# ASAv im GoTo (L3)-Modus mit AVS- ACI Version 1.2(x)

## Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfiguration Netzwerkdiagramm Konfigurationen Überprüfung Fehlerbehebung Zugehörige Informationen

# Einführung

In diesem Dokument wird beschrieben, wie ein Application Virtual Switch (AVS)-Switch mit einer ASAv-Einzelfirewall (Adaptive Security Virtual Appliance) im Routed/GOTO-Modus als L4-L7-Servicediagramm zwischen zwei Endpunktgruppen (EPGs) bereitgestellt wird, um die Kommunikation zwischen Client und Server mit der ACI 1.2(x)-Version herzustellen.

## Voraussetzungen

## Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Zugriffsrichtlinien konfiguriert und Schnittstellen eingerichtet und in Betrieb
- EPG, Bridge Domain (BD) und Virtual Routing and Forwarding (VRF) sind bereits konfiguriert.

## Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

Hardware und 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)
- Gerätepakete \*.zip wurde bereits heruntergeladen

Funktionen:

- AVS
- ASAv
- EPGs, BD, VRF
- Zugriffskontrollliste (ACL)
- L4-L7 Servicediagramm
- vCenter

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

# Konfiguration

## Netzwerkdiagramm

Wie im Bild gezeigt,



## Konfigurationen

Bei der Ersteinrichtung von AVS wird eine VMware vCenter-Domäne (VMM-Integration)2 erstellt

### Hinweis:

- Sie können mehrere Rechenzentren und DVS-Einträge (Distributed Virtual Switch) unter einer einzigen Domäne erstellen. Jedem Rechenzentrum kann jedoch nur ein Cisco AVS zugewiesen werden.
- Die Bereitstellung von Servicediagrammen mit Cisco AVS wird von der Cisco ACI Version 1.2(1i) mit Cisco AVS Version 5.2(1)SV3(1.10) unterstützt. Die gesamte Servicediagrammkonfiguration wird auf dem Cisco Application Policy Infrastructure Controller (Cisco APIC) durchgeführt.
- Die Bereitstellung von virtuellen Systemen (Service Virtual Machine, VM) mit Cisco AVS wird nur auf VM-Domänen (Virtual Machine Manager) mit VLAN-Kapselungsmodus (Virtual Local Area Networks) unterstützt. Die Computing-VMs (die Provider- und Consumer-VMs) können jedoch Teil von VMM-Domänen sein, die Virtual Extensible LAN (VXLAN)- oder VLAN-Kapselung verwenden.
- Beachten Sie außerdem, dass bei Verwendung von lokalem Switching keine Multicast-Adresse und kein Multicast-Pool erforderlich sind. Wenn kein lokales Switching ausgewählt ist, muss der Multicast-Pool konfiguriert werden, und die Fabric-weite Multicast-Adresse des AVS sollte nicht zum Multicast-Pool gehören. Der gesamte Datenverkehr, der vom AVS stammt, ist entweder VLAN- oder VXLAN-gekapselt.

Navigieren Sie zu VM Networking > VMWare > Create vCenter Domain (vCenter-Domäne erstellen), wie im Bild gezeigt:

|--|

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 Switchin	g		
Encapsulation:	VLAN VXLAN				
Associated Attachable Entity Profile:	AEP-AVS	-	æ		
VLAN Pool:	VlanPool-AVS(dynam	iic) 🗸	æ		
Security Domains:			× -	F	
	Name	Description	ı		
vCenter Credentials:				×	+
	Profile Name	Username	Description		
	vCenterCredentials	root			
vCenter:				×	+
	Name	IP	Туре	Stats Collection	1
	vCenterController	10.201.35.9	vCenter	Disabled	

Wenn Sie Port-Channel oder VPC (Virtual Port-Channel) verwenden, wird empfohlen, die vSwitch-Richtlinien so festzulegen, dass sie Mac Pinning verwenden.

Danach sollte der APIC die AVS-Switch-Konfiguration auf vCenter übertragen, wie im Bild gezeigt:



Auf dem APIC ist zu bemerken, dass eine VXLAN Tunnel Endpoint (VTEP)-Adresse der VTEP-Portgruppe für AVS zugewiesen wird. Diese Adresse wird unabhängig vom verwendeten Verbindungsmodus (VLAN oder VXLAN) zugewiesen.

Inventory S 🖸	Portgroup - vtep						i
Microsoft						General Faults	History
DenStack	0 F						
VMware							
4 () AVS	Properties						
Controllers	Name:	vtep					
<ul> <li>TR2 vCenterController</li> </ul>	Encap:	vlan-3967					
🖌 🥅 Hypervisors	Management Network Adapters:	Server Name	Name	State	MAC	IP Address	
▶ □ 10.201.35.218		10.201.35.219	vmk1	Up	00:50:56:68:CA:25	10.0.16.95	
▶ □ 10.201.36.219		10.201.35.218	vmk1	Up	00:50:56:61:07:CC	10.0.16.94	
4 🛄 DVS - AVS						$\sim$	
Portgroups							
Pod6-ALUMBRERIAVS-AEP-VMM-a	l						
▶ 10 quarantine							
► 🛄 uplink							
► 🛄 vtep							
► ① DVS							
		(   Page 1 Of		Objects Per	Page 15 👻	Displaying Objects 1	- 2 0/ 2

Installation der Cisco AVS Software in vCenter

• Laden Sie das vSphere-Installationspaket (VIB) über diesen Link von CCO herunter.

**Hinweis**: In diesem Fall verwenden wir ESX 5.5, Tabelle 1, zeigt die Kompatibilitätsmatrix für ESXi 6.0, 5.5, 5.1 und 5.0.

Tabelle 1: Kompatibilität der Host-Softwareversion für ESXi 6.0, 5.5, 5.1 und 5.0

THE R. P. LEWIS CO., LANSING MICH.	of the same second se			
Villware 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.v/b	VEM600-201512250119-8G- release zip (Offine) VEM600-201512250119-8G (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	VEM510-201512250107-8G- release.zip (Offine) VEM510-201512250107-8G (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

Innerhalb der ZIP-Datei gibt es 3 VIB-Dateien, eine für jede ESXi-Hostversion, wählen Sie die entsprechende für ESX 5.5 aus, wie im Bild gezeigt:

CiscoAVS_1.10-5.2	2.1.SV3.1.10			
		Q Sear	ch	
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
<sup>h</sup> 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

 Kopieren der VIB-Datei in den ESX-Datenspeicher - dies kann über die CLI oder direkt über vCenter erfolgen

**Hinweis:** Wenn eine VIB-Datei auf dem Host vorhanden ist, entfernen Sie sie mithilfe des Befehls **esxcli software vib** remove.

esxcli software vib remove -n cross\_cisco-vem-v197-5.2.1.3.1.5.0-3.2.1.vib

oder indem Sie direkt im Datenspeicher navigieren.

