# 使用AVS-ACI 1.2(x)版本的GoTo(L3)模式的ASAv

### 目錄

簡介 必要條件 需求 採用元件 設定 網路圖表 組態 驗證 疑難排解 相關資訊

# 簡介

本文說明如何使用ACI 1.2(x)版本在兩個端點組(EPG)之間將應用虛擬交換機(AVS)交換機與採用路 由/轉至模式的自適應安全虛擬裝置(ASAv)單防火牆部署為第4-7層服務圖,以建立客戶端到伺服器 的通訊。

## 必要條件

### 需求

思科建議您瞭解以下主題:

•已配置訪問策略,介面處於啟用狀態並處於服務狀態
•已配置EPG、橋接域(BD)和虛擬路由和轉發(VRF)

採用元件

本文中的資訊係根據以下軟體和硬體版本:

### 硬體和軟體:

- 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)
- 分葉/主幹 11.2(1i) 已下載裝置軟體包\*.zip

功能:

AVS

- ASAv
- EPG、BD、VRF
- •存取控制清單(ACL)
- L4-L7服務圖
- vCenter

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

### 設定

### 網路圖表

如圖所示,



### 組態

AVS初始設定建立VMware vCenter域(VMM整合)2

附註:

- 您可以在單個域下建立多個資料中心和分散式虛擬交換機(DVS)條目。但是,您只能為每個資料中心分配一個Cisco AVS。
- Cisco ACI版本1.2(1i)和Cisco AVS版本5.2(1)SV3(1.10)支援使用Cisco AVS部署服務圖。 整個 服務圖配置是在思科應用策略基礎架構控制器(思科APIC)上執行的。

- 僅在具有虛擬區域網(VLAN)封裝模式的虛擬機器管理器(VMM)域上支援使用Cisco AVS的服務 虛擬機器(VM)部署。但是,計算VM(提供者和使用者VM)可以是具有虛擬可擴展 LAN(VXLAN)或VLAN封裝的VMM域的一部分。
- 另請注意,如果使用本地交換,則不需要組播地址和池。如果未選擇本地交換,則必須配置組 播池,並且AVS交換矩陣範圍組播地址不應是組播池的一部分。源自AVS的所有流量將採用 VLAN或VXLAN封裝。

導覽至VM Networking > VMWare > Create vCenter Domain,如下圖所示:

reate vCenter Domain					i
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 Switchin	9		
Encapsulation:	VLAN				
	VXLAN				
Associated Attachable Entity Profile:	AEP-AVS	•	æ		
VLAN Pool:	VlanPool-AVS(dynam	nic) 🗸	æ		
Security Domains:			× +		
	Name	Description			
vCenter Credentials:				×	+
	Profile Name	Username	Description		-
	vCenterCredentials	root	Decemption		
vCenter:				×	+
	Name	IP	Туре	Stats Collection	
	vCenterController	10.201.35.9	vCenter	Disabled	

如果您使用埠通道或VPC(虛擬埠通道),建議將vSwitch策略設定為使用Mac固定。

之後,APIC應將AVS交換機配置推送到vCenter,如下圖所示:



在APIC上,您可以注意到VXLAN通道端點(VTEP)位址已指派給AVS的VTEP連線埠群組。無論使用 哪種連線模式(VLAN或VXLAN),都會分配此地址

Inventory	Portgroup - vtep					Orment Faults Hat	i
DenStack     DenStack     VMware	O₩						
AVS     Dortrollers     ATS     Controllers     ATS     Controllers	Properties Name: Encap:	vtep vlan-3967					
✓ Mypervisors ► ↓ 10.201.35.218	Management Network Adapters:	Server Name 10.201.35.219	Name vmk1	State Up	MAC 00:50:58:68: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     Portgroups     Pod6-ALUMBRERIAVS-AEP-VMM-a							
Quarantine     guink     li li li vien							
> () DVS							
		(   Page 1 Of	U D H	Objects Per I	Page: 15 👻	Displaying Objects 1 - 2 Of 2	

#### 在vCenter中安裝Cisco AVS軟體

• 使用此連結從CCO下載vSphere安裝套件(VIB)

注意: 在本例中, 我們使用ESX 5.5, 表1, 顯示了ESXi 6.0、5.5、5.1和5.0的相容性表

#### 表1 - ESXi 6.0、5.5、5.1和5.0的主機軟體版本相容性

Villware 1	VIB 2	VEM Bundle 2	Windows VC Installer	Linux vCenter Server Appliance
ESX 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	oross_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	oross_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檔案中,有3個VIB檔案(每個ESXi主機版本各一個),請選擇一個適用於ESX 5.5的檔案 ,如下圖所示:

Γ	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

• 將VIB檔案複製到ESX Datastore — 這可以通過CLI完成,也可以直接從vCenter完成

附註:如果主機上存在VIB檔案,請使用esxcli software vib remove命令將其刪除。

esxcli software vib remove -n cross\_cisco-vem-v197-5.2.1.3.1.5.0-3.2.1.vib

或者直接瀏覽Datastore。

• 在ESXi主機上使用以下命令安裝AVS軟體:

esxcli software vib install -v /vmfs/volumes/datastore1/cross\_cisco-vem-v250-5.2.1.3.1.10.0-3.2.1.vib —maintenance-mode —no-sig-check



• 虛擬乙太網路模組(VEM)啟動後,可以將主機新增到AVS中:

在Add Host to vSphere Distributed Switch對話方塊中,選擇連線到枝葉交換機的虛擬NIC埠(在本示例中,僅移動vmnic6),如下圖所示:

elect Host and Physical Adapter	5		Settings	View Incompatible H
twork Connectivity	Host/Physical adapters	In use by switch	Settings	Uplink port group
adv to Complete	E 10.201.35.218		View Details	
buy to complete	Select physical adapters			
	wmnic0	vSwitch0	View Details	uplink
	Vmnic1		View Details	uplink
	Vmnic10		View Details	uplink
	wmnic11		View Details	uplink
	Vmnic2		View Details	uplink
	Vmnic3		View Details	uplink
	Vmnic4	DVS	View Details	uplink
	Vmnics	DVS	View Details	uplink
	Vmnice		View Details	uplink
	Vmnic/		View Details	uplink
	Vmnice		View Details	uplink

- 按一下下一步
- •在「網路連線」對話方塊中,按一下**下一步**
- •在「虛擬機器網路」對話方塊中,按一下「下一**步」**
- •在「準備完成」對話方塊中,按一下「完**成」**

**附註**:如果使用多個ESXi主機,所有主機都需要運行AVS/VEM,以便它們可以從標準交換機 管理到DVS或AVS。

這樣,AVS整合已經完成,我們可以繼續部署L4-L7 ASAv:

### ASAv初始設定

• 下載Cisco ASAv裝置包並將其匯入APIC:

導覽至L4-L7 Services > Packages > Import Device Package,如下圖所示:

Fabric	VM Networking	L4-L7 Services	Admin	Operations				
		Inventory   Packages						
Quick Sta	rt							
HELP								
The <b>Packag</b> balancer, cor and network	The <b>Packages</b> menu allows you to import L4-L7 device packages, which are used to define, configure, and monitor a network service balancer, context switch, SSL termination device, or intrusion prevention system (IPS). Device packages contain descriptions of the fit and network connectivity information for each function. A network service device is deployed in the network by adding it to a service g							
You can use	the Import a Device Pa	ckage wizard to impo	t a device package for	a function that you want to m	nanage with APIC. We			
oonigunig a	In	nport Device P	ackage	i	×			
Quick Import a	Start Device Package	File Name:		BROWSE	Device Types			

