

# AVS- ACI 1.2(x) リリースを使用した GoTo ( L3 ) モードの ASA v

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

このドキュメントでは、ACI 1.2を使用してクライアントとサーバ間の通信を確立するために、L4-L7サービスグラフとして、Routed/GOTOモードの適応型セキュリティ仮想アプライアンス(ASA v)シングルファイアウォールを導入する方法について説明しますx)リリース

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- アクセスポリシーが設定され、インターフェイスがアップおよびインサービス
- EPG、ブリッジドメイン(BD)および仮想ルーティングおよび転送(VRF)はすでに設定されています

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

ハードウェアおよびソフトウェア :

- UCS C220 - 2.0(6d)
- ESXi/vCenter:5.5
- ASA v:asa-device-pkg-1.2.4.8
- AVS - 5.2.1.SV3.1.10
- APIC - 1.2(1i)
- リーフ/スパイン - 11.2(1i)
- デバイスパッケージ\*.zipはすでにダウンロードされています

機能

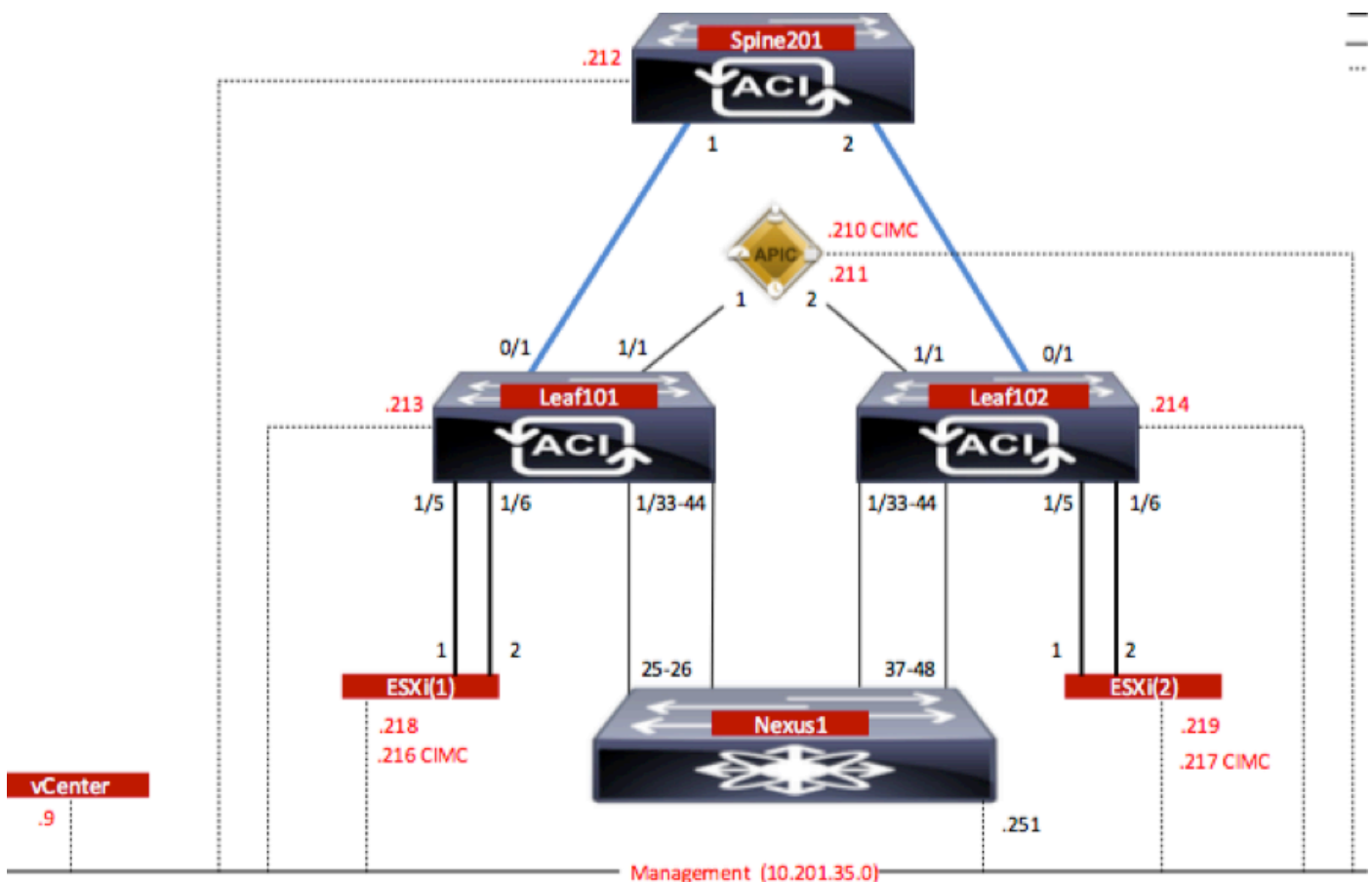
- AVS
- ASAv
- EPG、BD、VRF
- Access Control List ( ACL; アクセス コントロール リスト )
- L4-L7サービスグラフ
- vCenter