• Installieren Sie die AVS-Software mithilfe des folgenden Befehls auf dem 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 —wartungsmodus —no-sig-check

~ # esxcli softw Installation Res Message: Open Reboot Requir VIBs Installe VIBs Removed: VIBs Skipped: ~ # vem status	are vib inst ult ation finish ed: false d: Cisco_boo Cisco_bootb	all -v /vmfs ed successfu tbank_cisco- ank_cisco-ve	/volumes/datastore lly. vem-v250-esx_5.2.1 m-v197-esx_5.2.1.3	1/cross_ .3.1.10. .1.5.0-3	cisco-vem-v250-5.2.1.3.1.10.0-3.2.1.vibmaintenance-modeno-sig-check 0-3.2.1 3.2.1	
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 (vemdp	a) is runnin	g				
~ #						

• Wenn das Virtual Ethernet-Modul (VEM) aktiviert ist, können Sie Ihrem AVS Hosts hinzufügen:

Wählen Sie im Dialogfeld Host zu vSphere Distributed Switch hinzufügen die virtuellen NIC-Ports aus, die mit dem Leaf-Switch verbunden sind (in diesem Beispiel verschieben Sie nur vmnic6), wie im Bild gezeigt:

d Host to vSphere Distributed Switc	h			_ 0
elect Hosts and Physical Adapter Select hosts and physical adapters	s to add to this vSphere distributed switc	h.		
			Californi	Mary Terrorenthic Line
elect Host and Physical Adapters	Host/Dhusical adapter	To use by switch	Settings	. View Incompatible Host
rtual Machine Networking		th use by switch	Securitys	opinkportgroup
dy to Complete			view Dietalis	
	Select physical adapters	vCultrh0	Maw Datalla	ualisk
	Vinnico	VSWITCHU	View Details	uplink
	vmnic1		View Details	uplink
	vmnic10		View Details	uplink
	Vmnic11		View Details	uplink
	Vinnic2		View Details	uplink
	winnics	DVS	View Details	uplink
		DVS	View Details	uplink
		075	View Details	uplink
			View Details	uplick
			View Details	uplick
	vinnice vinnice		View Details	uplink
,			< Back	Next > Cancel

- Klicken Sie auf Weiter
- Klicken Sie im Dialogfeld Netzwerkverbindungen auf Weiter
- Klicken Sie im Dialogfeld Virtuelle Systemnetzwerke auf Weiter
- Klicken Sie im Dialogfeld Fertig stellen auf Fertig stellen

**Hinweis:** Wenn mehrere ESXi-Hosts verwendet werden, müssen alle diese AVS/VEM ausführen, damit sie vom Standard-Switch zum DVS oder AVS verwaltet werden können.

Damit ist die AVS-Integration abgeschlossen, und wir sind bereit, die Bereitstellung von L4-L7 ASAv fortzusetzen:

### Ersteinrichtung von ASAv

 Laden Sie das Cisco ASAv-Gerätepaket herunter, und importieren Sie es in den APIC: Navigieren Sie zu L4-L7 Services > Packages > Import Device Package (L4-L7-Dienste > Pakete > Gerätepaket importieren), wie im Bild gezeigt:

Fabric	VM Networking	L4-L7 Services	Admin	Operations	
		Inventory   Packages			
Quick S	Start				
HELF	)				
The <b>Pac</b> balance and net	<b>kages</b> menu allows you to in r, context switch, SSL termin work connectivity information	mport L4-L7 device pao ation device, or intrusio for each function. A ne	kages, which are used on prevention system (If etwork service device is	to define, configure, and moni PS). Device packages contain deployed in the network by a	itor a network service descriptions of the fu dding it to a service g
You can	use the Import a Device Pa	ckage wizard to impor	t a device package for a	a function that you want to ma	nage with APIC. We
oonigu	Ir	nport Device Pa	ackage	i	×
Qu	ick Start	File Name:			Davias Turses
Imp	oort a Device Package	File Name.		BROWSE	Device Types

• Wenn alles gut funktioniert, sehen Sie das importierte Gerätepaket, das den Ordner L4-L7 Service Device Types erweitert, wie im Bild gezeigt:

CLOSE

i

SUBMIT

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

				General	Operational	Faults	History
⊙₹						ACT	TIONS -
Properties							
Vendor:	CISCO						
Model:	ASA						
Capabilities:	GoThrough,GoTo						
Major Version:	1.2						
Minor Version:	4.8						
Minimum Required Controller Version:	1.1						
Logging Level:	DEBUG	•					
Package Name: 0	device_script.py						
Supported Protocols:							
Interface Labels:	<ul> <li>Name</li> </ul>						_
	cluster_ctrl_lk						
	external						
	failover_lan						
	failover_link						
	internal						
	mgmt						
	utility						

Bevor Sie fortfahren, müssen vor der eigentlichen L4-L7-Integration nur wenige Aspekte der Installation ermittelt werden:

Es gibt zwei Arten von Managementnetzwerken: In-Band-Management und Out-Of-Band (OOB), die zur Verwaltung von Geräten verwendet werden können, die nicht Teil der grundlegenden Application Centric Infrastructure (ACI) sind (Leaf, Spines oder APIC-Controller), zu denen ASAv, Load Balancer usw. gehören.

In diesem Fall wird OOB für ASAv mithilfe von Standard-vSwitch bereitgestellt. Verbinden Sie bei Bare-Metal-ASA- oder anderen Service-Appliances und/oder -Servern den OOB-Management-Port mit dem OOB-Switch oder -Netzwerk, wie im Bild gezeigt.



Die ASAv OOB-Management-Port-Management-Verbindung muss ESXi-Uplink-Ports für die Kommunikation mit dem APIC über OOB verwenden. Bei der Zuordnung von vNIC-Schnittstellen stimmt der Netzwerkadapter1 immer mit der Management0/0-Schnittstelle auf der ASAv überein, und der Rest der Datenebenenschnittstellen wird vom Netzwerkadapter 2 gestartet.

Tabelle 2 zeigt die Übereinstimmung der Netzwerkadapter-IDs und der ASAv-Schnittstellen-IDs:

### Tabelle 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

- Bereitstellen des ASAv VM über den Assistenten in der **Datei > OVF-Vorlage (Open Virtualization Format)**
- Wählen Sie asav-esxi aus, wenn Sie einen eigenständigen ESX-Server oder asav-vi für

vCenter verwenden möchten. In diesem Fall wird vCenter verwendet.



