

ASAv in modalità GoTo (L3) con l'uso di AVS-ACI 1.2(x) Release

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come implementare uno switch AVS (Application Virtual Switch) con un firewall ASAv (Adaptive Security Virtual Appliance) singolo in modalità Routed/GOTO come grafico di servizio L4-L7 tra due gruppi di endpoint (EPG) per stabilire la comunicazione tra client e server utilizzando ACI versione 1.2(x).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Criteri di accesso configurati e interfacce attive e attive
- EPG, Bridge Domain (BD) e Virtual Routing and Forwarding (VRF) già configurati

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

Hardware e 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)
- Foglia/aculei - 11.2(1i)
- Pacchetti dispositivo *.zip già scaricati

Caratteristiche:

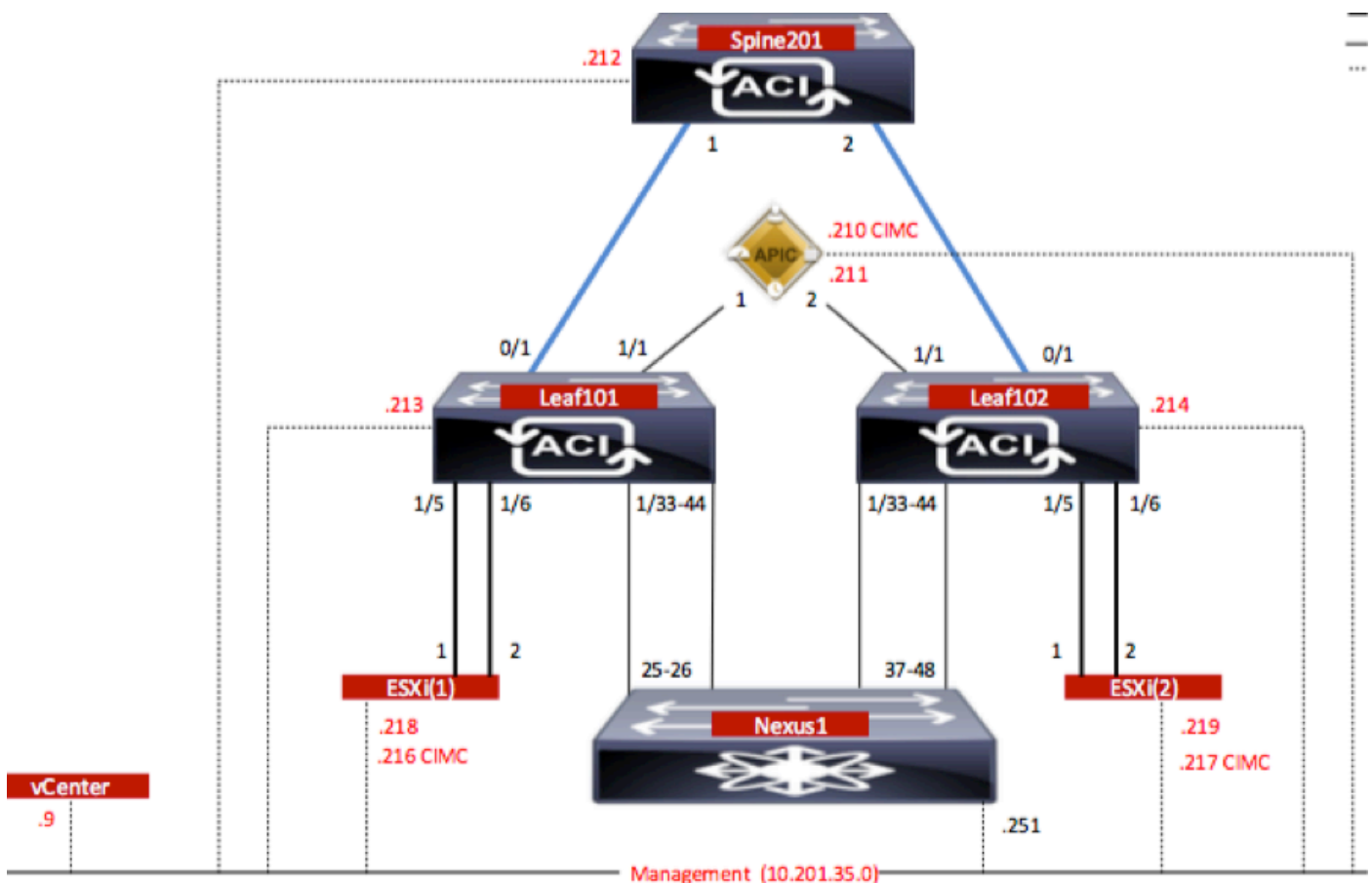
- AVS
- ASAv
- EPG, BD, VRF
- Access Control List (ACL)
- Grafico del servizio L4-L7
- vCenter

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete

Come mostrato nell'immagine,



Configurazioni

La configurazione iniziale di AVS crea un dominio VMware vCenter (integrazione VMM)2

Nota:

- È possibile creare più datacenter e voci DVS (Distributed Virtual Switch) in un singolo dominio. Tuttavia, a ciascun centro dati può essere assegnata una sola AVS Cisco.
- L'installazione di service graph con Cisco AVS è supportata da Cisco ACI versione 1.2(1i) con Cisco AVS versione 5.2(1)SV3(1.10). L'intera configurazione del grafico dei servizi viene eseguita sul Cisco Application Policy Infrastructure Controller (Cisco APIC).
- La distribuzione di Service Virtual Machine (VM) con Cisco AVS è supportata solo nei domini Virtual Machine Manager (VMM) con modalità di incapsulamento VLAN (Virtual Local Area Network). Tuttavia, le VM di elaborazione (le VM del provider e quelle del consumer) possono far parte di domini VMM con incapsulamento VLAN (Virtual Extensible LAN) o VXLAN.
- Si noti inoltre che se si utilizza la commutazione locale, l'indirizzo e il pool multicast non sono necessari. Se non è selezionata alcuna commutazione locale, è necessario configurare il pool multicast e l'indirizzo multicast a livello di infrastruttura AVS non deve far parte del pool multicast. Tutto il traffico proveniente dall'AVS sarà VLAN o incapsulato VXLAN.

Passare a **Rete VM > VMware > Crea dominio vCenter**, come mostrato nell'immagine:

Create vCenter Domain
i

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: x +

Name	Description

vCenter Credentials: x +

Profile Name	Username	Description
vCenterCredentials	root	

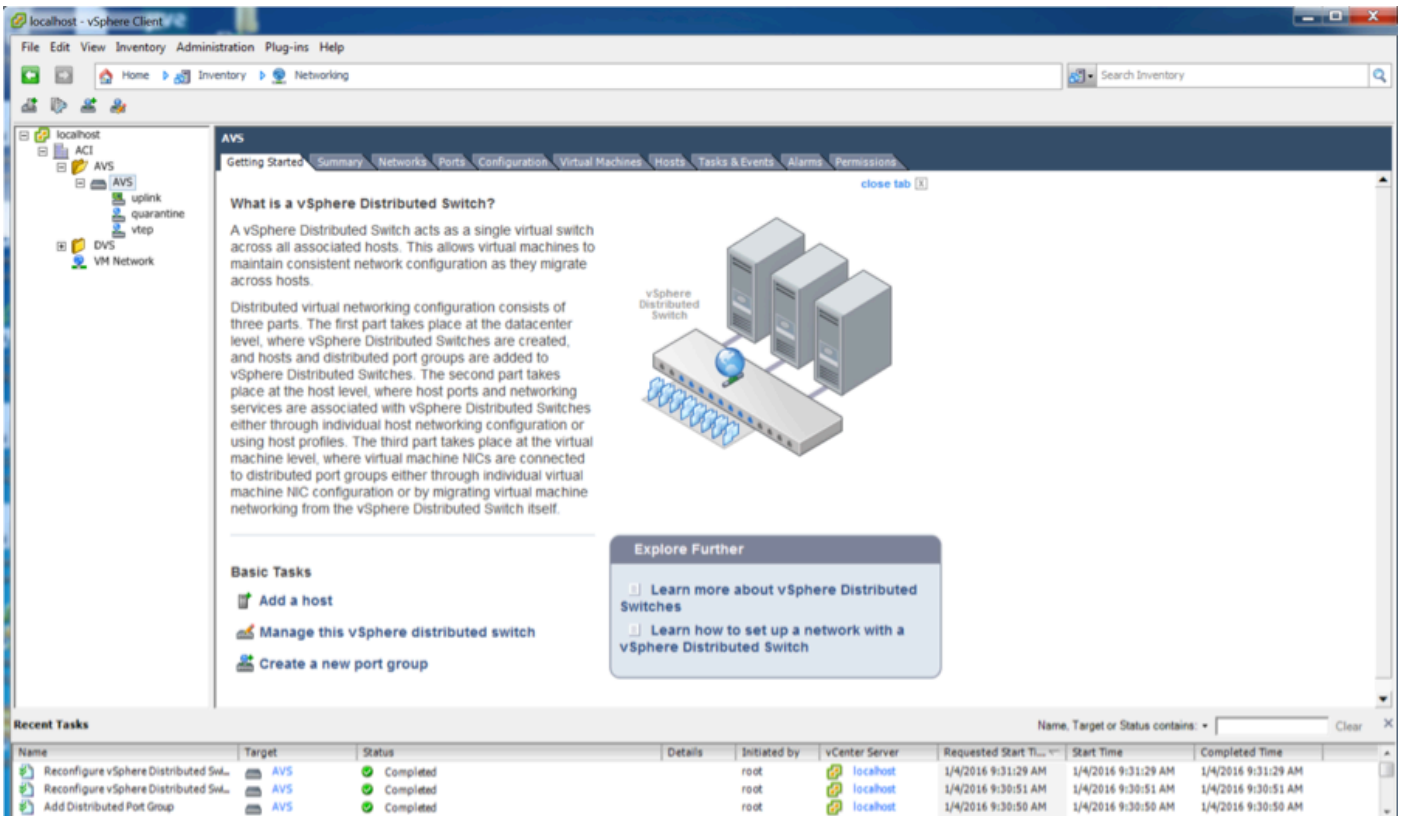
vCenter: x +

Name	IP	Type	Stats Collection
vCenterController	10.201.35.9	vCenter	Disabled

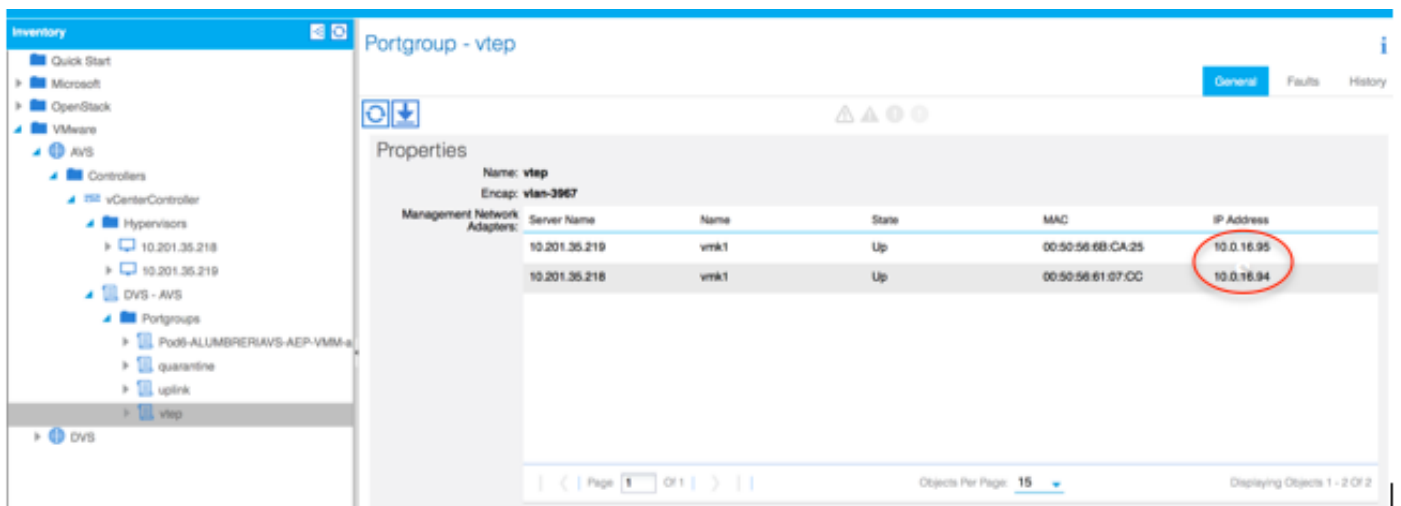
Se si utilizza Port-channel o VPC (Virtual Port-channel), si consiglia di impostare i criteri vSwitch

per l'utilizzo del ping Mac.

Quindi, APIC deve eseguire il push della configurazione dello switch AVS su vCenter, come mostrato nell'immagine:



Sull'APIC, un indirizzo VXLAN Tunnel Endpoint (VTEP) è assegnato al gruppo di porte VTEP per AVS. Questo indirizzo viene assegnato indipendentemente dalla modalità di connettività utilizzata (VLAN o VXLAN)



Installare il software Cisco AVS in vCenter

- Scaricare vSphere Installation Bundle (VIB) da CCO utilizzando questo [collegamento](#)

Nota: in questo caso si utilizza ESX 5.5, la tabella 1 mostra la matrice di compatibilità per ESXi 6.0, 5.5, 5.1 e 5.0

Tabella 1 - Compatibilità della versione del software host per ESXi 6.0, 5.5, 5.1 e 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

All'interno del file ZIP sono presenti 3 file VIB, uno per ciascuna versione host ESXi, selezionare quello appropriato per ESX 5.5, come mostrato nell'immagine:

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

- Copia del file VIB nell'archivio dati ESX: può essere eseguita tramite CLI o direttamente da vCenter

Nota: Se sull'host è presente un file VIB, rimuoverlo utilizzando il comando **esxcli software vib remove**.

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

oppure esplorando direttamente l'archivio dati.

- Installare il software AVS utilizzando il seguente comando sull'host ESXi:

installazione vib software esxcli -v /vmfs/umes/datastore1/cross_cisco-vem-v250-5.2.1.3.1.10.0-3.2.1.vib —modalità di manutenzione —nessun controllo-sig

```

~ # 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

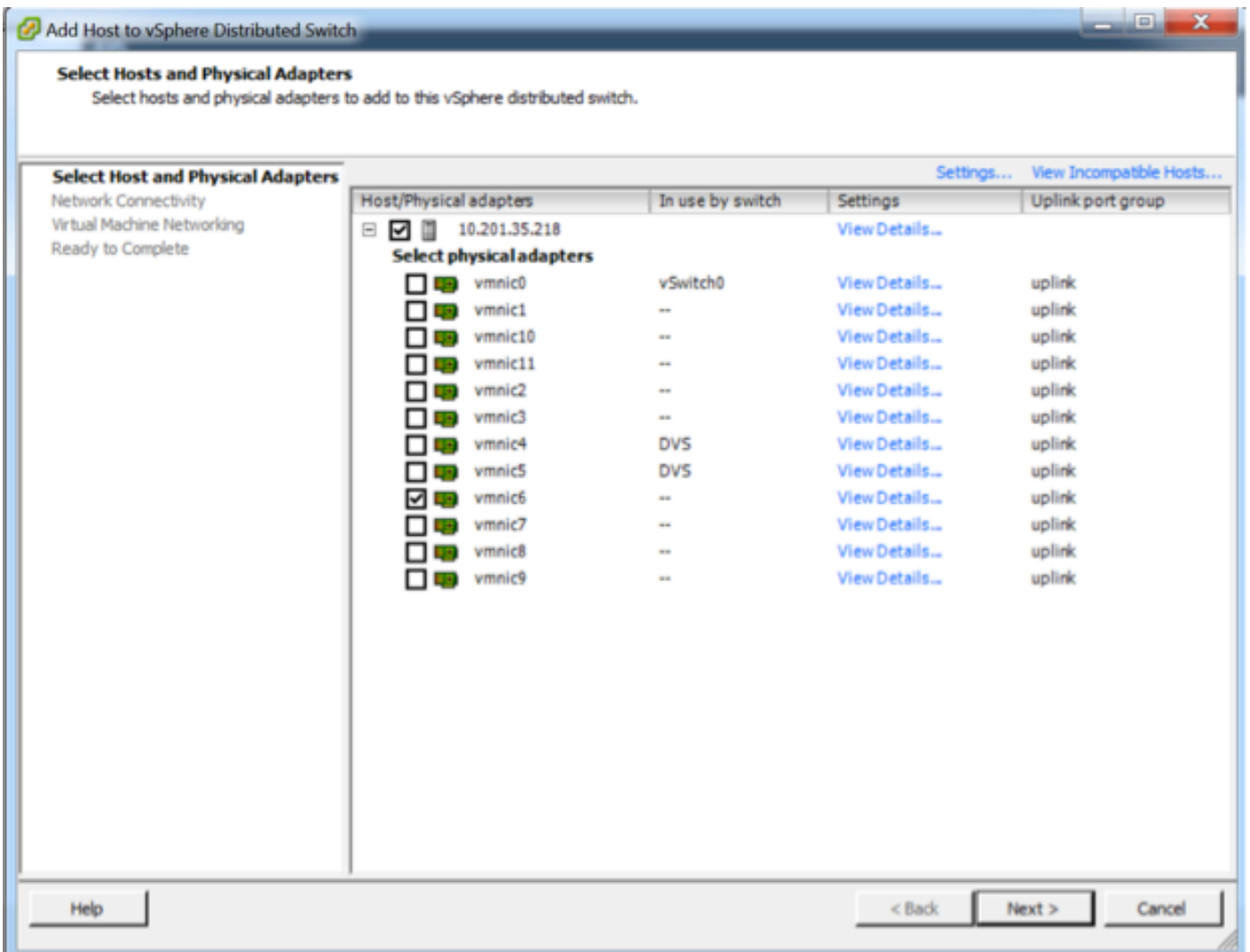
VEM Agent (vemdpa) is running

~ #

```

- Quando il modulo VEM (Virtual Ethernet Module) è attivo, è possibile aggiungere gli host all'AVS:

Nella finestra di dialogo Aggiungi host a switch distribuito vSphere, scegliere le porte NIC virtuali connesse allo switch foglia (in questo esempio si sposta solo vmnic6), come mostrato nell'immagine:



- Fare clic su **Avanti**.
- Nella finestra di dialogo Connettività di rete fare clic su **Avanti**
- Nella finestra di dialogo Rete macchina virtuale fare clic su **Avanti**
- Nella finestra di dialogo Pronto per il completamento fare clic su **Fine**

Nota: Se si utilizzano più host ESXi, tutti devono eseguire AVS/VEM in modo da poter essere gestiti da switch Standard a DVS o AVS.

L'integrazione di AVS è stata completata ed è ora possibile continuare l'installazione di ASAv L4-L7:

Configurazione iniziale di ASAv

- Scaricare il pacchetto del dispositivo Cisco ASAv e importarlo in APIC:

Passare a **L4-L7 Services > Packages > Import Device Package**, come mostrato nell'immagine:

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

- Se tutto funziona correttamente, è possibile vedere il pacchetto di dispositivi importati che espande la cartella L4-L7 Service Device Types, come mostrato nell'immagine:

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: |

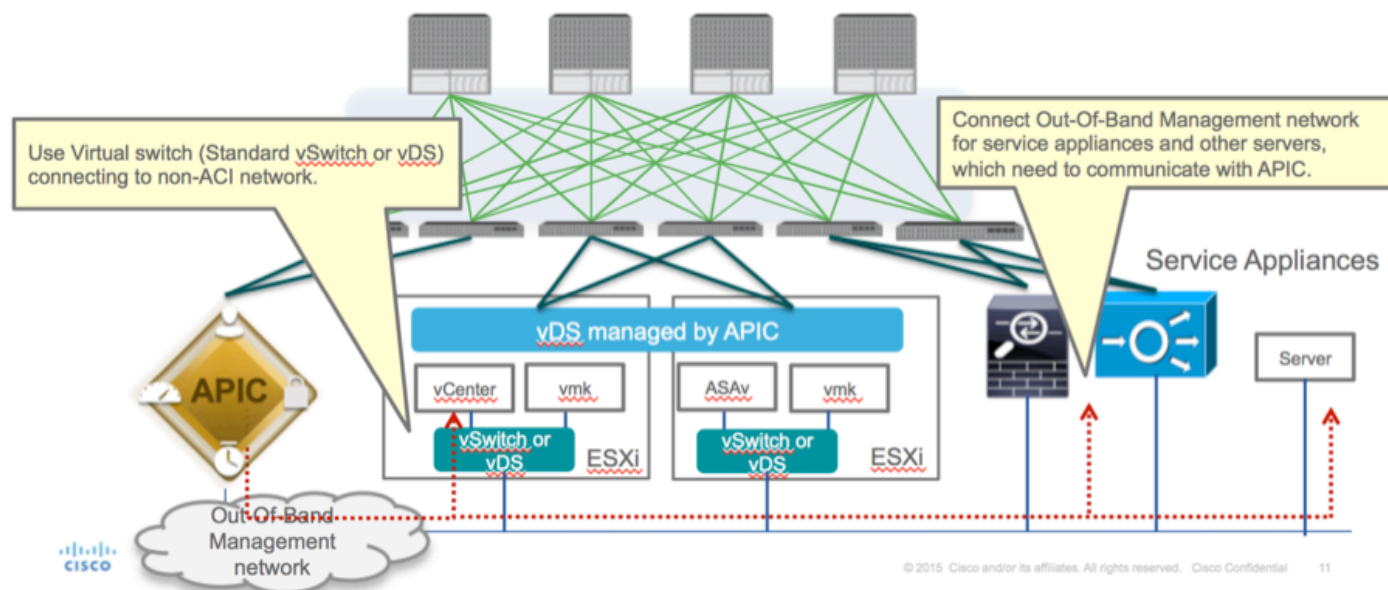
Interface Labels:

Name
cluster_ctrl_lk
external
failover_lan
failover_link
internal
mgmt
utility

Prima di continuare, è necessario determinare alcuni aspetti dell'installazione prima di eseguire l'integrazione L4-L7 effettiva:

Esistono due tipi di reti di gestione, gestione in banda e fuori banda (OOB, Out-Of-Band), che possono essere utilizzate per gestire dispositivi che non fanno parte dell'infrastruttura ACI (Application Centric Infrastructure) di base (foglia, spine o controller apic), tra cui ASAv, load balancer e così via.

In questo caso, la funzionalità OOB per ASAv viene implementata con lo switch vSwitch standard. Per le appliance ASA bare metal o altri accessori e/o server di servizio, collegare la porta di gestione OOB allo switch OOB o alla rete, come mostrato nell'immagine.



La connessione di gestione delle porte OOB ASAv deve utilizzare le porte uplink ESXi per comunicare con APIC tramite OOB. Quando si esegue il mapping delle interfacce vNIC, la scheda di rete 1 corrisponde sempre all'interfaccia di gestione 0/0 su ASAv e le altre interfacce del piano dati vengono avviate dalla scheda di rete 2.

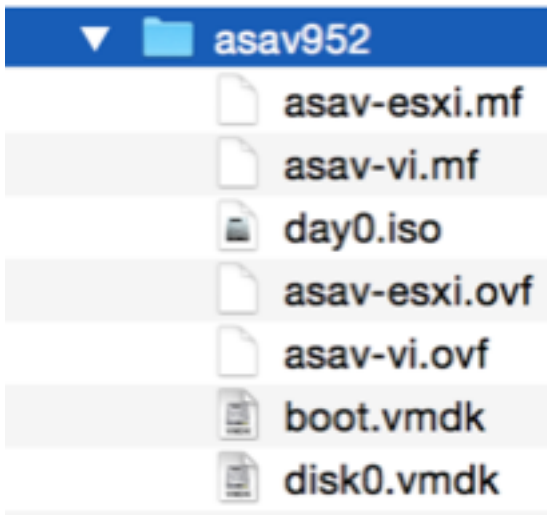
La tabella 2 mostra la concordanza tra gli ID delle schede di rete e gli ID dell'interfaccia ASAv:

Tabella 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

- Distribuire la VM ASAv tramite la procedura guidata da **File>Distribuisci modello OVF (Open Virtualization Format)**
- Selezionare **asav-esxi** se si desidera utilizzare ESX Server standalone o **asav-vi** per vCenter.

In questo caso, viene utilizzato vCenter.



- Completare l'installazione guidata e accettare termini e condizioni. Al centro della procedura guidata è possibile determinare diverse opzioni, ad esempio nome host, gestione, indirizzo IP, modalità firewall e altre informazioni specifiche relative ad ASA. Ricordarsi di usare la gestione OOB per ASA, in quanto in questo caso è necessario mantenere l'interfaccia Management0/0 mentre si usa la rete VM (switch standard) e l'interfaccia Gigabit Ethernet0-8 è la porta di rete predefinita.

Source

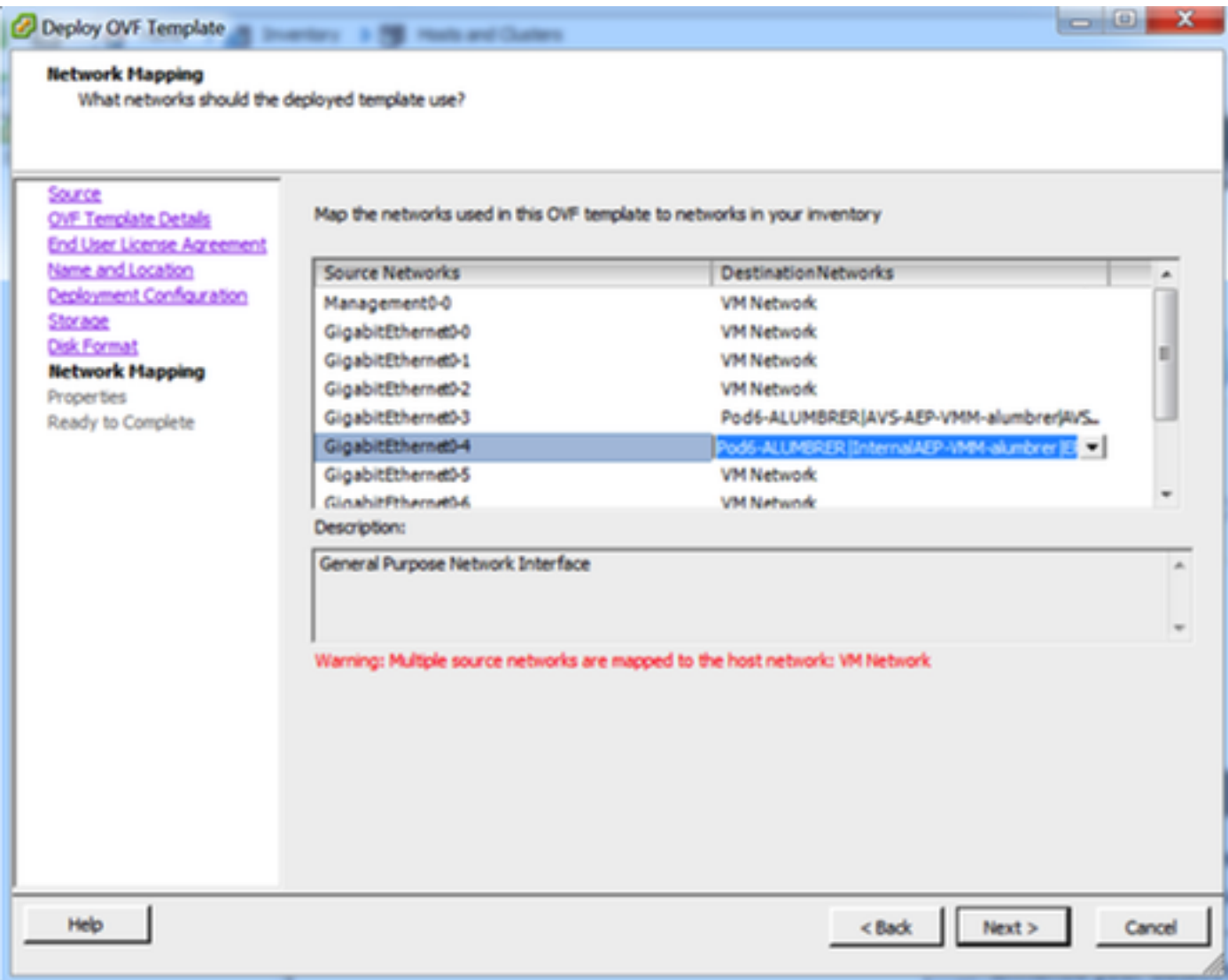
Select the source location.

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

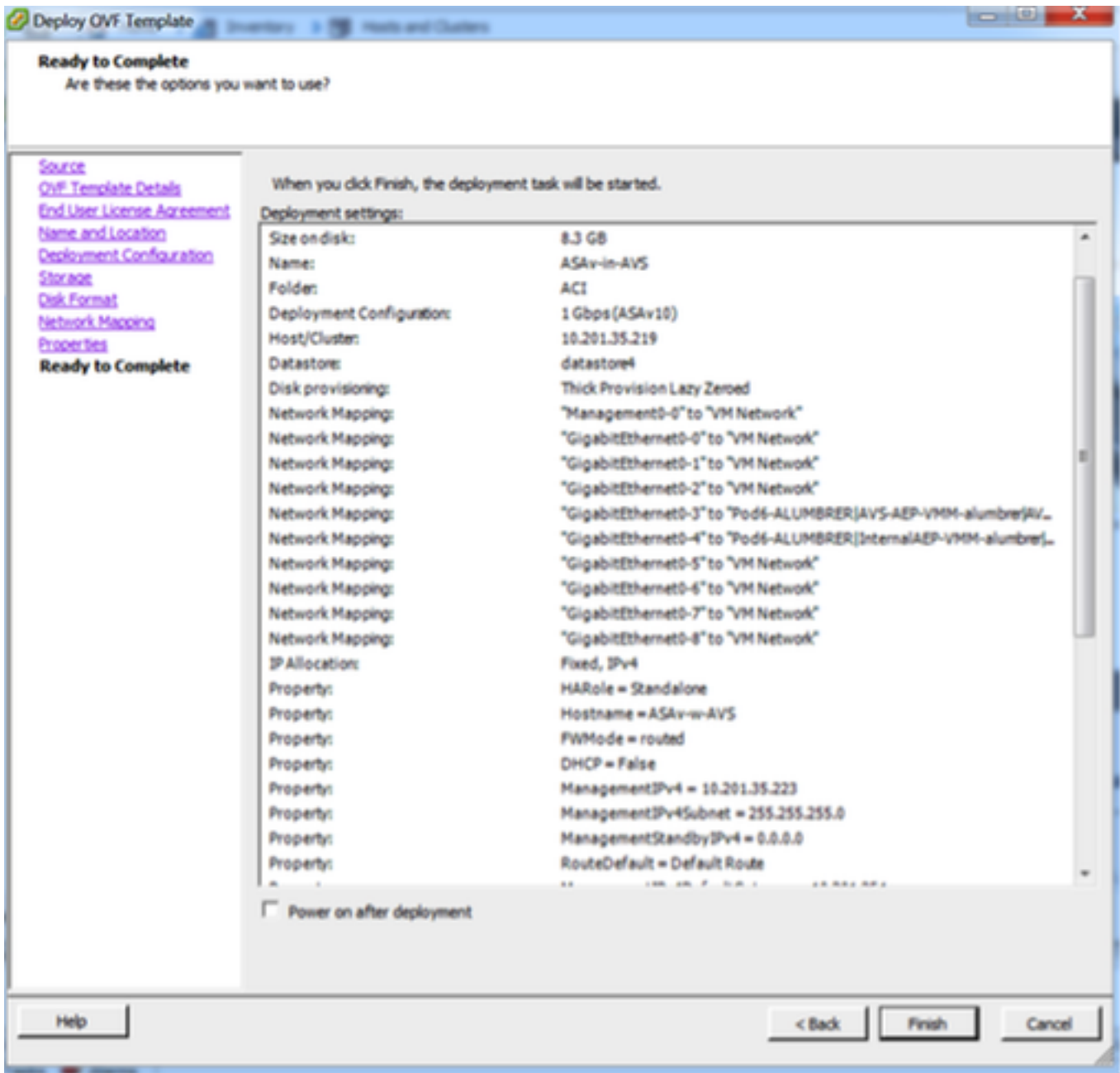
Firewall Properties
Firewall Mode
Select the Firewall Mode
routed

