# 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:

- Èpossibile 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 VLAN.
- 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:

eate vCenter Domain					i
Specify vCenter domain users and co	ontrollers				
Virtual Switch Name:	AVS	_			
Virtual Switch:	VMware vSphere Dis	stributed Switch	Cisco AVS		
Switching Preference:	No Local Switching	Local Switching			
Encapsulation:	VLAN VXLAN		_		
Associated Attachable Entity Profile:	AEP-AVS	•	æ		
VLAN Pool:	VlanPool-AVS(dynami	c) 🗸	æ		
Security Domains:			× +		
	Name	Description			
vCenter Credentials:				×	+
	Profile Name	Username	Description		
	vCenterCredentials	root			
vCenter:				×	+
	Name	IP	Туре	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)

Inventory 🔄 🖸	Portgroup - vtep					i
Quick Start     Microsoft						General Faults History
CopenStack	⊙₹					
A () AVS	Properties					
Controllers     VCenterController	Name: Encap:	vtep vtan-3967				
Hypenvisors	Management Network Adapters:	Server Name	Name	State	MAC	IP Address
ID:201.35.218		10.201.35.219	vmkt	Up	00:50:56:68:CA.25	10.0.16.95
▶ □ 10.201.35.219		10.201.35.218	vmk1	Up	00:50:58:61:07:CC	10.0.16.94
DVS - AVS						$\sim$
Portgroups						
PO08-ALUMBRERIAVS-AEP-VMM-a	4					
<ul> <li>P III. uplink</li> </ul>						
⊨ 11 vtep						
▶ () DVS	1					
		(   Page 1 0/1		Objects Per	Propr. 15 💌	Displaying Objects 1 - 2 Of 2

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

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

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:

CiscoAVS_1.10-5	i.2.1.SV3.1.10			
		Q Searc	h	
Name	Date Modified	Date Created	Size	Kind
License_Copyright_Document.pdf	Dec 9, 2015, 12:10 AM	Dec 9, 2015, 12:10 AM	1 MB	PDF Doc
README.txt	Dec 9, 2015, 12:10 AM	Dec 9, 2015, 12:10 AM	2 KB	text
cross_cisco-vem-v250-5.2.1.3.1.10.0-3.1.1.vib	Dec 9, 2015, 12:10 AM	Dec 9, 2015, 12:10 AM	8.9 MB	Unix E
Cross_cisco-vem-v250-5.2.1.3.1.10.0-3.2.1.vib	Dec 9, 2015, 12:10 AM	Dec 9, 2015, 12:10 AM	9 MB	Unix E
cross_cisco-vem-v250-5.2.1.3.1.10.0-6.0.1.vib	Dec 9, 2015, 12:10 AM	Dec 9, 2015, 12:10 AM	9 MB	Unix E
VEM510-201512250107-BG-release.zip	Dec 9, 2015, 12:10 AM	Dec 9, 2015, 12:10 AM	8.5 MB	ZIP arch
VEM550-201512250113-BG-release.zip	Dec 9, 2015, 12:10 AM	Dec 9, 2015, 12:10 AM	8.6 MB	ZIP arch
VEM600-201512250119-BG-release.zip	Dec 9, 2015, 12:10 AM	Dec 9, 2015, 12:10 AM	8.6 MB	ZIP arch

 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

<pre>~ # esxcli software vib install -v /vmfs/volumes/datastore1/cross_cisco-vem-v250-5.2.1.3.1.10.0-3.2.1.vibmaintenance-modeno-sig-check Installation Result Message: Operation finished successfully. Reboot Required: false VIBs Installed: Cisco_bootbank_cisco-vem-v250-esx_5.2.1.3.1.10.0-3.2.1 VIBs Removed: Cisco_bootbank_cisco-vem-v197-esx_5.2.1.3.1.5.0-3.2.1 VIBs Skipped: ~ # vem status</pre>						
VEM modules are	loaded					
Switch Name ∨Switch0 DVS Name DVS	Num Ports 5632 Num Ports 5632	Used Ports 8 Used Ports 10	Configured Ports 128 Configured Ports 512	MTU 1500 MTU 9000	Uplinks vmnic0 Uplinks vmnic5,vmnic4	
VEM Agent (vemdpa) is running ~ # ■						

 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:

			6-W	10
lect Host and Physical Adapters	Host/Dhusical adaptate	To use by switch	Settings	View Incompatible H
ual Machine Networking		an use by switch	View Dataile	opinikportgroup
ady to Complete	Select physical adapters		View Decalis	
		vSwitch0	View Details	uplink
	vmnic1		View Details	uplink
	vmnic10		View Details	uplink
	vmnic11		View Details	uplink
	vmnic2		View Details	uplink
	vmnic3		View Details	uplink
	vmnic4	DVS	View Details	uplink
	vmnic5	DVS	View Details	uplink
	Vmnic6		View Details	uplink
	vmnic7		View Details	uplink
	vmnic8		View Details	uplink
	vmnic9	**	View Details	uplink

- 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:

Fabri	c VM Networking	g L4-L7 Services	Admin	Operations	
		Inventory   Packages			
Quick	Start				
HEL The Pa balanc and ne You ca configu	P ickages menu allows you to er, context switch, SSL term twork connectivity information n use the <b>Import a Device I</b> iring a service graph.	import L4-L7 device pack ination device, or intrusion on for each function. A net Package wizard to import	ages, which are us prevention system work service device a device package fi	ed to define, configure, and mo a (IPS). Device packages conta a is deployed in the network by for a function that you want to m	onitor a network service in descriptions of the fu adding it to a service g nanage with APIC. We
Q	uick Start	File Name:		BROWSE	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:

SUBMIT

CLOSE

i

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

				General	Operational	Faults	History
⊙₹						ACT	TIONS -
Properties							
Vendor:	cisco						
Model:	ASA						
Capabilities:	GoThrough,GoTo						
Major Version:	1.2						
Minor Version:	4.8						
Minimum Required Controller Version:	1.1						
Logging Level:	DEBUG	•					
Package Name:	device_script.py						
Supported Protocols:							
Interface Labels:	<ul> <li>Name</li> </ul>						
	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 ASAv. Ricordarsi di usare la gestione OOB per ASAv, 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 2:1/Documents/GSP/ACTI/IMAGE/asav/952/asav-vi.ovf      rowse Enter a URL to download and install the OVF package from the Internet, or social hard drive, a network share, or a CD/DVD drive.
Help	< Back Next > Cancel

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

#### Properties

Customize the software solution for this deployment.