SUBMIT

CLOSE

i

						General	Operational	Faults	History
⊙₹								AC	TIONS -
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:									
Interface Labels:	<ul> <li>Name</li> </ul>								_
	cluster_ctrl_lk								
	external								
	failover_lan								
	failover_link								
	internal								
	mgmt								
	utility								

• 如果一切正常,您可以看到匯入的裝置包正在展開L4-L7 Service Device Types資料夾,如下圖

所示:

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

繼續之前,在執行實際的L4-L7整合之前,需要確定安裝的幾個方面:

有兩種管理網路:帶內管理和帶外(OOB),它們可用於管理不屬於基本以應用為中心的基礎設施 (ACI)的裝置(枝葉、主幹或apic控制器),包括ASAv、負載均衡器等。

在這種情況下,ASAv的OOB是使用標準vSwitch部署的。對於裸機ASA或其他服務裝置和/或伺服器 ,請將OOB管理埠連線到OOB交換機或網路,如下圖所示。



ASAv OOB管理埠管理連線需要使用ESXi上行鏈路埠通過OOB與APIC通訊。在對映vNIC介面時 ,網路介面卡1始終匹配ASAv上的管理0/0介面,其餘的資料平面介面從網路介面卡2啟動。

表2顯示了網路介面卡ID和ASAv介面ID的一致性:

### 表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

- 通過File>Deploy OVF(Open Virtualization Format)Template中的嚮導部署ASAv VM
- 如果要將獨立ESX Server或**asav-vi** for vCenter,請選擇**asav-esxi**。在這種情況下,使用 vCenter。



 通過安裝嚮導,接受條款和條件。在嚮導的中間,您可以確定多個選項,如主機名、管理、 ip地址、防火牆模式和其他與ASAv相關的特定資訊。請記住對ASAv使用OOB管理,因為在這 種情況下,在使用VM網路(標準交換機)時,您需要保持介面管理0/0,而介面 GigabitEthernet0-8是預設網路埠。

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          2:'Documents'(GSP')ACTUMAGE'(asav952'(asav-vi).ovf <ul> <li>Browse</li> </ul> Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.
Help	< Back Next > Cancel

ource VF Template Details nd User License Agreement	Map the networks used in this OVF 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         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         Management 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       .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         Oncose whether to use DHCP for Management interface configuration.       Imagement IP Address         Enter the Management IP-4 Address of the Active HA host.       10 . 201 . 35 . 223         Hanagement IP Subnet Hask       Imagement IP Subnet Hask	Properties		
Hostname         Host name for this system. A hostname must start and end with a letter or digit and have as interior duracters only letters, digits, or a hyphen.         ASAv-m-AVS         Firewall Properties         Firewall Mode         Select the Firewall Mode         routed         Management Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Hanagement IP-V4 Address         Enter the Management EV-4 Address. For HA-type deployments, this property specifies the Management EV-4 Address for the Active HA host.         10       .201         10       .201         Hanagement IP Subnet Hask	Ready to Complete	Hostname	
Hostname         Hostname for this system. A hostname must start and end with a letter or digit and have as interior divaracters only letters, digits, or a hyphen.         ASAv-m-AVS         Firewall Properties         Firewall Mode         Select the Firewall Mode         routed         Management Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Hanagement IP-v4 Address.         Enter the Management IP-v4 Address. For HA-type deployments, this property specifies the Management IP-v4 address of the Active HA host.         10       .201         10       .201         Hanagement IP-Subnet Hask			
Host name for this system. A hostname must start and end with a letter or digit and have as interior characters only letters, digits, or a hyphen.         ASAv-w-AVS         Firewall Properties         Firewall Mode         Select the Prevail Mode         routed         Management Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Hanagement IP Address         Enter the Management SV-4 Address. For HA-type deployments, this property specifies the Management IP-4 Address of the Active HA host.         10       .01         .01       .021         Help          Help		Hostname	
ASAr-w-AVS         Firewall Properties         Firewall Mode         Select the Firewall Mode         routed         Management Interface Settings         Management Interface OHCP mode         Choose whether to use DHOP for Management interface configuration.         Hanagement IP Address         Enter the Management IP Address.         Enter the Management IP-v4 Address. For HA-type deployments, this property specifies the Management IP-v4 Address of the Active HA host.         10       .201         Management IP Subnet Mask         Memory         Address         Management IP Subnet Mask		Host name for this system. A hostname must start and end with a letter or digit and have as interior characters only letters, digits, or a hyphen.	
Firewall Properties         Firewall Mode         Select the Prewall Mode         routed         management Interface Settings         Hanagement Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Hanagement IP-4 Address         Enter the Management IP-4 Address. For HA-type deployments, this property specifies the Management IP-4 Address of the Active HA host.         10       .201         Help       < Back		ASAv-w-AVS	
Help       < Back			
Help       < Back		Firewall Properties	
Select the Firewall Mode         routed         Management Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Imagement IP Address         Enter the Management IP-v4 Address. For HA-type deployments, this property specifies the Management IP-v4 Address of the Active HA host.         ID       .01         Hanagement IP Subnet Hask         Imagement IP Subnet Hask         Imagement IP Subnet Hask         Imagement IP Subnet Hask		Firewall Mode	
Management Interface Settings         Management Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Imagement IP Address         Enter the Management IPv4 Address. For HA-type deployments, this property specifies the Management IPv4 address of the Active HA host.         Imagement IP Subnet Hask         Help		Select the Firewall Mode	
Imagement Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Imagement IP Address         Enter the Management IP-v4 Address. For HA-type deployments, this property specifies the Management IP-v4 address of the Active HA host.         10       .201         Hanagement IP Subnet Hask         Ket       Cancel			
Hanagement Interface Settings         Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Imagement IP Address         Enter the Management IP v4 Address. For HA-type deployments, this property specifies the Management IP v4 address of the Active HA host.         Imagement IP Subnet Hask         Help            Ket >		routed	
Hanagement Interface DHCP mode         Choose whether to use DHCP for Management interface configuration.         Hanagement IP Address         Enter the Management IPv4 Address. For HA-type deployments, this property specifies the Management IPv4 address of the Active HA host.         10       . 201       . 35       . 223         Hanagement IP Subnet Hask		Management Interface Settings	
Help <back< td="">       Next &gt;       Cancel</back<>		Management Interface DHCP mode	
Hanagement IP Address         Enter the Management IP v4 Address. For HA-type deployments, this property specifies the Management IP v4 address of the Active HA host.         10       .201       .35       .223         Hanagement IP Subnet Hask       •              Heip         Cancel		Change whether to use PMCD for Management interface conferenties	
Hanagement IP Address         Enter the Management IPv4 Address. For HA-type deployments, this property specifies the Management IPv4 address of the Active HA host.         10       .201       .35       .223         Hanagement IP Subnet Hask		Choose whether to use CHCP for Management interface configuration.	
Enter the Management IPv4 Address. For HA-type deployments, this property specifies the         Management IPv4 address of the Active HA host.         10       .201       .35       .223         Hanagement IP Subnet Hask		Hanagement IP Address	
Hanagement IPv4 address of the Active HA host.       10 , 201 , 35 , 223       Hanagement IP Subnet Hask       Help       < Back		Enter the Management IPv4 Address. For HA-type deployments, this property specifies the	
10         201         35         223           Hanagement IP Subnet Hask         *		Management IPv4 address of the Active HA host.	
Hanagement IP Subnet Hask       Heip <back< td="">     Next &gt;     Cancel</back<>		10 . 201 . 35 . 223	
Help Kext > Cancel		Management IP Subnet Mask	-
Help <back next=""> Cancel</back>		I an and the second sec	
Help < Back Next > Cancel			
	Help	< Back Next >	Cancel