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

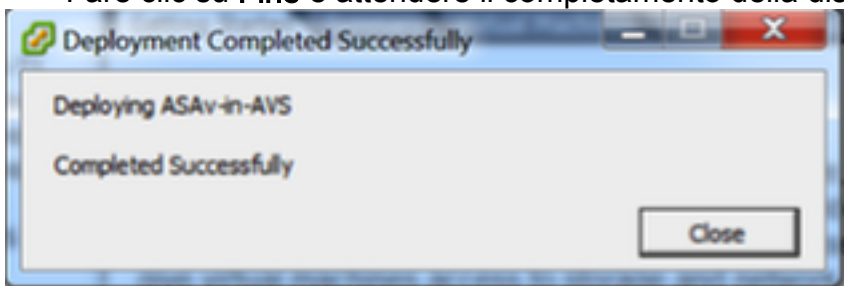
Management IP Address
Enter the Management IPv4 Address. For HA-type deployments, this property specifies the Management IPv4 address of the Active HA host.
10 . 201 . 35 . 223

Management IP Subnet Mask

Help < Back Next > Cancel



- Fare clic su **Fine** e attendere il completamento della distribuzione di ASAv



- Accendere la VM ASAv e accedere tramite la console per verificare la configurazione iniziale

```

?
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 --->_

```

- Come mostrato nell'immagine, alcune configurazioni di gestione sono già state trasferite al firewall ASA. Configurare il nome utente e la password amministratore. Il nome utente e la password vengono utilizzati dall'APIC per accedere e configurare l'ASA. L'ASA deve essere connessa alla rete OOB e deve essere in grado di raggiungere l'APIC.