Sizes       Off Tendata Details         Control Meet License Accessences       Type of deployment.         Sizes       Type of deployment.         Sizes       Sectores         Control Meet Conflocation       Select the type of ASA' host to install. When an HA type deployment is selected, the additional HA         Properties       Standatione         Ready to Complete       Mostname         Mostname       Mostname			
Oxf: Tenckate Details         Modules: Location         Management Configuration         Statistic         Statistic         Concomment Configuration         Statistic         Concomment Configuration         Statistic         Ready to Complete         Hostname         <	Source		
Item Litter Location       Deployment Type         Status       Type of deployment         Status       Sector         Sector       Sector         Management       Mathematic Sector         Management       Interface Settings         Management       Intenterface Settings	OVF Template Details		*
Name:       Type of deployment         Status       Select the type of ASAv host to instal. When an HA type deployment is selected, the additional HA Properties below should also be filed in.         Status       Standaione         Properties       Ready to Complete         Hostname       Hostname         Hostname       Hostname (bits, or a hyphen).         Adave::-AVS       Firewall Properties         Firewall Properties       Firewall Properties         Note:       Name(bits)         Management Interface Settings       Hanagement Interface Settings         Hanagement Interface DHCP mode       Choose whether to use CHOP for Management interface configuration.         10       .01       .05       .01         Hanagement Interface DHCP mode       Choose whether to use CHOP for Management interface configuration.       .01         10       .01       .05       .01       .01         Hanagement IP-4 Address.       For HA-type deployments, this property specifies the Management PP-4 Address of the Active HA host.       .00       .01       .01       .01       .01         Heip        Ketz the HA deces.       For HA-type deployments, this property specifies the Management PP-4 Address of the Active HA host.       .00       .01       .01       .01       .01       .01       .01	End User License Agreement	Deployment Type	
Descurators       Type of displayment         Statual       Statual         Oak Format       Second         Properties       Statual         Ready to Complete       Imagement for this system. A hostname must start and end with a letter or dgit and have as interior characters only letters, dgits, or a hyphen.         Addata       Addata         Imagement Interface Settings         Management Interface Settings         Management IP Address         Choose whether to use DHOP for Management interface configuration.         10 , 201 , 35 , 223         Heip         Meter Line Statue	Name and Location		
Select the type of ASAv has to install. When an HA type deployment is selected, the additional HA Properties Biow should also be filed in. Standards Properties Ready to Complete Hostname Hostn	Deployment Configuration	Type of deployment	
Disk format       Properties below should also be filed n.         Standalone       Image: Imag	Storage	Select the type of ASAv host to install. When an HA type deployment is selected, the additional HA	
Metadolice         Standalone         Properties         Ready to Complete         Hostname         Hostname filter         Hostname filter         Hostname filter         Adaracters only letters, digits, or a hyphen.         Management Interface Settings         Hanagement Interface OHCP mode         Choose whether to use DHCP for Management interface configuration.         Imagement IP-4 Address.         Enter the Management IP-4 Address. For HA-type deployments, this property specifies the Management IP-4 Address of the Active HA host.         Inter the Management IP-4 Address.         Hanagement IP-4 Address.         Hanagement IP-4 Address.         Hanagement IP-4 Address.         Management IP-4 Address.         Management IP-4 Eddress.         Management IP-4 Eddress.         Management IP-4 Eddress.         Management IP-4 Eddress.         <	Disk Format	Properties below should also be filled in.	1
Properties         Ready to Complete         Hostname         Hostname         Hostname for this system. A hostname must start and end with a letter or digit and have as interior characters only letters, digits, or a hyphen.         ASAv-en-AVS         Firewall Properties         Firewall Mode         Select the Firewall Mode         Foulted         Management Interface Settings         Management Interface Settings         Management Interface Settings         Management Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Imagement IP-4 address         Enter the Management IP-4 address of the Active HA host.         10       .201         Heagement IP Subset Hask	Network Mapping	Standalone •	
Ready to Complete       Hostname         Hostname       Hostname         Hostname       Hostname         Hostname       Hostname must start and end with a letter or digit and have as interior characters only letters, digits, or a hyphen.         ASAvrer-Avis       Firewall Properties         Firewall Properties       Firewall Mode         routed       Imagement Interface Settings         Hanagement Interface Settings       Hanagement Interface DHCP mode         Oncose whether to use DHCP for Management interface configuration.       Imagement IP Address         Enter the Management IP-4 Address of the Active HA host.       10 . 201 . 35 . 223         Hanagement IP Subnet Hask       Imagement IP Subnet Hask	Properties		
Hostname         Host name for this system. A hostname must start and end with a letter or digit and have as interior duracters only letters, digits, or a hyphen.         ASAv-m-AVS         Firewall Properties         Firewall Mode         Select the Firewall Mode         routed         Management Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Hanagement IP-V4 Address         Enter the Management EV-4 Address. For HA-type deployments, this property specifies the Management EV-4 Address for the Active HA host.         10       .201         10       .201         Hanagement IP Subnet Hask	Ready to Complete	Hostname	
Hostname         Hostname for this system. A hostname must start and end with a letter or digit and have as interior divaracters only letters, digits, or a hyphen.         ASAv-m-AVS         Firewall Properties         Firewall Mode         Select the Firewall Mode         routed         Management Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Hanagement IP-v4 Address.         Enter the Management IP-v4 Address. For HA-type deployments, this property specifies the Management IP-v4 address of the Active HA host.         10       .201         10       .201         Hanagement IP-Subnet Hask			
Host name for this system. A hostname must start and end with a letter or digit and have as interior characters only letters, digits, or a hyphen.         ASAv-w-AVS         Firewall Properties         Firewall Mode         Select the Prevail Mode         routed         Management Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Hanagement IP Address         Enter the Management SV-4 Address. For HA-type deployments, this property specifies the Management IP-4 Address of the Active HA host.         10       .01         .01       .021         Help          Help		Hostname	
ASAr-w-AVS         Firewall Properties         Firewall Mode         Select the Firewall Mode         routed         Management Interface Settings         Management Interface OHCP mode         Choose whether to use DHOP for Management interface configuration.         Hanagement IP Address         Enter the Management IP Address.         Enter the Management IP-v4 Address. For HA-type deployments, this property specifies the Management IP-v4 Address of the Active HA host.         10       .201         Management IP Subnet Mask         Memory         Address         Management IP Subnet Mask		Host name for this system. A hostname must start and end with a letter or digit and have as interior characters only letters, digits, or a hyphen.	
Firewall Properties         Firewall Mode         Select the Prewall Mode         routed         management Interface Settings         Hanagement Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Hanagement IP-4 Address         Enter the Management IP-4 Address. For HA-type deployments, this property specifies the Management IP-4 Address of the Active HA host.         10       .201         Help       < Back		ASAv-w-AVS	
Help       < Back			
Help       < Back		Firewall Properties	
Select the Firewall Mode         routed         Management Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Imagement IP Address         Enter the Management IP-v4 Address. For HA-type deployments, this property specifies the Management IP-v4 Address of the Active HA host.         ID       .01         Hanagement IP Subnet Hask         Imagement IP Subnet Hask         Imagement IP Subnet Hask         Imagement IP Subnet Hask		Firewall Mode	
Management Interface Settings         Management Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Imagement IP Address         Enter the Management IPv4 Address. For HA-type deployments, this property specifies the Management IPv4 address of the Active HA host.         Imagement IP Subnet Hask         Help            Ket >		Select the Firewall Mode	
Imagement Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Imagement IP Address         Enter the Management IP-v4 Address. For HA-type deployments, this property specifies the Management IP-v4 address of the Active HA host.         10       .201         Hanagement IP Subnet Hask         Ket       Cancel			
Hanagement Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Imagement IP Address         Enter the Management IP v4 Address. For HA-type deployments, this property specifies the Management IP v4 address of the Active HA host.         Imagement IP Subnet Hask         Help            Ket >		routed	
Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Hanagement IP Address         Enter the Management IPv4 Address. For HA-type deployments, this property specifies the Management IPv4 address of the Active HA host.         10       . 201       . 35       . 223         Hanagement IP Subnet Hask		Management Interface Settings	
Help <back< td="">       Next &gt;       Cancel</back<>		Management Interface DHCP mode	
Hanagement IP Address         Enter the Management IP v4 Address. For HA-type deployments, this property specifies the Management IP v4 address of the Active HA host.         10       .201       .35       .223         Hanagement IP Subnet Hask       •              Heip         Cancel		Change whether to use PMCD for Management interface conferenties	
Hanagement IP Address         Enter the Management IPv4 Address. For HA-type deployments, this property specifies the Management IPv4 address of the Active HA host.         10       .201       .35       .223         Hanagement IP Subnet Hask		Choose whether to use CHCP for Management interface configuration.	
Enter the Management IPv4 Address. For HA-type deployments, this property specifies the         Management IPv4 address of the Active HA host.         10       .201       .35       .223         Hanagement IP Subnet Hask		Hanagement IP Address	
Hanagement IPv4 address of the Active HA host.       10 , 201 , 35 , 223       Hanagement IP Subnet Hask       Help       < Back		Enter the Management IPv4 Address. For HA-type deployments, this property specifies the	
10         201         35         223           Hanagement IP Subnet Hask         *		Management IPv4 address of the Active HA host.	
Hanagement IP Subnet Hask       Heip <back< td="">     Next &gt;     Cancel</back<>		10 . 201 . 35 . 223	
Help Kext > Cancel		Management IP Subnet Mask	-
Help <back next=""> Cancel</back>		I an and the second sec	
Help < Back Next > Cancel			
	Help	< Back Next >	Cancel

