

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

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfiguration](#)

[Netzwerkdigramm](#)

[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:

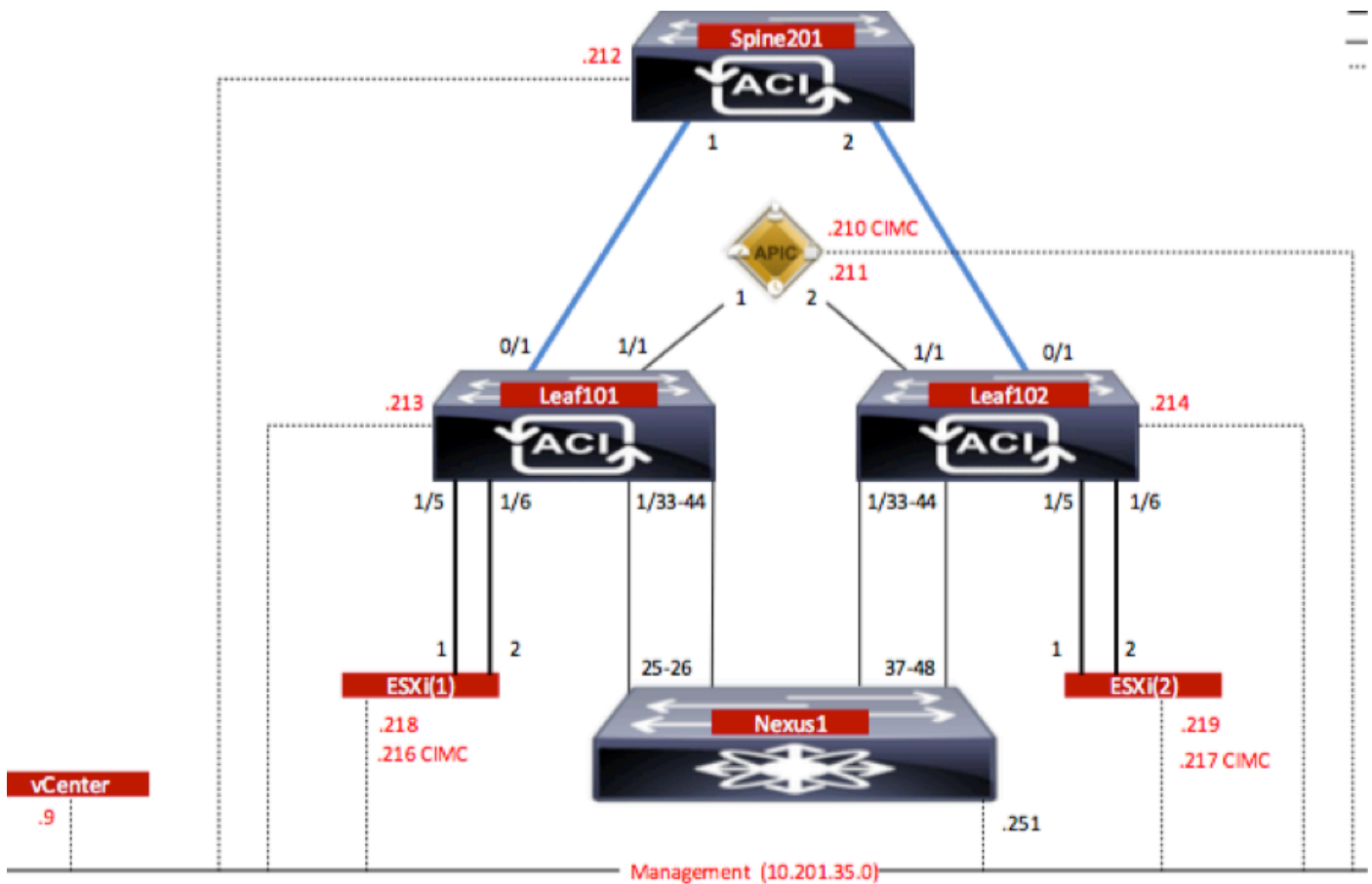
- AVS
- ASAv
- EPGs, BD, VRF
- Zugriffskontrollliste (ACL)
- L4-L7 Servicediagramm
- vCenter

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 controllers



Virtual Switch Name: AVS



Virtual Switch: VMware vSphere Distributed Switch **Cisco AVS**

Switching Preference: No Local Switching **Local Switching**



Encapsulation:  VLAN  
 VXLAN

Associated Attachable Entity Profile: AEP-AVS  



VLAN Pool: VlanPool-AVS(dynamic)  

Security Domains:  

Name	Description
------	-------------

vCenter Credentials:  

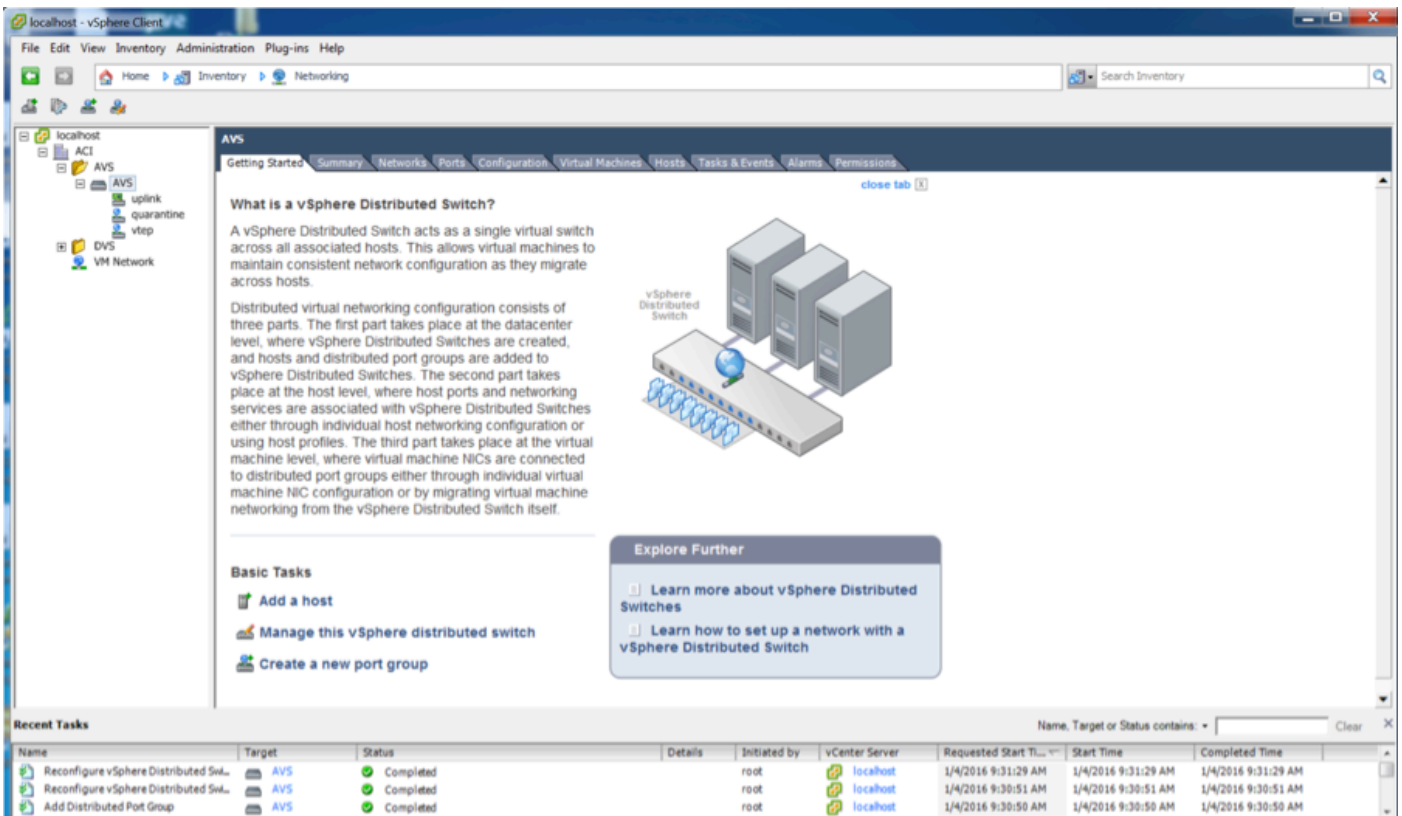
Profile Name	Username	Description
vCenterCredentials	root	

vCenter:  

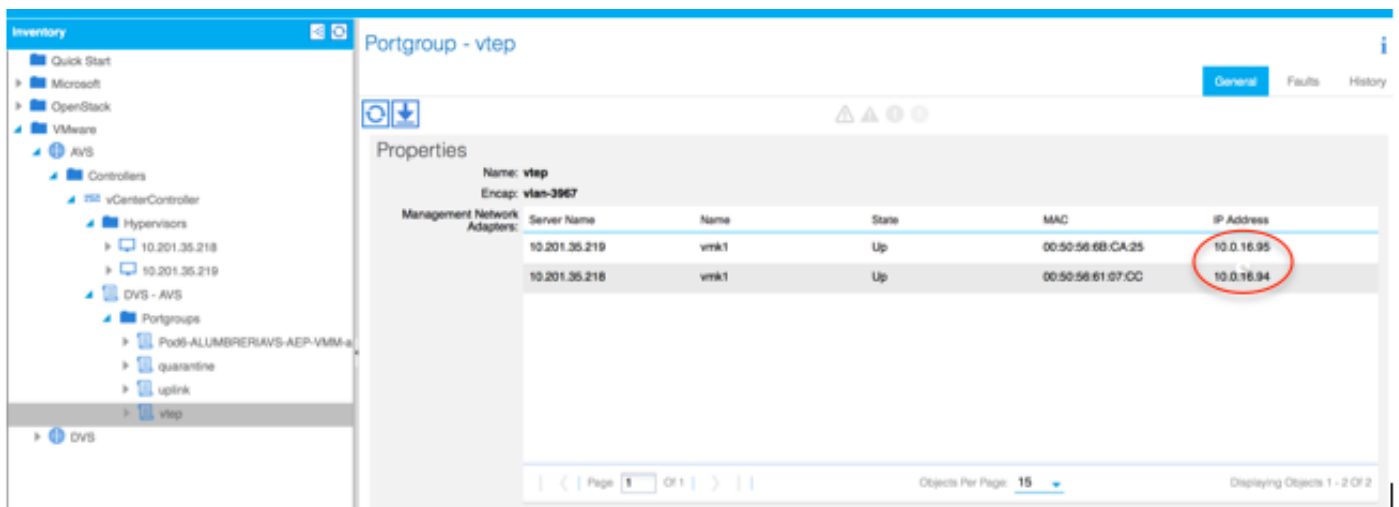
Name	IP	Type	Stats Collection
vCenterController	10.201.35.9	vCenter	Disabled

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.