 Lesen Sie den Installationsassistenten, und akzeptieren Sie die allgemeinen Geschäftsbedingungen. In der Mitte des Assistenten können Sie verschiedene Optionen wie Hostname, Verwaltung, IP-Adresse, Firewall-Modus und andere spezifische Informationen zu ASAv festlegen. Denken Sie daran, die OOB-Verwaltung für ASAv zu verwenden, da Sie in diesem Fall die Schnittstelle Management0/0 beibehalten müssen, während Sie das VM-Netzwerk (Standard-Switch) verwenden und die Schnittstelle GigabitEthernet0-8 die Standard-Netzwerk-Ports ist.

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 OHCP mode         Choose whether to use DHCP for Management interface configuration.         Imagement 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.         Inter the Management IP-4 Address.         Hanagement IP-4 Address.         Hanagement IP-4 Address.         Hanagement IP-4 Address.         Management IP-4 Address.         Management IP-4 Eddress.         Management IP-4 Eddress.         Management IP-4 Eddress.         Management IP-4 Eddress.         <	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         Heagement 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         Hanagement 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

Deploy OVF Template	vertery 1 1 1 Hosts and Chatters	(mill)	x
Ready to Complete Are these the options you	want to use?		
Source OVE Template Details End User License Acreement Name and Location Deployment Configuration Storage Disk Format Network Mapping Properties Ready to Complete	When you click Finish, the deployment Deployment settings: Size on disk: Name: Folder: Deployment Configuration: Host/Cluster: Datastore: Disk provisioning: Network Mapping: Network	ent task will be started. 8.3 G8 ASAv-in-AVS ACI 1 Gbps (ASAv10) 10.201.35.219 datastore4 Thick Provision Lazy Zeroed "Management0-0" to "VM Network" "GigabitEthernet0-0" to "VM Network" "GigabitEthernet0-0" to "VM Network" "GigabitEthernet0-1" to "VM Network" "GigabitEthernet0-2" to "VM Network" "GigabitEthernet0-3" to "Pod6-ALUMBRER AVS-AEP-VMM-alumbrer AV "GigabitEthernet0-3" to "Pod6-ALUMBRER AVS-AEP-VMM-alumbrer AV "GigabitEthernet0-5" to "VM Network" "GigabitEthernet0-6" to "VM Network] "Giga	•
Help	Property: Property: Property: Property: Property: Power on after deployment	Management/Pv4 = 10.201.35.223 Management/Pv4Subnet = 255.255.255.0 Management/Standby/Pv4 = 0.0.0.0 RouteDefault = Default Route	

• Klicken Sie auf Fertig stellen und warten Sie, bis die ASAv-Bereitstellung abgeschlossen ist.

Clos	e
	Clos

• Schalten Sie die ASAv VM ein, und melden Sie sich über die Konsole an, um die Erstkonfiguration zu überprüfen.

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 --->\_

 Wie im Bild gezeigt, wird eine bestimmte Management-Konfiguration bereits an die ASAv-Firewall weitergeleitet. Admin-Benutzername und -Kennwort konfigurieren. Dieser Benutzername und das Kennwort werden vom APIC zur Anmeldung und Konfiguration der ASA verwendet. Die ASA sollte über Konnektivität zum OOB-Netzwerk verfügen und in der Lage sein, den APIC zu erreichen.

username admin password <device\_password> verschlüsselte berechtigung 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)# \_

Aktivieren Sie darüber hinaus im globalen Konfigurationsmodus HTTP-Server:

http server aktivieren

http 0.0.0.0 0.0.0

#### L4-L7 für ASAv-Integration im APIC:

 Melden Sie sich bei der ACI-GUI an, und klicken Sie auf den Tenant, auf dem das Service-Diagramm bereitgestellt wird. Erweitern Sie L4-L7-Dienste am unteren Rand des Navigationsbereichs, und klicken Sie mit der rechten Maustaste auf L4-L7-Geräte, und klicken Sie auf L4-L7-Geräte erstellen, um den Assistenten zu öffnen.

• Für diese Implementierung werden die folgenden Einstellungen angewendet:

- Verwalteter Modus
- Firewall-Service
- Virtuelles Gerät
- Verbindung zur AVS-Domäne über einen einzelnen Knoten hergestellt

ASAv-Modell

-Gerouteter Modus (GoTo)

- Management Address (muss mit der zuvor der Mgmt0/0-Schnittstelle zugewiesenen Adresse übereinstimmen)

 HTTPS verwenden, da der APIC standardmäßig das sicherste Protokoll f
ür die Kommunikation mit ASAv verwendet

Create L4-L7 Device:	8					i)
STEP 1 > General					1. General 2. Device	Configuration
Please select device	package and enter connectivity info	rmation.				
General Managed: Name:	ASAv-AVS-Routed	Device 1 Management IP Address:	10.201.35.3	Avia AVIS - I	Management Port: https	•
Service Type:	Firewall	Device Interfaces:	voenter controller/Aa			× +
Device Type: VMM Domain: Mode: Device Package: Model: Function Type:	PHYSICAL VIRTUAL AVS C C C C C C C C C C C C C C C C C C C	Cluster Management IP Address: Cluster Interfaces:	Name GigabitEthernet0/0 GigabitEthernet0/1 10.201.35.3 Type provider	VNIC Network adapter 2 Network adapter 3	Path (Only For Route Peering) Node-102/MAC_Pinning Node-102/MAC_Pinning Management Port: https Concrete Interfaces Device 1/GigabitEthernet0/0	× +
Connectivity APIC to Device Management Connectivity:	<ul> <li>Out-Of-Band</li> <li>In-Band</li> </ul>		consumer	ClientInt	Device1/GigabitEthernet0/1	
Credentials Username: Password: Confirm Password:	admin					

• Die richtige Definition der Geräteschnittstellen und Cluster-Schnittstellen ist für eine erfolgreiche Bereitstellung von entscheidender Bedeutung.

Verwenden Sie für den ersten Teil Tabelle 2 im vorherigen Abschnitt, um die Netzwerkadapter-IDs den ASAv-Schnittstellen-IDs, die Sie verwenden möchten, richtig zuzuordnen. Der Pfad bezieht sich auf den physischen Port oder Port-Channel oder VPC, der den Weg in die Firewall-Schnittstellen und deren Entfernung ermöglicht. In diesem Fall befindet sich ASA in einem ESX-Host, wo ein- und ausgehende ASA-Geräte für beide Schnittstellen identisch sind. Bei einer physischen Appliance wären "Inside and Outside of the Firewall" (FW) verschiedene physische

Ports.