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 設定

### ネットワーク図

この図に示すように、



## 設定

AVS Initial Setup creates a VMware vCenter Domain ( VMM統合 ) 2

注：

- 1つのドメインに複数のデータセンターおよび分散仮想スイッチ(DVS)エントリを作成できます。ただし、各データセンターに割り当てることができるCisco AVSは1つだけです。

- Cisco AVSを使用したサービスグラフの導入は、Cisco ACIリリース1.2(1i)とCisco AVSリリース5.2(1)SV3(1.10)からサポートされています。サービスグラフ全体の設定は、Cisco Application Policy Infrastructure Controller(Cisco APIC)で行います。
- Cisco AVSを使用したサービス仮想マシン(VM)の展開は、Virtual Local Area Networks(VLAN)カプセル化モードを使用するVirtual Machine Manager(VMM)ドメインでのみサポートされます。ただし、コンピューティングVM (プロバイダーおよびコンシューマVM) は、Virtual Extensible LAN(VXLAN)またはVLANカプセル化を使用するVMMドメインに属することができます。
- また、ローカルスイッチングを使用する場合は、マルチキャストアドレスとプールは必要ありません。ローカルスイッチングが選択されていない場合は、マルチキャストプールを設定する必要があり、AVSファブリック全体のマルチキャストアドレスはマルチキャストプールに含まれません。AVSから発信されるすべてのトラフィックは、VLANまたはVXLANカプセル化されます。