## 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

VMware	VIB	VEM Bundle	Windows VC Installer	Linux vCenter Server Appliance
ESXi 6.0	cross_cisco-vem-v250-5.2.1.3.1.10.0-6.0.1.vib	VEM600-201512250119-BG-release.zip (Offline) VEM600-201512250119-BG (Online)	6.0	6.0
ESXi 5.5	cross_cisco-vem-v250-5.2.1.3.1.10.0-3.2.1.vib	VEM550-201512250113-BG-release.zip (Offline) VEM550-201512250113-BG (Online)	5.5	5.5
ESXi 5.1	cross_cisco-vem-v250-5.2.1.3.1.10.0-3.1.1.vib	VEM510-201512250107-BG-release.zip (Offline) VEM510-201512250107-BG (Online)	5.1	5.1
ESXi 5.0	cross_cisco-vem-v250-5.2.1.3.1.10.0-3.0.1.vib	VEM500-201512250101-BG-release.zip (Offline) VEM500-201512250101-BG (Online)	5.0	5.0

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:

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

- 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 software vib install -v /vmfs/volumes/datastore1/cross_cisco-vem-v250-5.2.1.3.1.10.0-3.2.1.vib --maintenance-mode --no-sig-check
Installation Result
Message: Operation finished successfully.
Reboot Required: false
VIBs Installed: Cisco_bootbank_cisco-vem-v250-esx_5.2.1.3.1.10.0-3.2.1
VIBs Removed: Cisco_bootbank_cisco-vem-v197-esx_5.2.1.3.1.5.0-3.2.1
VIBs Skipped:
~ # vem status