username admin password <password_dispositivo> privilegio crittografato 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)# _

```

Inoltre, dalla modalità di configurazione globale abilitare il server http:

abilitazione server http

gestione http 0.0.0.0.0.0

L4-L7 per l'integrazione ASA in APIC:

- Accedere alla GUI ACI, fare clic sul tenant in cui verrà distribuito il grafico del servizio. Espandere i servizi L4-L7 nella parte inferiore del riquadro di navigazione e fare clic con il pulsante destro del mouse su **L4-L7 Devices** e fare clic su **Create L4-L7 devices** per aprire la procedura guidata

- Per questa implementazione, verranno applicate le seguenti impostazioni:

-Modalità gestita

-Servizio firewall

-Dispositivo virtuale

-Connesso al dominio AVS con un singolo nodo

Modello ASAv

-Modalità Routed (GoTo)

-Management Address (deve corrispondere all'indirizzo precedentemente assegnato all'interfaccia Mgmt0/0)

- Per impostazione predefinita, usa HTTPS come APIC e usa il protocollo più sicuro per comunicare con ASAv

Create L4-L7 Devices i X

STEP 1 > General 1. General 2. Device Configuration

Please select device package and enter connectivity information.

General

Managed:

Name: ASAv-AVS-Routed

Service Type: Firewall

Device Type: PHYSICAL VIRTUAL

VMM Domain: AVS

Mode: Single Node HA Cluster

Device Package: CISCO-ASA-1.2

Model: ASAv

Function Type: GoThrough GoTo

Device 1

Management IP Address: 10.201.35.3 Management Port: https

VM: vCenterController/ASAv-in-AVS

Device Interfaces: x +

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: x +

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

Connectivity

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

Credentials

Username: admin

Password:

Confirm Password:

- La corretta definizione delle interfacce di dispositivo e delle interfacce cluster è fondamentale per una corretta distribuzione

Per la prima parte, usare la tabella 2 mostrata nella sezione precedente per far corrispondere correttamente gli ID delle schede di rete con gli ID dell'interfaccia ASAv che si desidera usare. Il percorso si riferisce alla porta fisica o al canale della porta o al VPC che consente l'ingresso e l'uscita dalle interfacce del firewall. In questo caso, l'ASA si trova in un host ESX, dove in e out sono gli stessi per entrambe le interfacce. In un accessorio fisico, le porte interne ed esterne al firewall (FW) sono diverse.

Per quanto riguarda la seconda parte, le interfacce cluster devono essere sempre definite senza

eccezioni (anche se Cluster HA non viene utilizzato), in quanto il modello a oggetti ha un'associazione tra l'interfaccia **mlf** (meta interface sul pacchetto del dispositivo), l'interfaccia **Lif** (leaf interface, ad esempio external, internal, inside, ecc.) e l'interfaccia **Cif** (concrete interface). I dispositivi concreti L4-L7 devono essere configurati in una configurazione cluster di dispositivi e questa astrazione è chiamata dispositivo logico. Il dispositivo logico dispone di interfacce logiche mappate a interfacce concrete sul dispositivo concreto.

Per questo esempio verrà utilizzata l'associazione seguente:

Gi0/0 = vmnic2 = IntServer/provider/server > EPG1

Gi0/1 = vmnic3 = IntClient/consumer/client > EPG2

L4-L7 Devices - ASAv-AVS-Routed

The screenshot displays the configuration for 'ASAv-AVS-Routed' devices. It is divided into several sections:

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

Name	VMNIC	Path (Only For Route Peering)
GigabitEthernet0/1	Network adapter 3	Node-102/MAC_Pinning, No...
GigabitEthernet0/2	Network adapter 4	Node-102/MAC_Pinning
- Cluster:** Management IP Address: 10.201.35.223, Management Port: 443. Cluster Interfaces table:

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

Nota: Per le installazioni di failover/HA, Gigabit Ethernet 0/8 è preconfigurato come interfaccia di failover.

Lo stato del dispositivo deve essere Stabile ed è necessario essere pronti per distribuire il modello del profilo funzione e del grafico del servizio

Tempo del grafico dei servizi

Innanzitutto, creare un profilo funzione per ASAv, ma prima è necessario creare un gruppo di profili funzione e quindi un profilo funzione servizi L4-L7 in tale cartella, come mostrato nell'immagine:

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 ...

- Selezionare il profilo **WebPolicyForRoutedMode** dal menu a discesa e procedere alla configurazione delle interfacce sul firewall. Da questo momento in poi, le fasi sono facoltative e possono essere implementate/modificate successivamente. Questi passaggi possono essere eseguiti in diverse fasi della distribuzione a seconda di quanto il grafico del servizio possa essere riutilizzabile o personalizzato.

Per questo esercizio, un firewall con routing (modalità GoTo) richiede che ogni interfaccia abbia un indirizzo IP univoco. La configurazione ASA standard ha anche un livello di sicurezza dell'interfaccia (l'interfaccia esterna è meno sicura, l'interfaccia interna è più sicura). È inoltre possibile modificare il nome dell'interfaccia in base alle proprie esigenze. In questo esempio vengono utilizzati i valori predefiniti.

- Espandere Configurazione specifica dell'interfaccia, aggiungere indirizzo IP e livello di protezione per ServerInt con il seguente formato per l'indirizzo IP **x.x.x/y.y.y** o **x.x.x/yy**. Ripetere il processo per l'interfaccia ClientInt.

