ASAv en el modo GoTo (L3) con el uso de AVS-ACI 1.2(x) versión

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Configurar Diagrama de la red Configuraciones Verificación Troubleshoot Información Relacionada

Introducción

Este documento describe cómo implementar un switch Application Virtual Switch (AVS) con un firewall único Adaptive Security Virtual Appliance (ASAv) en modo Routed/GOTO como un gráfico de servicio L4-L7 entre dos grupos de punto final (EPG) para establecer la comunicación cliente-servidor mediante la versión ACI 1.2(x).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Políticas de acceso configuradas e interconectadas en servicio
- EPG, dominio de puente (BD) y routing y reenvío virtual (VRF) ya configurados

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

Hardware y software:

- UCS C220 2.0(6 d)
- ESXi/vCenter 5.5
- ASAv asa-device-pkg-1.2.4.8
- AVS 5.2.1.SV3.1.10
- APIC 1.2(1i)
- Hoja/espinas 11.2(1i)
- Paquetes de dispositivos *.zip ya descargados

Funciones:

- AVS
- ASAv
- EPG, BD, VRF
- Lista de control de acceso (ACL)
- Gráfico de servicios L4-L7
- vCenter

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

Configurar

Diagrama de la red

Como se muestra en la imagen,



Configuraciones

La configuración inicial de AVS crea un dominio VMware vCenter (integración de VMware)2

Nota:

• Puede crear varios Data Centers y entradas de switch virtual distribuido (DVS) bajo un único

dominio. Sin embargo, sólo puede tener asignado un AVS de Cisco a cada Data Center.

- La implementación de gráficos de servicios con Cisco AVS es compatible con Cisco ACI versión 1.2(1i) con Cisco AVS versión 5.2(1)SV3(1.10). Toda la configuración del gráfico de servicios se realiza en el Cisco Application Policy Infrastructure Controller (Cisco APIC).
- La implementación de la máquina virtual de servicios (VM) con Cisco AVS solo se admite en dominios de Virtual Machine Manager (VM) con modo de encapsulación de redes de área local virtuales (VLAN). Sin embargo, las VM informáticas (las VM de proveedor y de consumidor) pueden formar parte de dominios de VM con Virtual Extensible LAN (VXLAN) o encapsulación de VLAN.
- Tenga en cuenta también que si se utiliza el switching local, no se requieren la dirección de multidifusión ni el conjunto. Si no se selecciona ninguna conmutación local, se debe configurar el conjunto de multidifusión y la dirección de multidifusión de AVS Fabric-wide no debe formar parte del conjunto de multidifusión. Todo el tráfico originado desde el AVS será VLAN o VXLAN encapsulado.

Navegue hasta VM Networking > VMWare > Create vCenter Domain, como se muestra en la imagen:



Specify vCenter domain users and co	ontrollers				
Virtual Switch Name:	AVS	_			
Virtual Switch:	VMware vSphere D	istributed Switch	Cisco AVS		
Switching Preference:	No Local Switching	Local Switching	9		
Encapsulation:	VLAN				
	O VXLAN				
Associated Attachable Entity Profile:	AEP-AVS	-	æ		
VLAN Pool:	VlanPool-AVS(dynam	ic) 🗸	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	

Si utiliza Port-Channel o VPC (Virtual Port-Channel), se recomienda establecer las políticas de vSwitch para utilizar Mac Pinning.

Después de esto, APIC debe enviar la configuración del switch AVS a vCenter, como se muestra en la imagen:



En APIC, puede observar que una dirección VXLAN Tunnel Endpoint (VTEP) se asigna al grupo de puertos VTEP para AVS. Esta dirección se asigna independientemente del modo de conectividad utilizado (VLAN o VXLAN)

Inventory 🗧 🖸	Portgroup - vtep			_	i
Microsoft				General Faults Hi	story
Generation Whyare					
🔺 🕕 AVS	Properties				
Controllers	Properties Management Network Server Name Name State MAX IP Address Management Network Server Name Name State MAX IP Address 10.201.35.219 vmk1 Up 00:50:56:68:CA.25 10.0.16.95 10.201.35.218 vmk1 Up 00:50:56:61:07:00 10.0.18.94				
WGenterControler MenterControler MenterControler	Portgroup - vtep Devent Paults Poults •••••••••••••••••••••••••				
▶ ↓ 10.201.35.218	Reference Portgroup - vtep				
► □ 10.201.35.219	Image: Portgroup - vtep Image: Paulie Image: Properties Image: Properties Image: Paulie Management Network Adageret Server Name Name Stare MAC IP Address 10 201.35.219 vrik1 Up 005056680.425 10.016.95 10.016.95 10 201.35.218 vrik1 Up 00505668107.00 10.016.95 10.016.95				
DVS - AVS Dressures	Image: server Name Name: rep Encap: vlas-3957 Management Network Adagers Sarver Name Mare Mare MAC P Address 10 201.35.219 vmk1 Up 005058680.A25 100.16.95 100.16.95 10 201.35.218 vmk1 Up 005058681.07.00 100.16.95 100.16.95				
Pods-ALUMBRERIAVS-AEP-VMM-a	Image: rest in the image: re				
Quarantine	Image: Portgroup - vtep Image: Portgroup - vtep Image: Properties Name: vtep Encap: vten-3867 Same Management Network Server Name 10.201.35.218 vmk1 Up 005056661.07.00				
Uplink	Portgroup - vtep Concell Faults Hat Properties Name: vtep Encar: vtep- Vtep- Vtep- Management Network Server Name Name State MAC IP Address 10.201.35.219 vmk1 Up 00.50:56:81:07:00 10.016.35 10.016.35				
O DVS				Owner Faults History IP Address 10.0.16.95 10.0.16.95 107.000 10.0.16.95 10.0.16.94	
	Stame: Variety Variety Stame: Variety Variety Variety	Displaying Objects 1 - 2 O	12		

Instale el software Cisco AVS en vCenter

• Descargue vSphere Installation Bundle (VIB) de CCO mediante este enlace

Nota: En este caso, utilizamos ESX 5.5, Tabla 1, que muestra la matriz de compatibilidad para ESXi 6.0, 5.5, 5.1 y 5.0