Read to Complete         Social Sect Leaves to take to use?         Social Sect Leaves Accesses	eploy OVF Template	vertery 1 🗃 Hasta and Clusters	المرافع	x
Source Out: Textures Ascrement Name and Looping Source Ascrement Name and Looping Source and Source Ascrement Name and Looping Name and Looping	Ready to Complete Are these the options you	want to use?		
Source 2017: Tenscharte Destals Childser: License Agreement Same and Location Development Configuration: Stream at Location Development Configuration: Network Mapping: Network Ma		1		_
Ind Laser License Agreement Same and Location       Size on disk:       8.3 GB         Name:       ASA vin-AVS         Poilde:       ACI         Deployment Configuration:       1 Gbps (ASAv10)         Name:       ASAvin-AVS         Poilde:       ACI         Deployment Configuration:       1 Gbps (ASAv10)         Note Test       Datastone:         Datastone:       Obstance:         Name:       Gatastone:         Datastone:       Obstance:         Network Mapping:       Thick Provision Lary Zened         Network Mapping:       "GigabitEthernet0-7" to "VM Network"         Network Mapping:       "GigabitEthernet0-7" to "VM Network"         Network Mapping:       "GigabitEthernet0-5" to "VM Network"         Network Mapping:       "GigabitEthernet0-6" to "VM Network"         Network Mapping:       "GigabitEthernet0-6" to "VM Network"         Network Mapping:       "GigabitEthernet	ource XVF Template Details	When you click Finish, the deploym	ent task will be started.	
since and location         codynamic Configuration         totade         dx Dermant         betwork Mapping:         totade         vetwork Mapping:         "GigabitEthermetb-0" to "VM Network"         Network Mapping:       "GigabitEthermetb-0" to "VM Network"         Network Mapping:       "GigabitEthermetb-0" to "VM Network"         Network Mapping:       "GigabitEthermetb-0" to "VM Network"         Network Mapping:       "GigabitEthermetb-0" to "VM Network"         Network Mapping:       "GigabitEthermetb-0" to "VM Network"         Network Mapping:       "GigabitEthermetb-0" to "VM Network"         Network Mapping:       "GigabitEthermetb-0" to "VM Network"         Network Mapping:       <	nd User License Agreement	Deployment settings:		
skoument Confouration Xaoa Kafornal Lexofi Macobio Deployment Configuration: 1 Gbps (ASAv10) Detatore: datastoref Disk provisioning: Thick Provision Lazy Zened Network Mapping: "GigabitEthernet0-0" to "VM Network" Network Mapping: "GigabitEtherne	me and Location	Size ondisk:	8.3 G8	
Not     Folder:     ACI       Constitution     Deployment Configuration:     1 Gbps (ASAv10)       wtites     Deployment Configuration:     1 Gbps (ASAv10)       dy to Complete     Disk provisioning:     Thick Provision Lazy Zeroed       Network Mapping:     "GigabitEthernet0-0" to "VM Network"       Network Mapping:     "GigabitEthernet0-1" to "VM Network"       Network Mapping:	oyment Configuration	Name:	ASAv-in-AVS	
Deployment Configuration: 1 Gbps(ASAv10) Host/Cluster: 10.201.35.219 Detastore: detastore! Disk provisioning: Thick Provision Lary Zeroed Network Mapping: "GigabitEthernet0-0" to "VM Network" Network Mapping: "GigabitEthernet0-0" to "VM Network" Network Mapping: "GigabitEthernet0-2" to "VM Network" Network Mapping: "GigabitEthernet0-2" to "VM Network" Network Mapping: "GigabitEthernet0-3" to "Pode-ALLUMBRER[AYS-AEP-VMM-alumbrer]//. Network Mapping: "GigabitEthernet0-5" to "VM Network" Network Mapping: "GigabitEthernet0-5" to "VM	22	Folder	ACI	
Most/Cluster       10.201.35.219         Ito Complete       Datastore:       datastore!         Disk provisioning:       Thick Provision Lazy Zeroed         Network Mapping:       "GigabitEthernetD-0" to "VM Network"         Network Mapping:       "GigabitEthernetD-1" to "VM Network"         Network Mapping:       "GigabitEthernetD-4" to "Pod6-ALUMBRERIAVS-AEP-VMM-alumbre/JW         Network Mapping:       "GigabitEthernetD-4" to "VM Network"         Network Mapping:       "GigabitEthernetD-4" to "VM Network"<	mat .	Deployment Configuration:	1 Gbps (ASAv10)	
o Complete       Datastore:         Disk provisioning:       Thick Provision Lazy Zeroed         Network Mapping:       "GigabitEthernet0-0" to "VM Network"         Network Mapping:       "GigabitEthernet0-1" to "VM Network"         Network Mapping:       "GigabitEthernet0-1" to "VM Network"         Network Mapping:       "GigabitEthernet0-1" to "VM Network"         Network Mapping:       "GigabitEthernet0-3" to "Pod6-ALUMBRER[AVS-AEP-VMM-alumbre/AV-         Network Mapping:       "GigabitEthernet0-4" to "Pod6-ALUMBRER[InternalAEP-VMM-alumbre/JM-         Network Mapping:       "GigabitEthernet0-5" to "VM Network"         Property:       HaRole = Standal	Magging .	Host/Cluster:	10.201.35.219	
Disk provisioning: Thick Provision Lazy Zeroed Network Mapping: "GigabitEthernet0-0" to "VM Network" Network Mapping: "GigabitEthernet0-1" to "VM Network" Network Mapping: "GigabitEthernet0-1" to "VM Network" Network Mapping: "GigabitEthernet0-1" to "Pod6-ALLUMBRER[AVS-AEP-VMM-alumbre/#W Network Mapping: "GigabitEthernet0-5" to "VM Network" Network Mapping: "GigabitEthernet0-5" to "VM	o Comolete	Datastore	datastore4	
Network Mapping:       "ManagementD-0" to "VM Network"         Network Mapping:       "GigabitEthernet0-0" to "VM Network"         Network Mapping:       "GigabitEthernet0-1" to "VM Network"         Network Mapping:       "GigabitEthernet0-2" to "VM Network"         Network Mapping:       "GigabitEthernet0-2" to "VM Network"         Network Mapping:       "GigabitEthernet0-4" to "VM Network"         Property:       HaRole = Standalone	Complete	Disk provisioning:	Thick Provision Lazy Zeroed	
Network Mapping:       "GigabitEthernet0-0" to "VM Network"         Network Mapping:       "GigabitEthernet0-0" to "VM Network"         Network Mapping:       "GigabitEthernet0-2" to "VM Network"         Network Mapping:       "GigabitEthernet0-3" to "Podd-ALLUMBRER[AVS-AEP-VMM-alumbrer]         Network Mapping:       "GigabitEthernet0-5" to "VM Network"         Network Mapping:       "GigabitEthernet0-6" to "VM Network"         Network Mapping:       Pixed, IP-4         Property:       HARole = Standalone         Property:       ManagementIP-4 = Soutas 52525.05         Property:       ManagementIP-4 = Soutas 52535.05 <t< td=""><td></td><td>Network Mapping</td><td>"Management0-0" to "VM Network"</td><td></td></t<>		Network Mapping	"Management0-0" to "VM Network"	
Network Mapping:       "GigabitEthernet0-1" to "VM Network"         Network Mapping:       "GigabitEthernet0-2" to "VM Network"         Network Mapping:       "GigabitEthernet0-3" to "Pod6-ALUMBRER[AVS-AEP-VMM-alumbre/AL         Network Mapping:       "GigabitEthernet0-4" to "Pod6-ALUMBRER[InternalAEP-VMM-alumbre/AL         Network Mapping:       "GigabitEthernet0-6" to "VM Network"         Property:       HARole = Standalone         Property:       Management3Pv4 = 10.201.35.223         Property:       Management3Endby		Network Mapping	"GioabitEthemet0-0" to "VM Network"	