Im zweiten Teil müssen die Cluster-Schnittstellen immer ohne Ausnahmen definiert werden (auch wenn Cluster HA nicht verwendet wird), da das Objektmodell eine Verbindung zwischen der **mlf**-Schnittstelle (Meta-Schnittstelle im Gerätepaket), der **Llf**-Schnittstelle (Leaf-Schnittstelle, z. B. extern, intern, innen usw.) und der **Clf** (konkrete Schnittstelle) aufweist. Die konkreten L4-L7-Geräte müssen in einer Geräte-Cluster-Konfiguration konfiguriert werden. Diese Abstraktion wird als logisches Gerät bezeichnet. Das logische Gerät verfügt über logische Schnittstellen, die konkreten Schnittstellen auf dem konkreten Gerät zugeordnet sind.

In diesem Beispiel wird die folgende Verknüpfung verwendet:

Gi0/0 = vmnic2 = ServerInt/Provider/Server > EPG1

#### Gi0/1 = vmnic3 = ClientInt/Consumer/Client > EPG2

		Policy Parame	ters Faults History
			ACTIONS -
Device 1 Management IP Address: 10.2 vCenter Name: vCe Interfaces:	101.35.223 M InterController	anagement Part: 443 VM Name: ASAv-in-AVS	x + Only For Route Peering)
	sbitEthernet0/1 Net	work adapter 3 Node	102/MAC_Pinning
Cluster Management IP Address: 10.2 Cluster Interfaces:	101.35.223 M	anagement Port: 443	• × +
Тур	e Name	Concrete Interfaces	
001	sumer Clientint	ASAv-AVS-Routed_Dev	vice_1/(GigabitEthermet0/2)
pro	ider Serverint	ASAv-AVS-Routed_Dev	vice_1/(GigabitEthernet0/1)
	Device 1 Management IP Address: 10.2 Ucenter Name: VCe Interfaces: Cluster Management IP Address: 10.2 Cluster Interfaces: Typ con	Cluster Management IP Address: 10.201.35.223 M  VCenter Name: VCenterController Interfaces:	Device 1         Management IP Address:       10.201.35.223         VCenter Name:       vCenterController         Interfaces:       VM Name:         A Name       VAIC         Paramet       VM Name:         A Name       VAIC         A Name

2

L4-L7 Devices - ASAv-AVS-Routed

**Hinweis:** Für Failover/HA-Bereitstellungen ist GigabitEthernet 0/8 als Failover-Schnittstelle vorkonfiguriert.

Der Gerätestatus sollte stabil sein, und Sie sollten bereit sein, das Funktionsprofil und die Servicediagrammvorlage bereitzustellen.

### Servicediagrammtempel

Erstellen Sie zunächst ein Funktionsprofil für ASAv, bevor Sie Funktionsprofilgruppe und dann das L4-L7-Servicefunktionsprofil unter diesem Ordner erstellen müssen, wie im Bild gezeigt:

Create L4-L7 Services F	unction Profile	Group		<b>1</b> ×	
Specify the information a	bout the Function	on Profile Group			
Name: Fun Description:	ProfGroup			_	
		[	SUBMIT	ANCEL	
Tenant Pod6-ALUMBRER	L4-L7 Services F	unction Profile Group	- FunProGroup		General Faulta History
Apploation Profiles	⊙₹				ACTIONS -
L4-L7 Service Parameters     Security Policies     Troubleshoot Policies	Properties Name: Description:	FunProGroup			
Monitoring Policies     L4-L7 Services	Service Function Profiles:	• Name	Associated Function	Description	× +
L4-L7 Service Graph Templates     Market Configurations     Image Service Configurations     Image Service Configurations			Se	No items have been found. lect Actions to create a new iter	
FunProGroup     EuroproGroup     Eu					
Imported Devices     Save as      Devices Selection     Save as      Designed Graph In     Save					
Deployed Devices     Inband Management Configuration for L4-L7 de	vio				

• Wählen Sie das **WebPolicyForRoutedMode-**Profil aus dem Dropdown-Menü aus, und konfigurieren Sie die Schnittstellen in der Firewall weiter. Von hier aus sind die Schritte optional und können später implementiert/modifiziert werden. Diese Schritte können in verschiedenen Phasen der Bereitstellung durchgeführt werden, je nachdem, wie wiederverwendbar oder benutzerdefiniert der Servicediagramm sein kann.

Bei dieser Übung erfordert eine geroutete Firewall (GoTo-Modus), dass jede Schnittstelle über eine eindeutige IP-Adresse verfügt. Die Standard-ASA-Konfiguration hat auch eine Schnittstelle-Sicherheitsstufe (die externe Schnittstelle ist weniger sicher, die interne Schnittstelle ist sicherer). Sie können auch den Namen der Schnittstelle entsprechend Ihren Anforderungen ändern. In diesem Beispiel werden Standardwerte verwendet.

 Erweitern Sie Schnittstellenspezifische Konfiguration, fügen Sie die IP-Adresse und die Sicherheitsstufe für ServerInt im folgenden Format für die IP-Adresse x.x.x.x/y.y.y oder x.x.x/yy hinzu. Wiederholen Sie den Vorgang für die ClientInt-Schnittstelle. **Create Function Profile** 

Name:	FunProf-ASA			
Description:	optional			
Over Existin Deally Dealers				
Copy Existing Profile Parameters: Profile:	CISCO-ASA-1 2/WebPolicyForRoutedMode	- 47		
Features and Parameters		<u> </u>		
	In order to auto apply new values to the parameters of	existing graph instance when users modify fu	nction profiles, the name of top folder r	nust be ended with -Defaul!
Features:	Basic Parameters All Parameters			
Interfaces	Folder/Param	Name Value	Mandatory Locked	Shared
Interfaces	😑 🔺 🚔 Device Config	Device		
AccessLists	Bridge Group Interface			
NAT	🖪 😑 🔺 🎯 Interface Related Configuration	externallf	false	false
<b>TrafficSelectionObjects</b>	E F C Access Group	ExtAccessGroup	false	
All	IPv6 Enforce EUI-64			
	E 🖌 🔁 Interface Specific Configur	axternallfCfg	false	
	Address Configura			
	IPv4 Address	pv4_address 192.168.10.1/24		
	IPv4 Standby Address	UPDATE RESET CANCE		
	IPv6 Address Configura			
	□ ▷ □ IPv6 Link Local Address			
				SUBMIT CANC

**Hinweis:** Sie können auch die Standardeinstellungen der Zugriffsliste ändern und eine eigene Basisvorlage erstellen. Standardmäßig enthält die RoutedMode-Vorlage Regeln für HTTP und HTTPS. Bei dieser Übung werden SSH und ICMP der Liste für den zulässigen externen Zugriff hinzugefügt.

