使用AVS-ACI 1.2(x)版本的GoTo(L3)模式中的 **ASAv**

目录

简介 <u>先决条件</u> 要求 使用的组件 配置 网络图 配置 验证 故障排除 相关信息

简介

本文档介绍如何在路由/GOTO模式下使用自适应安全虚拟设备(ASAv)单防火墙部署应用虚拟交换机 (AVS)交换机,作为两个终端组(EPG)之间的L4-L7服务图,以使用ACI 1.2(x)建立客户端到服务器通 信释放。

先决条件

要求

Cisco 建议您了解以下主题:

- •已配置访问策略,且接口已打开和正在使用 •已配置EPG、网桥域(BD)和虚拟路由和转发(VRF)

使用的组件

本文档中的信息基于以下软件和硬件版本:

硬件和软件:

- 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)
- 枝叶/主干 11.2(1i)
- 已下载设备包*.zip

功能:

- AVS
- ASAv
- EPG、BD、VRF
- •访问控制列表(ACL)
- L4-L7服务图
- vCenter

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

配置

网络图

如图所示,



配置

AVS初始设置创建VMware vCenter域(VMM集成)2

注意:

- 您可以在单个域下创建多个数据中心和分布式虚拟交换机(DVS)条目。但是,您只能将一个思 科AVS分配给每个数据中心。
- •思科AVS版本1.2(1i)和思科AVS版本5.2(1)SV3(1.10)支持使用思科AVS的服务图部署。 整个服

务图配置在思科应用策略基础设施控制器(思科APIC)上执行。

- 只有采用虚拟局域网(VLAN)封装模式的虚拟机管理器(VMM)域才支持使用思科AVS的服务虚拟机(VM)部署。但是,计算VM(提供商和消费者VM)可以是采用虚拟可扩展LAN(VXLAN)或VLAN封装的VMM域的一部分。
- 另请注意,如果使用本地交换,则不需要组播地址和池。如果未选择本地交换,则必须配置组播池,并且AVS交换矩阵范围的组播地址不应属于组播池。从AVS发起的所有流量都将封装为VLAN或VXLAN。

导航至VM Networking > VMWare > Create vCenter Domain,如图所示:

				ĺ
ontrollers				
AVS	_			
VMware vSphere Dis	stributed Switch	Cisco AVS		
No Local Switching	Local Switching	3		
VLAN				
O VXLAN				
AEP-AVS	•	æ		
VlanPool-AVS(dynamic	c) 🗸	æ		
		×	F	
Name	Description			
			×	+
Profile Name	Username	Description		
vCenterCredentials	root			
			×	+
Name	IP	Тире	State Collection	+
	Ontrollers AVS VMware vSphere Dist No Local Switching VLAN VXLAN AEP-AVS VlanPool-AVS(dynami Name Profile Name vCenterCredentials	Ontrollers AVS VMware vSphere Distributed Switch No Local Switching Local Switching VLAN VXLAN AEP-AVS VlanPool-AVS(dynamic) Name Description Profile Name Username vCenterCredentials root	AVS VMware vSphere Distributed Switch No Local Switching Local Switching VLAN VXLAN AEP-AVS VlanPool-AVS(dynamic) C X Name Description	AVS VMware vSphere Distributed Switch No Local Switching Local Switching VLAN VXLAN AEP-AVS VlanPool-AVS(dynamic) C Vame Description

如果您使用的是端口通道或VPC(虚拟端口通道),建议将vSwitch策略设置为使用Mac Pinning。 此后,APIC应将AVS交换机配置推送到vCenter,如图所示:



在APIC上,您可以注意到VXLAN隧道终端(VTEP)地址已分配给AVS的VTEP端口组。无论使用什么 连接模式(VLAN或VXLAN),都会分配此地址

Inventory	Portgroup - vtep					Ormeral Faults Hat	i
DeenStack Wavare	O₩			A A O O			
VS VS Ontrollers VCenterController	Properties Name: Encap:	vlep vlan-3967					
Hypervisors 10.201.35.218	Management Network Adapters:	Server Name 10.201.35.219	Name vmk1	State	MAC 00:50:56:68:CA:25	IP Address 10.0.16.95	-
► ↓ 10.201.36.219 ▲ 10 OVS - AVS		10.201.35.218	vmk1	Up	00.50.56.61.07.CC	10.0.18.94	
Portgroups Pod6-ALUMBRERIAVS-AEP-VMM-a							
Quarantine Quink Quarantine Quink							
DVS							
		(Page 1 Of	$ \rangle $	Objects Per	Page 15 -	Displaying Objects 1 - 2 Of 2	2

在vCenter中安装Cisco AVS软件

•使用此链接从CCO下载vSphere安装捆绑包(VIB)

注意:在本例中,我们使用ESX 5.5,表1显示ESXi 6.0、5.5、5.1和5.0的兼容性矩阵

表1 - ESXi 6.0、5.5、5.1和5.0的主机软件版本兼容性

Villware 1	vib 2	VEM Bundle 2	Windows VC Installer	Linux vCenter Server Appliance
ESXI 6.0	cross_cisco-vem- v250-5.2.1.3.1.10.0-6.0.1.vib	VEM600-201512250119-BG- missae.zip (Offine) VEM600-201512250119-BG (Online)	6.0	6.0
ESX 5.5	cross_cisco-vem-v250-5.2.1.3.1.10.0-3.2.1.vib	VEM550-201512250113-BG- release.zip (Offine) VEM550-201512250113-BG (Online)	5.5	5.5
ESXI 5.1	cross_cisco-vem- v250-5.2.1.3.1.10.0-3.1.1.vib	VEM510-201512250107-8G- release.zip (Offine) VEM510-201512250107-8G (Online)	5.1	5.1
ESX 5.0	cross_cisco-vem- v250-5.2.1.3.1.10.0-3.0.1.vib	VEM500-201512250101-8G- release zip (Offline) VEM500-201512250101-8G (Online)	5.0	5.0