Network Mapping:       "GigabitEthernet0-2" to "VM Netwok"         Network Mapping:       "GigabitEthernet0-3" to "Pod6-ALUMBRER[AVS-AEP-VMM-alumbref]#/         Network Mapping:       "GigabitEthernet0-4" to "Pod6-ALUMBRER[InternalAEP-VMM-alumbref]#/         Network Mapping:       "GigabitEthernet0-6" to "VM Netwok"         Property:       HARole = Standalone         Property:       Property:         Property:       ManagementEV+4 = 10.201.35.223         Property:       Route Of ault = Default Route		Network Mapping	"GioabitEthemet0-1" to "VM Network"	
Network Mapping:       "GigabitEthernet0-3" to "Pod6-ALLUMBRER[AVS-AEP-VMM-alumbre/AV         Network Mapping:       "GigabitEthernet0-3" to "Pod6-ALLUMBRER[InternalAEP-VMM-alumbre/JAV         Network Mapping:       "GigabitEthernet0-5" to "VM Network"         Property:       HARole = Standalone         Property:       Hostname = ASAv-w-AVS         Property:       Property:         Property:       ManagementEPv4 = 10.201.35.223         Property:       ManagementEstandory Ev4 = 0.0.0         Property:       RouteOefawlt = Defawlt Route         Power on after deployment       "Metwork" Asampted Asampted Asampted Asampted Asampted Asampted Asampted A		Network Mapping	"Gioabit@hemat0-2" to "VM Network"	
Network Mapping:       "GigabitEthernet0-4" to "Pod6-ALLUMBRER[InternalAEP-VMM-alumbred]         Network Mapping:       "GigabitEthernet0-5" to "VM Network"         Network Mapping:       "GigabitEthernet0-6" to "VM Network"         Network Mapping:       "GigabitEthernet0-8" to "VM Network"         Phoperty:       MARole = Standalone         Property:       Mostname = ASAv-w-AVS         Property:       MonagementIPv4 = 10.201.35.223         Property:       ManagementIPv4 = 0.20.0.0         Property:       ManagementStandbyIPv4 = 0.0.0.0         Property:       RouteOefawlt = Defawlt Route         Power on after deployment       Network Mapping:		Network Magning	"GinabitPharnat0-3" to "Pod4-ALLIMROFPLAVC-AFP-VMM-alumbur(AV-	
Network Mapping:       "GigabitEthemet0-5" to "VM Netwok"         Network Mapping:       "GigabitEthemet0-6" to "VM Netwok"         Property:       HARole = Standalone         Property:       Hostname = ASAv-w-AVS         Property:       PWMode = routed         Property:       ManagementStandby SPv4 = 0.0.0.0         Property:       ManagementStandby SPv4 = 0.0.0.0         Property:       Route Of ault = Default Route         Power on after deployment       To the default = Default Route		Network Mancing	"GinabitPharnat0-4" to "Pod4-ALLIMROFO InternalAFD-VMM-alumburi	
Network Mapping:     "GigabitEthemet0-6" to "VM Netwok"       Network Mapping:     "GigabitEthemet0-6" to "VM Netwok"       Network Mapping:     "GigabitEthemet0-6" to "VM Netwok"       PAllocation:     Fixed, Pv4       Property:     HARole = Standalone       Property:     Hostname = ASAv-w-AVS       Property:     PWMode = routed       Property:     DHCP = False       Property:     Management3Pv4 = 10.201.35.223       Property:     Management3Pv4 = 0.0.0.0       Property:     RouteDefault = Default Route		Natural Manager	*ClashiBhanato.C*to *M Naturd*	
Network Mapping:       "GigabitEthernet0-3" to "VM Network"         Network Mapping:       "GigabitEthernet0-3" to "VM Network"         IP Allocation:       Fixed, IPv4         Property:       HARole = Standalone         Property:       Hostname = ASAv-w-AVS         Property:       FWMode = routed         Property:       DHCP = False         Property:       ManagementIPv4 = 10.201.35.223         Property:       ManagementIPv4 = 0.0.0.0         Property:       RouteDefault = Default Route         Property:       RouteDefault = Default Route		Natwork Manning	"Cinabil@hamat0.6"to "VM Naturok"	
Network Mapping:       "GigabitEthernet0-8" to "VM Network"         IP Allocations       Fixed, IPv4         Property:       HARole = Standalone         Property:       Hostname = ASAv-w-AVS         Property:       PWMode = routed         Property:       DHCP = False         Property:       ManagementIPv4 = 10.201.35.223         Property:       ManagementIPv4 = 0.0.0.0         Property:       RouteDefault = Default Route         Property:       RouteDefault = Default Route		Natural Mansing	"Cinebilithemath, "to "VM Network"	
Internet Respire     Fixed, 3Pv4       IP Allocation:     Fixed, 3Pv4       Property:     HARole = Standalone       Property:     Hostname = ASAv-w-AVS       Property:     Fixed, 3Pv4       Property:     Hostname = ASAv-w-AVS       Property:     Fixed, 3Pv4       Property:     Hostname = ASAv-w-AVS       Property:     Fixed, 3Pv4       Property:     Fixed, 3Pv4       Property:     DHCP = False       Property:     Management3Pv4 = 10.201.35.223       Property:     Management3Pv4 = 0.0.0.0       Property:     Management3Pv4 = 0.0.0.0       Property:     RouteDefault = Default Route		Natural Mansing	"CiashiBhanath 8" to "VM Network"	U
Property: HARole = Standalone Property: Hostname = ASAv-w-AVS Property: PWMode = routed Property: DHCP = False Property: DHCP = False Property: Management3Pv4 = 10.201.35.223 Property: Management3Pv4Subnet = 255.255.255.0 Property: Management3Pv4Subnet = 255.255.255.0 Property: RouteDefault = Default Route		Precivors Happing:	East that	
Property:     Hokote = scandalode       Property:     Hostname = ASAv-w-AVS       Property:     PWMode = routed       Property:     DHCP = False       Property:     Management3Pv4 = 10.201.35.223       Property:     Management3Pv4Subnet = 255.255.255.0       Property:     Management3Pv4Subnet = 0.0.0.0       Property:     RouteDefault = Default Route       Power on after deployment     Host Adv		PANOCEDON	HABola - Chardalana	
Property:     Postname = ASAV-W-AVS       Property:     PWMode = routed       Property:     DHCP = False       Property:     Management3Pv4 = 10.201.35.223       Property:     Management3Pv4Subnet = 255.255.255.0       Property:     Management3Pv4 = 0.0.0       Property:     RouteDefault = Default Route		Property:	Hankole = Scandalone	
Property: DHCP = False Property: DHCP = False Property: Management3Pv4 = 10.201.35.223 Property: Management3Pv4Subnet = 255.255.255.0 Property: Management5tandby3Pv4 = 0.0.0 Property: RouteDefault = Default Route		Property:	Hostname #ASAV-W-AVS	
Property:     DHCP = Paise       Property:     Management3Pv4 = 10.201.35.223       Property:     Management3Pv4Subnet = 255.255.255.0       Property:     Management3Pv4Eubnet = 0.0.0       Property:     ManagementStandby3Pv4 = 0.0.0       Property:     RouteDefault = Default Route		Property:	PWPlode = routed	
Property: Management/Pv4 = 30.201.35.223 Property: Management/Pv4Subnet = 255.255.255.0 Property: Management/Standby/Pv4 = 0.0.0.0 Property: RouteDefault = Default Route    Power on after deployment		Property:	DHCP = Faise	
Property: Management2v+5ubnet = 255.255.255.25 Property: ManagementStandbyIPv4 = 0.0.0.0 Property: RouteDefault = Default Route		Propertys	Management3Pv4 = 10.201.35.223	
Property: ManagementStandbyDv4 = 0.0.00 Property: RouteDefault = Default Route  Power on after deployment		Property:	Management3Pv4Subnet = 255.255.255.0	
Property: RouteDefault = Default Route		Property:	ManagementStandby3Pv4 = 0.0.0.0	
Power on after deployment		Property:	RouteDefault = Default Route	
Power on after deployment		E		
		Power on after deployment		
< Back Finish Cancel	1		< Back Finish Cano	