図に示すように、[VM Networking] > [VMWare] > [Create vCenter Domain]に移動します。

Create vCenter Domain
i

---

### Specify vCenter domain users and controllers

Virtual Switch Name: AVS

Virtual Switch: VMware vSphere Distributed Switch Cisco AVS

Switching Preference: No Local Switching Local Switching

Encapsulation:  VLAN  VXLAN

Associated Attachable Entity Profile: AEP-AVS ▼ 📄

VLAN Pool: VlanPool-AVS(dynamic) ▼ 📄

Security Domains: × +

Name	Description

vCenter Credentials: × +

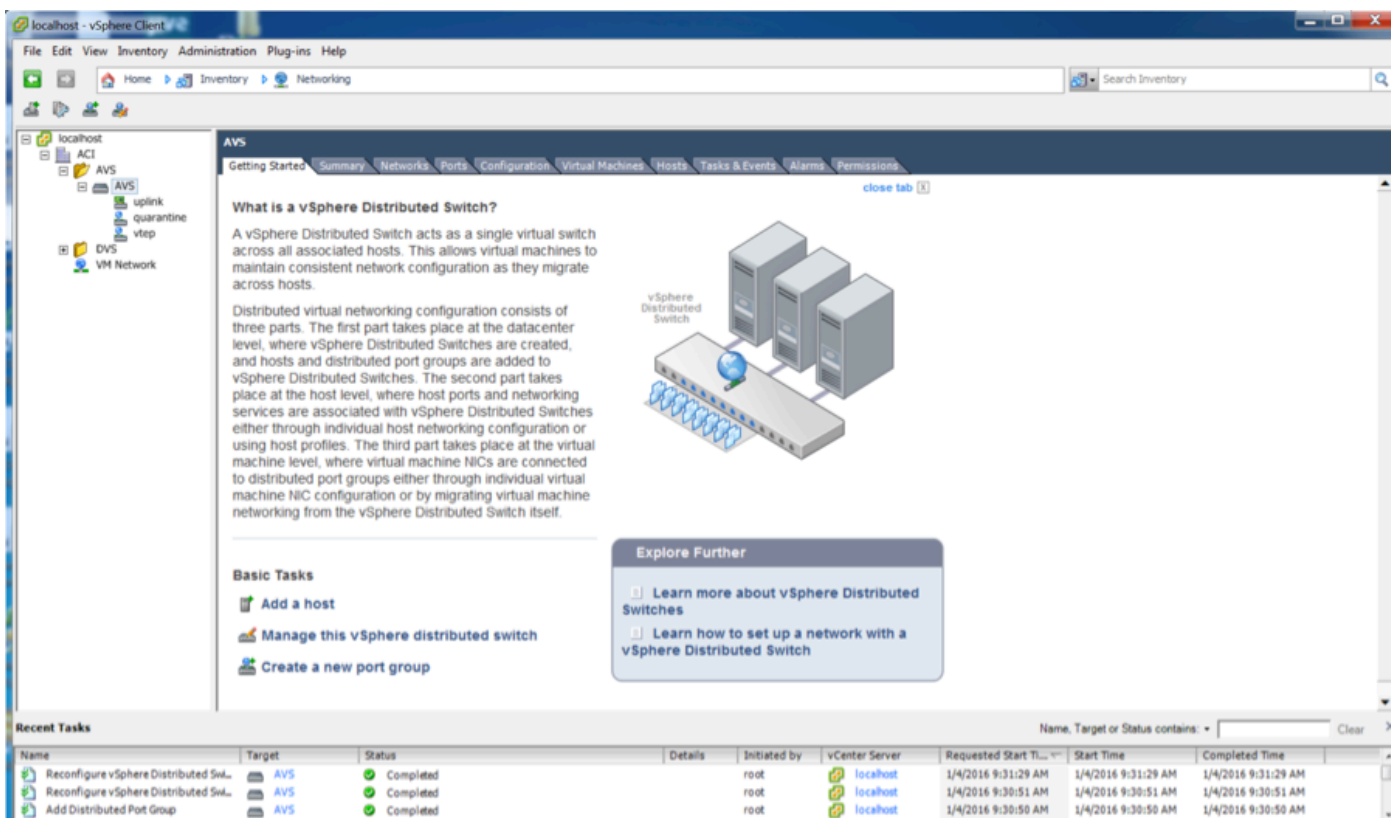
Profile Name	Username	Description
vCenterCredentials	root	

vCenter: × +

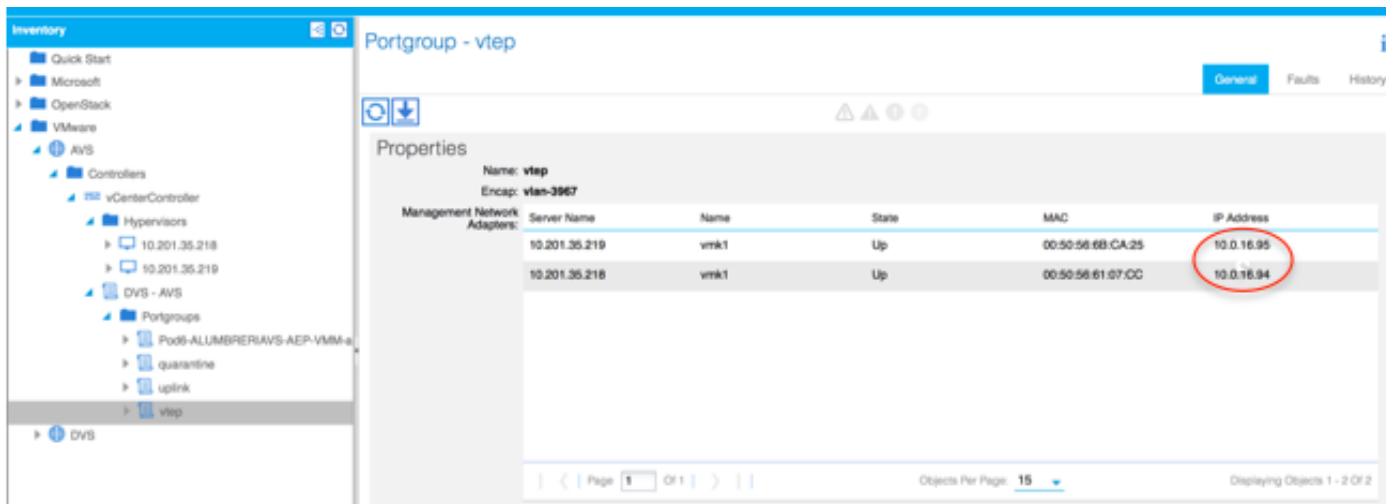
Name	IP	Type	Stats Collection
vCenterController	10.201.35.9	vCenter	Disabled