Tabla 1: Compatibilidad de la versión de software host para ESXi 6.0, 5.5, 5.1 y 5.0

THE R. P. LEWIS CO., LANSING MICH.	Type new contrast comparently reasons			
Villware 1	V18 2	VEM Bundle 3	Windows VC Installer	Linux vCenter Server Appliance
ESXI 6.0	cross_cisco-vem- x250-5.2.1.3.1.10.0-6.0.1.vib	VEM600-201512250119-8C- release zip (Offine) VEM600-201512250119-8C (Online)	6.0	6.0
ESX 5.5	cross_cisco-vem- x250-5.2.1.3.1.10.0-3.2.1.v/b	VEM550-201512250113-BG- release zip (Offine) VEM550-201512250113-BG (Online)	5.5	5.5
ESXI 5.1	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
ESX 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

Dentro del archivo ZIP hay 3 archivos VIB, uno para cada una de las versiones de host ESXi, seleccione el apropiado para ESX 5.5, como se muestra en la imagen:

	CiscoAVS_1.10-5.	2.1.SV3.1.10			
			Q Searc	h	
Π	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 archi

 Copie el archivo VIB en ESX Datastore; esto se puede hacer a través de CLI o directamente desde vCenter

Nota: Si existe un archivo VIB en el host, retírelo usando el comando esxcli software vib remove.

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

o explorando el almacén de datos directamente.

• Instale el software AVS mediante el siguiente comando en el host ESXi:

esxcli software vib install -v /vmfs/tomes/datastore1/cross_cisco-vem-v250-5.2.1.3.1.10.0-3.2.1.vib —maintenance-mode —no-sig-check

~ # esxcli softw	are vib inst	all -v /vmfs,	/volumes/datastore	1/cross_	cisco-vem-v250-5.2.1.3.1.10.0-3.2.1.vibmaintenance-modeno-sig-check	
Installation Res	ult					
Message: Open	ation finish	ed successfu	llv.			
Reboot Requir	ed: false					
VIRs Installe	d: Cisco boo	thank cisco-	vem_v250_esv 5 2 1	3 1 10	0-3 2 1	
VIDS Instarte	Cieco booth	ank cisco-ve	w_{-1} 107_0ev 5 2 1 3	1 5 0_3	2 1	
VIDS Kelloved.		unk_clsco-vei	1-v197-esx_9.2.1.9	.1.3.0-3	.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 (vemdp	a) is runnin	g				
~ #						j

• Una vez que el módulo Ethernet virtual (VEM) esté activo, puede agregar hosts a su AVS: En el cuadro de diálogo Add Host to vSphere Distributed Switch (Agregar host a switch distribuido de vSphere), elija los puertos NIC virtuales que están conectados al switch de hoja (en este ejemplo, sólo mueve vmnic6), como se muestra en la imagen:

lect Host and Physical Adapters	Markink start advance	To use her suited	Settings	View Incompatible H
twork Connectivity	Host/Physical adapters	In use by switch	Settings	Uplink port group
adv to Complete			view Details	
	Select physical adapters	vCultrh0	Mau Dataile	ualisk
		VSWIECHU	View Details	uplink
	wmnic1		View Details	uplink
			View Details	uplink
			View Details	uplink
			View Details	uplick
		DVS	View Details	uplick
		DVS	View Details	uplick
	Vmpic6		View Details	uplink
	wmpic7		View Details	uplink
	vmnic8		View Details	uplink
	vmnic9		View Details	uplink

- Haga clic en Next (Siguiente)
- En el cuadro de diálogo Conectividad de red, haga clic en Siguiente
- En el cuadro de diálogo Red de máquina virtual, haga clic en Siguiente
- En el cuadro de diálogo Preparado para completar, haga clic en Finalizar

Nota: Si se utilizan varios hosts ESXi, todos ellos necesitan ejecutar AVS/VEM para que puedan administrarse desde el switch estándar a DVS o AVS.

Con esto, se ha completado la integración de AVS y estamos preparados para continuar con la implementación de ASAv L4-L7:

Configuración inicial de ASAv

• Descargue el paquete de dispositivos Cisco ASAv e importe en APIC:

Navegue hasta Servicios L4-L7 > Paquetes > Importar paquete de dispositivos, como se muestra en la imagen:

Fabric	VM Networking	L4-L7 Services	Admin	Operations	
		Inventory Packages			
Quick Sta	rt				
HELP The Packag balancer, co and network	es menu allows you to ir ntext switch, SSL termin connectivity information	nport L4-L7 device pao ation device, or intrusio for each function. A ne	kages, which are used to on prevention system (IPS otwork service device is d t a device package for a f	o define, configure, and monitor 6). Device packages contain de eployed in the network by addi function that you want to mana	r a network service escriptions of the ft ng it to a service g as with APIC. We
configuring a	a service graph.	nport Device Pa	ackage	i s	
Quick	Start a Device Package	File Name:		BROWSE	Device Types

• Si todo funciona bien, puede ver el paquete de dispositivos importado expandiendo la carpeta Tipos de dispositivos de servicio L4-L7, como se muestra en la imagen:

SUBMIT

CLOSE

i

|--|

				General	Operational	Faults	History
⊙₹						ACT	
Properties							
Vendor:	CISCO altala 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:	1						
Interface Labels:	 Name 						_
	cluster_ctrl_lk						
	external						
	failover_lan						
	failover_link						
	internal						
	mgmt						
	utility						

Antes de continuar, hay algunos aspectos de la instalación que deben determinarse antes de realizar la integración L4-L7:

Existen dos tipos de redes de gestión: administración en banda y fuera de banda (OOB), que se pueden utilizar para administrar dispositivos que no forman parte de la infraestructura centrada en aplicaciones (ACI) básica (hoja, columna o controlador apic) que incluiría ASAv, equilibradores de carga, etc.

En este caso, OOB para ASAv se implementa con el uso de vSwitch estándar. Para el ASA sin software específico u otros dispositivos de servicio o servidores, conecte el puerto de administración OOB al switch OOB o a la red, como se muestra en la imagen.