### • 按一下Finish並等待,直到ASAv部署完成

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

• 開啟ASAv VM並通過控制檯登入以驗證初始配置

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 --->

 如圖所示,某些管理配置已推送到ASAv防火牆。配置管理員使用者名稱和密碼。APIC使用此 使用者名稱和密碼登入並配置ASA。ASA應能連線到OOB網路,並能夠訪問APIC。

username admin password <device\_password> encrypted privilege 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)# \_

此外,從全域性配置模式啟用http伺服器:

http server enable

http 0.0.0.0 0.0.0.0管理

L4-L7,用於APIC中的ASAv整合:

- 登入到ACI GUI,點選將部署服務圖的租戶。展開導航窗格底部的L4-L7服務,按一下右鍵L4-L7裝置,然後按一下Create L4-L7裝置開啟嚮導
- 對於此實施,將應用以下設定:

— 託管模式

— 防火牆服務

— 虛擬裝置

— 通過單個節點連線到AVS域

- -ASAv型號
- 路由模式(GoTo)

— 管理地址(必須與之前分配給Mgmt0/0介面的地址匹配)

• 預設使用HTTPS作為APIC,使用最安全的協定與ASAv通訊

STEP 1 > General					1. General 2. Devic	e Configuration
Please select device	package and enter connectivity info	rmation.				
General Managed: Name: Service Type: Device Type: VMM Domain: Mode: Device Package:	ASAv-AVS-Routed Firewall PHYSICAL VIRTUAL AVS Single Node HA Cluster CISCO-ASA-1.2	Device 1 Management IP Address: VM: Device Interfaces:	10.201.35.3 vCenterController/AS Name GigabitEthernet0/0 GigabitEthernet0/1	Av-in-AVS  CNIC Network adapter 2 Network adapter 3	Management Port: https Path (Only For Route Peering) Node-102/MAC_Pinning Node-102/MAC_Pinning	× +
Moder: Function Type:	GoThrough GoTo	Cluster Management IP Address: Cluster Interfaces:	10.201.35.3 Туре	Name	Management Port: https	• × +
Connectivity APIC to Device Management Connectivity:	Out-Of-Band In-Band		provider	ServerInt ClientInt	Device1/GigabitEthernet0/0 Device1/GigabitEthernet0/1	
Credentials Username: Password: Confirm Password:	admin					

(i) 🗙

#### 正確定義裝置介面和集群介面對於成功部署至關重要

對於第一部分,使用前面部分中顯示的表2,將網路介面卡ID與您要使用的ASAv介面ID正確匹配。 路徑是指允許進出防火牆介面的物理埠、埠通道或VPC。在這種情況下,ASA位於ESX主機中,其 中兩個介面的傳入和傳出相同。在物理裝置中,防火牆(FW)的內部和外部將是不同的物理埠。

在第二部分中,必須始終定義群集介面(即使未使用群集HA),這是因為,對象模型在mlf介面 (裝置包上的元介面)、Llf介面(葉介面,如外部、內部、內部等)和Clf(具體介面)之間存在關 聯。必須在裝置集群配置中配置L4-L7具體裝置,該抽象稱為邏輯裝置。邏輯裝置具有對映到具體 裝置上的具體介面的邏輯介面。

在本示例中,將使用以下關聯:

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

Gi0/1 = vmnic3 = ClientInt/consumer/client > 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 GoTo Context Aware: Reach Mode	Device 1 Management IP Address: vCenter Name: Interfaces:	10.201.35.223 vCenterController Name GigabitEthernet0/1 GigabitEthernet0/2	Manageme VM Network adap Network adap	nt Port: 443 Name: ASAv-in-v ner 3 ner 4	Path (Only F Node-102/M	or Route Per MAC_Pinnin	× + ering) g. Nod 9
Credentials Username: admin Password: Confirm Password: Configuration State	Cluster Management IP Address: Cluster Interfaces:	10.201.35.223 Type Consumer	Anagemer Name Clientint	Concrete Interfe	ted_Device_1	CHIQADATET	× +
Configuration Issues: Devices State: stable		provider	ServerInt	ASAy-AVS-Rou	ited_Device_1	(GigabitEth	emet0/1]

附註:對於故障切換/HA部署, GigabitEthernet 0/8已預配置為故障切換介面。

裝置狀態應為「穩定」,並且您應準備好部署功能配置檔案和服務圖模板

#### 服務圖廟

首先,為ASAv建立功能配置檔案,但在此之前,您需要在該資料夾下建立功能配置檔案組,然後建 立L4-L7服務功能配置檔案,如下圖所示:

Create L4-L7 Service	s Function Profile Group	() ×
Specify the information	n about the Function Profile Group	
Description:		
	[	SUBMIT CANCEL

Tenent Pod6-ALUMERER	L4-L7 Services Fi	unction Profile	Group - FunProGroup				
Cuick Start			enoop familiearoop		_		
Tenant Pod5-ALUMBRER					General	Faults	History
Application Profiles	O₩		A A 0 1			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 Fu	nction Profile						
Devices Selection   Save as							
Deployed Graph In 53 Post							
Deployed Devices							
Inband Management Configuration for L4-L7 devi	6						

 從下拉選單中選擇WebPolicyForRoutedMode Profile,然後繼續配置防火牆上的介面。從現在 起,這些步驟是可選的,以後可以實施/修改。這些步驟可以在部署的幾個不同階段執行,具體 取決於服務圖的可重複使用或自定義方式。

在本練習中,路由防火牆(轉到模式)要求每個介面都有一個唯一的IP地址。標準ASA配置還具有 介面安全級別(外部介面不太安全,內部介面更安全)。 您也可以根據需要更改介面名稱。本示例 中使用預設值。

• 展開Interface Specific Configuration,為ServerInt新增IP地址和安全級別,對於IP地址 x.x.x.x/y.y.y.y或x.x.x./yy,格式如下。對ClientInt介面重複此過程。

Name: Fur Description:	Prof-ASA			
Copy Existing Profile Parameters: 🗹 Profile: CIS	CO-ASA-1.2/WebPolicyForRoutedMode	<b>-</b> @		
atures and Parameters	In order to auto apply new values to the parameter	s of existing graph instance when users modify	r function profiles, the name of top	folder must be ended with -Defau
eatures:	Basic Parameters All Parameters			
Interfaces	Folder/Param	Name Value Device	Mandatory Locked	Shared
AccessLists	Bridge Group Interface			
NAL TrafficSelectionObjects	Access Group	externallf ExtAccessGroup	false	false
All	IPv6 Enforce EUI-64			
	A Contigur.     A Contiguration of the second contigu	externall*Cig	false	
	IPv4 Address IPv4 IPv4 Address	ipv4_address 192.168.10.1/24		
	IPv6 Address Configura.	UPDATE RESET CAN	CEL	
	IPv6 Link Local Address			