VEM modules are loaded

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

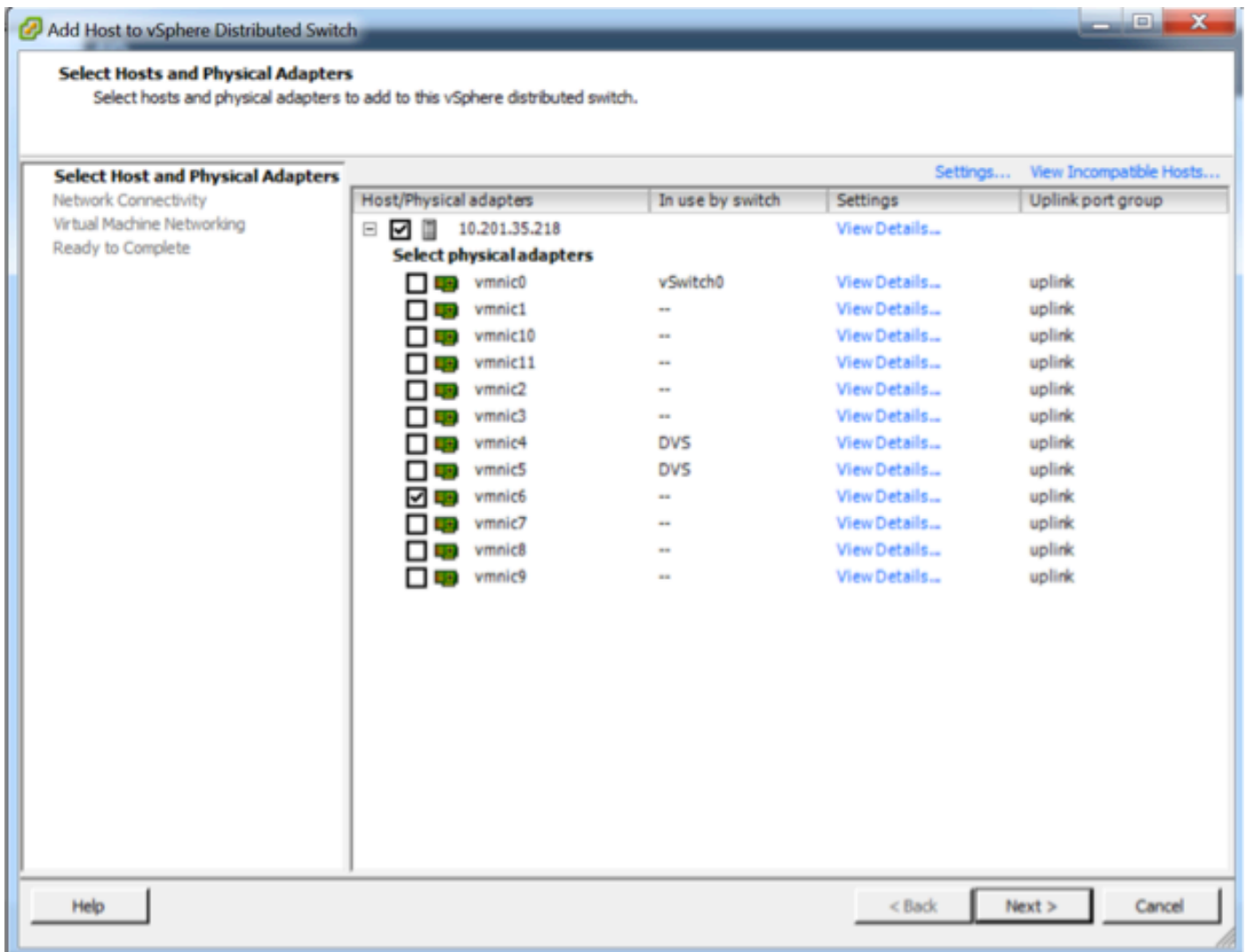
VEM Agent (vemdpa) is running

~ #

```

- 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:



- 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:

## Quick Start

### HELP

The **Packages** menu allows you to import L4-L7 device packages, which are used to define, configure, and monitor a network service balancer, context switch, SSL termination device, or intrusion prevention system (IPS). Device packages contain descriptions of the function and network connectivity information for each function. A network service device is deployed in the network by adding it to a service graph.

You can use the **Import a Device Package** wizard to import a device package for a function that you want to manage with APIC. We will walk you through configuring a service graph.

#### Quick Start

Import a Device Package

Import Device Package
i
✕

File Name:  BROWSE...

SUBMIT
CLOSE

Device Types

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

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

i

General
Operational
Faults
History

⏪ ⏴
ACTIONS ▾

**Properties**

Vendor: **CISCO**

Model: **ASA**

Capabilities: **GoThrough,GoTo**

Major Version: **1.2**

Minor Version: **4.8**

Minimum Required Controller Version: **1.1**

Logging Level: **DEBUG** ▾

Package Name: **device\_script.py**

Supported Protocols: |

Interface Labels:

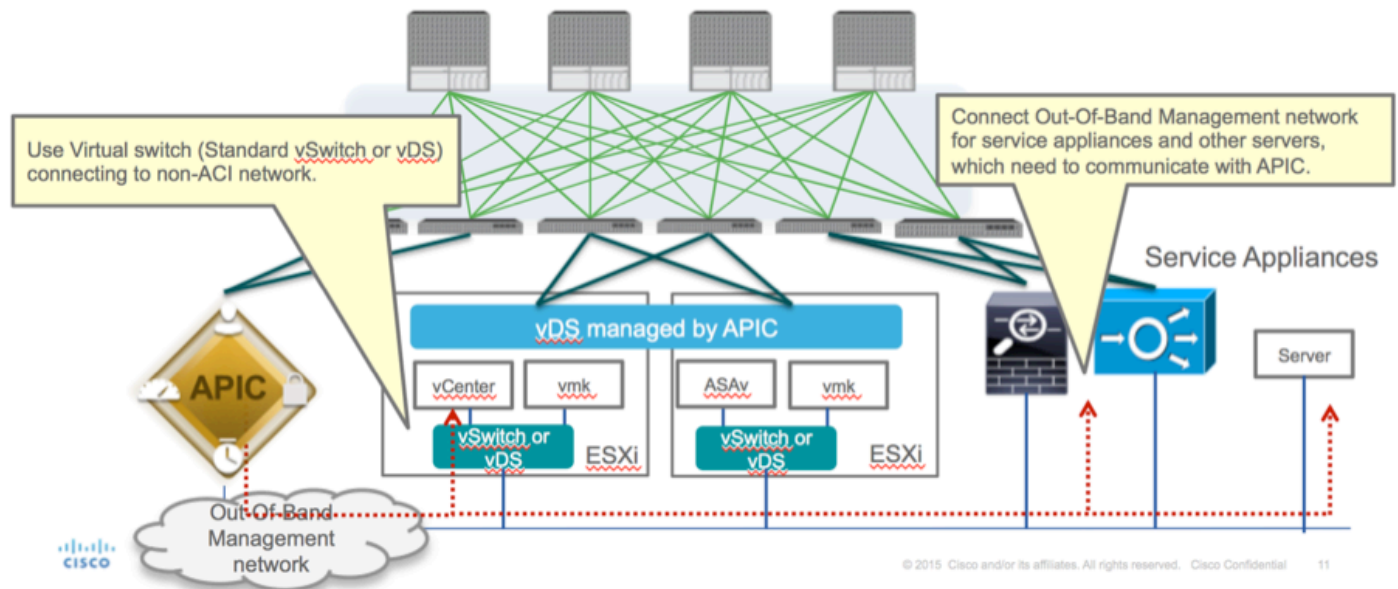
Name
cluster_ctrl_lk
external
failover_lan
failover_link
internal
mgmt
utility



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 ASA, Load Balancer usw. gehören.

In diesem Fall wird OOB für ASA 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 ASA 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 ASA überein, und der Rest der Datenebenenschnittstellen wird vom Netzwerkadapter 2 gestartet.

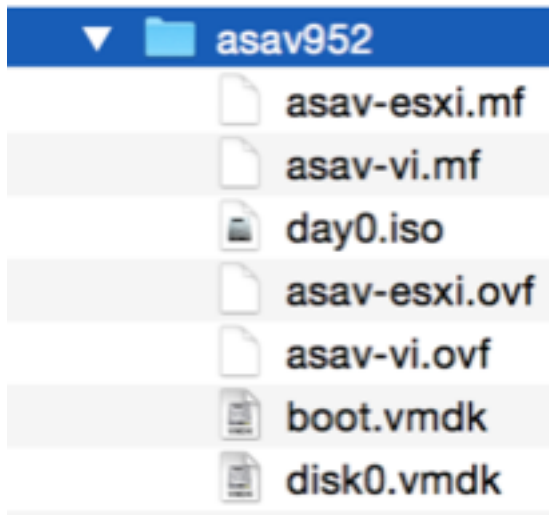
Tabelle 2 zeigt die Übereinstimmung der Netzwerkadapter-IDs und der ASA-Schnittstellen-IDs:

**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**

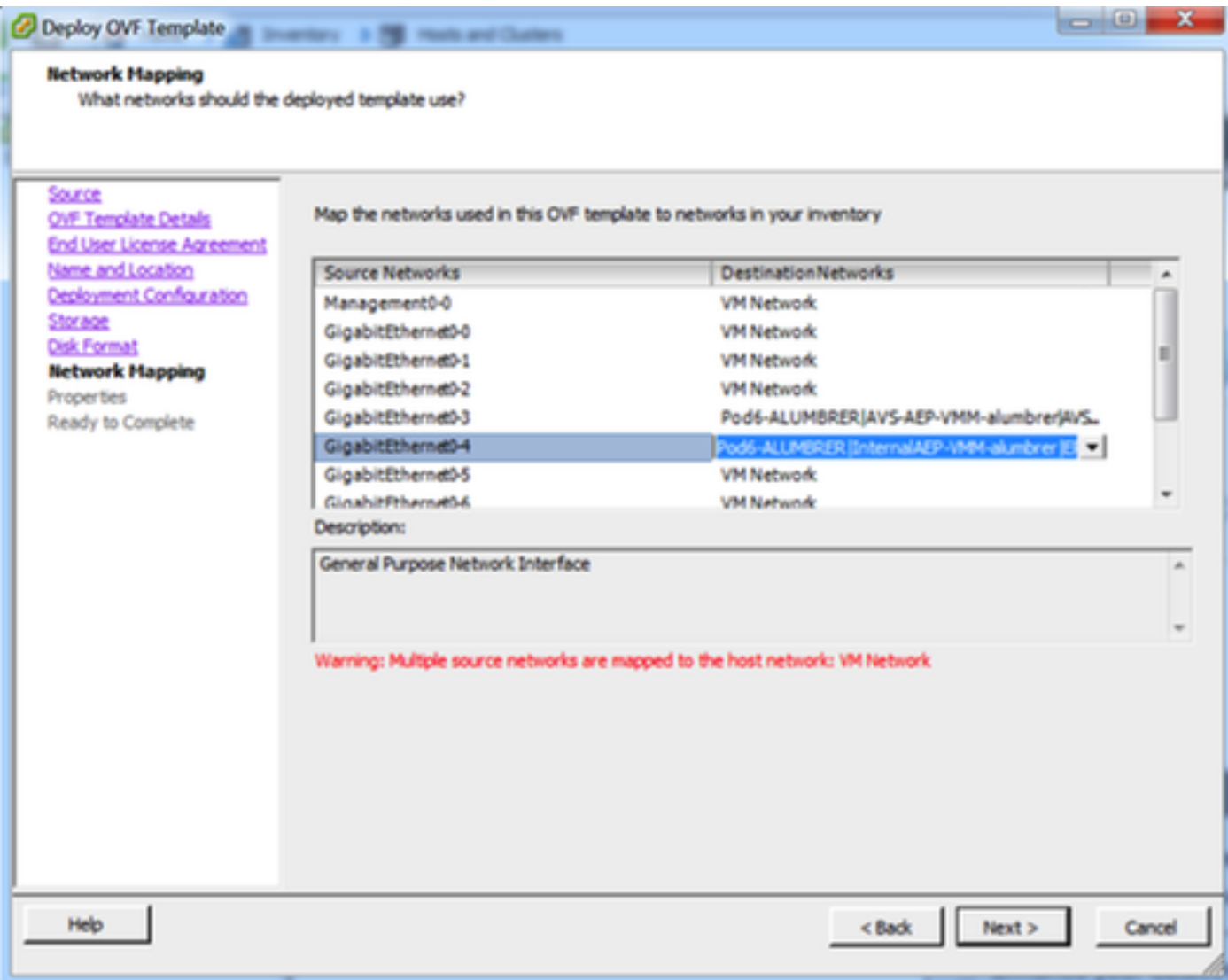
Select the source location.

**Source**

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

Deploy from a file or URL

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.



Deploy OVF Template

**Properties**  
Customize the software solution for this deployment.

[Source](#)  
[OVF Template Details](#)  
[End User License Agreement](#)  
[Name and Location](#)  
[Deployment Configuration](#)  
[Storage](#)  
[Disk Format](#)  
[Network Mapping](#)  
**Properties**  
Ready to Complete

**Deployment Type**  
**Type of deployment**  
Select the type of ASA v host to install. When an HA type deployment is selected, the additional HA Properties below should also be filled in.  
Standalone

**Hostname**  
**Hostname**  
Host name for this system. A hostname must start and end with a letter or digit and have as interior characters only letters, digits, or a hyphen.  
ASAv-w-AVS

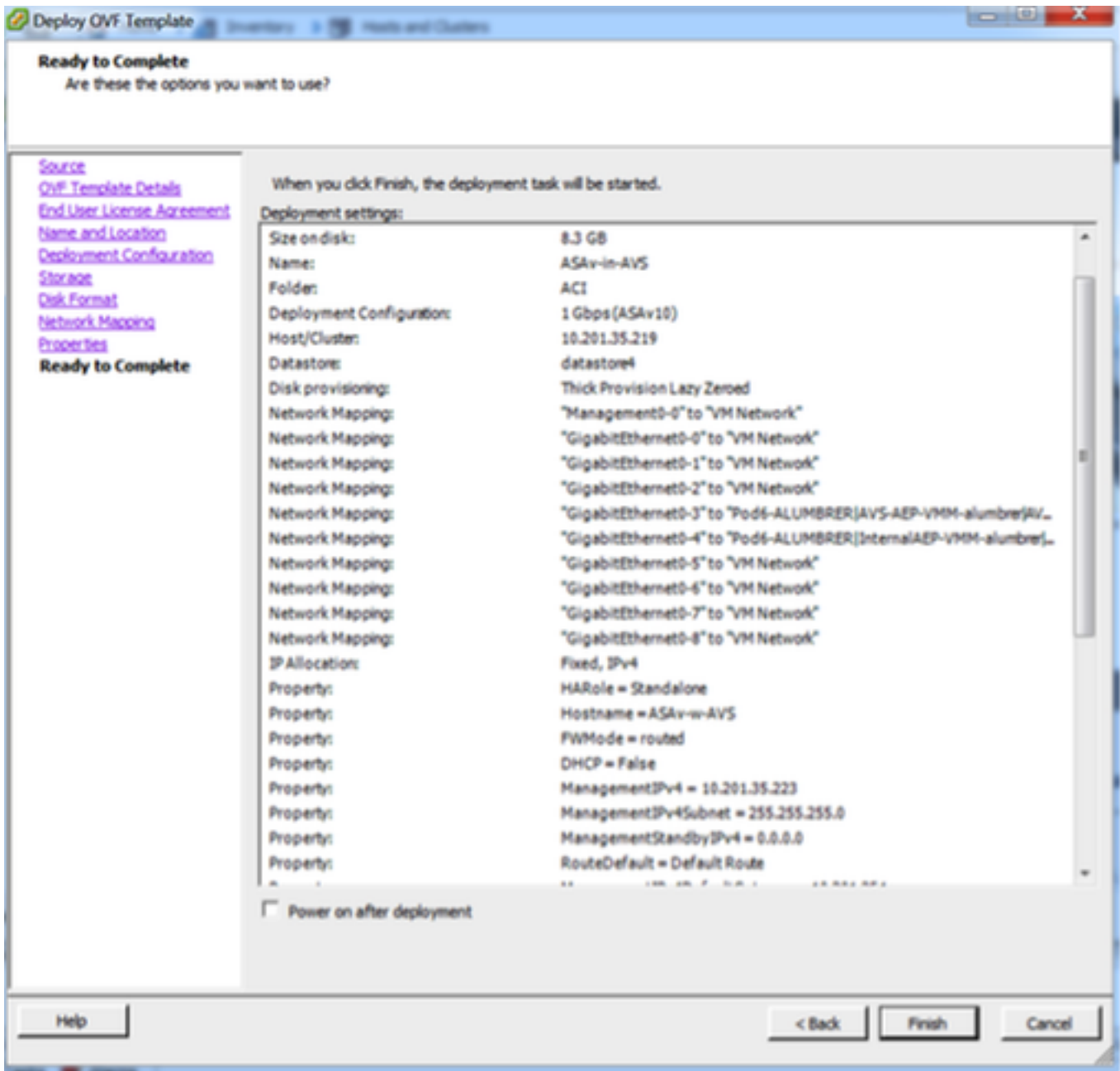
**Firewall Properties**  
**Firewall Mode**  
Select the Firewall Mode  
routed

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

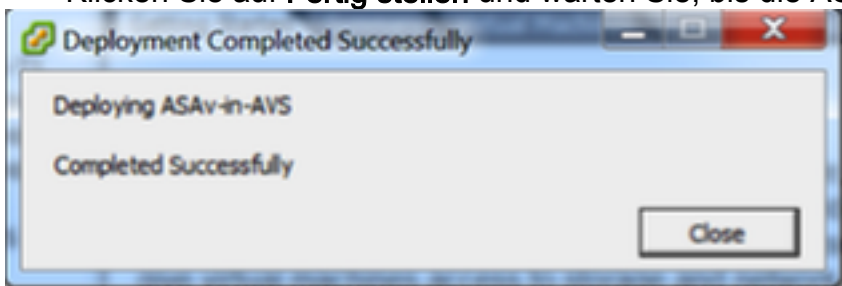
**Management IP Address**  
Enter the Management IPv4 Address. For HA-type deployments, this property specifies the Management IPv4 address of the Active HA host.  
10 . 201 . 35 . 223

**Management IP Subnet Mask**

Help < Back Next > Cancel



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



- 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
mtu management 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
route management 0.0.0.0 0.0.0.0 10.201.35.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
<--- More --->_

```

- Wie im Bild gezeigt, wird eine bestimmte Management-Konfiguration bereits an die ASA-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

```

ASA-v-w-AUS(config)# username admin password C1sc0123 privilege 15
ASA-v-w-AUS(config)# wr mem
Building configuration...
Cryptochecksum: d491b980 86fa522f 6f937baf b5bfb318

7977 bytes copied in 0.250 secs
[OK]
ASA-v-w-AUS(config)# ping 10.201.35.211
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.201.35.211, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
ASA-v-w-AUS(config)# _

```

Aktivieren Sie darüber hinaus im globalen Konfigurationsmodus HTTP-Server:

http server aktivieren

http 0.0.0.0 0.0.0

L4-L7 für ASA-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 für die Kommunikation mit ASAv verwendet

STEP 1 > General

Please select device package and enter connectivity information.