La conexión de administración del puerto de administración de OOB ASAv necesita utilizar los puertos de enlace ascendente ESXi para comunicarse con APIC a través de OOB. Al mapear interfaces vNIC, el adaptador de red1 siempre coincide con la interfaz Management0/0 en ASAv, y el resto de las interfaces del plano de datos se inician desde el adaptador de red2.

La tabla 2 muestra la concordancia de ID de adaptador de red e ID de interfaz ASAv:

Tabla 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

- Implemente la máquina virtual ASAv a través del asistente desde File>Deploy OVF (Open Virtualization Format) Template
- Seleccione asav-esxi si desea utilizar ESX Server independiente o asav-vi para vCenter. En

este caso, se utiliza vCenter.



 Vaya al asistente de instalación, acepte términos y condiciones. En medio del asistente puede determinar varias opciones, como nombre de host, administración, dirección ip, modo de firewall y otra información específica relacionada con ASAv. Recuerde utilizar la administración OOB para ASAv, como en este caso, debe mantener la interfaz Management0/0 mientras utiliza la red VM (switch estándar) y la interfaz GigabitEthernet0-8 son los puertos de red predeterminados.

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 OVP template to networks in your inventory					
ame and Location	Source Networks	DestinationNetworks				
eployment Configuration	Management0-0	VM Network				
lor age	GigabitEthernet0-0	VM Network				
etwork Happing	GigabitEthernet0-1	VM Network	1			
roperties	GigabitEthernet0-2	VM Network				
eady to Complete	GigabitEthernet0-3	Pod6-ALUMBRERJAVS-AEP-VMM-alumbrerJAVS				
	GigabitEthernet0-4	Pod6-ALUMERER [InternalAEP-VMM-alumbrer E				
	GigabitEthernet0-5	VM Network				
	GinabitPthemet0-6	VM Network	٠			
	Description:					
	General Purpose Network Interface		^			
	1		Ŧ			
	menning: mangate source methodika a					

Properties

Customize the software solution for this deployment.

Sizes Off Tendata Details Control Meet License Accessences Type of deployment. Sizes Type of deployment. Sizes Sectores Control Meet Conflocation Select the type of ASA' host to install. When an HA type deployment is selected, the additional HA Properties Standatione Ready to Complete Mostname Mostname Mostname			
Oxf: Tenckate Details Modules: Location Management Configuration Statistic Statistic Concomment Configuration Statistic Concomment Configuration Statistic Ready to Complete Hostname <	Source		
Item Litter Location Deployment Type Status Type of deployment Status Sector Sector Sector Management Mathematic Sector Management Interface Settings	OVF Template Details		*
Name: Type of deployment Status Select the type of ASAv host to instal. When an HA type deployment is selected, the additional HA Properties below should also be filed in. Status Standaione Properties Ready to Complete Hostname Hostname Hostname Hostname (bits, or a hyphen). Adave::-AVS Firewall Properties Firewall Properties Firewall Properties Note: Name(bits) Hanagement 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 HAnagement IP-4 Address. For HA-type deployments, this property specifies the Management IP-4 Address of the Active HA host. .00 .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 Metagement IP Subnet Hask	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 Oxoses 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 Management IP Subnet Hask		ASAv-w-AVS	
Help < Back			
Help < Back		Firewall Properties	
Select the Firewall Mode routed Management Interface Settings Hanagement Interface DHCP mode Choose whether to use DHCP for Management interface configuration. Imagement IP Address Enter the Management IP-v4 Address. For HA-type deployments, this property specifies the Management IP-v4 Address of the Active HA host. ID .01 Hanagement IP Subnet Hask Imagement IP Subnet Hask Imagement IP Subnet Hask Imagement IP Subnet Hask		Firewall Mode	
Management Interface Settings Management Interface DHCP mode Choose whether to use DHCP for Management interface configuration. Imagement IP Address Enter the Management IPv4 Address. For HA-type deployments, this property specifies the Management IPv4 address of the Active HA host. Imagement IP Subnet Hask Help 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 > 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 > 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

ploy OVF Template	ventory a 🗃 Heats and Clusters		2
ady to Complete	want to use?		
ALL LIESE LIE ODOLO 100	mant to coer		
1778			
F Template Details	When you click Finish, the deploym	ent task will be started.	
d User License Agreement	Deployment settings:		
me and Location	Size ondisk:	8.3 GB	
forment Configuration	Name:	ASAv-in-AVS	
1000 MOR	Folder	ACI	
Format	Deployment Configuration:	1 Gbps(ASAv10)	
NOTE PRODUCT	Host/Cluster:	10.201.35.219	
dy to Complete	Datastore	datastore4	
	Disk provisioning:	Thick Provision Lazy Zeroed	
	Network Mapping:	"Management0-0" to "VM Network"	
	Network Mapping:	"GigabitEthernet0-0" to "VM Network"	
	Network Mapping:	"GigabitEthernet0-1" to "VM Network"	6
	Network Mapping:	"GigabitEthernet0-2" to "VM Network"	
	Network Mapping:	"GloabitEthernet0-3" to "Pod6-ALUMBRERIAVS-AEP-VMM-alumbre/AV_	
	Network Mapping:	"GigabitEthernet0-4" to "Pod6-ALUMBRER InternalAEP-VMM-alumbrerL	
	Network Mapping:	"GigabitEthernet0-5" to "VM Network"	
	Network Mapping	"GigabitEthernet0-6" to "VM Network"	
	Network Mapping:	"GigabitEthernet0-7" to "VM Network"	
	Network Mapping	"GigabitEthernet0-8" to "VM Network"	
	12 Allocation	Fixed, Dv4	
	Property:	HARole = Standalone	
	Property:	Hostname = ASAv-w-AVS	
	Property:	FWMode = routed	
	Property:	DHCP = False	
	Property	Management3Pv4 = 10.201.35.223	
	Property:	ManagementIPv4Subnet = 255.255.255.0	
	Property:	ManagementStandbySPv4 = 0.0.0.0	
	Property	RouteDefault = Default Route	
		11 100 100 7 110 1 10 001 001	٠
	Power on after deployment		
- I			
ab .		< Back Pinish Cancel	