在ZIP文件中有3个VIB文件,每个ESXi主机版本对应一个,请选择适合ESX 5.5的一个文件,如图 所示:

CiscoAVS_1.10-5.2	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 archi
VEM550-201512250113-BG-release.zip	Dec 9, 2015, 12:10 AM	Dec 9, 2015, 12:10 AM	8.6 MB	ZIP archi
VEM600-201512250119-BG-release.zip	Dec 9, 2015, 12:10 AM	Dec 9, 2015, 12:10 AM	8.6 MB	ZIP archi

• 将VIB文件复制到ESX Datastore — 这可以通过CLI或直接从vCenter完成

注意:如果主机上存在VIB文件,请使用esxcli软件vib remove命令将其删除。

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

或直接浏览Datastore。

• 在ESXi主机上使用以下命令安装AVS软件:

esxcli软件vib install -v /vmfs/volumes/datastore1/cross_cisco-vem-v250-5.2.1.3.10.0-3.2.1.vib —maintenance-mode —no-sig-check



•一旦虚拟以太网模块(VEM)启动,您就可以将主机添加到AVS:

在向vSphere分布式交换机添加主机对话框中,选择连接到枝叶交换机的虚拟NIC端口(在本示例中,您仅移动vmnic6),如图所示:

dd Host to vSphere Distributed Swite	h			
Select Hosts and Physical Adapter	•			
Select hosts and physical adapters	to add to this vSphere distributed switd	h.		
Select Host and Physical Adapters			Settings	View Incompatible Host
Network Connectivity	Host/Physical adapters	In use by switch	Settings	Uplink port group
Artual Machine Networking	E I 10.201.35.218		View Details	
Ready to Complete	Select physical adapters			
	vmnic0	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
Hada I			and I	Count
help			< Back	Cancel

- 单击"下一步"
- 在Network Connectivity对话框中,单击Next(下一步)
- •在"虚拟机网络"对话框中,单击"下一步"
- •在准备完成对话框中,单击完**成**

注意:如果使用多台ESXi主机,则所有主机都需要运行AVS/VEM,以便从标准交换机管理到 DVS或AVS。

因此,AVS集成已完成,我们已准备好继续L4-L7 ASAv部署:

ASAv初始设置

• 下载Cisco ASAv设备包并将其导入APIC: 导航到**L4-L7服务>包>导入设备包,**如图所示:

Fabric	VM Networking	L4-L7 Services	Admin	Operations	
		Inventory Packages			
Quick Sta	rt				
HELP	es menu allows vou to in	nport L4-L7 device pac	kages, which are use	d to define, configure, and m	nonitor a network service
balancer, co and network	ntext switch, SSL termina connectivity information	tion device, or intrusio for each function. A ne	n prevention system twork service device	(IPS). Device packages cont is deployed in the network b	ain descriptions of the fi y adding it to a service ç
You can use configuring a	the Import a Device Pa	ckage wizard to import	a device package fo	r a function that you want to	manage with APIC. We
	In	nport Device Pa	ackage	i	×
Quick Import a	Start a Device Package	File Name:		BROWSE	Device Types

• 如果一切正常,您可以看到已导入的设备包正在扩展L4-L7服务设备类型文件夹,如图所示:

SUBMIT

CLOSE

i

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

					General	Operational	Faults	History
⊙₹							ACT	
Properties								
Vendor:	CISCO altalia 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							

在继续之前,在执行实际的L4-L7集成之前,需要确定安装的几个方面:

管理网络分为两种类型:带内管理和带外(OOB),它们可用于管理不属于基本以应用为中心的基础 设施(ACI)(枝叶、主干或apic控制器)的设备,包括ASAv、负载均衡器等。

在这种情况下,ASAv的OOB使用标准vSwitch进行部署。对于裸机ASA或其他服务设备和/或服务器 ,将OOB管理端口连接到OOB交换机或网络,如图所示。



ASAv OOB管理端口管理连接需要使用ESXi上行链路端口通过OOB与APIC通信。映射vNIC接口时 ,网络适配器1始终与ASAv上的Management0/0接口匹配,其余数据平面接口从网络适配器2启动

表2显示网络适配器ID和ASAv接口ID的协调:

表 2

0

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

• 通过File>Deploy OVF(Open Virtualization Format)Template中的向导部署ASAv VM

• 如果要**将独立**ESX Server或asav-vi用于vCenter,请选择asav-esxi。在本例中,使用vCenter。



 通过安装向导,接受条款和条件。在向导的中间,您可以确定多个选项,如主机名、管理、 IP地址、防火墙模式和与ASAv相关的其他特定信息。切记对ASAv使用OOB管理,在本例中,您需要在使用VM网络(标准交换机)时保留接口Management0/0,而接口GigabitEthernet0-8是默认网络端口。

Deploy OVF Template	
Source Select the source location.	
Source OVF Template Details Name and Location Storage Disk Format Ready to Complete	Deploy from a file or URL I: Documents'IGSP/ACT/IMAGE'asav952'asav-viLovf Image: Browse Ther a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.
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 IP-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 Ketter HA		ASAv-w-AVS	
Help < Back			
Help < Back		Firewall Properties	
Select the Firewall Mode routed Management Interface Settings Hanagement Interface DHCP mode Choose whether to use DHCP for Management interface configuration. Imagement IP Address Enter the Management IP-v4 Address. For HA-type deployments, this property specifies the Management IP-v4 Address of the Active HA host. ID .01 Hanagement IP Subnet Hask Imagement IP Subnet Hask Imagement IP Subnet Hask Imagement IP Subnet Hask		Firewall Mode	
Management Interface Settings Management Interface DHCP mode Choose whether to use DHCP for Management interface configuration. Imagement IP Address Enter the Management IPv4 Address. For HA-type deployments, this property specifies the Management IPv4 address of the Active HA host. Imagement IP Subnet Hask Help		Select the Firewall Mode	
Imagement Interface Settings Hanagement Interface DHCP mode Choose whether to use DHCP for Management interface configuration. Imagement IP Address Enter the Management IP-v4 Address. For HA-type deployments, this property specifies the Management IP-v4 address of the Active HA host. 10 .201 Hanagement IP Subnet Hask Ket Cancel			
Hanagement Interface Settings Hanagement Interface DHCP mode Choose whether to use DHCP for Management interface configuration. Imagement IP Address Enter the Management IP v4 Address. For HA-type deployments, this property specifies the Management IP v4 address of the Active HA host. Imagement IP Subnet Hask Help Ket >		routed	
Hanagement Interface DHCP mode Choose whether to use DHCP for Management interface configuration. Hanagement IP Address Enter the Management IPv4 Address. For HA-type deployments, this property specifies the Management IPv4 address of the Active HA host. 10 . 201 . 35 . 223 Hanagement IP Subnet Hask		Management Interface Settings	
Help <back< td=""> Next > 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