**General**

Managed:

Name: ASAv-AVS-Routed

Service Type: Firewall

Device Type:  PHYSICAL  VIRTUAL

MMM Domain: AVS

Mode:  Single Node  HA Cluster

Device Package: CISCO-ASA-1.2

Model: ASAv

Function Type:  GoThrough  GoTo

**Connectivity**

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

**Credentials**

Username: admin

Password: .....

Confirm Password: .....

**Device 1**

Management IP Address: 10.201.35.3

Management Port: https

VM: vCenterController/ASAv-in-AVS

Device Interfaces:

Name	VNIC	Path (Only For Route Peering)
GigabitEthernet0/0	Network adapter 2	Node-102/MAC_Pinning
GigabitEthernet0/1	Network adapter 3	Node-102/MAC_Pinning

**Cluster**

Management IP Address: 10.201.35.3

Management Port: https

Cluster Interfaces:

Type	Name	Concrete Interfaces
provider	ServerInt	Device1/GigabitEthernet0/0
consumer	ClientInt	Device1/GigabitEthernet0/1

- 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 **mif**-Schnittstelle (Meta-Schnittstelle im Gerätepaket), der **Lif**-Schnittstelle (Leaf-Schnittstelle, z. B. extern, intern, innen usw.) und der **Cif** (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

#### L4-L7 Devices - ASAv-AVS-Routed

The screenshot displays the configuration for 'ASAv-AVS-Routed' devices. On the left, the 'General' tab shows the device name 'ASAv-AVS-Routed', package 'CISCO-ASA-1.2', and type 'VIRTUAL'. The 'Configuration State' section indicates 'Devices State: stable'. The main area shows 'Device 1' configuration with Management IP Address 10.201.35.223 and Management Port 443. The 'Interfaces' table lists 'GigabitEthernet0/1' and 'GigabitEthernet0/2'. The 'Cluster' section shows 'Cluster Interfaces' with 'consumer' (ClientInt) and 'provider' (ServerInt) roles, both mapped to 'ASAv-AVS-Routed\_Device\_1' interfaces.

Name	vNIC	Path (Only For Route Peering)
GigabitEthernet0/1	Network adapter 3	Node-102/MAC_Pinning, Nod...
GigabitEthernet0/2	Network adapter 4	Node-102/MAC_Pinning

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

**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-Service funktionsprofil unter diesem Ordner erstellen müssen, wie im Bild gezeigt:

Create L4-L7 Services Function Profile Group

Specify the information about the Function Profile Group

Name: FunProfGroup

Description:

SUBMIT CANCEL

Tenant Pod9-ALUMBRER

L4-L7 Services Function Profile Group - FunProfGroup

General Faults History

Properties

Name: FunProfGroup

Description:

Service Function Profiles:

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

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

- 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

Copy Existing Profile Parameters:   
Profile: CISCO-ASA-1.2/WebPolicyForRoutedMode

Features and Parameters

In order to auto apply new values to the parameters of existing graph instance when users modify function profiles, the name of top folder must be ended with -Default.

Basic Parameters **All Parameters**

Folder/Param	Name	Value	Mandatory	Locked	Shared
Device Config	Device				
Bridge Group Interface					
Interface Related Configuration	externallif			false	false
Access Group	ExtAccessGroup			false	
IPv6 Enforce EUI-64					
Interface Specific Configur...	externallICfg			false	
IPv4 Address Configur...					
IPv4 Address	ipv4_address	192.168.10.1/24			
IPv4 Standby Address					
IPv6 Address Configura...					
IPv6 Link Local Address...					

UPDATE RESET CANCEL

SUBMIT CANCEL

**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: FunProf-ASA  
Description: optional

Copy Existing Profile Parameters:   
Profile: CISCO-ASA-1.2/WebPolicyForRoutedMode

Features and Parameters

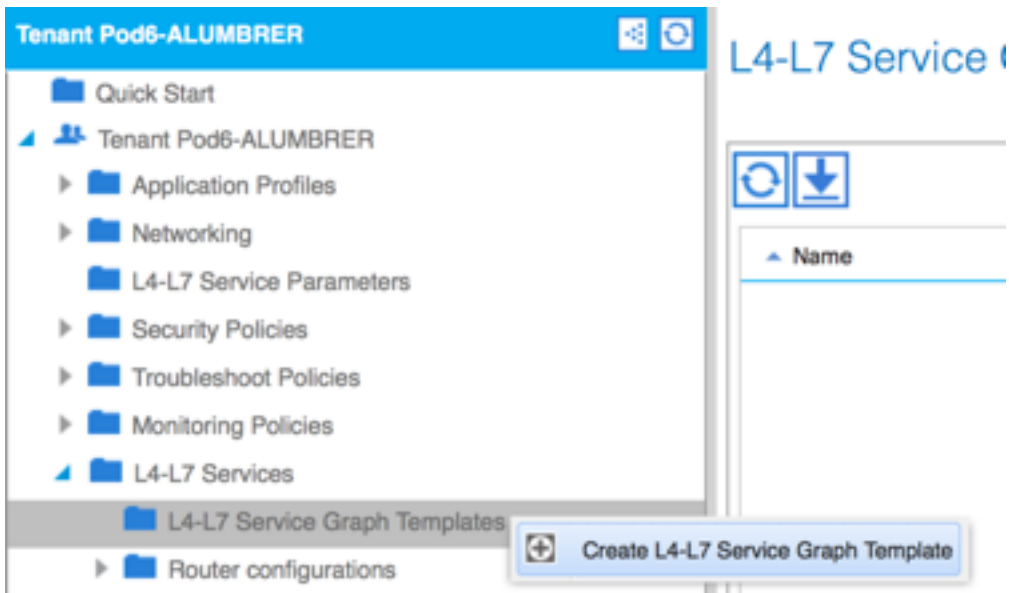
In order to auto apply new values to the parameters of existing graph instance when users modify function profiles, the name of top folder must be ended with -Default.

Basic Parameters **All Parameters**

Folder/Param	Name	Value	Mandatory	Locked	Shared
Destination Service	destination_service				
High Port					
Low Port	low_port	22		false	
Operator	operator	eq		false	
ICMP					
Logging					
Protocol					
Source Address					
Source Service					
Action	action	permit		false	
Order	order	30		false	

SUBMIT CANCEL

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



- 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:

Graph Type:  Create A New One  Clone An Existing One

**Consumer**

ASAv

**Provider**

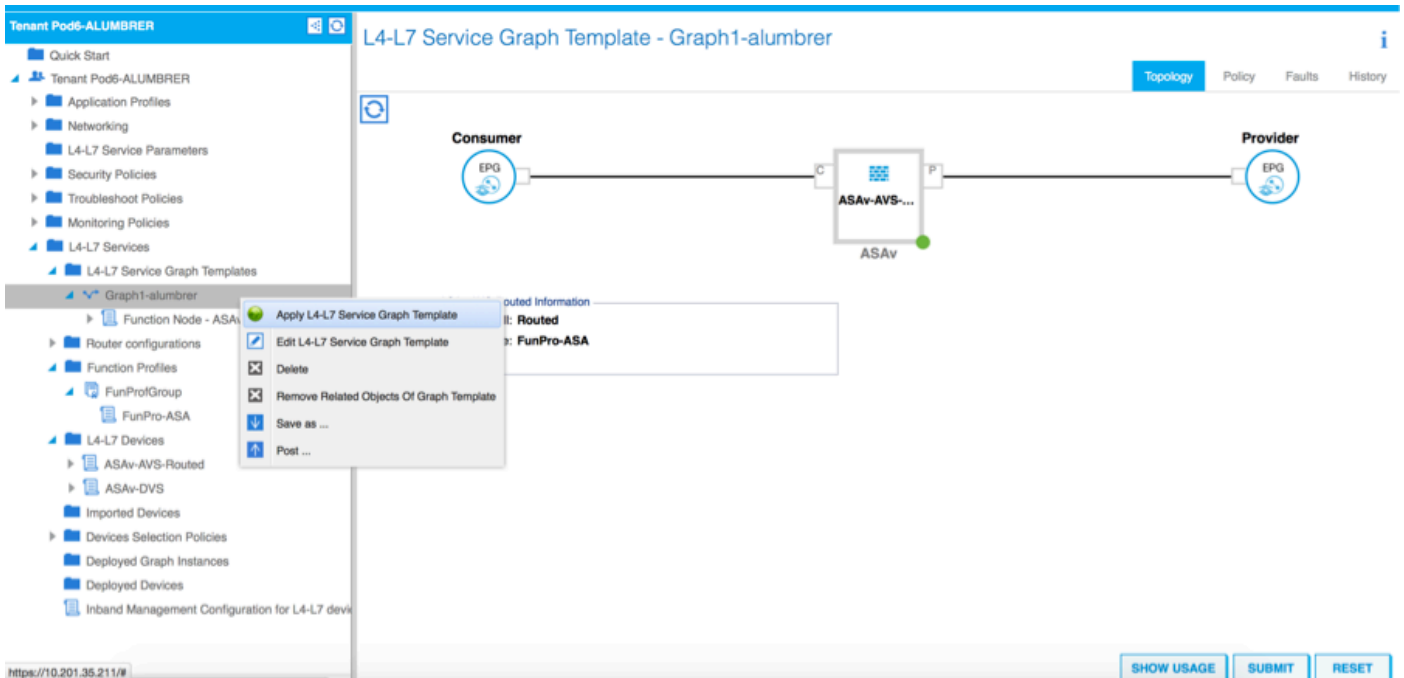
Please drag a device from devices table and drop it here to create a service node.