• Haga clic en Finalizar y espere hasta que finalice la implementación de ASAv



• Encienda su máquina virtual ASAv e inicie sesión a través de la consola para verificar la configuración inicial

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 --->

 Como se muestra en la imagen, ya se ha enviado parte de la configuración de administración al firewall ASAv. Configure el nombre de usuario y la contraseña del administrador. El APIC utiliza este nombre de usuario y contraseña para iniciar sesión y configurar el ASA. El ASA debe tener conectividad con la red OOB y debe poder alcanzar el APIC.

nombre de usuario admin password <device_password> privilegio cifrado 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)# _

Además, desde el modo de configuración global, habilite el servidor http:

http server enable

http 0.0.0.0 0.0.0.0

L4-L7 para la integración de ASAv en APIC:

 Inicie sesión en la GUI de ACI, haga clic en el arrendatario en el que se implementará el gráfico de servicios. Expanda los servicios L4-L7 en la parte inferior del panel de navegación y haga clic con el botón derecho en Dispositivos L4-L7 y haga clic en Crear dispositivos L4-L7 para abrir el asistente Para esta implementación, se aplicarán las siguientes configuraciones:
 -Modo administrado

-Servicio de firewall

-Dispositivo virtual

-Conectado al dominio AVS con un solo nodo

-Modelo ASAv

-Modo enrutado (GoTo)

-Dirección de administración (debe coincidir con la dirección asignada anteriormente a la interfaz Mgmt0/0)

Utilice HTTPS como APIC de forma predeterminada utiliza el protocolo más seguro para comunicarse con ASAv

Create L4-L7 Device	5					
STEP 1 > General					1. General 2. Device	e Configuration
Please select device	package and enter connectivity info	rmation.				
General Managed: Name:	ASAv-AVS-Routed	Device 1 Management IP Address:	10.201.35.3	Δν-in-ΔVS	Management Port: https	•
Service Type:	Firewall	Device Interfaces:	Voliter controller/Pior			× +
Device Type:	PHYSICAL VIRTUAL		Name	VNIC	Path (Only For Route Peering)	
VMM Domain:	AVS 🗸 🕑		GigabitEthernet0/0	Network adapter 2	Node-102/MAC_Pinning	
Mode:	Single Node		GigabitEthernetori	Network adapter 5	Node-Tozimiko_Fillining	
Device Package:	CISCO-ASA-1.2 🗸 🗗					
Model:	ASAv					
Function Type:	GoThrough GoTo	Cluster				
		Management IP Address:	10.201.35.3		Management Port: https	-
		Cluster Interfaces:				× +
			Туре	Name	Concrete Interfaces	
-			provider	ServerInt	Device1/GigabitEthernet0/0	
Connectivity APIC to Device Management Connectivity:	out-Of-Band ○ In-Band		consumer	ClientInt	Device1/GigabitEthernet0/1	
Credentials Username:	admin					
Password:						
Confirm Password:						

 La definición correcta de las interfaces de dispositivo y de las interfaces de clúster es fundamental para una implementación correcta

Para la primera parte, utilice la tabla 2 mostrada en la sección anterior para hacer coincidir correctamente los ID de adaptador de red con los ID de interfaz ASAv que desea utilizar. La ruta hace referencia al puerto físico, al canal de puerto o al VPC que habilita la entrada y salida de las interfaces de firewall. En este caso, ASA se encuentra en un host ESX, donde el ingreso y la salida son los mismos para ambas interfaces. En un dispositivo físico, el interior y el exterior del firewall (FW) serían puertos físicos diferentes.

Para la segunda parte, las interfaces de clúster deben definirse siempre sin excepciones (incluso

si no se utiliza Cluster HA), esto se debe a que el modelo de objetos tiene una asociación entre la interfaz **mlf** (metainterfaz en el paquete de dispositivos), la interfaz **Llf** (interfaz hoja como, por ejemplo, externa, interna, interna, etc.) y la **Clf** (interfaz de hormigemento). Los dispositivos concretos L4-L7 deben configurarse en una configuración de clúster de dispositivos y esta abstracción se denomina dispositivo lógico. El dispositivo lógico tiene interfaces lógicas asignadas a interfaces concretas en el dispositivo concreto.

Para este ejemplo, se utilizará la asociación siguiente:

- Gi0/0 = vmnic2 = ServerInt/Provider/server > EPG1
- Gi0/1 = vmnic3 = ClientInt/Consumer/client > EPG2

-Li Devices - ASAV-AVS-Houleu						1
				Policy Pr	arameters Faul	ts History
						ACTIONS -
eneral Managed: Name: ASAv-AVS-Routed Device Package: CISCO-ASA-1.2 Service Type: Firewall Device Type: VIRTUAL VMM Domain: AVS Context Aware: Single Function Type: GoThrough GoTo Cluster Mode: Single Node	Device 1 Management IP Address: vCenter Name: Interfaces:	10.201.35.223 vCenterController Name GigabitEthemet0/1 GigabitEthemet0/2	Managemer VM Network adap	nt Port: 443 Name: ASAv-In-AV ter 3 ter 4	Path (Only For Route Node-102/MAC_Pi Node-102/MAC_Pi	× + Peering) ming, Nod
Confirm Password:	Cluster Management IP Address: Cluster Interfaces:	10.201.35.223 Type	Managemer	tt Port: 443 Concrete Interface	•	× +
Configuration State	\subset	consumer	ClientInt	ASAn-AVS-Route	d_Device_1/(Gigab	RETHOMHO/2]
Configuration Issues: Devices State: stable		provider	ServerInt	ASAP-AVS-Houte	d_nevice_1/(cigab	te nometo/1]

Nota: Para implementaciones de failover/HA, GigabitEthernet 0/8 está preconfigurado como interfaz de failover.

