
access-list access-list-inl	oound extended	permit	tcp ar	ny any eq https	
access-list access-list-inl	oound extended	permit	tcp ar	ny any eq ssh	
access-list access-list-inl	oound extended	permit	: ісмра	any any	
λΩΟ−μ−ΑUS#					

 A new Contract is assigned under the EPGs. From now on, if you need to modify anything on the access-list, the change has to be done from the L4-L7 Service parameters of the Provider EPG.

Tenant Pode-ALUMBRER	L4-L7 Service Parame	eters					i
Cuick Start Cuick	Search By Name / Value:						
Application EPGs	Meta Folder/Param Key	Contract Name	Service Graph Name	Service Function Name	Folder/Param Instance Name	Value	Specific Device
C EPG AVS-EPG1	Interlace	EPG240-EPG1	Graph1-Temp-alumbrer	ASAv	ClientInt		
Domains (VMs and Bare-Metals)	Exint/ConfgRelFolder	EP024o-EP01	Graph1-Temp-alumbrer	ASAv	ExtConfig		
Static Bindings (Paths)	InintConfigRelFolder	EPG240-EPG1	Graph1-Temp-alumbrer	ASAv	IntConfig		
Static Bindings (Leaves)	Interface	EP024o-EP01	Graph1-Temp-alumbrer	ASAv	Serverint		
Contracts Static EndPoint Subnets L4-L7 Vinual Pe L4-L7 P Address Pool L4-L7 Envice Parameters M CP PA AVE EPG2	AccessLit	EP0240-EPG1	Grapht-Temp-aiumbrer	ASAv	access-list-inbound		

• On vCenter, you can also verify the Shadow EPGs are assigned to each of the FW interfaces:

For this test, I had the 2 EPGs communicating with standard contracts, these 2 EPGs are in different Domains and different VRFs, so route leaking between them was previously configured. This simplifies a bit after your insert the Service Graph as the FW sets up the routing and filtering in between the 2 EPGs. The DG previously configured under the EPG and BD can now be removed same as the contracts. Only the contract pushed by the L4-L7 should remain under the EPGs.

Quick Start	1	00111 0010								
Tenant Pod6-ALUMBRER Application Profiles		≎₹							ACTIONS -	1
AVS-AEP-VMM-alumbrer Application EPGs		 Tenant Name 	Contract Name	Contract Type	Provided / Consumed	QoS Class	State	Label	Subject Label	
▲ S EPG AVS-EPG1		G Contract Type: Co	ontract							
Domains (VMs and Bare-Me Static Bindings (Paths)		Pod6-ALUMBR	EPG2-to-EPG1	Contract	Provided	Unspecified	formed			
Static Bindings (Leaves)										
Contracts										
Static EndPoint										
Subnets										

As the standard contract is removed, you can confirm that traffic is now flows through the ASAv, the command show access-list should display the hit count for the rule incrementing every time the client sends a request to the server.



On the leaf, endpoints should be learned for client and server VMs as well as the ASAv interfaces

<pre>leaf2# show endpoint Legend: 0 - peer-attached H - vtep V - vpc-attached p - peer-a s - static-arp B - bounce</pre>	a - local ged L - local	ly-aged S - stat M - span	ic	
VLAN/ Domain	Encap VLAN	MAC Address	MAC Info/ Interfo IP Info	ace
+	+	++-		+
Pod6-ALUMBRER:VRF1-alumbrer		50.50.50.50 L		
14/Pod6-ALUMBRER:VRF1-alumbrer	vxlan-14778359	5897.bda4.f9bc L	eth	1/13
30	vian-98	0050.5689.1008 L	et et	:h1/7
Pod6-ALUMBRER:VRF1-alumbrer Ser	rver IP vlan-98	192.168.10.10 L	interface	
25 &	MAC vlan-94	0050.5689.ca89 14	(ServerInt	po4
Pod6-ALUMBRER:VRF1-alumbrer	vlan-94	192.168.10.1 L		
mgmt:inb		192.168.2.11 S		
21	vlan-97	0050.5689.3fca L	et	:h1/7
Pod6-ALUMBRER:VRF2	ent IP & vlon-97	172.16.1.10		
26	vlan-93	0050.5689.e7dd L		po4
Pod6-ALUMBRER:VRF2	vlan-93	172.16.1.1 L		
overlay-1		10.0.104.93		
overlay-1		10.0.96.67 L	FW	
13	vxlan-16777209	0050.5677.18a5 H	(ClientInt) unspeci	ified
overlay-1	vxlan-16777209	10.0.32.93 H	(chentint)	
13	vxlan-16777209	0050.5660.ddab H	unspeci	ified
overlay-1	vxlan-16777209	10.0.32.64 H		