Deploy OVF Template	Inventory 1 🗃 Husto and Clusters		x
Ready to Complete Are these the options yo	u want to use?		
Source OVF Template Details End User License Agreement	When you click Finish, the deploym Deployment settings:	ent task will be started.	
Name and Location	Size on disk:	8.3 G8	
Deployment Configuration	Name:	ASAv-in-AVS	
Storage	Folder	ACI	
Natural Marries	Deployment Configuration:	1 Gbps(ASAv10)	
Properties	Host/Cluster:	10.201.35.219	
Ready 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"	1
	Network Mapping:	"GigabitEthernet0-2" to "VM Network"	
	Network Mapping:	"GigabitEthernet0-3" to "Pod6-ALUMBRERIAVS-AEP-VMM-alumbreriAV	
	Network Mapping:	"GigabitEthernet0-4" to "Pod6-ALUMBRER InternalAEP-VMM-alumbref_	
	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"	u.
	IP Allocation:	Fixed, IPv4	
	Property:	HARole = Standalone	
	Property:	Hostname = ASAv-w-AVS	
	Property:	PWMode = routed	
	Property:	DHCP = False	
	Property	Management3Pv4 = 10.201.35.223	
	Property	Management2Pv4Subnet = 255.255.255.0	
	Property:	ManagementStandbyIPv4 = 0.0.0.0	
	Property:	RouteDefault = Default Route	
		11 100 200 F 110 1 28 003 00 2	٠
	Power on after deployment		
Help		< Back Finish Cano	el
10 M (10 m 10			

• 单击**Finish**,等待ASAv部署完成

Deployment Completed Successfully	X
Deploying ASAv-in-AVS	
Completed Successfully	
	Close

• 打开ASAv VM电源并通过控制台登录以验证初始配置

interface Management0/0 Management-only nameif management security-level 0 ip address 10.201.35.223 255.255.255.0 ftp mode passive pager lines 23 mtu management 1500 no failover icmp unreachable rate-limit 1 burst-size 1 no asdm history enable arp timeout 14400 no arp permit-nonconnected 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 --->

 如图所示,某些管理配置已推送到ASAv防火墙。配置管理员用户名和密码。此用户名和密码由 APIC用于登录和配置ASA。ASA应能连接到OOB网络,并且应能到达APIC。

username admin password <device_password> encrypted privilege 15

ASAv-w-AUS(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)# _

此外,在全局配置模式下启用http服务器:

HTTP服务器启用

http 0.0.0.0 0.0.0.0管理

APIC中ASAv集成的L4-L7:

- •登录ACI GUI,点击将部署服务图的租户。展开导航窗格底部的L4-L7服务,右键单击L4-L7设备,然后单击创建L4-L7设备以打开向导
- •对于此实施,将应用以下设置:

— 托管模式

— 防火墙服务

— 虚拟设备

— 通过单节点连接到AVS域

- -ASAv型号
- 路由模式(GoTo)

— 管理地址(必须与之前分配给Mgmt0/0接口的地址匹配)

•默认情况下,将HTTPS用作APIC使用最安全的协议与ASAv通信

STEP 1 > General					1. General 2. Devic	e Configuration
Please select device	package and enter connectivity info	rmation.				
General Managed: Name: Service Type:	ASAv-AVS-Routed	Device 1 Management IP Address: VM: Device Interfaces:	10.201.35.3 vCenterController/AS	Av-in-AVS 👻 🗗	Management Port: https	× +
Device Type: VMM Domain: Mode: Device Package: Model:	PHYSICAL VIRTUAL AVS C Single Node HA Cluster CISCO-ASA-1.2 C ASAv		Name GigabitEthernet0/0 GigabitEthernet0/1	VNIC Network adapter 2 Network adapter 3	Path (Only For Route Peering) Node-102/MAC_Pinning Node-102/MAC_Pinning	
Function Type:	GoThrough GoTo	Cluster Management IP Address: Cluster Interfaces:	10.201.35.3		Management Port: https	× +
			Type	Name	Concrete Interfaces	
Connectivity APIC to Device Management Connectivity:	Out-Of-Band In-Band		consumer	ClientInt	Device 1/GigabitEthernet0/1	
Credentials Username: Password: Confirm Password:	admin					

(i) X

•正确定义设备接口和集群接口对于成功部署至关重要

对于第一部分,使用上一节中显示的表2,将网络适配器ID与要使用的ASAv接口ID正确匹配。路径 是指启用进出防火墙接口的方式的物理端口或端口通道或VPC。在这种情况下,ASA位于ESX主机 中,其中传入和传出对于两个接口都是相同的。在物理设备中,防火墙(FW)的内部和外部是不同的 物理端口。

对于第二部分,必须始终定义集群接口,而不例外(即使不使用集群HA),这是因为对象模型在 mlf接口(设备包上的元接口)、Llf接口(枝叶接口,如外部、内部、内部等)与Clf(具体接口)。L4-L7具体设备必须在设备集群配置中配置,这种抽象称为逻辑设备。逻辑设备具有逻辑接口 ,这些逻辑接口映射到具体设备上的具体接口。