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

Nota: È inoltre possibile modificare le impostazioni predefinite dell'elenco degli accessi e creare un modello di base personalizzato. Per impostazione predefinita, il modello RoutedMode includerà regole per HTTP e HTTPS. Per questo esercizio, SSH e ICMP verranno aggiunti all'elenco degli accessi esterni consentiti.

Create Function Profile

Name: FunProf-ASA
Description: optional

Copy Existing Profile Parameters:

Profile: CISCO-ASA-1.2/WebPolicyForRoutedMode

Features and Parameters

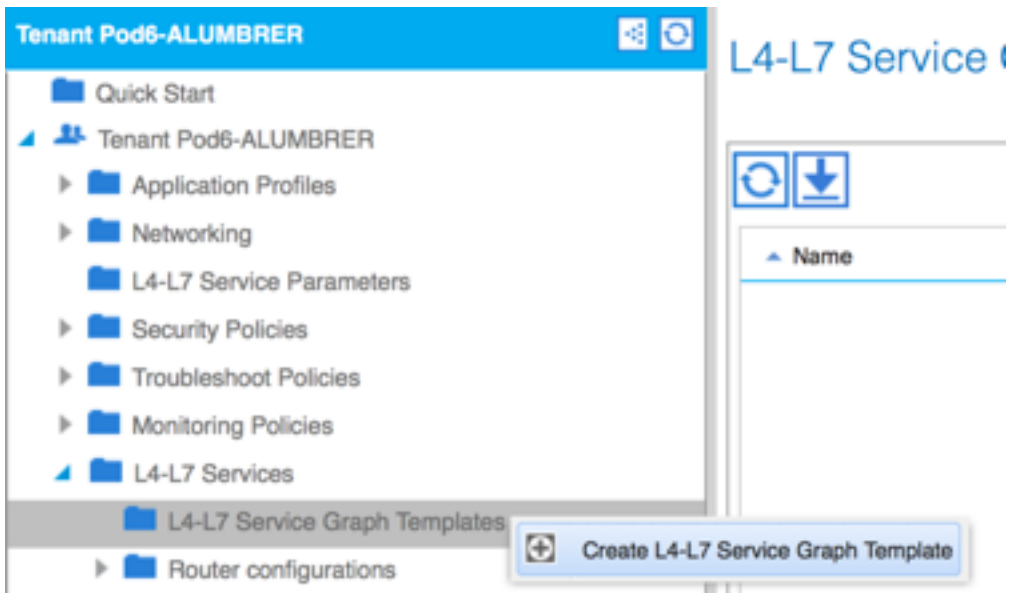
In order to auto apply new values to the parameters of existing graph instance when users modify function profiles, the name of top folder must be ended with -Default.

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

- Quindi fare clic su **Invia**
- Creare ora il modello Service Graph



- Trascinare e rilasciare il cluster di dispositivi a destra per creare la relazione tra consumer e provider, selezionare Modalità instradata e il profilo funzione creato in precedenza.

Graph Name:

Graph Type: Create A New One Clone An Existing One

Consumer

ASAv

Provider

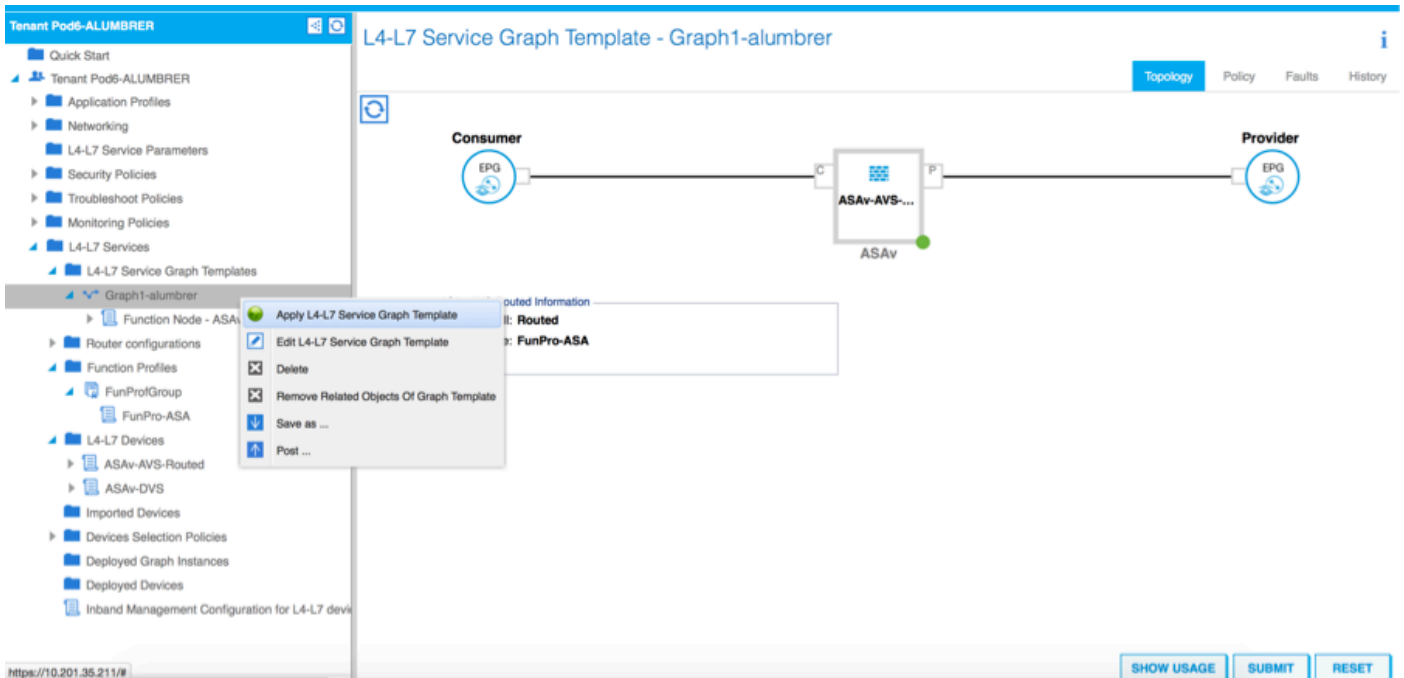
Please drag a device from devices table and drop it here to create a service node.

ASAv-AVS-Routed Information

Firewall: Routed Transparent

Profile:

- Verifica la presenza di errori nel modello. I modelli sono creati per essere riutilizzabili, quindi devono essere applicati a particolari EPG, ecc.
- Per applicare un modello, fare clic con il pulsante destro del mouse e selezionare Applica modello Service Graph L4-L7



- Definire quale EPG sarà sul lato consumer e sul lato provider. In questo esercizio, AVS-EPG2 è il consumer (client) e AVS-EPG1 è il provider (server). Tenere presente che non viene applicato alcun filtro, in modo che il firewall possa eseguire tutti i filtri basati sull'elenco degli accessi definito nell'ultima sezione della procedura guidata.
- Fare clic su **Avanti**.

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

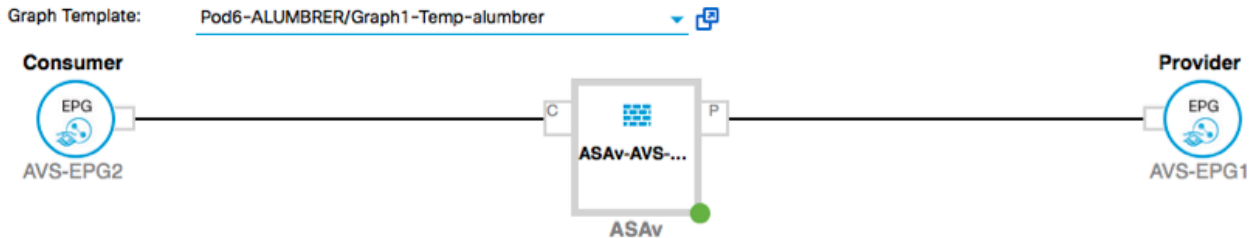
Contract Name: EPG2-to-EPG1

No Filter (Allow All Traffic):

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

PREVIOUS NEXT CANCEL

- Verificare le informazioni BD per ogni EPG. In questo caso, EPG1 è il fornitore del database IntBD e EPG2 è il consumatore di BD ExtBD. EPG1 si conetterà all'interfaccia del firewall ServerInt ed EPG2 sarà connesso all'interfaccia ClientInt. Entrambe le interfacce FW diventeranno la DG per ciascun EPG, quindi il traffico sarà sempre costretto a attraversare il firewall.
- Fare clic su **Avanti**.



ASAv-AVS-Routed Information

Firewall: routed
Profile: FunPro-ASA

Consumer Connector

Type: General Route Peering

BD: Pod6-ALUMBRER/ExtBD-alubrbrer

Cluster Interface: ClientInt

Provider Connector

Type: General Route Peering

BD: Pod6-ALUMBRER/IntBD-alubrbrer

Cluster Interface: ServerInt

PREVIOUS NEXT CANCEL

- Nella sezione Parametri di configurazione, fare clic su **Tutti i parametri** e verificare la presenza di indicatori RED da aggiornare/configurare. Nell'output, come mostrato nell'immagine, si noti che l'ordine nell'elenco degli accessi non è presente. Questo equivale all'ordine delle linee mostrato in un show ip access-list X.

STEP 3 > ASAv-AVS-Routed Parameters

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

config parameters for the selected device

Profile Name: FunPro-ASA

Features:

- Interfaces
- AccessLists
- NAT
- TrafficSelectorObjects
- All

Required Parameters All Parameters

Folder/Param	Name	Value	Write Domain
Access List	access-list-inbound		
Access Control Entry	ICMP		
Access Control Entry	SSH2		
Access Control Entry	SSH		
Destination Address			
Destination Service	destination_service		
ICMP			
Logging			
Protocol	protocol		
Source Address			
Source Service			
Action	action	permit	
Order	order	00	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

- È inoltre possibile verificare l'indirizzo IP assegnato dal profilo funzione definito in precedenza. Se necessario, è possibile modificare le informazioni. Una volta impostati tutti i parametri, fare clic su **Fine**, come mostrato nell'immagine:

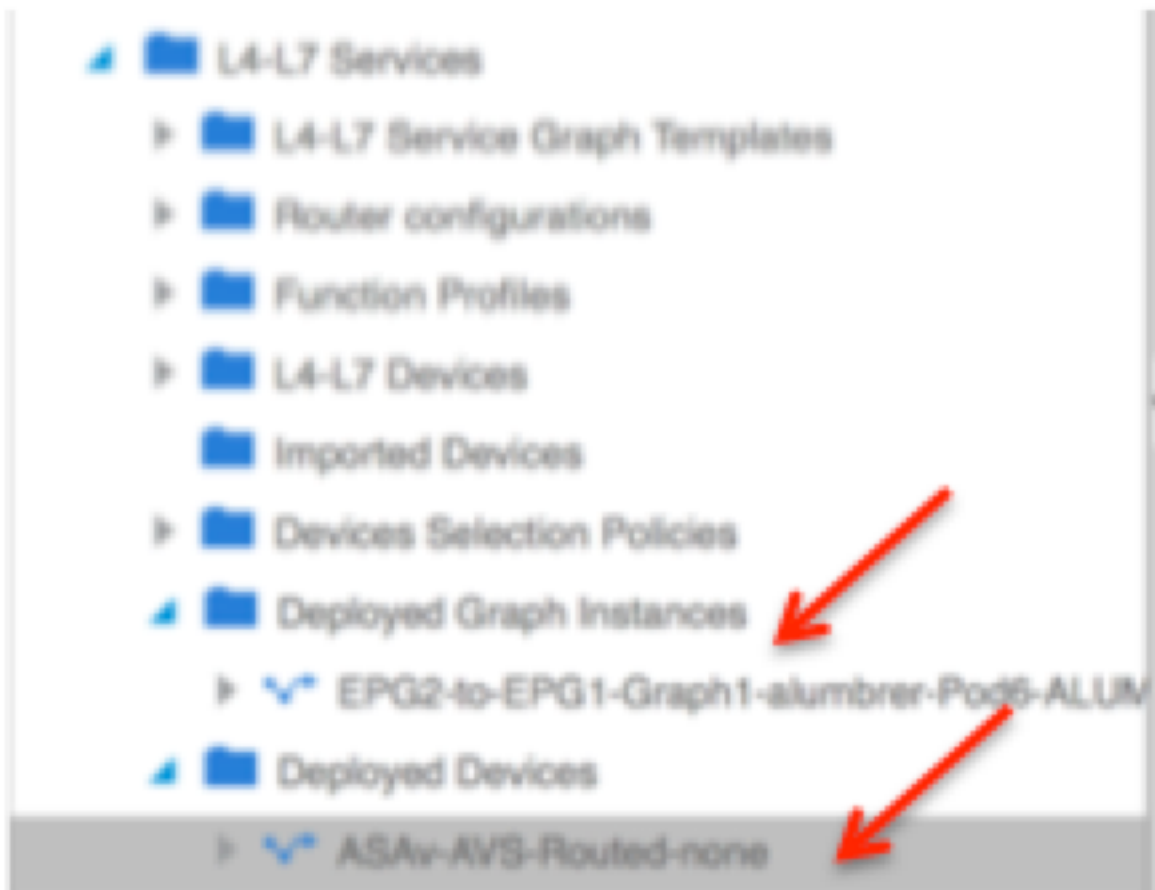
config parameters for the selected device

Profile Name: FunProf-ASA

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

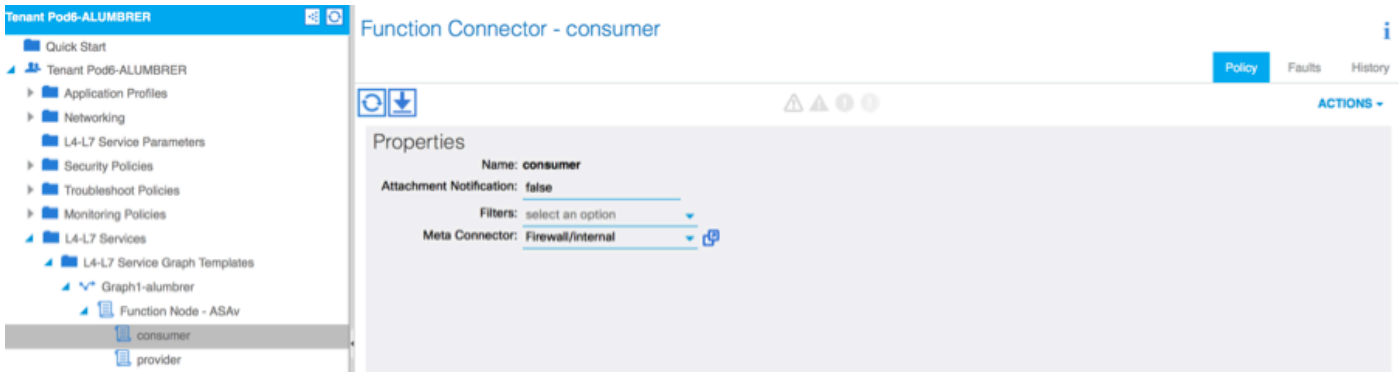
RED indicators parameters needed to be updated and GREEN indicates parameters will be submitted to the provider EPG.

- Se tutto va bene, dovrebbero essere visualizzati un nuovo dispositivo distribuito e una nuova istanza di Graph.

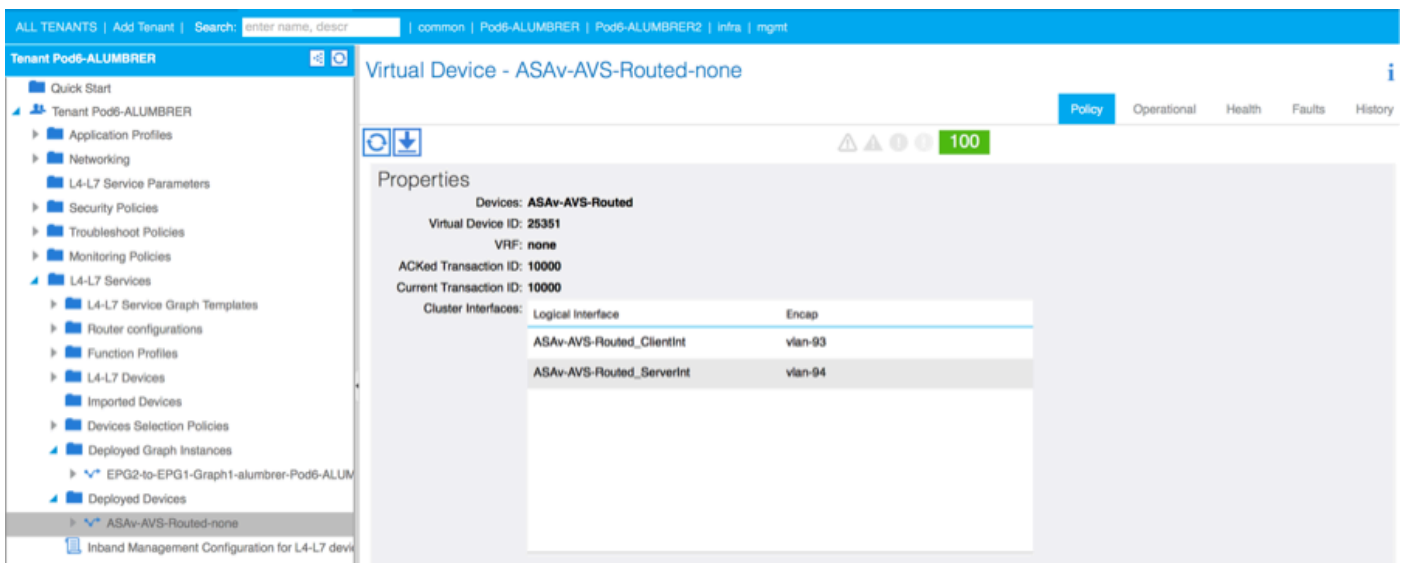


Verifica

- Una cosa importante da verificare dopo la creazione del grafico dei servizi è che la relazione tra consumer e provider è stata creata con un Meta Connector appropriato. Verificare in Proprietà connettore funzione.



Nota: A ciascuna interfaccia del firewall verrà assegnata una vlan di accesso (encap-vlan) dal pool dinamico AVS. Verificare che non vi siano errori.



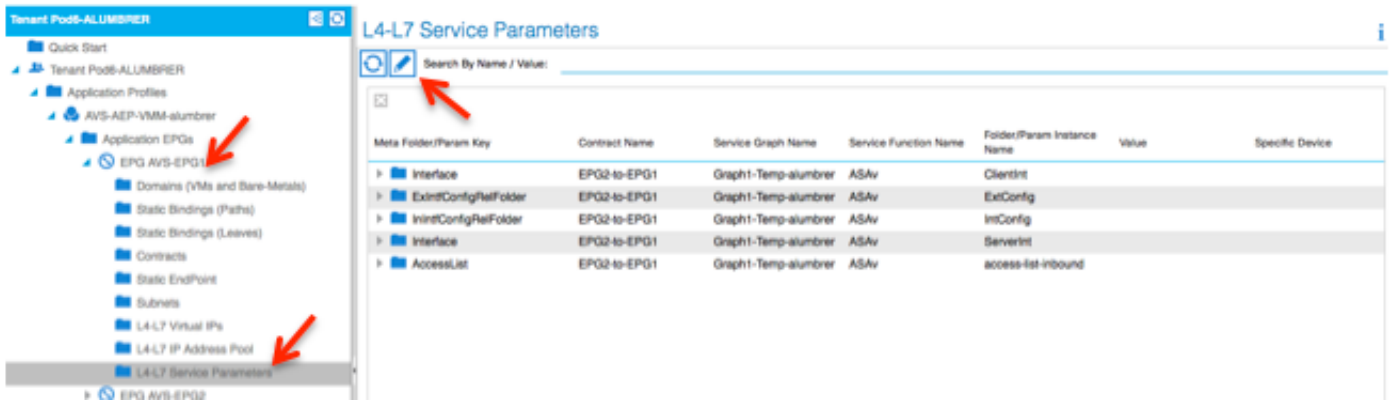
- A questo punto, è possibile anche verificare le informazioni inviate all'appliance ASAv