Create Function Profile							
Name: FunP	rof-ASA						
Description: option	nal						
Copy Existing Profile Parameters: 🔽			,				
Profile: CISC	O-ASA-1.2/WebP	PolicyForRoutedMode	<u> </u>				
Features and Parameters							
	In order to auto	apply new values to the parame	ters of existing graph i	nstance when users	modify function profiles, the	he name of top folde	r must be ended with -Default.
Features:	Basic Paramet	ters All Parameters					
Interfaces	Folder/	/Param	Name	Value	Mandatory	Locked	Shared
menacars	B	Destination Service	destination_serv	vice			
AccessLists		- 📃 High Port					
NAT		- 🖃 Low Port	low_port	22		false	
TrafficSelectionObjects		- E Operator	operator	eq		false	
All							
		Logging     Deviced					
		Source Address					
		Source Service					
		Action	action	permit		false	
	M	Order	order	30		false	

- Klicken Sie anschließend auf Senden.
- Erstellen Sie jetzt die Vorlage für Servicediagramme.

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

• Ziehen Sie den Geräte-Cluster nach rechts, um die Beziehung zwischen Consumer und Provider zu bilden. Wählen Sie Routed Mode und das zuvor erstellte Funktionsprofil aus.

Graph Name:	Graph1-alumbrer		
Graph Type:	Create A New One	Clone An Existing One	
Consumer		C ASAv-AVS	Provider
	Please drag a dev	ice from devices table and drop it here to create a service node.	
ASAv-AVS-Rou	uted Information		
Firewall:	Routed		
Profile:	Pod6-ALUMBRER/FunProfGroup/FunPr	o. ➡ 臣	
			SUBMIT CANCEL

- Überprüfen Sie die Vorlage auf Fehler. Die Vorlagen werden erstellt, um wiederverwendbar zu sein. Sie müssen dann auf bestimmte EPGs usw. angewendet werden.
- Um eine Vorlage zu übernehmen, klicken Sie mit der rechten Maustaste, und wählen Sie Apply L4-L7 Service Graph Template (L4-L7 Servicediagrammvorlage übernehmen) aus.

Tenant Pod6-ALUMBRER	1 4-1 7 Service Graph Template - Graph1-alumbrer		;
Culck Start			
Tenant Pod6-ALUMBRER	Tapology	Policy Faults	History
Application Profiles			
Networking	Canadian	Provider	
L4-L7 Service Parameters	Conductor	FIGVIDE	
Security Policies			
Troubleshoot Policies	ASAY-AVS	35	
Monitoring Policies			
L4-L7 Services	ASAV		
L4-L7 Service Graph Templates			
Graph1-alumbrer	outed Information		
Function Node - ASA Apply L4-L7 S	rvice Graph Template II: Routed		
Router configurations Edit L4-L7 Set	/ce Graph Template >: FunPro-ASA		
✓ E Function Profiles Delete			
A 🔯 FunProfGroup 🔀 Remove Relat	d Objects Of Graph Template		
E 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 dev			
			DEGET

- Legen Sie fest, welche EPG auf der Verbraucher- und Anbieterseite sein soll. In dieser Übung ist AVS-EPG2 der Kunde (Client) und AVS-EPG1 der Anbieter (Server). Beachten Sie, dass kein Filter angewendet wird. Dadurch kann die Firewall die gesamte Filterung auf der Grundlage der Zugriffsliste durchführen, die im letzten Abschnitt dieses Assistenten definiert wurde.
- Klicken Sie auf Weiter

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 N	etwork: Pod6-ALUMBRER/AVS-AEP-VMM 👻 🕒	G
	Pod6-ALUMBRER/AVS-AEP-VMM-	
Contract Information	alumbrer/epg-AVS-EPG1	
Contract:  Create A New Contract Choose An Existing Contract Subject	Pod6-ALUMBRER/InternalAEP-	
Contract Name: EPG2-to-EPG1	VMM-alumbrer/epg-EPG-Internal-	
No Filter (Allow All Traffic): 🗹	/AnyEPG	
	Pod6-ALUMBRER/VRF2/AnvEPG	
	Pod6-ALUMBRER/L3Out-N3K2/L3Net	

 Überprüfen Sie die BD-Informationen für die einzelnen EPGs. In diesem Fall ist EPG1 der Anbieter auf der IntBD DB und EPG2 der Verbraucher auf BD ExtBD. EPG1 stellt eine Verbindung mit der Firewall-Schnittstelle ServerInt her, und EPG2 wird über die Schnittstelle ClientInt verbunden. Beide FW-Schnittstellen werden zur DG-Nummer für die einzelnen EPGs, sodass der Datenverkehr jederzeit die Firewall passieren muss.

PREVIOUS NEXT CANCEL

#### • Klicken Sie auf Weiter

Graph Template:	Pod6-ALUMBRER/Graph1-Temp-alumbrer		-	ē			
Consumer EPG AVS-EPG2	{	С	ASAV-AVS ASAV	P		Provider EPG AVS-EPG1	
ASAv-AVS-Routed Infor Firewal Profile Consumer Connector Type: BD: Cluster Interface: Provider Connector – Type:	anation  results routed  results FunPro-ASA  analysis  Pod6-ALUMBRER/ExtBD-alumbrer  ClientInt  General  Route Peering  Pode-Route Peering Pode-Route Peerin	•	ርዋ ርዋ				
BD: Cluster Interface:	Pod6-ALUMBRER/IntBD-alumbrer Serverint	•	e e				
					PREVIOUS	NEXT	CANCEL

 Klicken Sie im Abschnitt Konfigurationsparameter auf Alle Parameter und überprüfen Sie, ob ROTE-Indikatoren aktualisiert/konfiguriert werden müssen. In der Ausgabe, wie im Bild gezeigt, ist festzustellen, dass die Reihenfolge in der Zugriffsliste verpasst wird. Dies entspricht der Leitungsreihenfolge, die Sie in einer show ip access-list X sehen.