El estado del dispositivo debe ser Estable y debe estar preparado para implementar el perfil de función y la plantilla de gráfico de servicios

Templo de gráfico de servicio

En primer lugar, cree un perfil de función para ASAv, pero antes de eso debe crear un grupo de perfiles de función y, a continuación, un perfil de función de servicios L4-L7 debajo de esa carpeta, como se muestra en la imagen:

L4-L7 Devices - ASAv-AVS-Routed

Create L4-L7 Services Fu	nction Profile	Group		i ×			
Specify the information at	out the Function	on Profile Group					
Name: FunP Description:	rofGroup						
		[SUBMIT	CANCEL			
Tenant Pod6-ALUMBRER	L4-L7 Services Fi	unction Profile Group	- FunProGroup			General R	i ulta History
Application Profiles	⊙₹						ACTIONS -
L4-L7 Service Parameters Security Policies Troubleshoot Policies	Properties Name: Description:	FunProGroup					
 Montoring Policies L4-L7 Services 	service Function Protect		Associated Exection	Description			× +
L4-L7 Service Graph Templates Pouter configurations Function Profiles L4-L7 Devices L4-L7 Devices Delete Delete Create L4-L7 Services Fu	nction Photfile	* Nane	Associated Function	No items have been four Select Actions to create a ne	an nd. wiltern.		
Devices Selection 1 Selection Deployed Graph in Deployed Devices Inband Management Configuration for L4-L7 devi	2						

 Seleccione el perfil WebPolicyForRoutedMode en el menú desplegable y proceda a configurar las interfaces en el firewall. A partir de aquí, los pasos son opcionales y se pueden implementar/modificar más adelante. Estos pasos se pueden realizar en varias etapas diferentes de la implementación en función de la reutilización o personalización del Gráfico de servicios.

Para este ejercicio, un firewall enrutado (modo GoTo) requiere que cada interfaz tenga una dirección IP única. La configuración estándar de ASA también tiene un nivel de seguridad de la interfaz (la interfaz externa es menos segura, la interfaz interna es más segura). También puede cambiar el nombre de la interfaz según sus requisitos. Los valores predeterminados se utilizan en este ejemplo.

• Expanda Interface Specific Configuration, agregue la dirección IP y el nivel de seguridad para ServerInt con el siguiente formato para la dirección IP x.x.x.x/y.y.y.y o x.x.x.x/yy. Repita el proceso para la interfaz ClientInt.

Create Function Profile

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

Nota: También puede modificar la configuración predeterminada de la lista de acceso y crear su propia plantilla base. De forma predeterminada, la plantilla RoutedMode incluirá reglas para HTTP y HTTPS. Para este ejercicio, SSH e ICMP se agregarán a la lista de acceso externa permitida.

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

- A continuación, haga clic en Enviar
- Ahora, cree la plantilla de gráficos de servicios

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

• Arrastre y suelte el clúster de dispositivos a la derecha para formar la relación entre consumidor y proveedor, seleccione Modo enrutado y el perfil de función creado anteriormente.

Graph Name:	Graph1-alumbrer		
Graph Type:	Create A New One	Clone An Existing One	
Consumer		C ASAv-AVS	Provider EPG
ACA: AVC Deuted	Please drag a d	levice from devices table and drop it here to create a service node.	
Firewall: Profile: Po	Information Routed Transpare	ent iPro- <mark>→</mark> ট	
			SUBMIT CANCEL

- Verifique la plantilla para ver si hay fallos. Las plantillas se crean para reutilizables, y después se deben aplicar a EPG particulares, etc.
- Para aplicar una plantilla, haga clic con el botón derecho del ratón y seleccione Aplicar plantilla de gráficos de servicios L4-L7

Tenant Pod6-ALUMBRER	1.4-1.7 Service Graph Template - Graph1-alumbrer		
Cuick Start			
Tenant Pod6-ALUMBRER	Topology	Policy Faults	History
Application Profiles	0		
Networking	Consumer	Provider	
L4-L7 Service Parameters	Consumer	Provider	
Security Policies			
Troubleshoot Policies	ASAv-AVS	3	
Monitoring Policies			
L4-L7 Services	ASAv		
L4-L7 Service Graph Templates			
Graph1-alumbrer	outed Information		
Function Node - ASA State - Apply L4-L7 Sen	rice Graph Template II: Routed		
Router configurations Edit L4-L7 Service	e Graph Template b: FunPro-ASA		
Function Profiles Delete			
FunProfGroup Remove Related	Objects Of Graph Template		
E FunPro-ASA			
▲ L4-L7 Devices			
ASAv-AVS-Routed			
ASAV-DVS			
Imported Devices			
Devices Selection Policies			
Deployed Graph Instances			
Deployed Devices			
 Inband Management Configuration for L4-L7 device 			
New //10 001 05 01 /#	SHOW USAGE	SUBMIT	RESET

- Defina qué EPG estará en el lado del consumidor y del proveedor. En este ejercicio, AVS-EPG2 es el consumidor (cliente) y AVS-EPG1 es el proveedor (servidor). Recuerde que no se aplica ningún filtro, esto permitirá que el firewall realice todo el filtrado basado en la lista de acceso definida en la última sección de este asistente.
- Haga clic en Next (Siguiente)

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 Netwo	k: Pod6-ALUMBRER/AVS-AEP-VMM 👻 📴	¢5
	Pod6-ALUMBRER/AVS-AEP-VMM-	
Contract Information	alumbrer/epg-AVS-EPG1	
Contract: Contract: Contract: Contract: Contract	Pod6-ALUMBRER/InternalAEP-	
Contrast Name: CDO0 to CDO1	VMM-alumbrer/epg-EPG-Internal-	
Contract Name: EPG2-to-EPG1	alumbrer	
No Filter (Allow All Traffic): 🗹	Pod6-ALUMBRER/VRF1-alumbrer /AnyEPG	
	Pod6-ALUMBRER/VRF2/AnyEPG	
	Pod6-ALUMBRER/L3Out-N3K2/L3Net	

 Verifique la información de BD para cada uno de los EPG. En este caso, EPG1 es el proveedor en la base de datos IntBD y EPG2 es el consumidor en BD ExtBD. EPG1 se conectará en la interfaz de firewall ServerInt y EPG2 se conectará en la interfaz ClientInt. Ambas interfaces FW se convertirán en la DG para cada uno de los EPG, por lo que el tráfico se verá obligado a cruzar el firewall en todo momento.