**附註**:您還可以修改預設訪問清單設定並建立自己的基本模板。預設情況下,RoutedMode模 板將包含HTTP和HTTPS規則。在本練習中,SSH和ICMP將新增到允許的外部訪問清單。

SUBMIT CANCEL

Create Function Profile								
Name: F	unProf-ASA							
Description:	optional							
Copy Existing Profile Parameters:	2							
Profile: C	CISCO-ASA-1.2/Web	PolicyForRoutedMode	<u> </u>					
Features and Parameters								
	In order to au	to apply new values to the parameter	ers of existing graph	instance when users	modify function profiles, th	ne name of top folder	must be ended with	-Default.
Features:	Basic Param	eters All Parameters						
Interfaces	Folde	er/Param	Name	Value	Mandatory	Locked	Shared	
International	8	Destination Service	destination_ser	vice				
AccessLists		- 📃 High Port						
NAT		- 📰 Low Port	low_port	22		false		
TrafficSelectionObjects		Operator	operator	eq		false		
All		F CMP						
		Logging						
		Protocol						
		Source Address						
		Source Service						
		Action	action	permit		false		
L		Order	order	30		false		

### • 然後點選**提交**

• 現在,建立服務圖模板	
Tenant Pod6-ALUMBRER	L4-L7 Service (
Cuick Start	
Tenant Pod6-ALUMBRER	
Application Profiles	<b>○</b> ★
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 Service Graph Template

### 將裝置集群拖放到右側,形成消費者和提供商之間的關係,選擇路由模式和先前建立的功能配 置檔案。

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

• 檢查模板是否有故障。模板建立為可重複使用,然後必須將其應用於特定EPG等。

Tenant Pod6-ALUMBRER	⊴ 0	L4-L7 Service Graph Template - Graph1-alumbrer			i.
Quick Start					
Tenant Pod6-ALUMBRER			Topology Po	olicy Fault	s History
Application Profiles		0			
Networking		Consumer		Provider	
L4-L7 Service Parameters					
Security Policies				EPG	
Troubleshoot Policies		ASAv-AVS		<b>S</b>	
Monitoring Policies					
L4-L7 Services		ASAv			
🔺 🚞 L4-L7 Service Graph Template	85				
4 💙 Graph1-alumbrer		outed Information			
Function Node - ASA	Apply L4-L7 Se	vice Graph Template II: Routed			
Router configurations	Edit L4-L7 Ser	ce Graph Template b: FunPro-ASA			
Function Profiles	Delete				
FunProtGroup	Remove Relat	J Objects Of Graph Template			
EunPro-ASA	Save as				
L4-L7 Devices	Doet				
ASAv-AVS-Routed	Post				
ASAV-DVS					
Imported Devices					
Devices Selection Policies					
E Deployed Graph Instances					
Deployed Devices					
📃 Inband Management Configur	ation for L4-L7 devi				
				augurt .	DECET

### •要應用模板,請按一下右鍵並選擇應用L4-L7服務圖模板

- 定義哪個EPG將位於消費方和提供方側。在本練習中,AVS-EPG2是消費者(客戶端),AVS-EPG1是提供商(伺服器)。 請記住,未應用任何過濾器,這將允許防火牆根據此嚮導的最後 一部分中定義的訪問清單執行所有過濾。
- 按一下下一步

STEP 1 > Contract			1. Contract	2. Graph
Config A Contract Between EPGs				
Consumer EPG / External Network: Pod6-ALUMBRER/AVS-AEP-VMM V	rovider EPG / External Network:	Pod6-ALUMBRER/AVS-AEP-VMM  Pod6-ALUMBRER/AVS-AEP-VMM- alumbrer/epg-AVS-EPG1	G	
Contract Information Contract:  Contract: Contract: Create A New Contract Contract Name: EPG2-to-EPG1	ntract Subject	Pod6-ALUMBRER/InternalAEP- VMM-alumbrer/epg-EPG-Internal- alumbrer		
No Filter (Allow All Traffic):		Pod6-ALUMBRER/VRF1-alumbrer /AnyEPG		
		Pod6-ALUMBRER/VRF2/AnyEPG Pod6-ALUMBRER/L3Out-N3K2/L3Net		

 驗證每個EPG的BD資訊。在這種情況下,EPG1是IntBD DB上的提供商,EPG2是BD ExtBD上 的消費者。EPG1將在防火牆介面ServerInt上連線,EPG2將在介面ClientInt上連線。兩個FW介 面將成為每個EPG的DG,因此流量始終被迫通過防火牆。

• 按一下下一步

Graph Template:	Pod6-ALUMBRER/Graph1-Temp-alumbrer			• Ø		
Consumer						Provider
AVS-EPG2		С	ASAV-AVS	P		AVS-EPG1
			ASAv	•		
- ASAv-AVS-Routed Infor Firewal Profile	mation I: routed 9: FunPro-ASA					
Consumer Connector Type:	General O Route Peering					
BD:	Pod6-ALUMBRER/ExtBD-alumbrer	Ŧ	e			
Cluster Interface:	ClientInt	•	Ø			
Provider Connector – Type:	General					
BD:	Pod6-ALUMBRER/IntBD-alumbrer	•	ø			
Cluster Interface:	ServerInt	•	æ			

PREVIOUS NEXT CANCEL

PREVIOUS NEXT CANCEL

• 在Config Parameters部分,按一下All Parameters,並驗證是否有需要更新/配置的RED指示燈

。在輸出中(如圖所示),可以看到存取清單上的順序遺漏。這等效於您將在show ip access-

#### list X中看到的行順序。 STEP 3 > ASAv-AVS-Routed Parameters

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

PREVIOUS FINISH CANCEL

config parameters for the selected device

config parameters for the selected device

05:	Required Parameters Al Parameters		
	Folder/Param	Name Value Witte Domain	
	Access List	access-list-inbound	
essLists	E     F P Access Control Entry	ICMP	
	Access Control Entry	542	
	😝 🛛 🔺 🎯 Access Control Entry	55H	
	Destination Address		
		destination_service	
	Image:		
	Logging		
	Protocol	protocol	
	Source Address		
	E Source Service		
	Action	action permit	
	Crider	order (30) select asa domai	n
	Access Control Entry		
	Access Control Entry	UPDATE RESET CANCEL	

●您也可以驗證從前面定義的功能配置檔案中分配的IP編址,如果有需要,這裡是一個更改資訊的好機會。設定好所有引數後,按一下「Finish」,如下圖所示:

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

Profile Name: FunProf-ASA		
Features:	Required Parameters All Parameters	
later factor	Folder/Param Name	Value Write Domain
internacios	E 🖌 🖼 Device Config Device	1
AccessLists	E P Cacess List access-list-inbound	
NAT	🔲 🗈 🏳 Bridge Group Interface	
TrafficSelectionObjects	Interface Related Configuration	
All	E Access Group ExtAccessGroup	
	☑ Inbound Access List name	access-list-inbound
	Outbound Access List	
	IPv6 Enforce EUI-64	
	Interface Specific Configuration	
	IPv4 Address Configuration	
	IPv4 Address ipv4_address	192.168.10.1/24
	IPv4 Standby Address	
	I Pv6 Address Configuration	
	IPv6 Link Local Address Configuration	
	I □ IPv& Router Advertisements	

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

### •如果一切正常,應顯示新的已部署裝置和圖形例項。



# 驗證

• 建立「服務」圖形後需要驗證的一個重要事項是,建立消費者/提供商關係時使用了正確的元聯 結器。在「Function Connector Properties(功能聯結器屬性)」下驗證。