```

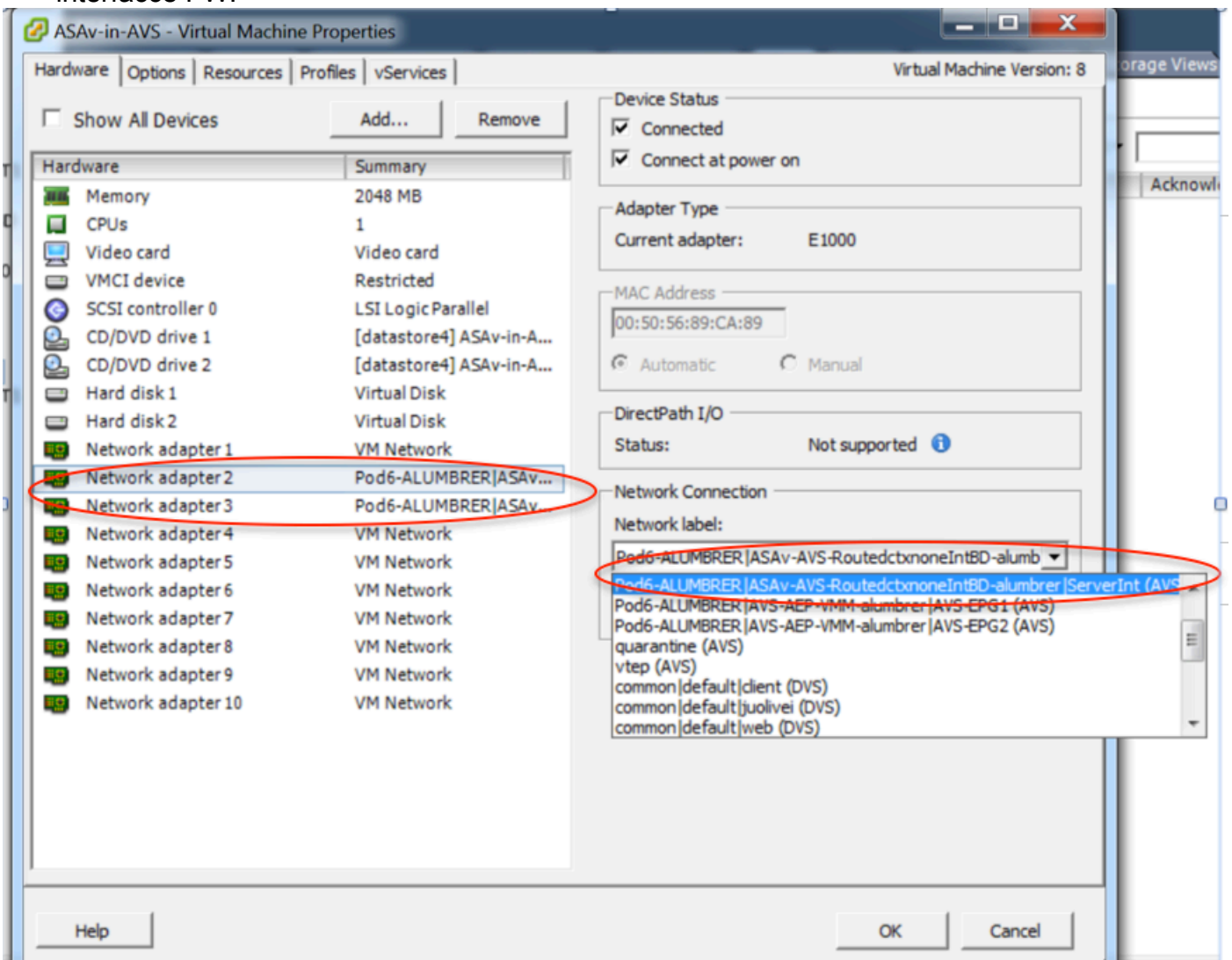
ASA0-W-AUS# show interface ip brief
Interface          IP-Address      OK? Method Status      Prot
ocol
GigabitEthernet0/0 192.168.10.1    YES manual  up          up
GigabitEthernet0/1 172.16.1.1     YES manual  up          up
GigabitEthernet0/2 unassigned      YES unset   administratively down up
GigabitEthernet0/3 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#

```

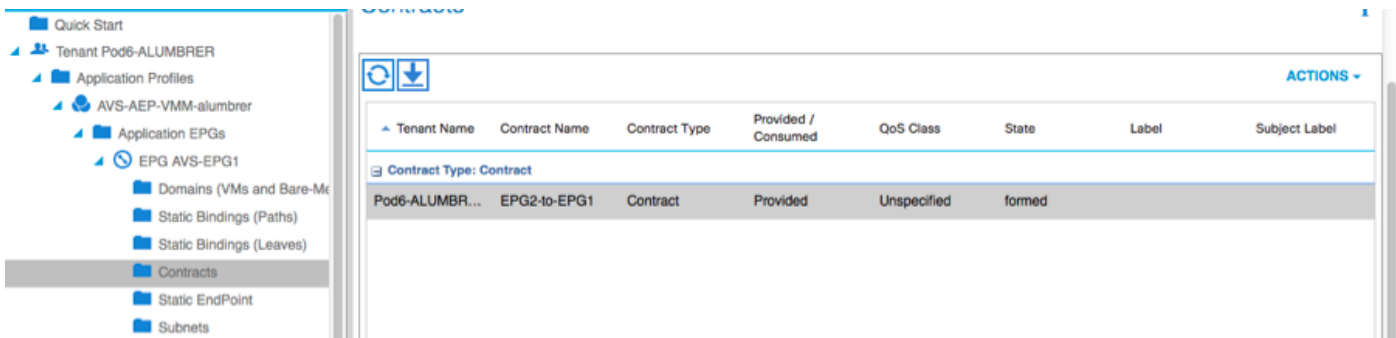
- Un nuovo contratto è assegnato nell'ambito degli EPG. D'ora in poi, se è necessario modificare qualcosa sull'elenco degli accessi, la modifica deve essere effettuata dai parametri del servizio L4-L7 del provider EPG.



- Su vCenter, è inoltre possibile verificare che gli EPG shadow siano assegnati a ciascuna delle interfacce FW:



Per questo test, avevo i 2 EPG che comunicavano con contratti standard, questi 2 EPG sono in domini diversi e VRF diversi, quindi il percorso che perdeva tra di loro era stato precedentemente configurato. Ciò semplifica un po' le operazioni successive all'inserimento del grafico del servizio, poiché il firmware imposta il routing e il filtraggio tra i 2 EPG. La DG precedentemente configurata nell'ambito dell'EPG e di BD può ora essere rimossa come i contratti. Solo il contratto spinto dall'L4-L7 dovrebbe rimanere sotto gli EPG.



Quando si rimuove il contratto standard, è possibile confermare che il traffico ora scorre attraverso l'ASAv. Il comando show access-list deve visualizzare il numero di accessi alla regola, in modo da aumentare ogni volta che il client invia una richiesta al server.

```

ASA# 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#
  
```

Nell'ultima parte è necessario apprendere gli endpoint per le VM client e server e le interfacce ASAv

```

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                                   vlan-98         0050.5689.f008 L          eth1/7
Pod6-ALUMBRER:VRF1-alumbrer      Server IP & MAC  vlan-98         192.168.10.10 L          FW
25                                   vlan-94         0050.5689.ca89 L          interface
Pod6-ALUMBRER:VRF1-alumbrer      (ServerInt
mgmt:inb                             192.168.2.11 S          )
21                                   vlan-97         0050.5689.3fca L          eth1/7
Pod6-ALUMBRER:VRF2      Client IP & MAC  vlan-97         172.16.1.10 L
26                                   vlan-93         0050.5689.e7dd L          po4
Pod6-ALUMBRER:VRF2      vlan-93         172.16.1.1 L
overlay-1                     10.0.104.93 L          FW
overlay-1                     10.0.96.67 L          interface
13                             vxlan-16777209 0050.5677.18a5 H          (ClientInt)
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
  
```

vedere entrambe le interfacce firewall collegate a VEM.

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		

```
~ #
```

Infine, le regole del firewall possono essere verificate anche a livello foglia se si conoscono i tag PC per gli EPG di origine e destinazione:

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

Gli ID filtro possono essere abbinati ai tag PC sulla foglia per verificare le regole FW.


```
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#
```

Nota: Le classi PCT/Sclass EPG non comunicano mai direttamente. La comunicazione viene interrotta o legata tramite gli EPG shadow creati dall'inserimento del grafico del servizio L4-L7.

E la comunicazione tra client e server funziona.

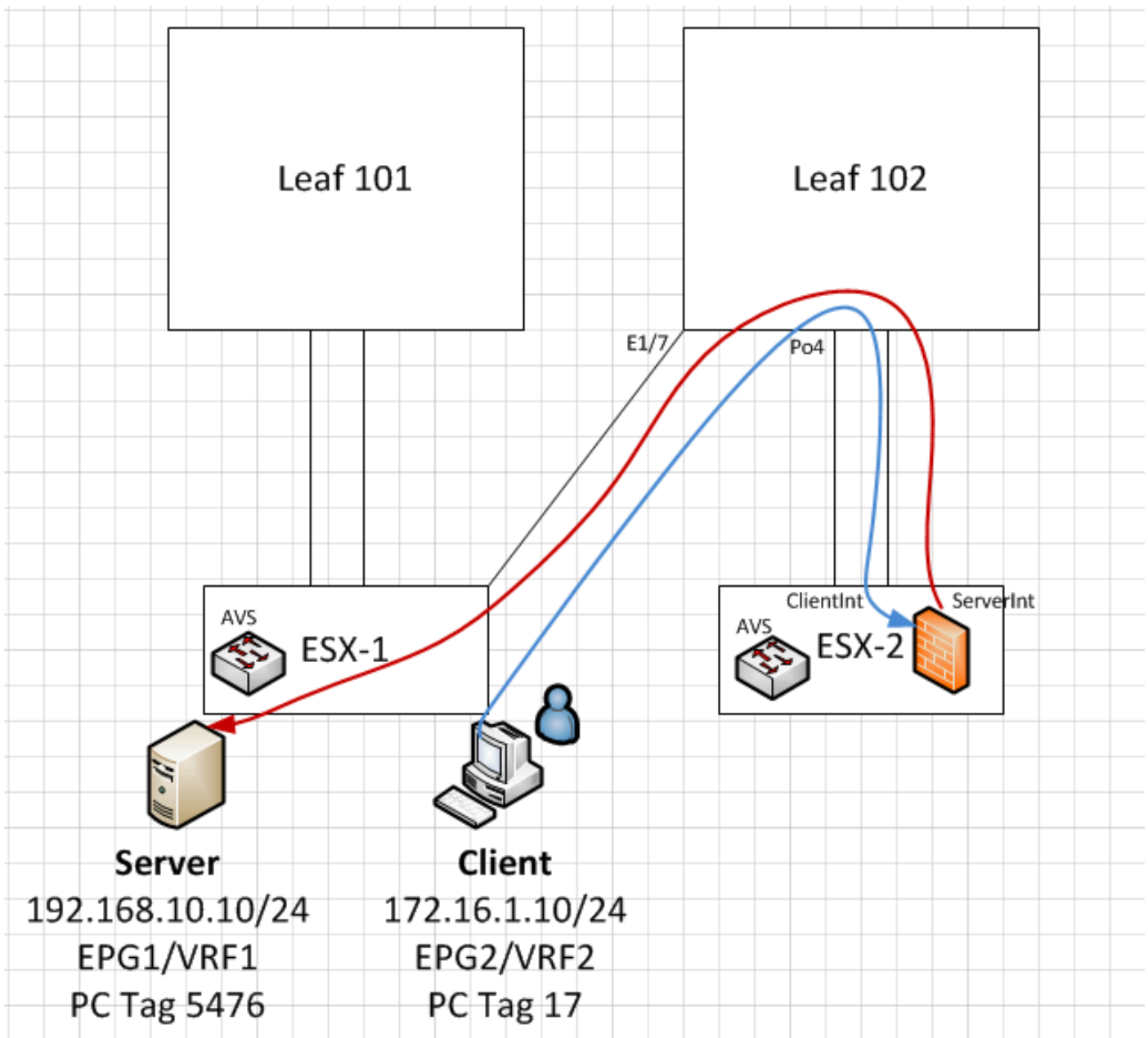
```
cisco@cisco-UbuntuClient:~$ ifconfig
eth1      Link encap:Ethernet  HWaddr 00:50:56:89:3f:ca
          inet addr:172.16.1.10  Bcast:172.16.1.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe89:3fca/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        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