PREVIOUS NEXT CANCEL

• Haga clic en Next (Siguiente)

Graph Template:	Pod6-ALUMBRER/Graph1-Temp-alumbrer 🚽 🗗			
Consumer EPG AVS-EPG2	ASAv-AVS	[Provider EPG AVS-EPG1	
ASAv-AVS-Routed Info Firewa Profile Consumer Connector Type: BD: Cluster Interface: BD: Cluster Interface:	nation : routed : FunPro-ASA @ General			
		PREVIOUS	NEXT	CANCE

 En la sección Config Parameters, haga clic en All Parameters y verifique si hay indicadores RED que necesitan actualizarse/configurarse. En el resultado, como se muestra en la imagen, se puede observar que se ha perdido el orden en la lista de acceso. Esto equivale al orden de línea que verá en un show ip access-list X.

STEP 3 > ASAv-AVS-Routed Parameters

		older/Param	Name Value	Witte Domain
icterfaces.		4 🥶 Access List	access-list-inbound	
AccessLists		Access Control Entry	ICMP	
		Access Control Entry	51812	
TrafficSelectionObjects	8	4 🤿 Access Control Entry	SSH	
MI .		Destination Address		
	8	Destination Service	destination_service	
		EMP		
		Logging		
	8	Protocol	protocol	
		Source Address		
		Source Service		
		Action	action permit	
		Order	order 30	select asa domain
		Access Control Entry	UPDATE RESET CANCEL	
		Access Control Entry	of only the other of the other	

• También puede verificar el direccionamiento IP asignado desde el perfil de función definido anteriormente. Hay una buena oportunidad de cambiar la información si es necesario. Una vez configurados todos los parámetros, haga clic en **Finalizar**, como se muestra en la imagen:

config parameters for the selected device

Profile Name: FunProf-ASA						
Features:	Re	equired	ed Parameters All Parameters			
Interfaces		F	Folder/Param	Name	Value	Write Domain
Interlaces		8	🔺 😅 Device Config	Device		
AccessLists		B	Access List	access-list-inbound		
NAT			Bridge Group Interface			
TrafficSelectionObjects		B	Interface Related Configuration	externalif		
All		8	Access Group	ExtAccessGroup		
			Inbound Access List	name	access-list-inbound	
			Outbound Access List			
			IPv6 Enforce EUI-64			
		8	Interface Specific Configuration	externallfCfg		
		8	IPv4 Address Configuration	IPv4Address		
			IPv4 Address	ipv4_address	192.168.10.1/24	
			IPv4 Standby Address			
			IPv6 Address Configuration			
			IPv6 Link Local Address Configuration			
	173		IPv& Router Advertisemente			

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

• Si todo va bien, debería aparecer un nuevo dispositivo implementado e instancia de gráfico.



Verificación

 Una cosa importante para verificar después de crear el gráfico de servicios es que la relación consumidor/proveedor se creó con el Meta Connector adecuado. Verifique bajo Propiedades del Conector de Función.



Nota: Cada interfaz del firewall se asignará con una vlan encap del grupo dinámico AVS. Verifique que no haya fallas.

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
Cuick Start Cuick	O ★ Properties		A A O O 100	Policy	Operational	Health	Faults	History
Security Policies Troubleshoot Policies Monitoring Policies Le-L7 Services	Devices: Virtual Device ID: VRF: ACKed Transaction ID: Current Transaction ID:	ASAv-AVS-Routed 25351 none 10000 10000						
L4-L7 Service Graph Templates Router configurations Eunction Profiles	Cluster Interfaces:	Logical Interface ASAv-AVS-Routed_ClientInt	Encep vlan-93	_				
L4-L7 Devices Imported Devices Devices Selection Policies Deviced Graph Instances	ł	ASAv-AVS-Routed_ServerInt	vlan-94					
V* EPG2-to-EPG1-Graph1-alumbrer-Pod6-ALUM Deployed Devices V* ASAv-AVS-Routed-none Inband Management Configuration for L4-L7 device								

Ahora, también puede verificar la información enviada al ASAv

NSAv-w-AVS# show interface	ip brief		
Interface	IP-Address	OK? Method Status	Prot
ocol			
igabitEthernet0/0	192.168.10.1	YES manual up	սք
iigabitEthernet0/1	172.16.1.1	YES manual up	սք
iigabitEthernet0/2	unassigned	YES unset administratively dow	ւ սթ
iigabitEthernet0/3	unassigned	YES unset administratively dow	ւ սթ
iigabitEthernet0/4	unassigned	YES unset administratively dow	ւ սթ
iigabitEthernet0/5	unassigned	YES unset administratively dow	ւ սթ
iigabitEthernet0/6	unassigned	YES unset administratively dow	ւ սթ
iigabitEthernet0/7	unassigned	YES unset administratively dow	ւ սթ
iigabitEthernet0/8	unassigned	YES unset administratively dow	ւ սթ
lanagement0/0	10.201.35.223	YES CONFIG up	սք
ISAv-w-AVS# show run access	-list		
uccess-list access-list-inf	ound extended	permit tcp any any eq www	
uccess-list access-list-inf	ound extended	permit tcp any any eq https	
uccess-list access-list-inf	ound extended	permit tcp any any eq ssh	
uccess-list access-list-int	oound extended	permit icmp any any	
ISAU-W-AUS#			

 Se asigna un nuevo contrato en los EPG. A partir de ahora, si necesita modificar algo de la lista de acceso, el cambio debe hacerse a partir de los parámetros de servicio L4-L7 de la EPG del proveedor.