Tenant Pod6-ALUMBRER	Function Connector - consumer	i
Quick Start  Guick	Policy	Faults History
Application Profiles     Metworking		ACTIONS -
L4-L7 Service Parameters  Security Policies  Toubleaboot Policies	Properties Name: consumer Attachment Notification: false	
Monitoring Policies      L4-L7 Services	Filters: select an option	
L4-L7 Service Graph Templates     V* Graph1-alumbrer     II. Function Node - ASAv		
consumer     provider		

附註:從AVS動態池為防火牆的每個介面分配一個encap-vlan。驗證沒有故障。

ALL TENANTS   Add Tenant   Search: enter name, descr	common   Pod6-AL	UMBRER   Pod6-ALUMBRER2   infra   m	gmt						
Tenant Pod6-ALUMBRER 🛛 🖉 🖸	Virtual Device - A	SAv-AVS-Routed-none							i
Quick Start									
Tenant Pod6-ALUMBRER					Policy	Operational	Health	Faults	History
Application Profiles	<b>○ ±</b>			100					
Networking  L4-L7 Service Parameters   Security Policies  Monitoring Policies  Monitoring Policies  L4-L7 Service Graph Templates  L4-L7 Service Graph Templates  L4-L7 Services  L4-L7 Devices  Devices Selection Policies  Devices Selection Policies  Component Devices  Component Selection Policies  Compo	Properties Devices: Vinual Device ID: VRF: ACKed Transaction ID: Current Transaction ID: Cluster Interfaces:	ASAv-AVS-Routed 25351 none 10000 Logical interface ASAv-AVS-Routed_ClientInt ASAv-AVS-Routed_ServerInt	Encap vlan-93 vlan-94						

### • 現在,您還可以驗證推送到ASAv的資訊

ISAv-w-AVS# show interface	ip brief				
Interface	IP-Address	OK?	Method	Status	Prot
ocol					
iigabitEthernet0/0	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	perмit	tcp ar	ny any eq ымы	
ccess-list access-list-inl	oound extended	permit	tcp ar	ny any eq https	
access-list access-list-ind	oound extended	permit	tcp ar	ny any eq ssh	
access-list access-list-ind	oound extended	permit	ісмр а	any any	
ASAU-W-AUS#					

•新合約在EPG下分配。從現在起,如果您需要修改訪問清單中的任何內容,則必須使用提供程 式EPG的第4-7層服務引數完成更改。

Tenant Pod6-ALUMBRER	L4-L7 Service Parame	eters					i
Quick Start     Janant Pod6-ALUMBRER	Search By Name / Value:						
Application Profiles     Ali Av5-AEP-VMM-alumbrer     Ali Av5-AEP-VMM-alumbrer					Folder/Param Instance		
A Q EPG AVS-EPG1	Meta Folder/Param Key	Contract Name	Service Graph Name	Service Function Name	Name	Value	Specific Device
Domains (Albia and Bare Matala)	Interface	EPG240-EPG1	Graph1-Temp-alumbrer	ASAv	ClientInt		
Ends Rinding (Print and Safety Interaction	ExintConfigRelFolder	EP024o-EP01	Graph1-Temp-alumbrer	ASAv	ExtConfig		
orasic binoings (Hama)	InintConfigRelFolder	EPG240-EPG1	Graph1-Temp-alumbrer	ASAV	IntConfig		
Static Bindings (Leaves)	Interlace	EP024o-EP01	Graph1-Temp-alumbrer	ASAv	Serverint		
Contracts Static EndPoint Subnets L4-L7 Vinual IPs L4-L7 IP Address Pool L4-L7 Envice Parameters	AccessList	EPG240-EPG1	Graph1-Temp-alumbrer	ASAv	access-list-inbound		

• 在vCenter上,您還可以驗證影子EPG已分配到每個防火牆介面:

(	🕗 AS	Av-in-AVS - Virtual Machine Pro	operties		
	Hard	ware Options Resources Profi	les vServices	Virtual Machine Version: 8 orage View	/S
		Show All Devices	Add Remove	Connected	-
	Hard	dware	Summary	Connect at power on	
C D T		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 2 Network adapter 3 Network adapter 4 Network adapter 5	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 VM Network VM Network	Adapter Type Current adapter: E 1000 MAC Address 00:50:56:89:CA:89 Automatic C Manual DirectPath I/O Status: Not supported Network Connection Network Connection Network label: PedG-ALUMBRER [ASAv-AVS-RoutedctxnoneIntBD-alumb	
		Network adapter 6 Network adapter 7 Network adapter 8 Network adapter 9 Network adapter 10	VM Network VM Network VM Network VM Network	Pod6-ALUMBRER IAVS-AEP-VMM alumbrer IAVS-EPG1 (AVS)         Pod6-ALUMBRER IAVS-AEP-VMM-alumbrer IAVS-EPG2 (AVS)         quarantine (AVS)         vtep (AVS)         common [default]client (DVS)         common [default]juolivei (DVS)         common [default]web (DVS)         common [default]web (DVS)	

在本測試中,我讓2個EPG與標準合約進行通訊,這些2個EPG位於不同的域和不同的VRF中,因此 先前已配置它們之間的路由洩漏。在插入服務圖後,當防火牆在2個EPG之間設定路由和過濾時 ,這可以簡化一些操作。以前在EPG和BD下配置的DG現在與合約一樣被刪除。只有L4-L7推行的合 約應保留在EPG下。

Quick Start	1									
Tenant Pod6-ALUMBRER	Ш.,									
Application Profiles		੦±							ACTIONS -	١.
AVS-AEP-VMM-alumbrer	117									
Application EPGs		<ul> <li>Tenant Name</li> </ul>	Contract Name	Contract Type	Consumed	QoS Class	State	Label	Subject Label	
Seps Avs-EPG1		Contract Type: Co	ontract							
Domains (VMs and Bare-Me		Pode ALLIMER	EPG2.to.EPG1	Contract	Drouidad	Linepacified	formed			
Static Bindings (Paths)		FOUD-ALDIMIDH	EFGENDEFGT	Contract	FIONODU	Unspecified	Ionned			
Static Bindings (Leaves)										
Contracts										
Static EndPoint										
Subnets										

刪除標準合約後,您可以確認流量現在流經ASAv,每次客戶端向伺服器傳送請求時,命令show access-list應顯示規則的命中計數,該計數將遞增。

ASA∿-w-AVS#	
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-m-AAS#	

### 在枝葉上,應該學習客戶端、伺服器VM以及ASAv介面的終端

leaf2# show endpoint				
Legend:				
0 - peer-attached H - vtep	a - locali	ly-aged S - sta	tic	
V - vpc-attached p - peer-ag	ed L - local	M - spa	n	
s - static-arp B - bounce				
<b>+</b>			+-	+
VLAN/	Encap	MAC Address	MAC Info/	Interface
Domain	VLAN	IP Address	IP Info	
Pod6_ALIMEREP:VRE1_alumbran		50 50 50 50 1	+-	+
14 /DodG_ALLMPDED:\/DE1_clumbnon	w1 ap 14779250	50.50.50.50 L		ath1 /12
14/PODO-ALUMBRER; VRF1-GLUMDPEP	VXLan-14//6559	0050 5600 tons		eth1/15
	vian-98	0050.5089.1008	FW	eth1/7
Podb-ALUMBKEK:VKF1-alumbrer Ser	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	nt IP & vlan-97	172.16.1.10		
26 MA	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		

### 檢視連線到VEM的兩個防火牆介面。

ESX-1

~ # ve	mcmd 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	Po1	UP	UP	FWD		0		0	0		