在本例中,将使用以下关联:

Gi0/0 = vmnic2 = 服务器接口/提供商/服务器> EPG1

Gi0/1 = vmnic3 =客户端接口/消费者/客户端> EPG2

L4-L7 Devices - ASAv-AVS-Routed							i
				Policy	Parameters	Faults	History
						AC	TIONS -
General 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 CleTe	Device 1 Management IP Address: vCenter Name: Interfaces:	10.201.35.223 vCenterController Name GigabitEthemet0/1 GigabitEthemet0/2	Managemer VM Vetwork adapt Network adapt	nt Part: 443 Name: ASAv-in-J Ner 3 Ner 4	Path (Only Fe Node-102/M	er Route Per AC_Pinning	× + ering) g. Nod
Credentials Username: admin Password:	Cluster Management IP Address: Cluster Interfaces:	10.201.35.223 Type	Managemen Name Classifiet	Concrete Interfa	ces fed_Device_1/	¢ (Gigeoritim	× +
Configuration State Configuration Issues: Devices State: stable	<	provider	Serverint	ASAv-AVS-Rou	ited_Device_1/	(GigabitEth	emet0/1]

注意:对于故障切换/HA部署,GigabitEthernet 0/8已预配置为故障切换接口。

设备状态应为"稳定",您应准备好部署功能配置文件和服务图模板

服务图庙

首先,为ASAv创建功能配置文件,但在此之前,您需要在该文件夹下创建功能配置文件组,然后创 建L4-L7服务功能配置文件,如图所示:

Create L4-L7 Service	s Function Profile Group	i ×
Specify the informatio	n about the Function Profile Group	
Name:	FunProfGroup	
Description:		
		SUBMIT CANCEL

Tenent Pod6-ALUMORER 🔄 🖸	L4-L7 Services Fi	unction Profile	Group - FunProGroup				
Quick Start	1						
Tenant Pod8-ALUMBRER					General	Faults	History
Application Profiles	OF					AC	TIONS -
Networking							
L4-L7 Service Parameters	Properties						
Security Policies	Name:	FunProGroup					
Troubleshoot Policies	Description:						
Monitoring Policies	Service Function Profiles:						× +
L4-L7 Services							~ +
L4-L7 Service Graph Templates		 Name 	Associated Function	Description			
Router configurations				No items have been found.			
🔺 🖿 Function Profiles			,	select Actions to create a new item.			
C FunProGroup							
L4-L7 Devices Delete							
Imported Devices Create L4-L7 Services F	unction Profile						
Devices Selection Save as							
Deployed Graph In Kar Post							
Deployed Devices	-						
Inband Management Configuration for L4-L7 dev	ko						

 从下拉菜单中选择WebPolicyForRoutedMode 配置文件,然后继续配置防火墙上的接口。从此 开始,这些步骤是可选的,可以稍后实施/修改。这些步骤可在部署的几个不同阶段执行,具体 取决于服务图的可重用性或自定义程度。

在本练习中,路由防火墙(GoTo模式)要求每个接口都有唯一的IP地址。标准ASA配置还具有接口 安全级别(外部接口安全性较低,内部接口安全性较高)。 您还可以根据需要更改接口的名称。本 示例中使用默认值。

• 展开接口特定配置,为ServerInt添加IP地址和安全级别,IP地址为**x.x.x.x/y.y.y.或 x.x.x.x/yy,格式如下**。对ClientInt接口重复该过程。

Create Function Profile				
Name: Description:	FunProf-ASA optional			
Copy Existing Profile Parameters: Profile:	CISCO-ASA-1.2/WebPolicyForRoutedMode	-		
Features and Parameters	In order to auto apply new values to the parameters	of existing graph instance when users modify	function profiles, the name of top fol	der must be ended with -Default.
Features:	Basic Parameters All Parameters		Mandatan	O toread
Interfaces	Folder/Param	Name Value	Mandatory Locked	Shared
AccessLists	Bridge Group Interface			
NAT	📰 😑 🛛 🔺 🖼 Interface Related Configuration	externalif	false	false
TrafficSelectionObjects	Access Group	ExtAccessGroup	false	
All	IPv6 Enforce EUI-64			
	E Interface Specific Configur	. externallfCfg	false	
	Pv4 Address Configura. Pv4 Address Pv4 Address Pv4 Address Pv4 Address	pv4_address 192.168.10.1/24		
	IPv6 Address Configura.	UPDATE RESET CAN	CEL	
	I Pv6 Link Local Address.	9		

SUBMIT CANCEL

注意:您还可以修改默认访问列表设置并创建您自己的基本模板。默认情况下,路由模式模板 将包含HTTP和HTTPS规则。在本练习中,SSH和ICMP将添加到允许的外部访问列表。

Name:	FunProf-ASA							
Description:	optional							
Copy Existing Profile Parameters:	•							
Profile:	CISCO-ASA-1.2/Web	PolicyForRoutedMode	- CP					
eatures and Parameters								
	In order to au	to apply new values to the paramet	ters of existing graph	instance when users	modify function profiles, the	he name of top folder	must be ended with -	Default.
Features:	Basic Param	All Parameters						
Interfaces	Folde	er/Param	Name	Value	Mandatory	Locked	Shared	
internaces	8	Destination Service	destination_ser	vice				
AccessLists		- 📃 High Port						
NAT		- 🔁 Low Port	low_port	22		false		
TrafficSelectionObjects		Operator	operator	eq		false		
All		E CMP						
		Logging						
		Protocol						
		Source Address						
		Source Service						
		Action	action	permit		false		
		- El Order	order	30		false		