VF Template	
o Complete hese the options you want to use?	
When you cick Finish, the de	coment task will be started.
Livence Accement Darlowment actions:	and lines or mean rule and and and
Location Gra and sky	1168
Configuration Name:	400 000
Folder	40
Deployment Configuration	1 Chee (ASAv10)
Mast/Cluster	10003(404410)
Prosiçõester:	datastand
mplete Disk scauldinger	Thick Provision I are Torond
Natural Manajar	"Massagements A" to "UN Naturals"
Network Mapping:	"ClashitBharash.d"to "UM Naturd"
Network Mapping	Clashit Bharrath, 17to 3/04 Natural
Network Mapping:	GlashitBharash 7 to 304 Natural
Network Mapping	Clash PErkersets 7"to "Do de al LIMESTE ALE VAM al minimular
Network Manajary	"Clashittherest d"to "bade to INBOED latere 140, 1000 alumber
Network Mapping:	"ClashitBharash. E"to "Pool-ALUMOREX Jacemerator" annora-
Network Mapping:	Gigeorethemeto-5 to VPI Network
Network Mapping	Gigabitthemeto-6 to VM Network
Network Mapping:	GigabitEtherneto-7 to VM Network
Network Mapping:	Gigabitthemeto-8" to "VM Network"
IP Allocation:	Fixed, JPv4
Property:	HARole = Standalone
Property:	Hostname = ASAv-w-AV5
Property:	PWMode = routed
Property:	DHCP = Faise
Propertys	ManagementIPv4 = 10.201.35.223
Propertys	ManagementIPv4Subnet = 255.255.255.0
Property:	ManagementStandby3Pv4 = 0.0.0.0
Property:	RouteDefault = Default Route +
E annual data	
Power on after deployment	4
	< Back Finish 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 ntu management 1500 no failover icmp unreachable rate-limit 1 burst-size 1 no asdm history enable arp timeout 14400 no arp permit-nonconnected oute management 0.0.0.0 0.0.0.0 10.201.35.1 1 timeout xlate 3:00:00 timeout pat-xlate 0:00:30 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute timeout tcp-proxy-reassembly 0:01:00 timeout floating-conn 0:00:00 More --->

 Come mostrato nell'immagine, alcune configurazioni di gestione sono già state trasferite al firewall ASAv. 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

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

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

#### abilitazione server http

gestione http 0.0.0.0.0.0.0

#### L4-L7 per l'integrazione ASAv 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

1 1 1 1

Create L4-L7 Device.	5						
STEP 1 > General					1. General 2. Device	Configura	ation
Please select device	package and enter connectivity info	rmation.					
General Managed: Name:	ASAv-AVS-Routed	Device 1 Management IP Address:	10.201.35.3		Management Port: https		<u>-</u>
Service Type:	Firewall	Device Interfaces:	VCenterController/AS			x +	
Device Type: VMM Domain:	PHYSICAL VIRTUAL AVS	Device menaces.	Name GigabitEthernet0/0	VNIC Network adapter 2	Path (Only For Route Peering) Node-102/MAC_Pinning	~ 1	-
Mode:	Single Node		GigabitEthemetori	Network adapter 3	Node-Tu2/MAG_Pinning		
Device Package:	CISCO-ASA-1.2 👻 🗗						
Model:	ASAv						
Function Type:	GoThrough GoTo	Cluster					
		Management IP Address:	10.201.35.3		Management Port: https		<u>_</u>
		Cluster Interfaces:				× +	_
			Туре	Name	Concrete Interfaces		
Connectivity			provider	Serverint	Device1/GigabitEthemet0/0		
APIC to Device Management Connectivity:	⊚ Out-OI-Band ⊝ In-Band		consumer	ClientInt	Device1/GigabitEthernet0/1		
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 **Llf** (leaf interface, ad esempio external, internal, inside, ecc.) e l'interfaccia **Clf** (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