	-											
~ # ve	# 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	0	0		Client1-AVS.eth0	
52		UP	UP	FWD		0	6	0	0		Server1-AVS.eth0	
1040	Po1	UP	UP	FWD		0		0	0			
~ #												

最後,如果知道源EPG和目標EPG的PC標籤,也可以在枝葉級別驗證防火牆規則:

EPG1								
Tenant Pod6-ALUMBRER					Policy C	operational Stats	Health Faults	History
Application Profiles							second state of Party and Party and	d Blacksonder
AVS-AEP-VMM-alumbrer					A8	KOARDO EPIGA	ssociated External Houter	d reneworks
Application EPGs	⊙₹						~	CTIONS -
P G EPG AVS-EPG1	Pearter	Description	State	Issues	QoS	Encep	PC Teg	
Indeg EPGs	AVS-EPG1		applied		Unspecified		17	
L4-L7 Service Parameters	EPG-Internal-alumbre	r	applied		Unspecified		32772	
🕨 🚭 InternalAEP-VMM-alumbrer								
Networking								
Bridge Domains								
VRFs	•							
VRF1-alumbrer								
N9F2								

### EPG2

<ul> <li>Domains (VMs and Bare-Metals)</li> <li>Static Bindings (Paths)</li> </ul>					Policy	perational Stats	Health Faults	History
Static Bindings (Leaves)					Ass	colated EPGs A	ssociated External Route	d Networks
Contracts	DI							CTIONS -
Static EndPoint								
Subnets	- Name	Description	State	Issues	QeS	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								

可以將篩選器ID與枝葉上的PC標籤匹配以驗證FW規則。

leaf2# show zor	<u>ning-rule   gr</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#							

**附註**: EPG PCTags/Sclass從不直接通訊。通過L4-L7服務圖插入建立的影子EPG中斷通訊或 將通訊捆綁在一起。

Client to Server通訊正常。

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:~\$ \$



# 疑難排解

未分配VTEP地址

驗證是否已在AEP下檢查基礎架構VLAN:

Policies 🧃 🖸	Attachable Access En	ntity Profile - AEP-AVS		1					
Cuick Start		·							
Switch Policies									
Module Policies									
Interface Policies									
Global Policies	Properties	Properties							
Attachable Access Entity Profiles	Name:	AEP-AVS							
📜 AEP-AVS	Description:	: optional							
AEP_DVS	i i i i i i i i i i i i i i i i i i i								
L3Out-N3K2-alumbrer	Enable Infrastructure VLAN:								
L3OutN3k-AEP	Domains (VMM, Physical or External)								
📃 default	Associated to Interfaces:			× +					
QOS Class Policies		A Name	State						
DHCP Relay Policies		AVS (Vmm-VMware)	formed						
MCP Instance Policy default	•								
EP Loop Protection Policy									
Error Disabled Recovery Policy									
Rogue EP Control Policy									
Monitoring Policies									
Troubleshoot Policies	VSwitch Policies								
Pools	Port Channel Policy:	select a value 🗸 🕞							
Physical and External Domains	LLDP Policy:	select a value							
	CDP Policy								
	CDF Folicy.								
	STP Policy:	select a value 👻 🗗							
	Firewall Policy:	select a value							

#### 不支援的版本

#### 驗證VEM版本是否正確並支援適當的ESXi VMWare系統。

~ # 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和交換矩陣通訊不起作用

- 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 -1 Interface Port Group/DVPort IP Family IP Address Netmask Broadcast MAC Address MTU TSO MSS Enabled Type vmk0 

#### 此時,可以確定ESXi主機和枝葉之間的交換矩陣通訊不能正常工作。可以在枝葉端檢查某些驗證命 令以確定根本原因。

leaf2# show cdp ne

Capabi	ility Codes:	R - Route S - Switc V - VoIP- s - Suppo	r, T - T h, H - H Phone, D rts-STP-	rans-B ost, I - Rem Disput	ridge, - IGM otely- e	B - S P, r - Manage	ource-Rout Repeater, d-Device,	e-Bridg	e
Device	e-ID	Local In	trfce H	ldtme	Capab	ility	Platform	Ро	rt ID
AVS:10	calhost.loca	aldomainma	in						
		Eth1/5		169	S	I s	VMware	ESXi	vmnic4
AVS:10	calhost.loca	aldomainma	in						
		Eth1/6		169	S	I s	VMware	ESXi	vmnic5
N3K-2	(FOC1938R02L)	)							
		Eth1/1	3	166	R	SIS	N3K-C31	72PQ-1	Eth1/13
leaf2 Flags:	<pre># show port-o : D - Down I - Indiv: s - Suspen S - Switcl U - Up (po M - Not in F - Config</pre>	P - idual H - nded r - ned R - ort-channe n use. Min guration f	Up in p Hot-sta Module- Routed l) -links n ailed	ort-ch ndby (: remove ot met	annel LACP o d	(membe nly)	rs)		
Group	Port- Channel	Туре	Protocol	Memb	er Por	ts			
5	Po5 (SU)	Eth	LACP	Eth1	 /5(P)	Eth	 1/6(P)		

### 通過Po5連線的ESXi中使用了2個埠

#### 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	

從上面的輸出中可以看到,Infra Vlan不允許通過,也不通過指向ESXi主機的上行鏈路埠(1/5-6)。 這表示在APIC上配置了介面策略或交換機策略的配置錯誤。

檢查兩者:

Access Policies > Interface Policies > Profiles Access Policies > Switch Policies > Profiles 在這種情況下,介面配置檔案連線到錯誤的AEP(用於DVS的舊AEP),如下圖所示:

Access Port Policy Group	o - AVS-102_1-ports-7	_PolGrp							i X
							Policy Fau	lts	History
⊙±								ACT	
Properties									
Name:	AVS-102_1-ports-7_PolGrp								
Description:	optional								
Label:									
Link Level Policy:	1GigAuto	· @							
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							
Connectivity Filters:				×	+				
	Switch IDs		Interfaces						
						SHOW USAGE	SUBMIT	С	LOSE

為AVS設定正確的AEP後,現在我們可以看到通過枝葉上的正確Unlinks(解除連結)可以看到Infra Vlan:

leaf2# show vlan extended

22 enet CE

VLAN	Name			Status	Ports	
13	infra:default			active	Eth1/1, Eth1/5, Eth1/20, Po5	Eth1/6,
19				active		
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	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: 10.0.0.30 Port: 8000 Infra vlan: 3967 FTEP IP: 10.0.0.32 Switching Mode: unknown Encap Type: unknown NS GIPO: 0.0.0.0 ~ # vemcmd show opflex Status: 12 (Active) Channel0: 12 (Active), Channel1: 0 (Discovering) Dvs name: comp/prov-VMware/ctrlr-[AVS]-vCenterController/sw-dvs-129 Remote IP: 10.0.0.30 Port: 8000 Infra vlan: 3967 FTEP IP: 10.0.32 Switching Mode: LS Encap Type: unknown NS GIPO: 0.0.0.0

# 相關資訊

應用程式虛擬交換機安裝

<u>Cisco Systems, Inc.思科應用虛擬交換機安裝指南5.2(1)SV3(1.2)版</u> 使用VMware部署ASAv

Cisco Systems, Inc.思科自適應安全虛擬裝置(ASAv)快速入門手冊9.4

Cisco ACI和Cisco AVS

<u>Cisco Systems, Inc. Cisco ACI虛擬化指南,版本1.2(1i)</u>

思科以應用為中心的基礎設施服務圖設計白皮書

思科以應用為中心的基礎設施服務圖設計白皮書

技術支援與文件 - Cisco Systems