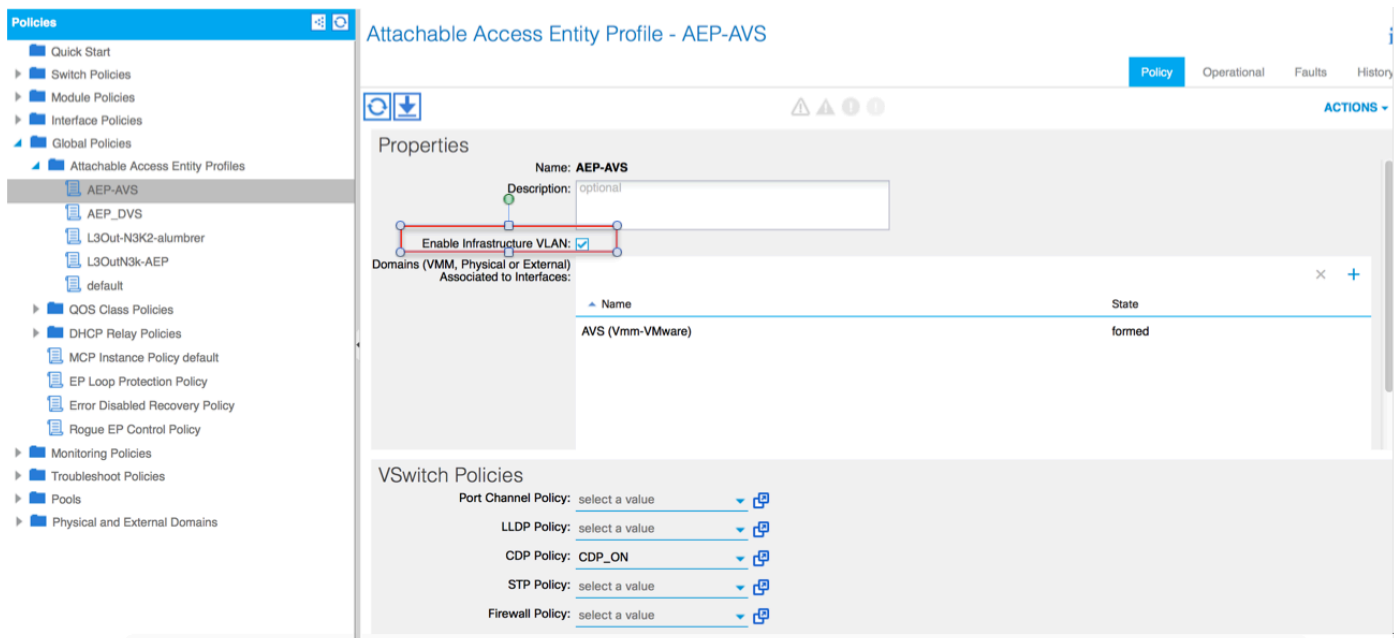
Last login: Mon Feb  1 10:14:11 2016 from 172.16.1.10
cisco@cisco-UbuntuClient:~$ $
```



Risoluzione dei problemi

Indirizzo VTEP non assegnato

Verificare che la Vlan di infrastruttura sia controllata in AEP:



Versione non supportata

Verificare che la versione VEM sia corretta e che supporti il sistema ESXi VMWare appropriato.

```
~ # 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
```

Comunicazione VEM e fabric non funzionante

- Check VEM status

```
vem status
```

- Try reloading or restating the VEM at the host:

```
vem reload
vem restart
```

- Check if there's connectivity towards the Fabric. You can try pinging 10.0.0.30 which is (infra:default) with 10.0.0.30 (shared address, for both Leafs)

```
~ # vmkping -I vmk1 10.0.0.30
PING 10.0.0.30 (10.0.0.30): 56 data bytes
```

```
--- 10.0.0.30 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
```

If ping fails, check:

- Check OpFlex status - The DPA (DataPathAgent) handles all the control traffic between AVS and APIC (talks to the immediate Leaf switch that is connecting to) using OpFlex (opflex client/agent).

```
All EPG communication will go thru this opflex connection. ~ # vemcmd show opflex
Status: 0 (Discovering) Channel0: 0 (Discovering), Channel1: 0 (Discovering)
Dvs name: comp/prov-VMware/ctrlr-[AVS]-vCenterController/sw-dvs-129
Remote IP: 10.0.0.30 Port: 8000 Infra vlan: 3967
FTEP IP: 10.0.0.32 Switching Mode: unknown Encap Type: unknown NS GIPO: 0.0.0.0
you can also check the status of the vmnics at the host level:
~ # esxcfg-vmknic -l
Interface Port Group/DVPort IP Family IP Address Netmask Broadcast MAC Address MTU TSO MSS Enabled Type vmk0
```

```

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

```

A questo punto è possibile determinare che la comunicazione Fabric tra l'host ESXi e il Leaf non funziona correttamente. Alcuni comandi di verifica possono essere controllati sul lato foglia per determinare la causa principale.

```
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)

```

Esistono 2 porte utilizzate in ESXi collegate tramite Po5

```
leaf2# show vlan extended
```

VLAN	Name	Status	Ports
13	infra:default	active	Eth1/1, Eth1/20
19	--	active	Eth1/13
22	mgmt:inb	active	Eth1/1
26	--	active	Eth1/5, Eth1/6, Po5
27	--	active	Eth1/1
28	::	active	Eth1/5, Eth1/6, Po5
36	common:pod6_BD	active	Eth1/5, Eth1/6, Po5

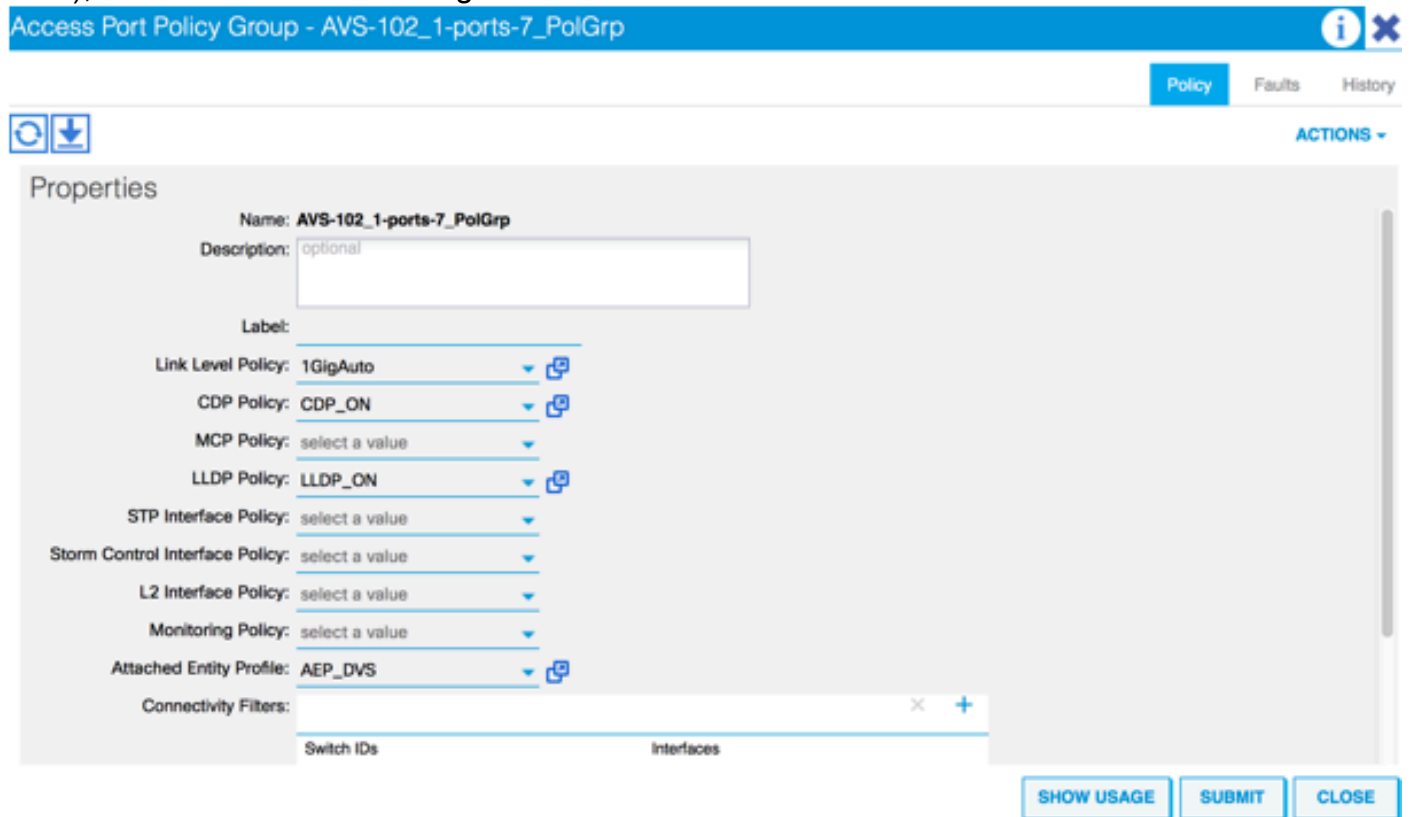
VLAN	Type	Vlan-mode	Encap
13	enet	CE	vxlan-16777209, vlan-3967
19	enet	CE	vxlan-14680064, vlan-150
22	enet	CE	vxlan-16383902
26	enet	CE	vxlan-15531929, vlan-200
27	enet	CE	vlan-11
28	enet	CE	vlan-14
36	enet	CE	vxlan-15662984

Dall'output sopra riportato si può osservare che la Vlan ad infrarossi non è consentita né passata attraverso le porte Uplink che vanno all'host ESXi (1/5-6). Ciò indica una configurazione errata con i criteri di interfaccia o di switch configurati su APIC.

Selezionare entrambe le opzioni:

Criteri di accesso > Criteri interfaccia > Criteri di accesso profili > Cambia criteri > Profili

In questo caso, i profili dell'interfaccia sono collegati all'AEP errato (vecchia AEP utilizzata per DVS), come mostrato nell'immagine:



Dopo aver impostato l'AEP corretta per l'AVS, ora possiamo vedere che l'Infra Vlan è vista attraverso gli Scollegamenti appropriati in corrispondenza della Foglia:

```
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
```

Informazioni correlate

Installazione switch virtuale applicazione

[Guida all'installazione di Cisco Application Virtual Switch, Cisco Systems, Inc., versione 5.2\(1\)SV3\(1.2\)](#)

Distribuire ASAv utilizzando VMware

[Guida introduttiva di Cisco Systems, Inc. Cisco Adaptive Security Virtual Appliance \(ASAv\), 9.4](#)

Cisco ACI e Cisco AVS

[Cisco Systems, Inc. Cisco ACI Virtualization Guide, versione 1.2\(1i\)](#)

White paper sulla progettazione di Service Graph con infrastruttura Cisco incentrata sulle applicazioni

[White paper sulla progettazione di Service Graph con infrastruttura Cisco incentrata sulle applicazioni](#)

[Documentazione e supporto tecnico – Cisco Systems](#)