• 然后单击Submit

• 现在,创建服务图模板		
Tenant Pod6-ALUMBRER	 O 	L4-L7 Service
Cuick Start		
Tenant Pod6-ALUMBRER		
Application Profiles		⊖±
Networking		Name
L4-L7 Service Parameters		- Name
Security Policies		
Troubleshoot Policies		
Monitoring Policies		
🔺 💼 L4-L7 Services		
L4-L7 Service Graph Templates		
Router configurations	Create L4-L7 S	service Graph Template

• 将设备集群拖放到右侧以形成消费者和提供商之间的关系,选择路由模式和先前创建的功能配置文件。

Graph Name:	Graph1-alumbrer		
Graph Type:	Create A New One	Clone An Existing One	
Consumer EPG		ASAv-AVS	vider PG
ASAV-AVS-BOU	Please drag a de	vice from devices table and drop it here to create a service node.	
Firewall:	 Routed Transpare 	ıt	
Profile:	Pod6-ALUMBRER/FunProfGroup/FunF	ro 👻 🔁	
		SUBMIT CA	NCEL

•检查模板是否存在故障。模板创建为可重用,然后必须应用于特定EPG等。

Tenant Pod6-ALUMBRER 🛛 🖉 🖸	L4-L7 Service Graph Template - Graph1-alumbrer		i
Quick Start			
Tenant Pod6-ALUMBRER	Topology Pr	plicy Faults	History
Application Profiles			
Networking	Consumer	Provider	
L4-L7 Service Parameters			
Security Policies			
Troubleshoot Policies	ASAY-AVS	S	
Monitoring Policies			
L4-L7 Services	ASAy		
L4-L7 Service Graph Templates			
Graph1-alumbrer	outed information		
Function Node - ASA Apply L4-L7 S	rvice Graph Template II: Routed		
Router configurations Edit L4-L7 Ser	ice Graph Template p: FunPro-ASA		
I Function Profiles Delete			
A 🔯 FunProfGroup 🔀 Remove Relat	d 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 dev			
		CURNET	DEGET

•要应用模板,请右键单击并选择应用L4-L7服务图模板

- 定义哪个EPG将位于消费者端和提供商端。在本练习中,AVS-EPG2是消费者(客户端),AVS-EPG1是提供商(服务器)。请记住,未应用过滤器,这将允许防火墙根据此向导最后一节中定义的访问列表执行所有过滤。
- 单击"下一步"

TEP 1 > Contract			1. Contract	2. Graph
Config A Contract Between EPGs				
EPGs Information	Provider EPG / External Network:		5	
	Provider EPG / External Network.	Pod6-ALUMBRER/AVS-AEP-VMM	3	
Contract Information		alumbrer/epg-AVS-EPG1		
Contract: Create A New Contract Choose Ar	Existing Contract Subject	Pod6-ALUMBRER/InternalAEP-		
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		

• 验证每个EPG的BD信息。在这种情况下,EPG1是IntBD DB上的提供商,EPG2是BD ExtBD上 的消费者。EPG1将连接到防火墙接口ServerInt,EPG2将连接到接口ClientInt。两个防火墙接 口将成为每个EPG的DG,因此流量会被迫始终通过防火墙。

• 单击"下一步"

Graph Template:	Pod6-ALUMBRER/Graph1-Temp-alumbrer		•	e e	
Consumer EPG AVS-EPG2	C	D	ASAv-AVS ASAv	P	AVS-EPG1
ASAV-AVS-Routed Infor Firewal Profile Consumer Connector	mation I: routed b: FunPro-ASA				
BD: Cluster Interface:	General O Houte Peering Pod6-ALUMBRER/ExtBD-alumbrer ClientInt	•	æ		
Provider Connector – Type: BD:	General General ORoute Peering Pod6-ALUMBRER/IntBD-alumbrer	•	æ		
Cluster Interface:	ServerInt	Ŧ	æ		

PREVIOUS NEXT CANCEL

PREVIOUS NEXT CANCEL

• 在"配置参数"部分,单击"所**有参数"**,并验证是否有需要更新/配置的红色指示灯。在如图所示的 输出中,可以注意到访问列表上的顺序丢失。这相当于您在show ip access-list X中看到的行顺

PREVIOUS FINISH CANCEL

config	paramet	iers for	the se	lected	device
--------	---------	----------	--------	--------	--------

			Alama	Abb us	Utility Property
200.		A Constant	access list internet	Veloe	witte Domein
st.inma		Access Control Entry	ICMP		
		Access Control Entry	5100		
		Access Control Entry	SSH		
		Destination Address			
	8	Destination Service	destination_service		
		EMP			
		Eogging			
	8	Protocol	protocol		
		Source Address			
		Source Service			
		3 Action	action	permit	
		Crder	order	(30)	select asa domain
	78	Access Control Entry		100	
		Access Control Entry	UPDATE MEDICI CA	MUEL .	

您还可以验证从前面定义的功能配置文件分配的IP编址,如果需要,此处是更改信息的良机。
 设置所有参数后,单击完成,如图所示:

TEP 3 > ASAv-AVS-Route	ed Parameters	1. Contra	act 2. Graph	3. ASAv-AVS-Routed Parameters
config parameters for the sele	ected device			
Profile Name: FunProf-ASA	1			
Features:	Required Parameters All Parameters			
Interfaces	Folder/Param	Name	Value	Write Domain
Accessi inte	E 🔺 😅 Device Config	Device		
Accessuists		access-list-inbound		
NAT	📰 🔲 🕨 💭 Bridge Group Interface			
TrafficSelectionObjects	Interface Related Configuration	externalif		
All	E 🔺 🖼 Access Group	ExtAccessGroup		
	Inbound Access List	name	access-list-inbound	
	Outbound Access List			
	IPv6 Enforce EUI-64			
	Interface Specific Configuration	externalIfCfg		
	E IPv4 Address Configuration	IPv4Address		
	IPv4 Address	ipv4_address	192.168.10.1/24	
	IPv4 Standby Address			
	IPv6 Address Configuration			
	IPv6 Link Local Address Configuration			
	IPuR Router Advertisements			