+-L7 Devices - ASAV-AVS-Houled						1
				Policy F	Parameters Faults	History
<b>★</b>					AC	TIONS -
eneral Managed: Name: ASAv-AVS-Routed Device Package: CISCO-ASA-1.2 Servico Type: Firewall Device Type: VIRTUAL VMM Domain: AVS ✓ Context Aware: Single Function Type: GoThrough GoTo	Device 1 Management IP Address: vCenter Name: Interfaces:	10.201.35.223 vCenterController Name GigabitEthemet0/1 GigabitEthemet0/2	Managem Vilic Network add	nent Part: 643 M Name: ASAv-in-A apter 3 apter 4	Path (Only For Route Pe Node-102/MAC_Pinnin Node-102/MAC_Pinnin	x + aring) g. Nod g
Cluster Mode: Single Node edentials Username: admin Password:	Cluster Management IP Address: Cluster Interfaces:	10.201.35.223	Managem	ent Port: 443	•	× +
Confirm Password:		Туре	· Neme	ASAv-AVS-Rout	ed Device 1/(GigabitEth	0met0/21
Configuration State	<	provider	Serverint	ASAv-AVS-Rout	ed_Device_1/(GigabitEth	ernet0/1]

**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

#### Tempio 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:

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

Create L4-L7 Services Fu	nction Profile	Group		0×		
Specify the information ab	out the Function	on Profile Group				
Name: FunP Description:	rofGroup					
			SUBMIT	ANCEL		
Tenant Pod6-ALUMERER	L4-L7 Services F	unction Profile Group	- FunProGroup			i
Tenant Pode-ALUMERER     Application Profiles     Metworking	⊙₹					ACTIONS -
L4-L7 Service Parameters     Security Policies     Troubleshoot Policies     Monitorion Policies	Properties Name: Description: Service Function Profiles:	FunProGroup				
L4-L7 Services      L4-L7 Service Graph Templates		- Name	Associated Function	Description		× +
	nction Photle		2	No items have been found elect Actions to create a new	L Barn.	

 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.x/y.y.y o x.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	U	
	In order to auto apply new values to the parameters of existing graph instance when users modify function profiles	s, the name of top folder must be ended with -Default.
Features:	Basic Parameters All Parameters	
Interfaces	Folder/Param Name Value Mandatory	Locked Shared
Accession	E 🖌 🖼 Device Config Device	
AccessLists	Bridge Group Interface	
NAT	📰 😑 🛛 🔺 🔤 Interface Related Configuration externallf	false false
<b>TrafficSelectionObjects</b>	KACcess Group     ExtAccessGroup	false
All	IPv6 Enforce EUI-64	
	Interface Specific Configur externallfCfg	false
	IPv4 Address Configura	
	IPv4 Address Ipv4_address 192.168.10.1/24	
	Pv4 Standby Address	
	IPv6 Address Configura	
	IPv6 Link Local Address	
		SUBMIT

**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: FunPr	rof-ASA							
Description: option	nal							
Copy Existing Profile Parameters: 🔽								
Profile: CISC	O-ASA-1.2/Webl	PolicyFo	orRoutedMode	<u> </u>				
- Features and Parameters								
	In order to aut	o apply r	new values to the paramete	ers of existing graph i	nstance when users	modify function profiles, th	he name of top folde	r must be ended with -Default.
Features:	Basic Parame	eters	All Parameters					
Interferen	Folder	/Param		Name	Value	Mandatory	Locked	Shared
Interraces	8	-	Destination Service	destination_serv	rice			
AccessLists			High Port					
NAT			Low Port	low_port	22		false	
TrafficSelectionObjects			Operator	operator	eq		false	
All		•	ICMP					
		P 4	Logging					
			Source Service					
			Action	action	permit		false	
	R		Order	order	30		false	

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

Tenant Pod6-ALUMBRER	S 0	L4-L7 Service (
Quick Start		
Tenant Pod6-ALUMBRER		
Application Profiles		⊖±
Networking		Name
L4-L7 Service Parameters		<ul> <li>Name</li> </ul>
Security Policies		
Troubleshoot Policies		
Monitoring Policies		
4 💼 L4-L7 Services		
L4-L7 Service Graph Templates	<b>1</b>	
Router configurations	Create L4-L7	Service Graph Template

• 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:	Graph1-alumbrer		
Graph Type:	Create A New One	Clone An Existing One	
Consumer (EPG)		C ASAv-AVS ASAv	Provider EPG
	Please drag a dev	vice from devices table and drop it here to create a service node.	
ASAv-AVS-Rou	ted Information		
Firewall:	Routed	t	
Profile:	Pod6-ALUMBRER/FunProfGroup/FunPr	ro <sup>,</sup> 👻 🗗	
			SUBMIT CANCEL