 En vCenter, también puede verificar que los EPG de la sombra estén asignados a cada una de las interfaces FW:

1	🕜 AS	Av-in-AVS - Virtual Machine Pro	perties		
l	Hard	ware Options Resources Profile	es VServices	Virtual Machine Version: 8	ge Views
l	_			Device Status	
I		Show All Devices	Add Remove	Connected	
П	Hard	dware	Summary	Connect at power on	
	100	Memory	2048 MB	- Advator Tura	Acknowl
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		
I	0	CD/DVD drive 1	[datastore4] ASAv-in-A	00:50:50:63:CA:63	
d		CD/DVD drive 2	[datastore4] ASAv-in-A	Automatic C Manual	
T,		Hard disk 1	Virtual Disk		
I		Hard disk 2	Virtual Disk	DirectPath I/O	
I		Network adapter 1	VM Network	Status: Not supported 🕦	
I		Network adapter 2	Pod6-ALUMBRER ASAv	Network Connection	
1		Network adapter 3	Pod6-ALUMBRER ASAv	Network lebels	0
I		Network adapter 4	VM Network	Network label:	_
I		Network adapter 5	VM Network	Pad6-ALUMBRER ASAv-AVS-RoutedctxnoneIntBD-alumb	
I		Network adapter 6	VM Network	Pod6-ALUMBRER ASAV-AVS-RoutedcbmoneIntBD-alumbrer ServerInt	AVS
I		Network adapter 7	VM Network	Pod6-ALUMBRER AVS-AEP-VMM-alumbrer AVS-EPG2 (AVS)	
I		Network adapter 8	VM Network	quarantine (AVS)	=
I		Network adapter 9	VM Network	common default client (DVS)	
I		Network adapter 10	VM Network	common [default]juolivei (DVS)	
I				common default web (DVS)	•
I					
I					
I					
I					
		ush (or locut l	
		Help		OK Cancel	

Para esta prueba, tuve los 2 EPG comunicándose con los contratos estándar, estos 2 EPG están en diferentes dominios y VRF diferentes, por lo que la fuga de ruta entre ellos se configuró previamente. Esto simplifica un poco después de insertar el Gráfico de servicios, ya que el firewall configura el enrutamiento y el filtrado entre los 2 EPG. La DG configurada anteriormente en el EPG y el BD ahora puede eliminarse del mismo modo que los contratos. Sólo el contrato impulsado por la L4-L7 debe permanecer bajo los EPG.

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

A medida que se elimina el contrato estándar, puede confirmar que el tráfico ahora fluye a través de ASAv, el comando show access-list debería mostrar el recuento de aciertos para la regla que aumenta cada vez que el cliente envía una solicitud al servidor.



En la hoja, se deben aprender los terminales para las VM de cliente y servidor, así como para las interfaces ASAv

<pre>leaf2# show endpoint Legend:</pre>	a - locali	v-cood S - stati	<i>c</i>	
V - vpc-attached p - peer-aa	ed L - local	M - span		
s - static-arp B - bounce		epair		
+	+			+
VLAN/	Encap	MAC Address	AC Info/	Interface
Domain	VLAN	IP Address 1	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.fd0a L	FW	eth1/7
Pod6-ALUMBRER:VRF1-alumbrer Serv	ver IP vlan-98	192.168.10.10 L	interface	
25 & M	AC 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 Clien	nt IP & Jan-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		

vea ambas interfaces de firewall conectadas al VEM.

ESX-1

10.00	amond about a	In the set									
~ # V	emana snow p	OFT VL	an								
LTL	VSM Port	Admin	Link	State	Cause	PC-LTL	SGID	ORG	svcpath	Туре	Vem Port
22	Eth1/5	UP	UP	FWD	-	1040	4	0	0		vmnic4
23	Eth1/6	UP	UP	FWD		1040	5	0	0		vmnic5
50		UP	UP	FWD	-	0	4	0	0		vmk1
51		UP	UP	FWD	-	0	4	0	0		ASAv-in-AVS.eth1
52		UP	UP	FWD	-	0	4	0	0		ASAv-in-AVS.eth2
1040	Pol	UP	UP	FWD		0	_	0	0		

ESX-2

~ # vemand 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				
~ #													

Por último, las reglas del firewall también se pueden verificar en el nivel de hoja si conocemos las etiquetas de PC para los EPG de origen y destino:

EPG1					Balay	Crate	Marith Faultz Mature	
Application Profiles					rowy		neer reuta natory	
AVS-AEP-VMM-alumbrer					Aas	sociated EPGs /	associated External Routed Networks	J.
Application EPGs	⊙±						ACTIONS -	
► S EPG AVS-EPG1	NUTTO	Description	State	Issues	QoS	Encep	PC Tag	
Viero Arto-Eroz	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								
▶ 10 MMS								

EPG2								
 Domains (VMs and Bare-Metals) Static Bindings (Paths) Static Bindings (Leaves) 					Policy	Operational Stats	Health Faults	History
Contracts Static EndPoint Contracts	O₹					-	ACT	10NS -
L4-L7 Virtual IPs L4-L7 Virtual IPs L4-L7 IP Address Pool L4-L7 Service Parameters	AWS-EPG2	Description	applied	lisues	QoS Unspecified	Encep	5476	
Useg EPGs L4-L7 Service Parameters MonosAEP-VMM-alumbrer Metworking								
Bridge Domains Millinge Domains VIRPs VIRP1-alumbrer VIRP1-alumbrer VIRP2 Millinged Networks								

Los ID de filtro pueden coincidir con las etiquetas de PC de la hoja para verificar las reglas de FW.

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

Nota: El PCTags/Sclass de EPG nunca se comunica directamente. La comunicación se interrumpe o se une a través de los EPG de sombra creados por la inserción del gráfico de servicio L4-L7.

Y la comunicación Cliente a Servidor funciona.