**ASAv-AVS-Routed Information**

Firewall:  Routed  Transparent

Profile:

- 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.



- 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 Network: Pod6-ALUMBRER/AVS-AEP-VMM

Contract Information

Contract:  Create A New Contract     Choose An Existing Contract Subject

Contract Name: EPG2-to-EPG1

No Filter (Allow All Traffic):

Pod6-ALUMBRER/AVS-AEP-VMM-alumbrer/epg-AVS-EPG1

Pod6-ALUMBRER/InternalAEP-VMM-alumbrer/epg-EPG-Internal-alumbrer

Pod6-ALUMBRER/VRF1-alumbrer/AnyEPG

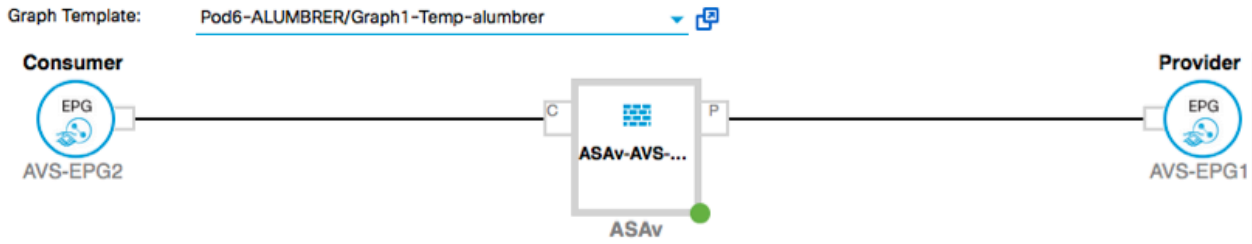
Pod6-ALUMBRER/VRF2/AnyEPG

Pod6-ALUMBRER/L3Out-N3K2/L3Net

PREVIOUS    NEXT    CANCEL

- 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.

- Klicken Sie auf **Weiter**



ASAv-AVS-Routed Information

Firewall: routed  
Profile: FunPro-ASA

Consumer Connector

Type:  General  Route Peering

BD: Pod6-ALUMBRER/ExtBD-alubrер

Cluster Interface: ClientInt

Provider Connector

Type:  General  Route Peering

BD: Pod6-ALUMBRER/IntBD-alubrер

Cluster Interface: ServerInt

PREVIOUS NEXT CANCEL

- 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.

STEP 3 > ASAv-AVS-Routed Parameters

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

config parameters for the selected device

Profile Name: FunPro-ASA

Required Parameters All Parameters

Folder/Param	Name	Value	Write Domain
Access List	access-list-inbound		
Access Control Entry	ICMP		
Access Control Entry	SSH2		
Access Control Entry	SSH		
Destination Address			
Destination Service	destination_service		
ICMP			
Logging			
Protocol	protocol		
Source Address			
Source Service			
Action	action	permit	
Order	order	100	select asa domain
Access Control Entry			
Access Control Entry			

UPDATE RESET CANCEL

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

PREVIOUS FINISH CANCEL

- 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 > ASA-ASV-Routed Parameters

1. Contract 2. Graph 3. ASA-ASV-Routed Parameters

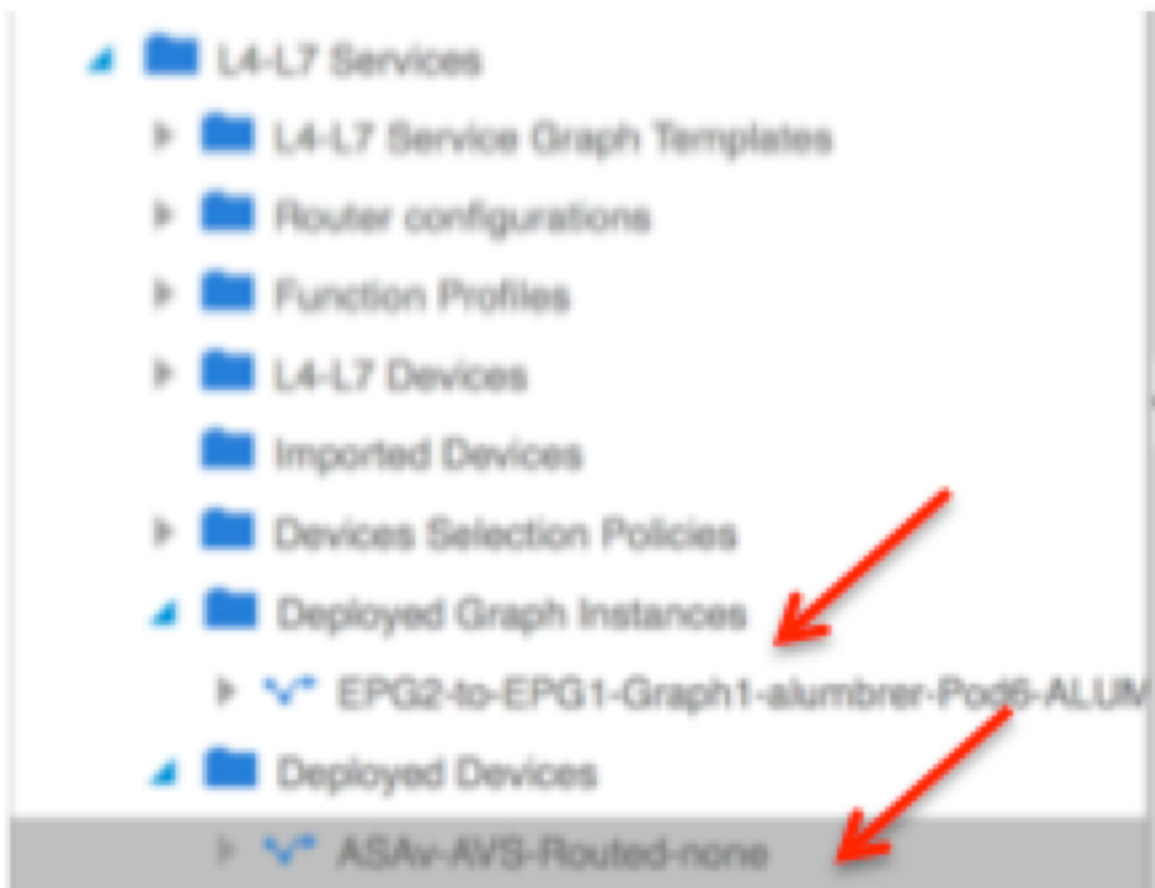
config parameters for the selected device

Profile Name: FunProf-ASA

Folder/Param	Name	Value	Write Domain
Device Config	Device		
Access List	access-list-inbound		
Bridge Group Interface			
Interface Related Configuration	externalif		
Access Group	ExtAccessGroup		
Inbound Access List	name	access-list-inbound	
Outbound Access List			
IPv6 Enforce EUI-64			
Interface Specific Configuration	externalIfCfg		
IPv4 Address Configuration	IPv4Address		
IPv4 Address	ipv4_address	192.168.10.1/24	
IPv4 Standby Address			
IPv6 Address Configuration			
IPv6 Link Local Address Configuration			
IPv6 Router Advertisements			

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

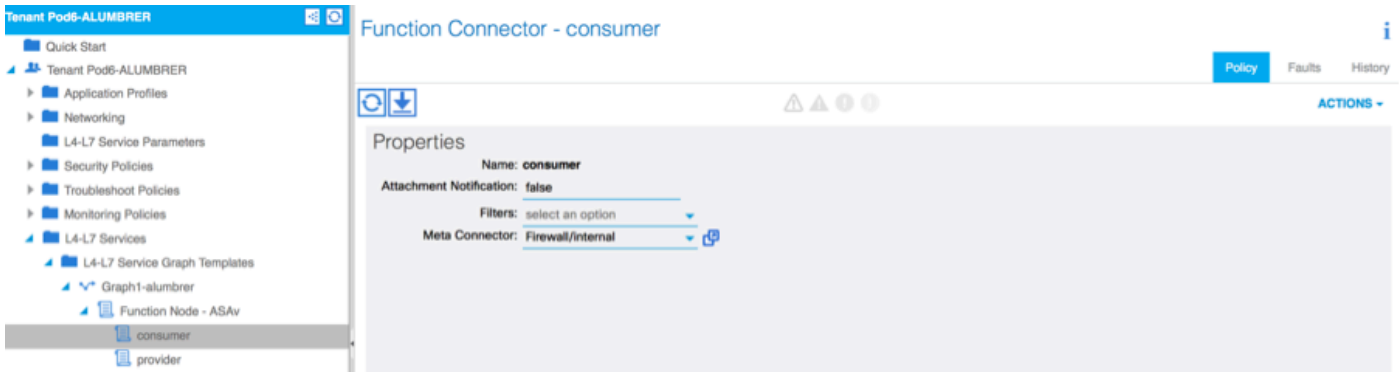
- Wenn alles in Ordnung ist, sollten ein neues bereitgestelltes Gerät und eine neue Diagramminstanz angezeigt werden.