- 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

Tenant Pod6-ALUMBRER		⊴ ⊙	1 4-1 7 Service	Graph Tem	nlate - Granh1-ali	Imbrer				
Cuick Start			24 27 001100	andphi long	plate Graphi an					1
Tenant Pod6-ALUMBRER								Topology	Policy Fa	ults History
Application Profiles			O							
Networking			Canada						Drawldor	
L4-L7 Service Parameters			Consul	ner					Provider	
Security Policies			( EPG			C P	1		-	
Troubleshoot Policies			(a)			ASAv-AVS			3	
Monitoring Policies										
L4-L7 Services						ASAv				
🔺 🚞 L4-L7 Service Graph Templa	ntes									
4 💙 Graph1-alumbrer				outed Information						
Function Node - ASA	•	Apply L4-L7 Ser	vice Graph Template	II: Routed						
Router configurations		Edit L4-L7 Servi	ce Graph Template	:: FunPro-ASA						
Function Profiles	×	Delete								
🔺 🕎 FunProtGroup		Remove Relate	d Objects Of Graph Template							
FunPro-ASA	Ψ	Save as								
L4-L7 Devices		Doet								
ASAv-AVS-Routed		POSt								
I ASAV-DVS										
Imported Devices										
Devices Selection Policies										
Deployed Graph Instances										
Deployed Devices										
🛄 Inband Management Configu	uration	for L4-L7 devi								
https://10.201.35.211/#								SHOW USAGE	SUBMIT	RESET

- 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 Net	work: Pod6-ALUMBRER/AVS-AEP-VMM 👻 📴	\$
	Pod6-ALUMBRER/AVS-AEP-VMM-	
Contract Information	alumbrer/epg-AVS-EPG1	
Contract:      Create A New Contract     Choose An Existing Contract Subject	Pod6-ALUMBRER/InternalAEP-	
Contract Name: EPG2-to-EPG1	VMM-alumbrer/epg-EPG-Internal- alumbrer	
	Pod6-ALUMBRER/VRF1-alumbrer	
No Filter (Allow All Traffic): 🗹	/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 connetterà 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.

Graph Template:	Pod6-ALUMBRER/Graph1-Temp-alumbrer		- <b>P</b>					
Consumer EPG AVS-EPG2	C	ASAv-/	NS	]	 	{	Provider EPG SS AVS-EPG1	
ASAv-AVS-Routed Infor Firewal Profile Consumer Connector Type: BD: Cluster Interface: Provider Connector – Type: BD: Cluster Interface:	mation : routed : FunPro-ASA General  Route Peering Pod6-ALUMBRER/ExtBD-alumbrer ClientInt General  Route Peering Pod6-ALUMBRER/IntBD-alumbrer ServerInt	• 伊 • 伊 • 伊						
						PREVIOUS	NEXT	CANCE

 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.

file Name: FunPro-ASA	e 🐧				
atures:	Requir	ed Parameters Al Parameters			
		Folder/Param	Name	Value	Write Domain
	8	Access List	access-list-inbound		
AccessLists	E 8	Access Control Entry	ICMP		
NAT		Access Control Entry	\$102		
TrafficSelectionObjects	8	<ul> <li>Access Control Entry</li> </ul>	SSH		
All		Destination Address			
	8	Destination Service	destination_service		
		► 🛄 ICMP			
		Logging			
	8	Protocol	protocol		
		Source Address			
		Source Service			
		El Action	action	permit	
		Crider	order	(M)	select asa domain
		Access Control Entry	UPDATE RESET CA	ANCEL	
	RED I	Action     Action	action order UPDATE RESET C/ GREEN indicates parameters will be summitted to	ancel the provider EPG.	select asa

• Èinoltre 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			
Features:	Required Parameters All Parameters		
Interfaces	Folder/Param	Name Value Write Domain	n
1110110000	😑 🔺 😅 Device Config	Device	
AccessLists	E  Access List	access-list-inbound	
NAT	📰 🔲 🕨 💭 Bridge Group Interface		
TrafficSelectionObjects	E 🛛 🔿 Interface Related Configuration	externalif	
All	😑 🔰 💜 Access Group	ExtAccessGroup	
	Inbound Access List	name access-list-inbound	
	Outbound Access List		
	IPv6 Enforce EUI-64		
	E Interface Specific Configuration	externalIfCfg	
	IPv4 Address Configuration	IPv4Address	
	IPv4 Address	ipv4_address (192.168.10.1/24)	
	IPv4 Standby Address		
	IPv6 Address Configuration		
	IPv6 Link Local Address Configuration		
	🕅 🗖 🕨 🕞 IPvR Router Advertisements		

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

ALL TENANTS   Add Tenant   Search: enter name, descr	common   Pod6-AL	UMBRER   Pod6-ALUMBRER2   infra	mgmt					
Tenant Pod6-ALUMBRER	Virtual Device - A	SAv-AVS-Routed-none						i
Quick Start  A  Tenant Pod6-ALUMBRER  Application Profiles				Policy	Operational	Health	Faults	History
Networking      L4-L7 Service Parameters      Security Policies      Monitoring Policies      Monitoring Policies      L4-L7 Services      L4-L7 Services	Properties Devices: Virtual Device ID: VIR: ACKed Transaction ID: Current Transaction ID:	ASAv-AVS-Routed 25351 none 10000 10000						
Router configurations     Encition Profiles     L4-L7 Devices	Cluster memacos.	Logical Interface ASAv-AVS-Routed_ClientInt ASAv-AVS-Routed_ServerInt	Encep vlan-93 vlan-94					
Imported Devices  Devices Selection Policies  Deployed Graph Instances  V* EPG2-to-EPG1-Graph1-alumbrer-Pod6-ALUM  Deployed Devices  V* ASAv-AVS-Routed-none Inband Management Configuration for L4-L7 device								