	à 1	folder/Param	Name	Value	Witte Domain
erfaces.	8	Access List	access-list-inbound		
cessLists	<b>D B</b>	Access Control Entry	ICMP		
		Access Control Entry	518-2		
fficSelectionObjects	8	Access Control Entry	SSH		
		Destination Address			
	8	Destination Service	destination_service		
		EMP			
		Logging			
	8	Protocol	protocol		
		Source Address			
		Source Service			
		E Action	action	permit	
		Cider	order	20	select asa domain
	78	Access Control Entry	UPDATE RESET CANCEL		
/		Access Control Entry			

• Sie können auch die IP-Adressierung überprüfen, die aus dem zuvor definierten Funktionsprofil zugewiesen wurde. Es besteht die gute Möglichkeit, Informationen bei Bedarf zu ändern. Wenn alle Parameter festgelegt sind, klicken Sie auf **Fertig stellen**, wie im Bild gezeigt:

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

 config parameters for the selected device

 Profile Name:
 FunProf-ASA [2]

Features:	Required Parameters All Parameters	
	Folder/Param	Name Value Write Domain
Interfaces	E 🔺 🎯 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	externallfCfg
	IPv4 Address Configuration	IPv4Address
	IPv4 Address	ipv4_address (192.168.10.1/24)
	IPv4 Standby Address	
	IPv6 Address Configuration	
	IPv6 Link Local Address Configuration	
	III IPuß Router Advertisements	

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

• Wenn alles in Ordnung ist, sollten ein neues bereitgestelltes Gerät und eine neue Diagramminstanz angezeigt werden.

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

# Überprüfung

 Nach der Erstellung des Service-Diagramms ist es wichtig zu überprüfen, dass die Beziehung zwischen Verbraucher und Anbieter mit einem geeigneten Meta Connector erstellt wurde. Überprüfen Sie unter Eigenschaften des Funktionsanschlusses.



**Hinweis:** Jede Schnittstelle der Firewall wird mit einem encap-VLAN aus dem dynamischen AVS-Pool zugewiesen. Stellen Sie sicher, dass keine Fehler vorliegen.

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
Quick Start					-		_	
Tenant Pod6-ALUMBRER				Policy	Operational	Health	Faults	History
Application Profiles	$\mathbf{O}$		A A O O 100					
Networking								
L4-L7 Service Parameters	Properties							
Security Policies	Devices:	ASAv-AVS-Routed						
Troubleshoot Policies	Virtual Device ID:	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:	Leolar Interface	France					
Router configurations		Logical Interface	Encap	_				
Function Profiles		ASAv-AVS-Routed_ClientInt	vian-93					
L4-L7 Devices		ASAv-AVS-Routed_ServerInt	vlan-94					
Imported Devices								
Devices Selection Policies								
Deployed Graph Instances								
EPG2-to-EPG1-Graph1-alumbrer-Pod6-ALUN								
Deployed Devices								
ASAv-AVS-Routed-none								
Inband Management Configuration for L4-L7 devi								

#### • Jetzt können Sie auch die Informationen überprüfen, die an die ASAv gesendet wurden

ASAv-w-AVS# show interface	ip brief				
Interface	IP-Address	OX?	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
ligabitEthernet0/2	unassigned	YES	unset	administratively dow	ո սթ
ligabitEthernet0/3	unassigned	YES	unset	administratively dow	ո սթ
igabitEthernet0∕4	unassigned	YES	unset	administratively dow	ո սթ
ligabitEthernet0/5	unassigned	YES	unset	administratively dow	ո սթ
ligabitEthernet0/6	unassigned	YES	unset	administratively dow	ո սթ
ligabitEthernet0/7	unassigned	YES	unset	administratively dow	ո սթ
ligabitEthernet0/8	unassigned	YES	unset	administratively dow	ո սթ
lanagement0/0	10.201.35.223	YES	CONFIG	up	սթ
ISAv-w-AVS# show run access	s-list				
ccess-list access-list-inl	ound extended	permit	t top ai	ny any eq www	
ccess-list access-list-inl	ound extended	permit	t top an	ny any eq https	
ccess-list access-list-inl	ound extended	permit	t top an	ny any eq ssh	
ccess-list access-list-inl	ound extended	permit	t icmp a	any any	
ISAV-M-AUS#					

 Unter den EPGs wird ein neuer Vertrag zugewiesen. Wenn Sie von nun an etwas in der Zugriffsliste ändern müssen, muss die Änderung von den L4-L7-Service-Parametern der Provider EPG vorgenommen werden.



 In vCenter können Sie auch überprüfen, ob die Schatten-EPGs jeder FW-Schnittstelle zugewiesen sind:

		I Machine Properties	🕜 ASAv-in-AVS - Virtual Machi	
ige Views	Virtual Machine Version: 8	sources Profiles VServices	Hardware Options Resources	I
	Device Status			I
	Connected	Add Remove	Show All Devices	I
	Connect at power on	Summary	Hardware	η
ACKNOWI	Adapter Type	2048 MB	Memory	
1	Ourrent adapter: E1000	1	CPUs	٩
	Content adapter.	Video card	📃 📃 Video card	
	MAC Address	Restricted	VMCI device	١
	00:50:56:89:CA:89	LSI Logic Parallel	SCSI controller 0	I
		[datastore4] ASAv-in-A	CD/DVD drive 1	I
	Automatic     O Manual	[datastore4] ASAv-in-A	CD/DVD drive 2	l
	DirectPath I/O	Virtual Disk	Hard disk 1	٦
	Statue: Not supported	Virtual Disk	Hard disk 2	I
		1 VM Network	Network adapter 1	I
	Network Connection	2 POD6-ALUMBRERIASAV	Network adapter 2	
	Network label:	4 VM Network	Network adapter 3	1
	Ped6-ALUMBRER IASAV-AVS-RoutedctxnoneIntBD-alumb	VM Network	Network adapter 4	I
(AVS	2-d6-ALUMBRER JASAV-AVS-RoutedctxnoneInt8D-alumbrer IServer	5 VM Network	Network adapter 5	I
	Pod6-ALUMBRER AVS-AEP-VMM-alumbrer AVS-EPG1 (AVS)	7 VM Network	Network adapter 7	I
=	Pod6-ALUMBRER AVS-AEP-VMM-alumbrer AVS-EPG2 (AVS)	8 VM Network	Network adapter 8	I
	vtep (AVS)	9 VM Network	Network adapter 9	I
	common  default dient (DVS)	10 VM Network	Network adapter 10	I
-	common  default web (DVS)			I
				I
				I
				I
				I
			I	
	OK Cancel		Help	
(4	Network Connection         Network label:         Ded6-ALUMBRER  ASAv-AVS-RoutedctxnoneIntBD-alumbrer  Server)         Pod6-ALUMBRER  ASAv-AVS-RoutedctxnoneIntBD-alumbrer  Server)         Pod6-ALUMBRER  AVS-AEP-VMM-alumbrer  AVS-EPG1 (AVS)         Pod6-ALUMBRER  AVS-AEP-VMM-alumbrer  AVS-EPG2 (AVS)         quarantine (AVS)         vtep (AVS)         common  default client (DVS)         common  default juolivei (DVS)         common  default web (DVS)	2 Pod6-ALUMBRER ASAv 3 Pod6-ALUMBRER ASAv. 4 VM Network 5 VM Network 6 VM Network 7 VM Network 8 VM Network 9 VM Network 10 VM Network	Network adapter 2 Network adapter 3 Network adapter 4 Network adapter 5 Network adapter 6 Network adapter 7 Network adapter 8 Network adapter 9 Network adapter 10 Help	)