• 如果一切正常,应显示新的已部署设备和图形实例。



验证

创建服务图后需要验证的一件重要事是,使用正确的元连接器创建了消费者/提供商关系。在"函数连接器属性"下验证。

Tenant Podb-ALUMBRER	Function Connec	ctor - consume	er					- i
Quick Start								
Tenant Pod6-ALUMBRER						Policy	Faults	History
Application Profiles							AC	TIONS -
Networking				6				
L4-L7 Service Parameters	Properties							
Security Policies	Name	consumer						
Troubleshoot Policies	Attachment Notification:	false						
Monitoring Policies	Filters	select an option	-					
L4-L7 Services	Meta Connector:	Firewall/internal	- d	ዋ				
L4-L7 Service Graph Templates								
🖌 💙 Graph1-alumbrer								
4 📃 Function Node - ASAv								
Consumer								
📃 provider								

注意:防火墙的每个接口将分配一个来自AVS动态池的encap-vlan。验证是否没有故障。

ALL TENANTS Add Tenant Search: enter name, descr	common Pod6-AL	UMBRER Pod6-ALUMBRER2 Infra n						
Tenant Pod6-ALUMBRER 🛛 🗐 🖸	Virtual Device - A	SAv-AVS-Routed-none						i
Quick Start				_	-			
Tenant Pod6-ALUMBRER				Polic	y Operational	Health	Faults	History
Application Profiles	€		A A O O 1	00				
Networking	Descettes							
L4-L7 Service Parameters	Properties							
Security Policies	Devices:	ASAv-AVS-Routed						
Troubleshoot Policies	VIRUAI Device ID:	25351						
Monitoring Policies	ACKed Transaction ID:	10000						
L4-L7 Services	Current Transaction ID:	10000						
L4-L7 Service Graph Templates	Cluster Interfaces:	Logical Interface	Encap					
Router configurations		ASAv-AVS-Bouted Clientint	vian-01					
Function Profiles			THEFT					
L4-L7 Devices		ASAv-AVS-Routed_ServerInt	vlan-94					
Imported Devices								
Devices Selection Policies								
Deployed Graph Instances								
EPG2-to-EPG1-Graph1-alumbrer-Pod6-ALUN								
Deployed Devices								
ASAv-AVS-Routed-none								
 Inband Management Configuration for L4-L7 devi 								

• 现在,您还可以验证推送到ASAv的信息

ISAv-w-AVS# show interface	ip brief				
Interface	IP-Address	OX?	Method	Status	Prot
ocol					
igabitEthernet0/0	192.168.10.1	YES	manua l	սք	սք
iigabitEthernet0/1	172.16.1.1	YES	manua l	սք	սք
iigabitEthernet0/2	unassigned	YES	unset	administratively down	սք
iigabitEthernet0/3	unassigned	YES	unset	administratively down	սք
igabitEthernet0/4	unassigned	YES	unset	administratively down	սք
iigabitEthernet0/5	unassigned	YES	unset	administratively down	սք
iigabitEthernet0/6	unassigned	YES	unset	administratively down	սք
iigabitEthernet0/7	unassigned	YES	unset	administratively down	սք
iigabitEthernet0/8	unassigned	YES	unset	administratively down	սք
lanagement0/0	10.201.35.223	YES	CONFIG	սք	սք
ISAv-w-AVS# show run access	s-list				
ccess-list access-list-inl	oound extended	permit	; tcp ar	ny any eq ымы	
access-list access-list-ind	oound extended	permit	tcp ar	ny any eq https	
access-list access-list-ind	oound extended	permit	tcp an	ny any eq ssh	
access-list access-list-ind	oound extended	permit	ісмра	any any	
42UA-u-AUS#					

• 在EPG下分配新合同。从现在起,如果您需要修改访问列表上的任何内容,则必须从提供商 EPG的L4-L7服务参数进行更改。

Tenant Pod6-ALUMERER	L4-L7 Service Parame	eters					i
Quick Start Jan Tenant Pod6-ALUMBRER	Search By Name / Value:						
Application Profiles	•				Ecider Param Instance		
A S EPG AV8-EPG	Meta Folder/Param Key	Contract Name	Service Graph Name	Service Function Name	Name	Value	Specific Device
Provide Calls and Bars Marchill	Interface	EPG240-EPG1	Graph1-Temp-alumbrer	ASAv	Clientint		
Contains (Viva and bare-weakly	ExintConfigRelFolder	EPG24o-EPG1	Graph1-Temp-alumbrer	ASAv	ExtConfig		
State Bindings (Paths)	InintConfigRelFolder	EPG240-EPG1	Graph1-Temp-alumbrer	ASAv	IntConfig		
Static Bindings (Leaves)	Interface	EP024o-EP01	Graph1-Temp-alumbrer	ASAv	Serverint		
Contracts Static EndPoint L4-L7 Vinual Pe L4-L7 IP Address Pool L4-L7 Envice Parameters C4-L7 Envice Parameters	AccessList	EPG240-EPG1	Graph1-Temp-alumbrer	ASAv	access-list-inbound		

• 在vCenter上,您还可以验证影子EPG是否已分配给每个防火墙接口:

ſ	🕜 AS	Av-in-AVS - Virtual Machine Pro	operties		
H	Hardv	vare Options Resources Prof	iles vServices	Virtual Machine Version: 8 orage Vie	ws
		Show All Devices	Add Remove	Device Status Connected	_
r I	Hard	lware	Summary	Connect at power on	
		Memory CPUs Video card VMCI device SCSI controller 0 CD/DVD drive 1 CD/DVD drive 2 Hard disk 1 Hard disk 2 Network adapter 1 Network adapter 3 Network adapter 4 Network adapter 5 Network adapter 6 Network adapter 7	2048 MB 1 Video card Restricted LSI Logic Parallel [datastore4] ASAv-in-A [datastore4] ASAv-in-A Virtual Disk Virtual Disk Virtual Disk VM Network Pod6-ALUMBRER ASAv Pod6-ALUMBRER ASAv Pod6-ALUMBRER ASAv VM Network VM Network VM Network VM Network VM Network	Adapter Type Current adapter: E1000 MAC Address 00:50:56:89:CA:89 Automatic O Manual DirectPath I/O Status: Not supported Network Connection Network Connection Network label: Ped6-ALUMBRER JASAV-AVS-RoutedctxnoneIntBD-alumb Pod6-ALUMBRER JASAV-AVS-RoutedctxnoneIntBD-alumbrer [ServerInt (AVS Pod6-ALUMBRER JAVS-AEP-VMM-alumbrer [AVS-EPG1 (AVS) Pod6-ALUMBRER JAVS-AEP-VMM-alumbrer [AVS-EPG1 (AVS) Pod6-ALUMBRER JAVS-AEP-VMM-alumbrer [AVS-EPG1 (AVS)	
		Network adapter 8 Network adapter 9 Network adapter 10	VM Network VM Network VM Network	PODS-ALL/MIDRER JAVS-AEP-VIMIM-alumprer JAVS-EPG2 (AVS) quarantine (AVS) vtep (AVS) common default client (DVS) common default juolivei (DVS) common default web (DVS)	

在本测试中,我让2个EPG与标准合同通信,这2个EPG位于不同的域和不同的VRF中,因此它们之间的路由泄漏已预先配置。当防火墙在2个EPG之间设置路由和过滤时,这样在插入服务图后会简化一点。EPG和BD下之前配置的DG现在可以与合同一样删除。只有L4-L7推送的合同应保留在EPG下。

Quick Start	1								
Tenant Pod6-ALUMBRER	ll a								
Application Profiles		<u>ା ±</u>							ACTIONS -
AVS-AEP-VMM-alumbrer	117								
Application EPGs		 Tenant Name 	Contract Name	Contract Type	Provided / Consumed	QoS Class	State	Label	Subject Label
Seps AVS-EPG1		G Contract Type: Co	ontract						
Domains (VMs and Bare-Me		Dodific ALLIMPD	EBC2 to EBC1	Contract	Drouidod	Linenseitied	formed		
Static Bindings (Paths)		POUC-ALOMDIN	EFG2-I0-EFG1	Contract	FIONODU	onspecified	lonned		
Static Bindings (Leaves)									
Contracts									
Static EndPoint									
Subnets									

在删除标准合同后,您可以确认流量现在是否流经ASAv,命令show access-list应显示每次客户端 向服务器发送请求时递增的规则的命中计数。

ASAA-M-AAS#	
ASAV-M-AAS#	show access-list
access-list	cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
	alert-interval 300
access-list	access-list-inbound; 4 elements; name hash: 0xcb5bd6c7
access-list	access-list-inbound line 1 extended permit tcp any any eq www (hitcn
t=0) 0xc873a	747
access-list	access-list-inbound line 2 extended permit tcp any any eq https (hit
cnt=0) 0x481	pedbdd
access-list	access-list-inbound line 3 extended permit tcp any any eq ssh (hitcn
t=4) 0x532fd	157a
access-list	access-list-inbound line 4 extended permit icmp any any (hitcnt=4) 0
ke4b5a75d	
ASAv-w-AVS#	

在枝叶上,应为客户端和服务器虚拟机以及ASAv接口学习终端

Leaf2# show endpoint			
Legend:	- 11		
0 - peer-attached H - vtep	a - Local	ly-aged S - static	
V - vpc-attached p - peer	-aged L - local	M - span	
s - static-arp B - bound	ce		
+	Encap	MAC Address MA	C 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	vian-98	0050.5689.1d08 L	eth1/7
Pod6-ALUMBRER:VRF1-alumbrer	Server IP vlan-98	192.168.10.10 L	, interface
25	& MAC vlan-94	0050.5689.ca89 1/	(ServerInt Po4
Pod6-ALUMBRER:VRF1-alumbrer	vlan-94	192.168.10.1 L]
mgmt:inb		192.168.2.11 S	
21	vlan-97	0050.5689.3fca L	eth1/7
Pod6-ALUMBRER:VRF2	Client IP & vlan-97	172.16.1.10	
26	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	

参见连接到VEM的两个防火墙接口。

ESX-1

~	# ven	ncmd show p	ort vla	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	Ø	0		ASAv-in-AVS.eth2
	1040	Pol	UP	UP	FWD		0		0	0		

ESX-2

~ # ver	# vemand show port vlan										
LTL	VSM Port	Admin	Link	State	Cause	PC-LTL	SGID	ORG	svcpath	Туре	Vem Port
24	Eth1/7	UP	ŲΡ	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		
~ #											

最后,如果我们知道源和目标EPG的PC标记,也可以在枝叶级别验证防火墙规则:

EPG1					Policy Or	erational Stats	Health Faults	History
Application Profiles AVS-AEP-VMM-alumbrer					Asso	clated EPGs A	asociated External Routed	Networks
Application EPGs	⊙₹						ACT	nons -
FO EPG AVS-EPG1	NUTTO	Description	State	Issues	QoS	Encep	PC Teg	
ulleg EPOs	AVS-EPG1		applied		Unspecified		17	
L4-L7 Service Parameters	EPG-Internal-alumbrer	EPO-Internal-alumbrer		appled			32772	
InternalAEP-VMM-alumbrer								
Networking								
Bridge Domains								
VRFs	1							
VRF1-alumbrer								
> 🔁 V78/2								

EPG2

 Domains (VMs and Bare-Metals) Static Bindings (Paths) 					Policy	perational Stats	Health Faults Histor	y
Static Bindings (Leaves)					Ass	ociated EPGs At	ssociated External Routed Networks	8
Contracts	0 V						ACTIONS -	
Static EndPoint								
Subnets	- Name	Description	State	Issues	QoS	Encep	PC Tag	
L4-L7 Virtual IPs	AVS-EPG2		applied		Unspecified		5476	
L4-L7 IP Address Pool							\sim	
L4-L7 Service Parameters								
USeg EPGs								
L4-L7 Service Parameters								
InternalAEP-VMM-alumbrer								
Networking								
Bridge Domains								
🖌 🖿 VRFs								
VRF1-alumbrer								
VRF2								
External Bridged Networks								