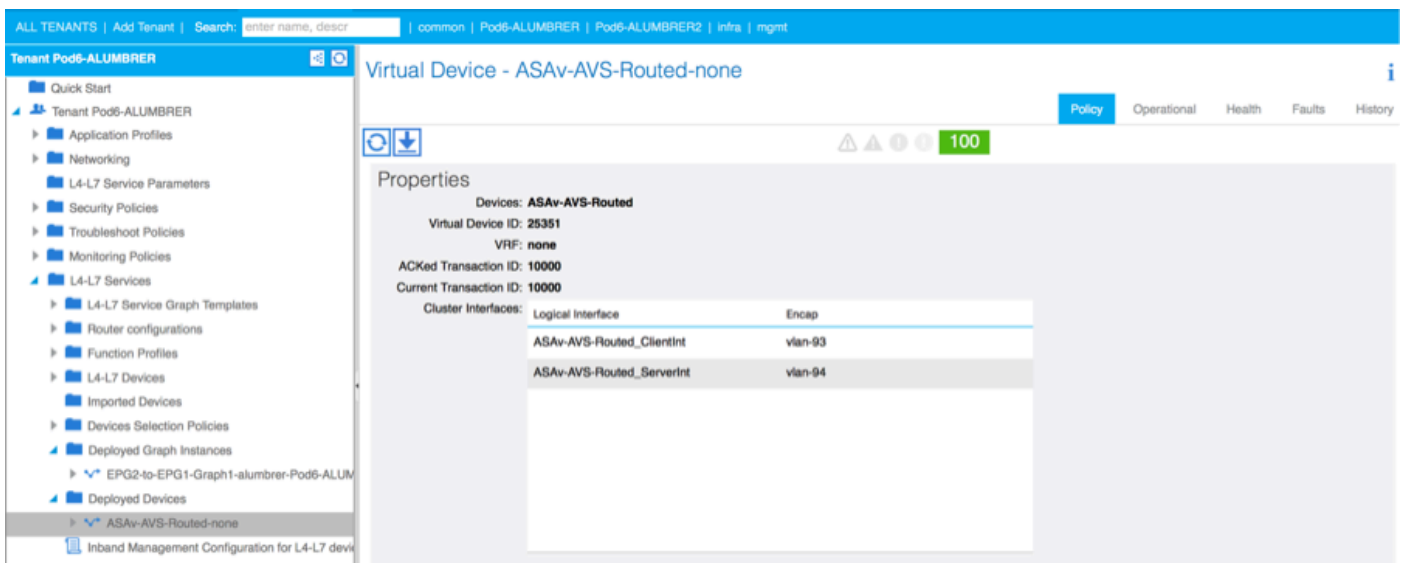
## Überprüfung

- 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.



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

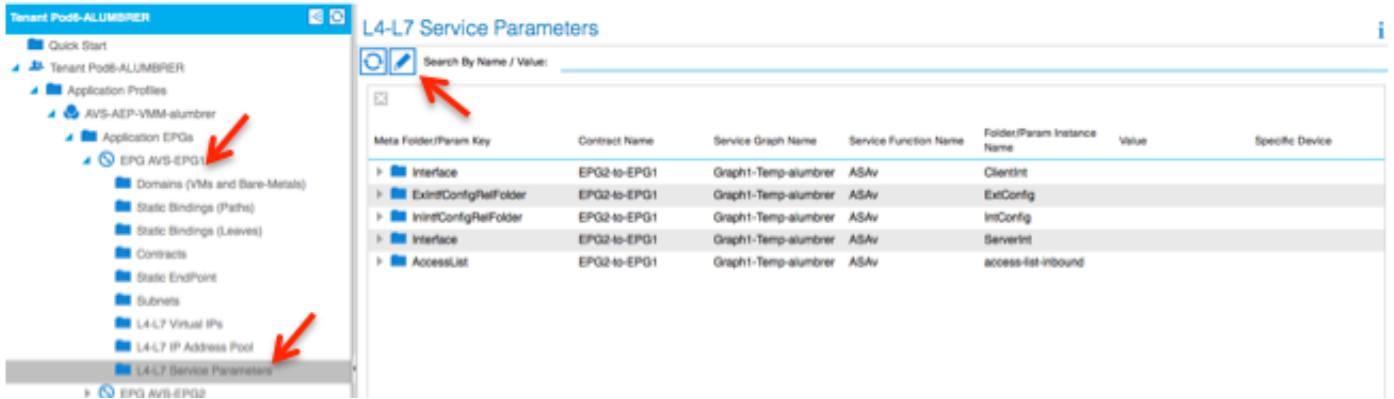
```

ASA0-W-AUS# show interface ip brief
Interface          IP-Address      OK? Method Status      Prot
ocol
GigabitEthernet0/0 192.168.10.1    YES manual  up          up
GigabitEthernet0/1 172.16.1.1      YES manual  up          up
GigabitEthernet0/2 unassigned      YES unset   administratively down up
GigabitEthernet0/3 unassigned      YES unset   administratively down up
GigabitEthernet0/4 unassigned      YES unset   administratively down up
GigabitEthernet0/5 unassigned      YES unset   administratively down up
GigabitEthernet0/6 unassigned      YES unset   administratively down up
GigabitEthernet0/7 unassigned      YES unset   administratively down up
GigabitEthernet0/8 unassigned      YES unset   administratively down up
Management0/0      10.201.35.223  YES CONFIG up          up
ASA0-W-AUS# show run access-list
access-list access-list-inbound extended permit tcp any any eq www
access-list access-list-inbound extended permit tcp any any eq https
access-list access-list-inbound extended permit tcp any any eq ssh
access-list access-list-inbound extended permit icmp any any
ASA0-W-AUS#

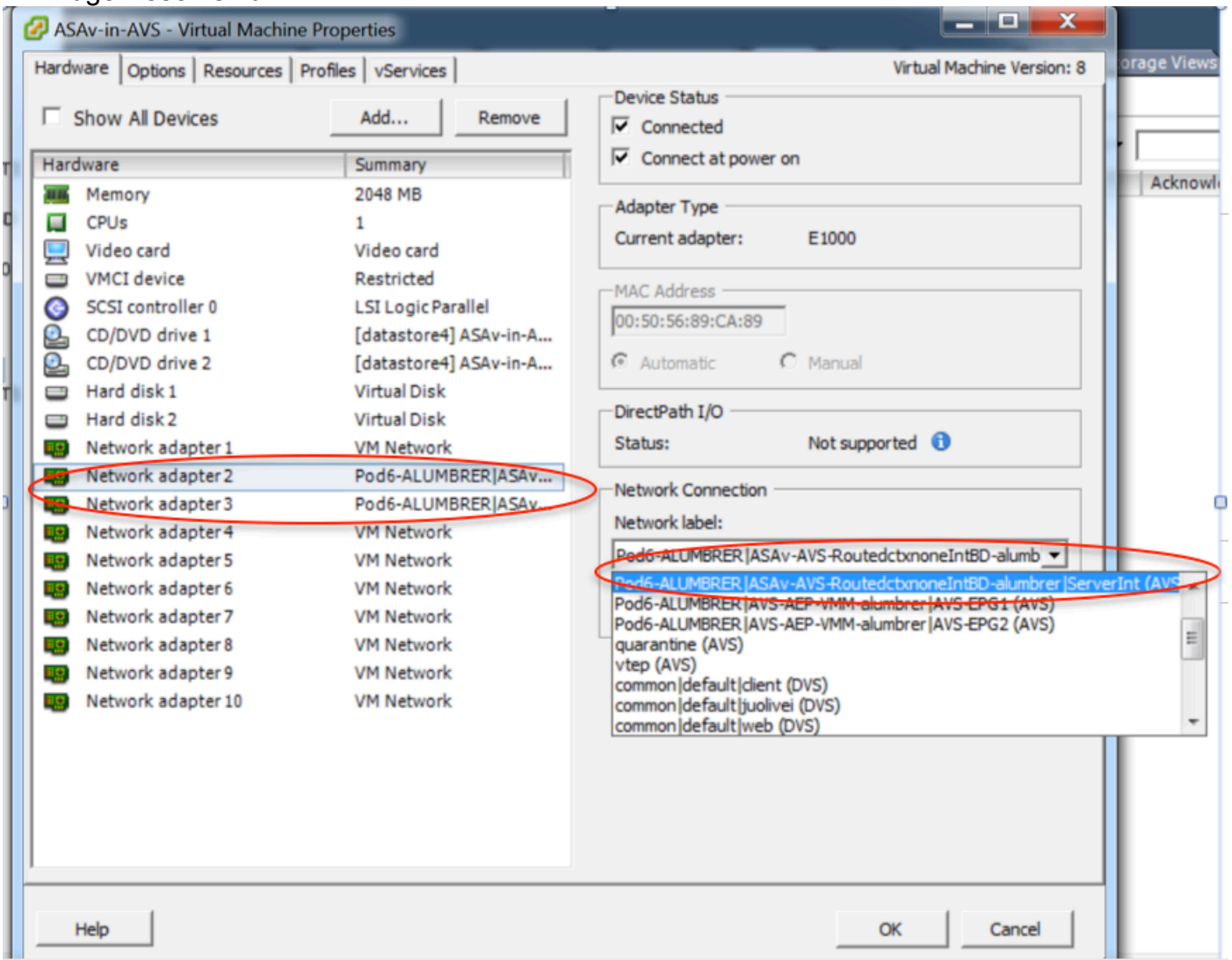
```

- 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.

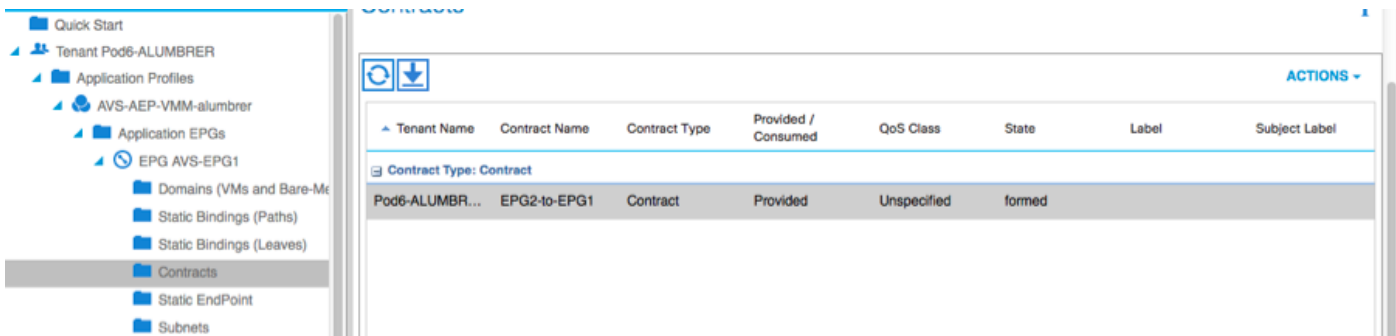




- In vCenter können Sie auch überprüfen, ob die Schatten-EPGs jeder FW-Schnittstelle zugewiesen sind:



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.