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

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

1	🕜 AS	Av-in-AVS - Virtual Machine Pro	perties		
I	Hard	ware Options Resources Profile	es VServices	Virtual Machine Version: 8	orage Views
l	_			Device Status	
I		Show All Devices	Add Remove	Connected	
П	Hard	dware	Summary	Connect at power on	
	-	Memory	2048 MB	- Adapter Tuna	Acknowle
q		CPUs	1	Adapter Type	
		Video card	Video card	Current adapter: E 1000	
٩		VMCI device	Restricted	-MAC Address	
I	0	SCSI controller 0	LSI Logic Parallel	00:50:56:89:04:89	
I		CD/DVD drive 1	[datastore4] ASAv-in-A	00.00.00.00.00	
1		CD/DVD drive 2	[datastore4] ASAv-in-A	C Automatic C Manual	
T		Hard disk 1	Virtual Disk	DirectDath I/O	
I		Hard disk 2	Virtual Disk	DirectPath 1/0	
I		Network adapter 1	VM Network	Status: Not supported U	
	1	Network adapter 2	Pod6-ALUMBRER ASAv	Network Connection	
1		Network adapter 3	Pod6-ALUMBRER ASAv	Network label:	-
I		Network adapter 4	VM Network	Dede stratepop IASAu AVS Deutedeturgens IntPD shund a	
I		Network adapter 5	VM Network	Dade ALL MRDER JASAV-AVS-Routeuctononeintbu-alumb	Tot (AVS
I		Network adapter 6	VM Network	Pod6-ALUMBRER AVS-AEP-VMM-alumbrer AVS-EPG1 (AVS)	INCOAVE
I		Network adapter 7	VM Network	Pod6-ALUMBRER AVS-AEP-VMM-alumbrer AVS-EPG2 (AVS)	=
I	2	Network adapter 8	VM Network	vtep (AVS)	
I	2	Network adapter 9	VM Network	common  default client (DVS)	
I		Network adapter 10	VM Network	common  default juolivei (DVS)	-
I					
I					
I					
I					
I					
1					
		Help		OK Cancel	
1					

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.



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 - locall	y-aged S - sta	tic	
V - vpc-attached p - peer-aged	L - local	M - spa	in	
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	0050.5689.1008 L	FW	eth1/7
Pod6-ALUMBRER:VRF1-alumbrer Server	vlan-98	192.168.10.10 L	interface	
25 & MAC	vlan-94	0050.5689.ca89	(ServerInt	po4
Pod6-ALUMBRER:VRF1-alumbrer	vlan-94	192.168.10.1 L	)	
mgmt:inb		192.168.2.11 S		
21	vlan-97	0050.5689.3fca L		eth1/7
Pod6-ALUMBRER:VRF2	8 vlan-97	172.16.1.10		
26 MAC	vlan-93	0050.5689.e7dd L		po4
Pod6-ALUMBRER:VRF2	vlan-93	172.16.1.1 L		
overlay-1		10.0.104.93		
overlay-1		10.0.96.67 L	FW	
13	vxlan-16777209	0050.5677.18a5 H	interface	unspecified
overlay-1	vxlan-16777209	10.0.32.93 H	(Clientint)	
13	vxlan-16777209	0050.5660.ddab H		unspecified
overlay-1	vxlan-16777209	10.0.32.64 H		

vedere entrambe le interfacce firewall collegate a VEM.

#### ESX-1

10.00	H unrend chew next illen										
~ # V	# Venchia show port vian										
LTL	VSM Port	Admin	Link	State	Cause	PC-LTL	SGID	ORG	svcpath	Туре	Vem Port
22	Eth1/5	UP	UP	FWD	-	1040	4	0	0		vmnic4
23	Eth1/6	UP	UP	FWD		1040	5	0	0		vmnic5
50		UP	UP	FWD	-	0	4	0	0		vmk1
51		UP	UP	FWD	-	0	4	0	0		ASAv-in-AVS.eth1
52		UP	UP	FWD	-	0	4	0	0		ASAv-in-AVS.eth2
1040	Pol	UP	UP	FWD		0	_	0	0		

ESX-2

~ # ve	# vemcmd show port vlan										
LTL	VSM Port	Admin	Link	State	Cause	PC-LTL	SGID	ORG	svcpath	Туре	Vem Port
24	Eth1/7	UP	UP	FWD		1040	6	0	0		vmnic6
50		UP	UP	FWD	-	0	6	0	0		vmk1
51		UP	UP	FWD	-	0	6	Ø	0		Client1-AVS.eth0
52		UP	UP	FWD	-	0	6	0	0		Server1-AVS.eth0
1040	Pol	UP	UP	FWD	-	0		0	0		
~ #											