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 encantlocal Loophack
ipet addr:127 0 0 1 Mack:255 0 0 0
ipaté addr. 127.0.0.1 Mask.255.0.0.0
UD LOODBACK DUNNING MILLEFERE Matrice1
DV packate 178258 assassie despendie everyweie frameie
TX packets:170350 errors:0 dropped:0 overruns:0 rrame:0
IX packets:1/0350 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)
<pre>* Documentation: https://help.ubuntu.com/</pre>
Last login: Mon Feb 1 10:14: <u>1</u> 1 2016 from 172.16.1.10
cisco@cisco-UbuntuClient:~\$ \$



Troubleshoot

La dirección VTEP no está asignada

Verifique que la VLAN de infraestructura esté verificada bajo AEP:

Policies 🔮 🖸	Attachable Access En	tity Profile - AEP-AVS				i
Switch Policies			Policy	Operational	Faults	History
Module Policies						
Interface Policies						CTIONS -
Global Policies	Properties					
Attachable Access Entity Profiles	Name:	AEP-AVS				
AEP-AVS	Description:	optional				
AEP_DVS	Ă.					
L3Out-N3K2-alumbrer	Enable Infrastructure VLAN:					
L3OutN3k-AEP	Domains (VMM, Physical or External)				~	
📃 default	Associated to Interfaces:				0	
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						
E Rogue EP Control Policy						
Monitoring Policies						
Troubleshoot Policies	VSwitch Policies					
Pools	Port Channel Policy:	select a value				
Physical and External Domains	LLDP Policy:	select a value 👻 🗗				
	CDP Policy:	CDP_ON 🗸 🗗				
	STP Policy:	select a value				
	Firewall Policy:	select a value				
	· · · · · · · · · · · · · · · · · · ·					

Versión no admitida

Verifique que la versión de VEM sea correcta y admita el sistema VMWare de ESXi adecuado.

```
~ # 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
```

No funciona la comunicación de VEM y fabric

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 En este punto, se puede determinar que la comunicación del fabric entre el host ESXi y la hoja no funciona correctamente. Algunos comandos de verificación se pueden verificar en el lado de la hoja para determinar la causa raíz.

leaf2# show cdp ne Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge S - Switch, H - Host, I - IGMP, r - Repeater, V - VoIP-Phone, D - Remotely-Managed-Device, s - Supports-STP-Dispute Device-ID Local Intrfce Hldtme Capability Platform Port ID AVS:localhost.localdomainmain 169 S I s VMware ESXi Eth1/5 vmnic4 AVS:localhost.localdomainmain Eth1/6 169 SIS VMware ESXi vmnic5 N3K-2(FOC1938R02L) Eth1/13 166 R S I S N3K-C3172PQ-1 Eth1/13 leaf2# show port-c sum Flags: D - Down P - Up in port-channel (members) I - Individual H - Hot-standby (LACP only) s - Suspended r - Module-removed S - Switched R - Routed U - Up (port-channel) M - Not in use. Min-links not met F - Configuration failed _____ _____ Group Port-Protocol Member Ports Туре Channel _____ Eth LACP Eth1/5(P) Eth1/6(P) 5 Po5(SU) Hay 2 puertos que se utilizan en el ESXi conectados a través de un 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	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	

A partir del resultado anterior, se puede observar que la Vlan Infra no está permitida ni pasa a través de los puertos Uplinks que van al host ESXi (1/5-6). Esto indica un error de configuración con la política de interfaz o la política de switch configurada en APIC. Verifique ambos:

Políticas de acceso > Políticas de interfaz > Perfiles Políticas de acceso > Políticas de switch > Perfiles

En este caso, los perfiles de interfaz se conectan al AEP incorrecto (antiguo AEP utilizado para DVS), como se muestra en la imagen:

Access Port Policy Group	- AVS-102_1-ports-7	_PolGrp						Ð	×
						Poli	sy Fault	s Histo	ŋ
⊙±								ACTIONS	
Properties									
Name:	AVS-102_1-ports-7_PolGrp								ï
Description:	optional								
Label:									
Link Level Policy:	1GigAuto	· @							
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								l
Attached Entity Profile:	AEP_DVS	e							
Connectivity Filters:				×	+				
	Switch IDs		Interfaces						
						SHOW USAGE	SUBMIT	CLOSE	

Después de configurar el AEP correcto para AVS, ahora podemos ver que la Vlan Infra se ve a través de los Unlinks adecuados en la hoja:

leaf2# show vlan extended

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

```
VLAN Type Vlan-mode Encap
 _____ _____
13
    enet CE
                    vxlan-16777209, vlan-3967
                    vxlan-14680064, vlan-150
19 enet CE
22 enet CE
                   vxlan-16383902
26 enet CE
                   vxlan-15531929, vlan-200
    enet CE
27
                    vlan-11
28
    enet CE
                     vlan-14
 36 enet CE
                    vxlan-15662984
and Opflex connection is restablised after restarting the VEM module:
~ # vem restart
stopDpa
VEM SwISCSI PID is
Warn: DPA running host/vim/vimuser/cisco/vem/vemdpa.213997
Warn: DPA running host/vim/vimuser/cisco/vem/vemdpa.213997
watchdog-vemdpa: Terminating watchdog process with PID 213974
~ # vemcmd show opflex
Status: 0 (Discovering)
Channel0: 14 (Connection attempt), Channel1: 0 (Discovering)
Dvs name: comp/prov-VMware/ctrlr-[AVS]-vCenterController/sw-dvs-129
Remote IP: 10.0.0.30 Port: 8000
Infra vlan: 3967
FTEP IP: 10.0.32
Switching Mode: unknown
Encap Type: unknown
NS GIPO: 0.0.0.0
~ # vemcmd show opflex
Status: 12 (Active)
Channel0: 12 (Active), Channel1: 0 (Discovering)
Dvs name: comp/prov-VMware/ctrlr-[AVS]-vCenterController/sw-dvs-129
Remote IP: 10.0.0.30 Port: 8000
Infra vlan: 3967
FTEP IP: 10.0.0.32
Switching Mode: LS
Encap Type: unknown
NS GIPO: 0.0.0.0
```

Información Relacionada

Instalación del switch virtual de la aplicación

<u>Cisco Systems, Inc. Guía de Instalación de Cisco Application Virtual Switch, Versión</u> <u>5.2(1)SV3(1.2)</u> Implemente ASAv con VMware

<u>Guía de inicio rápido de Cisco Systems, Inc. Cisco Adaptive Security Virtual Appliance (ASAv),</u> <u>9.4</u>

Cisco ACI y Cisco AVS

Cisco Systems, Inc. Guía de virtualización de Cisco ACI, versión 1.2(1i)

Informe técnico sobre diseño de gráficos de servicios con Cisco Application Centric Infrastructure

Informe técnico sobre diseño de gráficos de servicios con Cisco Application Centric Infrastructure

Soporte Técnico y Documentación - Cisco Systems