Wenn der Standardvertrag entfernt wird, können Sie bestätigen, dass der Datenverkehr jetzt über die ASA vfließt. 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.

```

ASA-v-w-AUS#
ASA-v-w-AUS# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
  alert-interval 300
access-list access-list-inbound; 4 elements; name hash: 0xcb5bd6c7
access-list access-list-inbound line 1 extended permit tcp any any eq www (hitcnt=0) 0xc873a747
access-list access-list-inbound line 2 extended permit tcp any any eq https (hitcnt=0) 0x48bedbdd
access-list access-list-inbound line 3 extended permit tcp any any eq ssh (hitcnt=4) 0x532fd57a
access-list access-list-inbound line 4 extended permit icmp any any (hitcnt=4) 0xe4b5a75d
ASA-v-w-AUS#
  
```

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

```

leaf2# show endpoint
Legend:
  0 - peer-attached      H - vtep          a - locally-aged    S - static
  V - vpc-attached      p - peer-aged    L - local           M - span
  s - static-arp        B - bounce
+-----+-----+-----+-----+-----+
| VLAN/ | Encap | MAC Address | MAC Info/ | Interface |
| Domain| VLAN  | IP Address  | IP Info   |            |
+-----+-----+-----+-----+-----+
Pod6-ALUMBRER:VRF1-alumbrer          50.50.50.50 L
14/Pod6-ALUMBRER:VRF1-alumbrer      vxlan-14778359 5897.bda4.f9bc L          eth1/13
30          vxlan-98 0050.5689.f008 L          eth1/7
Pod6-ALUMBRER:VRF1-alumbrer      Server IP & MAC vxlan-98 192.168.10.10 L          po4
25          vxlan-94 0050.5689.ca89 L
Pod6-ALUMBRER:VRF1-alumbrer          vxlan-94 192.168.10.1 L
mgmt:inb          192.168.2.11 S
21          vxlan-97 0050.5689.3fca L          eth1/7
Pod6-ALUMBRER:VRF2      Client IP & MAC vxlan-97 172.16.1.10 L
26          vxlan-93 0050.5689.e7dd L          po4
Pod6-ALUMBRER:VRF2          vxlan-93 172.16.1.1 L
overlay-1          10.0.104.93 L          FW interface (ServerInt)
overlay-1          10.0.96.67 L          FW interface (ClientInt)
13          vxlan-16777209 0050.5677.18a5 H          unspecified
overlay-1          vxlan-16777209 10.0.32.93 H          unspecified
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

```
~ # vemcmd show port vlan
```

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

## ESX-2

```
~ # vemcmd show port vlan
```

LTL	VSM Port	Admin	Link	State	Cause	PC-LTL	SGID	ORG	svcp	Type	Vem Port
24	Eth1/7	UP	UP	FWD	-	1040	6	0	0		vmnic6
50		UP	UP	FWD	-	0	6	0	0		vmk1
51		UP	UP	FWD	-	0	6	0	0		Client1-AVS.eth0
52		UP	UP	FWD	-	0	6	0	0		Server1-AVS.eth0
1040	Po1	UP	UP	FWD	-	0	0	0	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

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

### EPG2

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

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

```
leaf2# show zoning-rule | grep '17\|5476'
```

4141	17	32775	default	enabled	2916352	permit	src_dst_any(5)
4142	32775	17	default	enabled	2916352	permit	src_dst_any(5)
4139	5476	49156	14	enabled	2555904	permit	src_dst_any(5)
4140	49156	5476	14	enabled	2555904	permit	src_dst_any(5)

```
leaf2#
```

**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)

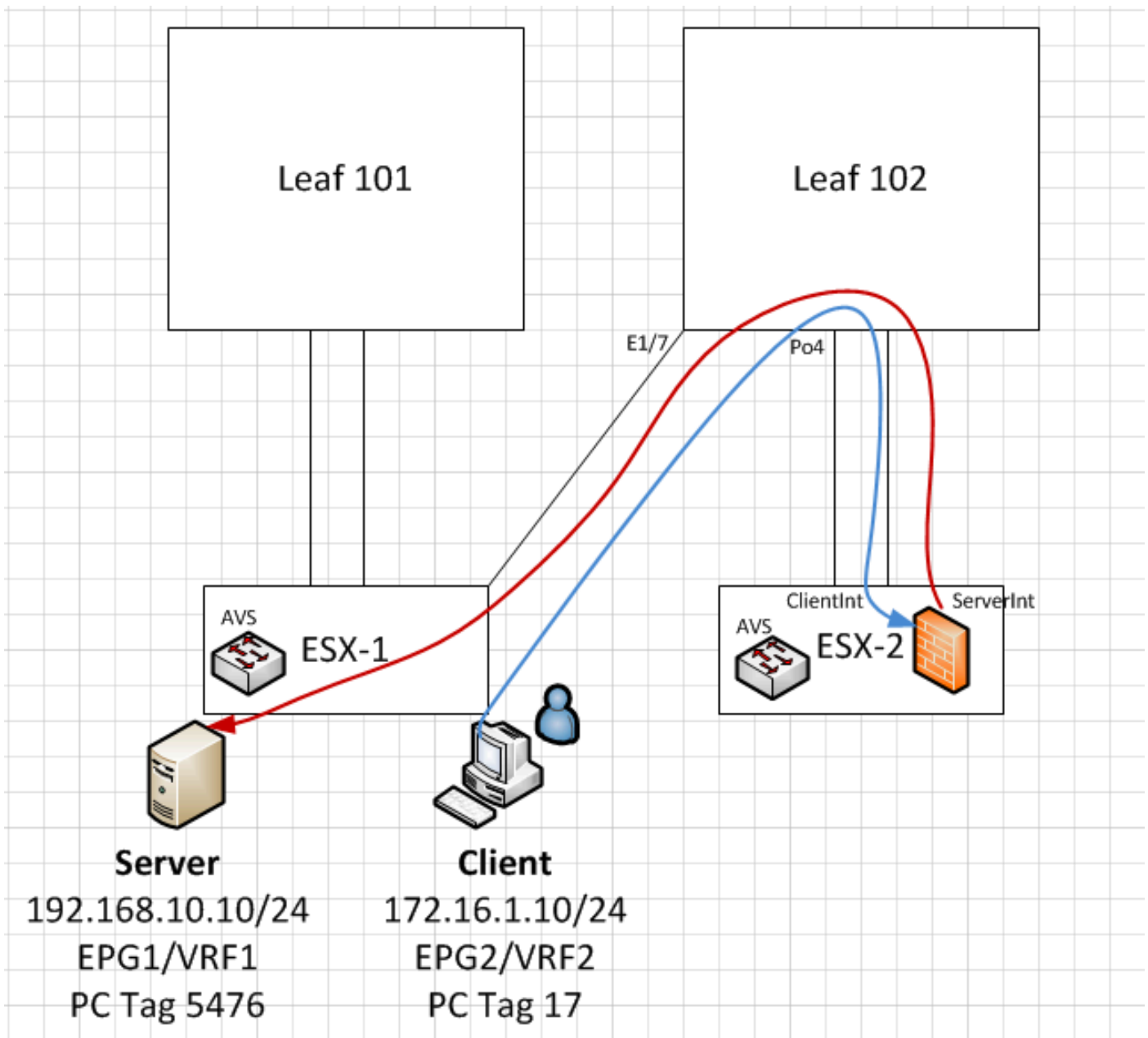
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:170350  errors:0  dropped:0  overruns:0  frame:0
          TX packets:170350  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:0
          RX bytes:18739044 (18.7 MB)  TX bytes:18739044 (18.7 MB)

cisco@cisco-UbuntuClient:~$ ssh 192.168.10.10
cisco@192.168.10.10's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

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

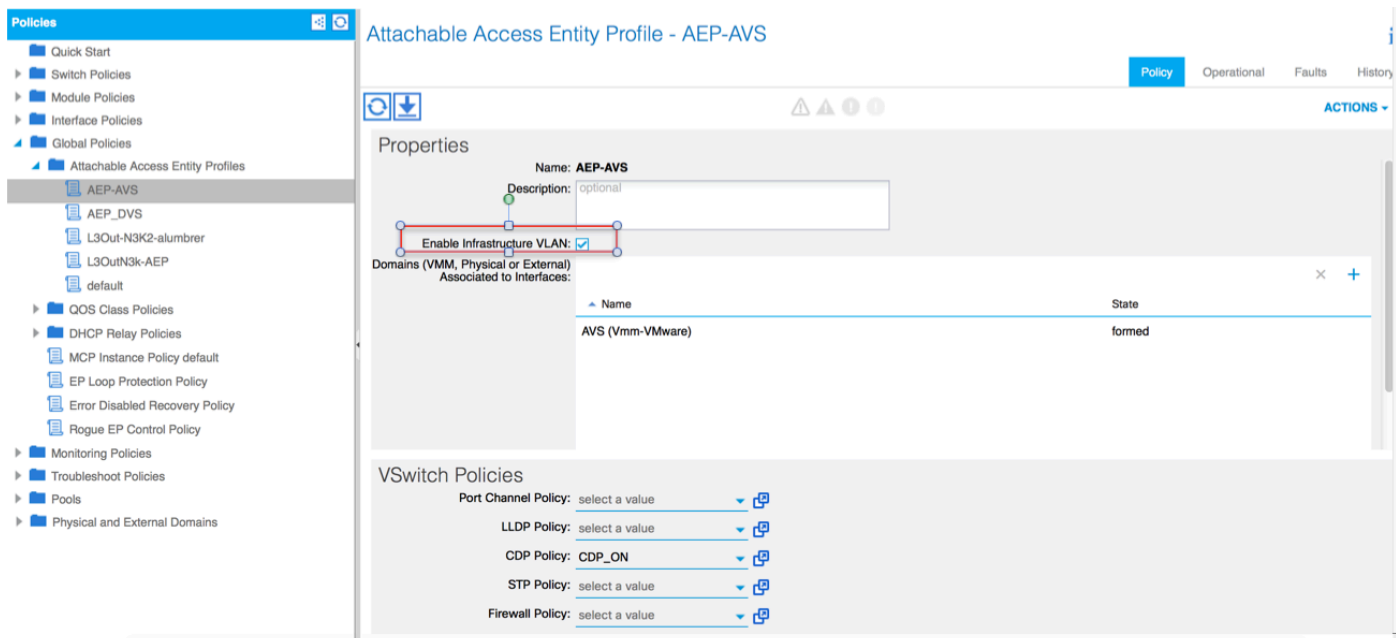




## Fehlerbehebung

VTEP-Adresse ist nicht zugewiesen

Überprüfen Sie, ob das Infrastruktur-VLAN unter AEP:



## 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 -l Interface Port