see both firewall interfaces attached to the VEM.

ESX-1

_											
~ # V	rememd 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	2	UP	UP	FWD	_	0	4	0	0		ASAv-in-AVS.eth2
1040	Po1	UP	UP	FWD		0		0	0		

ESX-2

	-										
~ # ver	mcmd show p	ort vlo	an								
LTL	VSM Port	Admin	Link	State	Cause	PC-LTL	SGID	ORG	svcpath	Туре	Vem Port
24	Eth1/7	UP	UP	FWD		1040	6	0	0		vmnic6
50		UP	UP	FWD	-	0	6	0	0		vmkl
51		UP	UP	FWD	-	0	6	Ø	0		Client1-AVS.eth0
52		UP	UP	FWD	-	0	6	0	0		Server1-AVS.eth0
1040	Po1	UP	UP	FWD	-	0		0	0		
~ #											

Finally, the Firewall rules can be verified at the leaf level too if we know the PC Tags for source and destination EPGs:

EPG1								
Tenant Pod6-ALUMBRER					Policy O	perational Sta	its Health F	aults History
Application Profiles								
AVS-AEP-VMM-alumbrer					A30	ooased EPGs	Associated External	Houled Networks
Application EPGs	€							ACTIONS -
P G EPG AVS-EPG1	Name	Description	State	Issues	QoS	Encep	PC Te	0
 Control Ano-EPice Indeg EPGs 	AVS-EPG1		applied		Unspecified		17	
L4-L7 Service Parameters	EPO-Internal-alumbrer		applied		Unspecified		32772	1
🕨 🚭 InternalAEP-VMM-alumbrer								
Networking								
Bridge Domains								
VRFs	1							
VRF1-alumbrer								
• C VRF2								

EPG2



Filter IDs can be matched with the PC tags on the leaf to verify the FW rules.

interrupted or tied together via the shadow EPGs created by the L4-L7 service graph

insertion.

And communication Client to Server works.

cisco@cisc	o-UbuntuClient:~\$ ifconfig
ethi	Link encap:Ethernet HWaddr 00:50:56:89:3f:ca
	inet addr: 1/2.10.1.10 BCast:1/2.10.1.255 Mask:255.255.255.0
	UP BROADCAST RUNNING MULTICAST MILLISAA Metricii
	RX packets:346596 errors:0 dropped:97 overrups: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
	ineto addr: ::1/128 Scope:Host
	UP LOUPBACK RUNNING MIU:05530 METRIC:1
	TX packets:170350 errors:0 dropped:0 overruns:0 rrame:0
	collisions: 0 traveuelen:0
	RX bytes:18739044 (18.7 MB) TX bytes:18739044 (18.7 MB)
ciscolcisc	0-UbuntuClient:-\$ ssb 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)
* Documen	tation: https://help.ubuntu.com/
Last login	: Mon Feb 1 10:14:11 2016 from 172.16.1.10
cisco@cisc	o-UbuntuClient:~\$ \$
	Leaf 101 Leaf 102
	E1/7 Po4
AVS	



Troubleshoot

VTEP address is not assigned

Verify that Infrastructure Vlan is checked under the AEP:

Policies 🔄 🖸	Attachable Access En	tity Profile - AEP-AVS				-
Quick Start						
Switch Policies			Policy	Operational F	aults	History
Module Policies	⊖ ↓				AC	TIONS -
Interface Policies						
Global Policies	Properties					
Attachable Access Entity Profiles	Name:	AEP-AVS				
AEP-AVS	Description:	optional				
AEP_DVS						
L3Out-N3K2-alumbrer	Enable Infrastructure VLAN:					
L3OutN3k-AEP	Domains (VMM, Physical or External)					
📃 default	Associated to Interfaces:				~	-
QOS Class Policies		▲ Name	State			- 1
DHCP Relay Policies	1	AVS (Vmm-VMware)	formed			- 11
MCP Instance Policy default						- 11
EP Loop Protection Policy						- 11
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	LLDP Policy:					
	LEDT Folicy.					
	CDP Policy:	CDP_ON				
	STP Policy:	select a value 🗸 🔁				
	Firewall Policy:	select a value V				

Unsupported Version

client/agent).

Verify VEM version is correct and support appropriate ESXi VMWare system.

```
~ # 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 and Fabric communication not working

Check 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

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! 0.0.0.0.bootpc > 255.255.255.bootps: BOOTP/DHCP, Request from 00:50:56:6b:ca:25 (oui Unknown), length 300

At this point it can be determined that Fabric communication between the ESXi host and the Leaf does not work properly. Some verification commands can be checked at the leaf side to determine root cause.

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 Local Intrfce Hldtme Capability Platform Port ID Device-ID AVS:localhost.localdomainmain Eth1/5 169 SIS VMware ESXi vmnic4 AVS:localhost.localdomainmain Eth1/6 169 SIS 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 _____ Туре Group Port-Protocol Member Ports Channel _____ Po5(SU) Eth LACP Eth1/5(P) Eth1/6(P) 5 There are 2 Ports used in the ESXi connected via a Po5 leaf2# show vlan extended

VLAN NameStatusPorts---------13infra:defaultactiveEth1/1, Eth1/2019--activeEth1/1322mgmt:inbactiveEth1/1

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	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	

From the above output it can be observed that the Infra VIan is not allowed or passed through the Uplinks ports that go to the ESXi host (1/5-6). This indicates a misconfiguration with the Interface Policy or Switch Policy configured on APIC.

Check both:

Access Policies > Interface Policies > Profiles Access Policies > Switch Policies > Profiles In this case, the interface profiles are attached to the wrong AEP (old AEP used for DVS), as shown in the image:

Access Port Policy Group	- AVS-102_1-ports-7	_PolGrp							i X
						P	olicy Fa	ults	History
⊙±								ACT	IONS +
Properties									
Name:	AVS-102_1-ports-7_PolGrp								
Description:	optional								
Label:									
Link Level Policy:	1GigAuto	æ							
CDP Policy:	CDP_ON	e							
MCP Policy:	select a value								
LLDP Policy:	LLDP_ON	e							
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	æ							
Connectivity Filters:				×	+				
	Switch IDs		Interfaces						
						SHOW USAGE	SUBMIT	c	LOSE

After setting of the correct AEP for AVS, we can now see that the Infra VIan is seen thru the proper Unlinks at the 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
                    vxlan-14680064, vlan-150
19 enet CE
                   vxlan-16383902
vxlan-15531929, vlan-200
22 enet CE
26 enet CE
    enet CE
                    vlan-11
27
28
     enet CE
                     vlan-14
                    vxlan-15662984
 36 enet CE
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
```

Related Information

Application Virtual Switch Installation

<u>Cisco Systems, Inc. Cisco Application Virtual Switch Installation Guide, Release</u> <u>5.2(1)SV3(1.2)</u> Deploy the ASAv Using VMware

<u>Cisco Systems, Inc. Cisco Adaptive Security Virtual Appliance (ASAv) Quick Start Guide,</u> <u>9.4</u>

Cisco ACI and Cisco AVS

Cisco Systems, Inc. Cisco ACI Virtualization Guide, Release 1.2(1i)

Service Graph Design with Cisco Application Centric Infrastructure White Paper

Service Graph Design with Cisco Application Centric Infrastructure White Paper

Technical Support & Documentation - Cisco Systems