Für diesen Test kommunizierten die beiden EPGs mit Standardverträgen. Diese beiden EPGs befinden sich in unterschiedlichen Domänen und VRFs. Daher war das Route Leaking zwischen den EPGs zuvor konfiguriert. Dies vereinfacht ein wenig nach dem Einfügen des Servicediagramms, da die FW das Routing und Filtern zwischen den beiden EPGs konfiguriert. Die zuvor im Rahmen der EPG und der BD konfigurierte GD kann jetzt wie die Verträge entfernt werden. Lediglich der von den L4-L7 gedrängte Vertrag sollte unter den EPGs bleiben.

Quick Start	1	001110010							1
Tenant Pod6-ALUMBRER	ll e								
Application Profiles		€±							ACTIONS -
AVS-AEP-VMM-alumbrer					Provided /				
Application EPGs		<ul> <li>Tenant Name</li> </ul>	Contract Name	Contract Type	Consumed	QoS Class	State	Label	Subject Label
EPG AVS-EPG1		G Contract Type: Co	ontract						
Domains (VMs and Bare-Me		Pod6-ALUMBB	EPG2-to-EPG1	Contract	Provided	Unspecified	formed		
Static Bindings (Paths)		10007600001	21 0210-21 01	Comment	1101000	Chapterined	Ionnou		
Static Bindings (Leaves)									
Contracts									
Static EndPoint									
Subnets									

Wenn der Standardvertrag entfernt wird, können Sie bestätigen, dass der Datenverkehr jetzt über die ASAv fließt. Der Befehl show access-list sollte die Trefferanzahl für die Regel anzeigen, die schrittweise erhöht wird, wenn der Client eine Anforderung an den Server sendet.

#2110_11_020	
13NV-W-NV3#	
ASA∧-M-AAS#	show access-list
access-list	cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
	alert-interval 300
access-list	access-list-inbound; 4 eleмents; naмe hash: Øxcb5bd6c7
access-list	access-list-inbound line 1 extended permit tcp any any eq www (hitcn
t=0) 0xc873a	747
access-list	access-list-inbound line 2 extended permit tcp any any eq https (hit
cnt=0) 0x481	pedbdd
access-list	access-list-inbound line 3 extended permit tcp any any eq ssh (hitcn
t=4) 0x532fd	157a
access-list	access-list-inbound line 4 extended permit icmp any any (hitcnt=4) 0
ke4b5a75d	
ASAv-w-AVS#	

Auf dem Leaf sollten die Endpunkte für die Client- und Server-VMs sowie die ASAv-Schnittstellen erfasst werden.

leaf2# show endpoint				
Legend:				
0 - peer-attached H - vtep	a - locall	y-aged S - sta	tic	
V - vpc-attached p - peer-aged	L - local	M - spa	n	
s - static-arp B - bounce				
+	++	++	+-	+
VLAN/	Encap	MAC Address	MAC Info/	Interface
Domain	VLAN	IP Address	IP Info	
+	++	++	+-	+
Pod6-ALUMBRER:VRF1-alumbrer		50.50.50.50 L		
14/Pod6-ALUMBRER:VRF1-alumbrer	vxlan-14778359	5897.bda4.f9bc L		eth1/13
30	vlan-98	0050.5689.td08 L	FIAT	eth1/7
Pod6-ALUMBRER:VRF1-alumbrer Server	vlan-98	192.168.10.10 L	, interface	
25 & MAC	vlan-94	0050.5689.ca89	(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		eth1/7
Pod6-ALUMBRER:VRF2 Client IP	8 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 L	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 H		unspecified
overlay-1	vxlan-16777209	10.0.32.64 H		

sehen Sie beide mit dem VEM verbundenen Firewall-Schnittstellen.

#### ESX-1

10.00	amond about a	In the set									
~ # V	emana snow p	OFT 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	# vemcmd show port vlan										
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		vmk1
51		UP	UP	FWD	-	0	6	Ø	0		Client1-AVS.eth0
52		UP	UP	FWD	-	0	6	0	0		Server1-AVS.eth0
1040	Pol	UP	UP	FWD	-	0		0	0		
~ #											

Schließlich können die Firewall-Regeln auch auf Leaf-Ebene überprüft werden, wenn die PC-Tags für die Ausgangs- und Ziel-EPGs bekannt sind:

EPG1					Policy	perational Stats	Health Faults Hi	istory
Application Profiles AVS-AEP-VMM-alumbrer					Ass	ociated EPGs A	ssociated External Routed Netw	vorks
A Popleation EPGs	⊙±						ACTION	is -
FO EPG AVS-EPGT b S EPG AVS-EPG2	TABITE	Description	State	Issues	QoS	Encep	PC Teg	
> deg EPOs	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								
VRF2								

EPG2								
<ul> <li>Domains (VMs and Bare-Metals)</li> <li>Static Bindings (Paths)</li> <li>Static Bindings (Leaves)</li> </ul>					Poli	Operational Associated EPGs	Stats Health Associated Exter	Faults History
Contracts Static EndPoint	⊙₹							ACTIONS -
Subnets L4-L7 Virtual IPs L4-L7 IP Address Pool L4-L7 Service Parameters L4-L7 Service Parameters L4-L7 Service Parameters L4-L7 Service Parameters L5 ThtemalAEP-VMM-alumbrer L6 ThtemalAEP-VMM-alumbrer L6 VIPS L7	Avro	Description	State applied	hsues	Qo5 Unspec	Encirp	p PC	78

Filter-IDs können den PC-Tags auf dem Leaf zugeordnet werden, um die FW-Regeln zu überprüfen.