```

Group/DVPort IP Family IP Address Netmask Broadcast MAC Address MTU TSO MSS Enabled Type vmk0
Management Network IPv4 10.201.35.219 255.255.255.0 10.201.35.255 e4:aa:5d:ad:06:3e 1500 65535
true STATIC vmk0 Management Network IPv4 fe80::e6aa:5dff:fead:63e 64 e4:aa:5d:ad:06:3e 1500
65535 true STATIC, PREFERRED vmk1 160 IPv4 10.0.32.65 255.255.0.0 10.0.255.255 00:50:56:6b:ca:25
1500 65535 true STATIC vmk1 160 IPv6 fe80::250:56ff:fe6b:ca25 64 00:50:56:6b:ca:25 1500 65535
true STATIC, PREFERRED ~ # - Also on the host, verify if DHCP requests are sent back and forth:
~ # tcpdump-uw -i vmk1 tcpdump-uw: verbose output suppressed, use -v or -vv for full protocol
decode listening on vmk1, link-type EN10MB (Ethernet), capture size 96 bytes 12:46:08.818776 IP
truncated-ip - 246 bytes missing! 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request
from 00:50:56:6b:ca:25 (oui Unknown), length 300 12:46:13.002342 IP truncated-ip - 246 bytes
missing! 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 00:50:56:6b:ca:25
(oui Unknown), length 300 12:46:21.002532 IP truncated-ip - 246 bytes missing! 0.0.0.0.bootpc >
255.255.255.255.bootps: BOOTP/DHCP, Request from 00:50:56:6b:ca:25 (oui Unknown), length 300
12:46:30.002753 IP truncated-ip - 246 bytes missing! 0.0.0.0.bootpc > 255.255.255.255.bootps:
BOOTP/DHCP, Request from 00:50:56:6b:ca:25 (oui Unknown), length 300

```

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	Eth1/5	169	S I s	VMware ESXi	vmnic4
AVS:localhost.localdomainmain	Eth1/6	169	S I s	VMware ESXi	vmnic5
N3K-2 (FOC1938R02L)	Eth1/13	166	R S I s	N3K-C3172PQ-1	Eth1/13

```
leaf2# show port-c sum
```

```

Flags: D - Down          P - Up in port-channel (members)
       I - Individual    H - Hot-standby (LACP only)
       s - Suspended     r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
       F - Configuration failed

```

```

-----
Group Port-      Type      Protocol  Member Ports
Channel
-----
5      Po5 (SU)    Eth      LACP      Eth1/5 (P)  Eth1/6 (P)
-----

```

In der ESXi werden zwei Ports verwendet, die über einen Po5 verbunden sind.

```
leaf2# show vlan extended
```

VLAN	Name	Status	Ports
13	infra:default	active	Eth1/1, Eth1/20
19	--	active	Eth1/13
22	mgmt:inb	active	Eth1/1
26	--	active	Eth1/5, Eth1/6, Po5
27	--	active	Eth1/1
28	::	active	Eth1/5, Eth1/6, Po5

```
36 common:pod6_BD active Eth1/5, Eth1/6, Po5
```

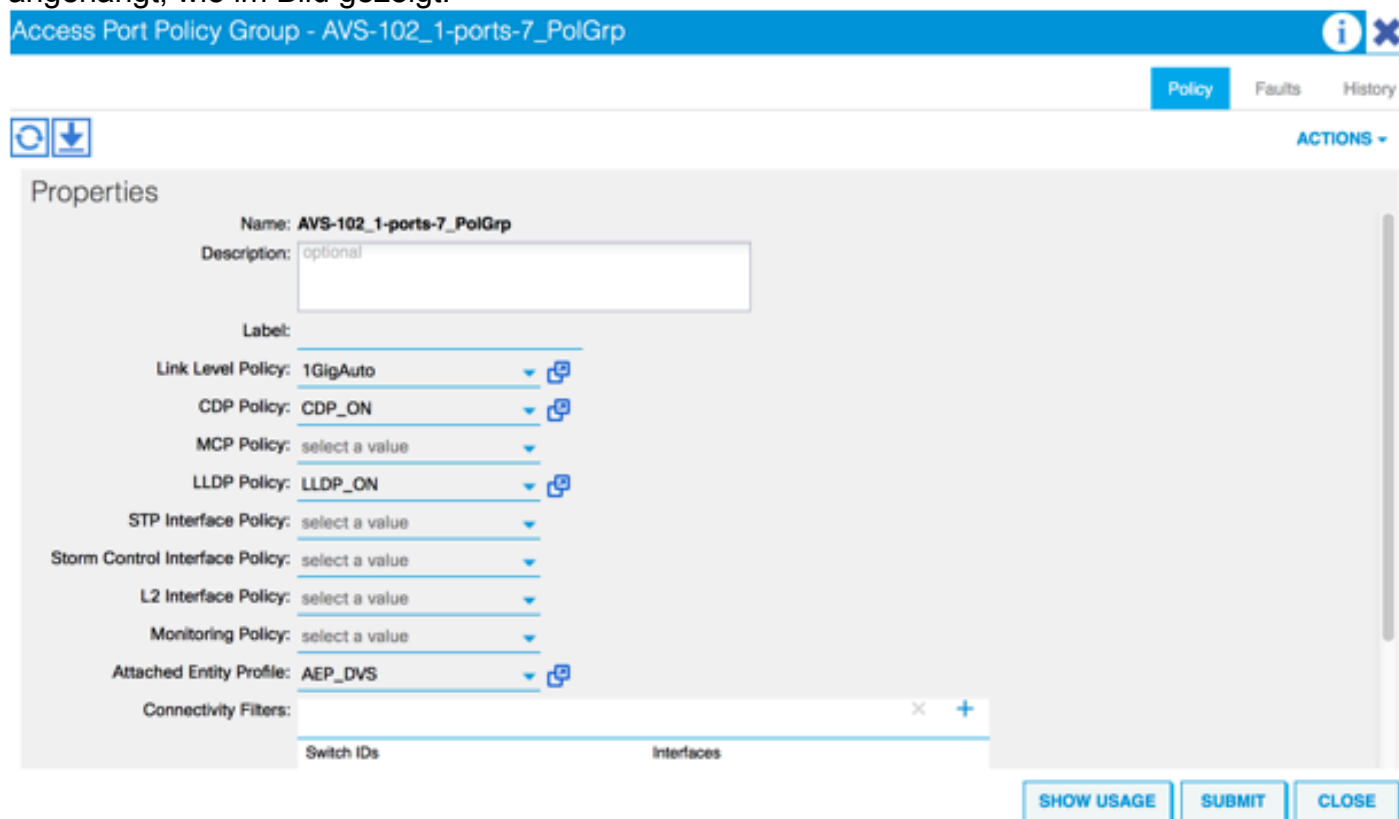
VLAN	Type	Vlan-mode	Encap
13	enet	CE	vxlan-16777209, vlan-3967
19	enet	CE	vxlan-14680064, vlan-150
22	enet	CE	vxlan-16383902
26	enet	CE	vxlan-15531929, vlan-200
27	enet	CE	vlan-11
28	enet	CE	vlan-14
36	enet	CE	vxlan-15662984

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:



Nachdem Sie die richtige AEP für AVS festgelegt haben, können Sie jetzt sehen, dass das Infra-VLAN über die entsprechenden Uplinks 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
13	enet	CE	vxlan-16777209, vlan-3967
19	enet	CE	vxlan-14680064, vlan-150
22	enet	CE	vxlan-16383902
26	enet	CE	vxlan-15531929, vlan-200
27	enet	CE	vlan-11
28	enet	CE	vlan-14
36	enet	CE	vxlan-15662984

and Opflex connection is reestablished after restarting the VEM module:

```

~ # vem restart
stopDpa
VEM SwISCSI PID is
Warn: DPA running host/vim/vimuser/cisco/vem/vemdpa.213997
Warn: DPA running host/vim/vimuser/cisco/vem/vemdpa.213997
watchdog-vemdpa: Terminating watchdog process with PID 213974

~ # vemcmd show opflex
Status: 0 (Discovering)
Channel0: 14 (Connection attempt), Channel1: 0 (Discovering)
Dvs name: comp/prov-VMware/ctrlr-[AVS]-vCenterController/sw-dvs-129
Remote IP: 10.0.0.30 Port: 8000
Infra vlan: 3967
FTEP IP: 10.0.0.32
Switching Mode: unknown
Encap Type: unknown
NS GIPO: 0.0.0.0

~ # vemcmd show opflex
Status: 12 (Active)
Channel0: 12 (Active), Channel1: 0 (Discovering)
Dvs name: comp/prov-VMware/ctrlr-[AVS]-vCenterController/sw-dvs-129
Remote IP: 10.0.0.30 Port: 8000
Infra vlan: 3967
FTEP IP: 10.0.0.32
Switching Mode: LS
Encap Type: unknown
NS GIPO: 0.0.0.0

```

## Zugehörige Informationen

Installation von virtuellen Anwendungs-Switches

[Cisco Systems, Inc. Installationsanleitung für Cisco Application Virtual Switch, Version 5.2\(1\)SV3\(1.2\)](#)

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](#)