过滤器ID可以与枝叶上的PC标记匹配,以验证防火墙规则。

leaf2# show zor	ning-rule gr	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#							

注意:EPG PCTags/Sclass从不直接通信。通信通过L4-L7服务图插入创建的影子EPG被中断 或绑定在一起。

通信客户端到服务器工作正常。

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



故障排除

未分配VTEP地址

验证是否在AEP下检查了Infrastructure Vlan:

Policies 🦉 🖸	Attachable Access Entity Profile - AEP-AVS							
Cuick Start			_			1		
Switch Policies			Policy	Operational	Faults	History		
Module Policies		A A O O			A	CTIONS -		
Interface Policies								
Global Policies	Properties	Properties						
Attachable Access Entity Profiles	Name:	AEP-AVS				1		
📜 AEP-AVS	Description:	optional						
AEP_DVS								
L3Out-N3K2-alumbrer	Enable Infrastructure VLAN:							
L3OutN3k-AEP	Domains (VMM, Physical or External)	0						
📃 default	Associated to Interfaces:				×	+		
QOS Class Policies		 Name 	State					
DHCP Relay Policies		AVS (Vmm-VMware)	formed			- 11		
MCP Instance Policy default						- 11		
EP Loop Protection Policy						- 11		
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:	select a value						
	CDB Policy							
	CDP Policy.							
	STP Policy:	select a value 👻 🗗						
	Firewall Policy:	select a value 🔹 🔽						

不支持的版本

验证VEM版本是否正确,并支持适当的ESXi VMWare系统。

~ # vem version
Running esx version -1746974 x86_64
VEM Version: 5.2.1.3.1.10.0-3.2.1
OpFlex SDK Version: 1.2(1i)
System Version: VMware ESXi 5.5.0 Releasebuild-1746974
ESX Version Update Level: 0

VEM和交换矩阵通信不工作

- 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

此时可以确定ESXi主机和枝叶之间的交换矩阵通信无法正常工作。可以在枝叶端检查某些验证命令 以确定根本原因。

leaf2# show cdp ne

Capability Codes: R	S - Switch, H -	Host, I	гіаде, в — S — IGMP, r —	Repeater,	ldge
V	/ - VoIP-Phone,	D - Rem	otely-Manage	d-Device,	
s	s - Supports-STI	P-Disput	e		
Device-ID	Local Intrfce	Hldtme	Capability	Platform	Port ID
AVS:localhost.local	.domainmain				
	Eth1/5	169	SIS	VMware ESXi	vmnic4
AVS:localhost.local	.domainmain				
	Eth1/6	169	SIS	VMware ESXi	vmnic5
N3K-2(FOC1938R02L)					
	Eth1/13	166	RSIS	N3K-C3172PQ-	-1 Eth1/13
leaf2# show port-c	sum .				
Flags: D - Down	P-Upin	port-ch	annel (membe	rs)	
l - Individ	lual H - Hot-si	tandby (.	LACP only)		
s - Suspend	led r - Module	e-remove	a		
S - Switche	a R - Routed	1			
U - Up (por	(t-channel)				
M - Not in R Gamfian	use. Min-links	not met			
F - Conligu					
Group Port- I	'vpe Protoco	ol Memb	er Ports		
Channel					
5 Po5(SII) F	י+h ד.גמטי	 v+b1	 /E(D) E+b	1/6(D)	

通过Po5连接的ESXi中有2个端口

leaf2# show vlan extended

Name	Status	Ports
infra:default	active	Eth1/1, Eth1/20
	active	Eth1/13
mgmt:inb	active	Eth1/1
	active	Eth1/5, Eth1/6, Po5
	active	Eth1/1
::	active	Eth1/5, Eth1/6, Po5
common:pod6_BD	active	Eth1/5, Eth1/6, Po5
	<pre>Name infra:default mgmt:inb common:pod6_BD</pre>	Name Status

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

从上述输出中可以看到,Infra Vlan不允许或通过通往ESXi主机的上行链路端口(1/5-6)。 这表示 APIC上配置了接口策略或交换机策略的配置错误。

同时检查:

访问策略>接口策略>配置文件访问策略>交换机策略>配置文件

在这种情况下,接口配置文件连接到错误的AEP(用于DVS的旧AEP),如图所示:

Access Port Policy Group	- AVS-102_1-ports-7	_PolGrp						
						Policy	Faults	History
⊙±							AC	CTIONS -
Properties								
Name:	AVS-102_1-ports-7_PolGrp							
Description:	optional							
Label:								
Link Level Policy:	1GigAuto	e						
CDP Policy:	CDP_ON	e e						
MCP Policy:	select a value							
LLDP Policy:	LLDP_ON	e 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 e						
Connectivity Filters:				× +				
	Switch IDs		Interfaces					
					SHOW USAG	E SUBI	ит	CLOSE

在为AVS设置正确的AEP后,我们现在可以看到,通过枝叶上的正确的取消链路可以看到基础设施 VLAN:

leaf2# show vlan extended

22

enet CE

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	commo	n: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		

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

相关信息

应用虚拟交换机安装

<u>思科系统公司思科应用虚拟交换机安装指南,版本5.2(1)SV3(1.2)</u> 使用VMware部署ASAv

思科系统公司思科自适应安全虚拟设备(ASAv)快速入门指南,9.4

思科ACI和思科AVS

<u>思科系统公司思科ACI虚拟化指南,版本1.2(1i)</u>

使用思科以应用为中心的基础设施设计服务图白皮书

使用思科以应用为中心的基础设施设计服务图白皮书

<u>技术支持和文档 - Cisco Systems</u>