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#							

**Hinweis:** Die EPG-PCTags/Sclass kommunizieren niemals direkt. Die Kommunikation wird unterbrochen oder über die Schatten-EPGs verbunden, die durch die Einfügung der L4-L7-Servicediagramme erstellt werden.

und Kommunikation zwischen Client und Server funktioniert.

cisco@cisco-UbuntuClient:~\$ ifconfig
eth1 Link encap:Ethernet HWaddr 00:50:56:89:3f:ca
inet addr:172.16.1.10 Bcast:172.16.1.255 Mask:255.255.255.0
inet6 addr: fe80::250:56ff:fe89:3fca/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:346596 errors:0 dropped:97 overruns:0 frame:0
TX packets:533034 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:33670388 (33.6 MB) TX bytes:42734068 (42.7 MB)
to Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:170350 errors:0 dropped:0 overruns:0 frame:0
TX packets:170350 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:18739044 (18.7 MB) TX bytes:18739044 (18.7 MB)
cisco@cisco-UbuntuClient:~\$ ssh 192.168.10.10
cisco@192.168.10.10's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)
* Documentation: https://help.ubuntu.com/
Last login: Mon Feb 1 10:14:11 2016 from 172.16.1.10
cisco@cisco-UbuntuClient:~\$ \$



## Fehlerbehebung

VTEP-Adresse ist nicht zugewiesen

Überprüfen Sie, ob das Infrastruktur-VLAN unter AEP:

Policies 🥺 🖸	Attachable Access Entity Profile - AEP-AVS					
Cuick Start						1
Switch Policies			Policy C	Operational F	aults	History
Module Policies		A A O O			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)	0				
📃 default	Associated to Interfaces:				×	+
QOS Class Policies		A Name	State			- 11
DHCP Relay Policies		AVS (Vmm-VMware)	formed			- 11
MCP Instance Policy default	•					- 11
EP Loop Protection Policy						- 11
Error Disabled Recovery Policy						Ŭ
Rogue EP Control Policy						
Monitoring Policies						
Troubleshoot Policies	VSwitch Policies					
Pools	Port Channel Policy:	select a value 🗸 📮				
Physical and External Domains	LLDP Policy:	select a value				
	CDB Palian					
	CDP Policy:					
	STP Policy:	select a value 🗸 🛃				
	Firewall Policy:	select a value 🗾 🔁				

#### Nicht unterstützte Version

Überprüfen Sie, ob die VEM-Version korrekt ist und das entsprechende ESXi VMWare-System unterstützt.

~ # 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- und Fabric-Kommunikation funktioniert nicht - 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 -1 Interface Port

An diesem Punkt kann festgestellt werden, dass die Fabric-Kommunikation zwischen dem ESXi-Host und dem Leaf nicht ordnungsgemäß funktioniert. Einige Überprüfungsbefehle können auf der Leaf-Seite überprüft werden, um die Ursache zu bestimmen.

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-Туре Protocol Member Ports Channel \_\_\_\_\_ Po5(SU) Eth LACP Eth1/5(P) Eth1/6(P) In der ESXi werden zwei Ports verwendet, die über einen Po5 verbunden sind.

leaf2# show vlan extended

VLAN Name Status Ports \_\_\_\_ \_\_\_\_ infra:default active Eth1/1, Eth1/20 13 19 \_ \_ active Eth1/13 22 active Eth1/1 mamt:inb 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

Aus der obigen Ausgabe kann festgestellt werden, dass das Infra-VLAN nicht zugelassen ist oder über die Uplinks-Ports weitergeleitet wird, die zum ESXi-Host führen (1/5-6). Dies weist auf eine Fehlkonfiguration mit der auf dem APIC konfigurierten Schnittstellenrichtlinie oder Switch-Richtlinie hin.

Überprüfen Sie beide:

**Zugriffsrichtlinien > Schnittstellenrichtlinien > Profile Access Policies > Switch Policies > Profile** In diesem Fall werden die Schnittstellenprofile an den falschen AEP (alte AEP für DVS verwendet) angehängt, wie im Bild gezeigt:

Access Port Policy Group	- AVS-102_1-ports-7	_PolGrp							()	×
						P	olicy	Faults	Histo	хy
⊙±								A	CTIONS	•
Properties										
Name:	AVS-102_1-ports-7_PolGrp									
Description:	optional									
Label:										
Link Level Policy:	1GigAuto -	e								
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									l
Attached Entity Profile:	AEP_DVS	æ								
Connectivity Filters:				×	۰.					
	Switch IDs		Interfaces							
						SHOW USAGE	SUBMI	r I I	CLOSE	٦

Nachdem Sie die richtige AEP für AVS festgelegt haben, können Sie jetzt sehen, dass das Infra-VLAN über die entsprechenden Unlinks am Leaf angezeigt wird:

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
 _____ _____
                    vxlan-16777209, vlan-3967
13
    enet CE
19 enet CE
                    vxlan-14680064, vlan-150
22 enet CE
                    vxlan-16383902
    enet CE
26
                    vxlan-15531929, vlan-200
 27
     enet CE
                    vlan-11
                    vlan-14
28 enet CE
                    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: 10.0.30 Port: 8000
Infra vlan: 3967
FTEP IP: 10.0.0.32
Switching Mode: unknown
Encap Type: unknown
NS GIPO: 0.0.0.0
~ # vemcmd show opflex
Status: 12 (Active)
Channel0: 12 (Active), Channel1: 0 (Discovering)
Dvs name: comp/prov-VMware/ctrlr-[AVS]-vCenterController/sw-dvs-129
Remote IP: 10.0.0.30 Port: 8000
Infra vlan: 3967
FTEP IP: 10.0.0.32
Switching Mode: LS
Encap Type: unknown
NS GIPO: 0.0.0.0
```

## Zugehörige Informationen

Installation von virtuellen Anwendungs-Switches

<u>Cisco Systems, Inc. Installationsanleitung für Cisco Application Virtual Switch, Version</u> <u>5.2(1)SV3(1.2)</u>

Bereitstellung der ASAv mit VMware

Cisco Systems, Inc. Cisco Adaptive Security Virtual Appliance (ASAv) - Kurzreferenz 9.4

Cisco ACI und Cisco AVS

Cisco Systems, Inc. Cisco ACI-Virtualisierungsleitfaden, Version 1.2(1i)

Whitepaper: Service Graph Design mit Cisco Application Centric Infrastructure

Whitepaper: Service Graph Design mit Cisco Application Centric Infrastructure

Technischer Support und Dokumentation für Cisco Systeme