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					Policy C	perational Stats	Health Faults Hist	ory
Application Profiles AVS-AEP-VMM-alumbrer					Ass	ociated EPGs A	ssociated External Routed Netwo	rics
A Popleation EPGs	⊙±						ACTIONS	•
FO EPG AVS-EPGT b S EPG AVS-EPG2	TABITE	Description	State	Issues	QoS	Encep	PC Teg	
> deg EPOs	AVS-EPG1		applied		Unspecified		17	
L4-L7 Service Parameters	EPG-Internal-alumbrer		applied		Unspecified		32772	
InternalAEP-VMM-alumbrer								
Networking								
Bridge Domains								
VRFs	1							
VRF1-alumbrer								
VRF2								



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

leaf2# show zo	<u>ning-rule  </u>	grep '17\15476'					
4141	17	32775	default	enabled	2916352	permit	<pre>src_dst_any(5)</pre>
4142	32775	17	default	enabled	2916352	permit	<pre>src_dst_any(5)</pre>
4139	5476	49156	14	enabled	2555904	permit	<pre>src_dst_any(5)</pre>
4140	49156	5476	14	enabled	2555904	permit	<pre>src_dst_any(5)</pre>
leaf2#							

**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:255.255.255.6
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: <u>1</u> 1 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:

Policies 🔄 🖸	Attachable Access En	ntity Profile - AEP-AVS		
Quick Start		,		1
Switch Policies			Policy Operation	al Faults History
Module Policies		A A O O		ACTIONS -
Interface Policies		E # 0 0		
Global Policies	Properties			
Attachable Access Entity Profiles	Name:	AEP-AVS		
📜 AEP-AVS	Description:	: optional		
AEP_DVS	a I			
L3Out-N3K2-alumbrer	Enable Infrastructure VLAN:			
L3OutN3k-AEP	Domains (VMM, Physical or External)			
📃 default	Associated to Interfaces:			× +
QOS Class Policies		A Name	State	
DHCP Relay Policies		AVS (Vmm-VMware)	formed	
MCP Instance Policy default				
EP Loop Protection Policy				
Error Disabled Recovery Policy				
Rogue EP Control Policy				
Monitoring Policies				
Troubleshoot Policies	VSwitch Policies			
Pools	Port Channel Policy:	select a value 🗸 🔽		
Physical and External Domains	LLDP Policy:			
	CDP Policy:	CDP_ON C		
	STP Policy:	select a value 🗸 🗗		
	Firewall Policy:	select a value 🗸 🗗		

#### 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 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 SIS 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-Туре Protocol Member Ports Channel \_\_\_\_\_ LACP 5 Po5(SU) Eth 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	Ethl/1, Ethl/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	Туре	Vlan-mode	Encap
13	enet	CE	vxlan-16777209, vlan-3967
19	enet	CE	vxlan-14680064, vlan-150
22	enet	CE	vxlan-16383902
26	enet	CE	vxlan-15531929, vlan-200
27	enet	CE	vlan-11
28	enet	CE	vlan-14
36	enet	CE	vxlan-15662984

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:

Access Port Policy Group	- AVS-102_1-ports-7	_PolGrp						(j) 🕽
						F	olicy Faul	ts History
⊙₹								ACTIONS -
Properties								
Name:	AVS-102_1-ports-7_PolGrp							
Description:	optional							
Label:				J				
Link Level Policy:	1GigAuto	e						
CDP Policy:	CDP_ON	e						
MCP Policy:	select a value							
LLDP Policy:	LLDP_ON	e						
STP Interface Policy:	select a value							
Storm Control Interface Policy:	select a value							
L2 Interface Policy:	select a value							
Monitoring Policy:	select a value							
Attached Entity Profile:	AEP_DVS	e						
Connectivity Filters:					× +			
	Switch IDs		Interfaces					
						SHOW USAGE	SUBMIT	CLOSE

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 Type Vlan-mode Encap

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

\_\_\_\_\_ vxlan-16777209, vlan-3967 enet CE 13 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 vxlan-15662984 36 enet CE and Opflex connection is restablised after restarting the VEM module: ~ # vem restart stopDpa VEM SwISCSI PID is Warn: DPA running host/vim/vimuser/cisco/vem/vemdpa.213997 Warn: DPA running host/vim/vimuser/cisco/vem/vemdpa.213997 watchdog-vemdpa: Terminating watchdog process with PID 213974 ~ # vemcmd show opflex Status: 0 (Discovering) Channel0: 14 (Connection attempt), Channel1: 0 (Discovering) Dvs name: comp/prov-VMware/ctrlr-[AVS]-vCenterController/sw-dvs-129 Remote IP: 10.0.30 Port: 8000 Infra vlan: 3967 FTEP IP: 10.0.32 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: 10.0.30 Port: 8000 Infra vlan: 3967 FTEP IP: 10.0.32 Switching Mode: LS Encap Type: unknown NS GIPO: 0.0.0.0

## Informazioni correlate

Installazione switch virtuale applicazione

<u>Guida all'installazione di Cisco Application Virtual Switch, Cisco Systems, Inc., versione</u> <u>5.2(1)SV3(1.2)</u> 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