ポートチャネルまたはVPC (仮想ポートチャネル) を使用している場合は、vSwitchポリシーを設定してMacピンングを使用することを推奨します。

この後、図に示すように、APICはAVSスイッチ設定をvCenterにプッシュする必要があります。



APICでは、VXLANトンネルエンドポイント(VTEP)アドレスがAVSのVTEPポートグループに割り当てられていることがわかります。このアドレスは、使用されている接続モード (VLANまたは VXLAN ) に関係なく割り当てられます



## vCenterへのCisco AVSソフトウェアのインストール

- このリンクを使用してCCOからvSphere Installation Bundle(VIB)をダウンロード [します](#)

注：この場合、ESX 5.5を使用しています。表1に、ESXi 6.0、5.5、5.1、および5.0の互換性マトリクスを示します

表1:ESXi 6.0、5.5、5.1、および5.0のホストソフトウェアバージョンの互換性

VMware 1	VIB 2	VEM Bundle 3	Windows VC Installer	Linux vCenter Server Appliance
ESXi 6.0	cross_cisco-vem-v250-5.2.1.3.1.10.0-6.0.1.vib	VEM600-201512250119-BG-release.zip (Offline) VEM600-201512250119-BG (Online)	6.0	6.0
ESXi 5.5	cross_cisco-vem-v250-5.2.1.3.1.10.0-3.2.1.vib	VEM550-201512250113-BG-release.zip (Offline) VEM550-201512250113-BG (Online)	5.5	5.5
ESXi 5.1	cross_cisco-vem-v250-5.2.1.3.1.10.0-3.1.1.vib	VEM510-201512250107-BG-release.zip (Offline) VEM510-201512250107-BG (Online)	5.1	5.1
ESXi 5.0	cross_cisco-vem-v250-5.2.1.3.1.10.0-3.0.1.vib	VEM500-201512250101-BG-release.zip (Offline) VEM500-201512250101-BG (Online)	5.0	5.0

ZIPファイル内には3つのVIBファイルがあり、ESXiホストバージョンごとに1つずつ、図に示すようにESX 5.5に適した1つを選択します。

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

- VIBファイルをESX Datastoreにコピーします。これは、CLIを使用するか、vCenterから直接実行できます

注：VIBファイルがホスト上に存在する場合は、`esxcli software vib remove`コマンドを使用して削除します。

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

またはデータストアを直接参照します。

- ESXiホストで次のコマンドを使用して、AVSソフトウェアをインストールします。

`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`

```

~ # esxcli software vib install -v /vmfs/volumes/datastore1/cross_cisco-vem-v250-5.2.1.3.1.10.0-3.2.1.vib --maintenance-mode --no-sig-check
Installation Result
Message: Operation finished successfully.
Reboot Required: false
VIBs Installed: Cisco_bootbank_cisco-vem-v250-esx_5.2.1.3.1.10.0-3.2.1
VIBs Removed: Cisco_bootbank_cisco-vem-v197-esx_5.2.1.3.1.5.0-3.2.1
VIBs Skipped:
~ # vem status

VEM modules are loaded

Switch Name      Num Ports  Used Ports  Configured Ports  MTU      Uplinks
vSwitch0         5632       8           128               1500     vmnic0
DVS Name         Num Ports  Used Ports  Configured Ports  MTU      Uplinks
DVS              5632       10          512               9000     vmnic5,vmnic4

VEM Agent (vemdpa) is running

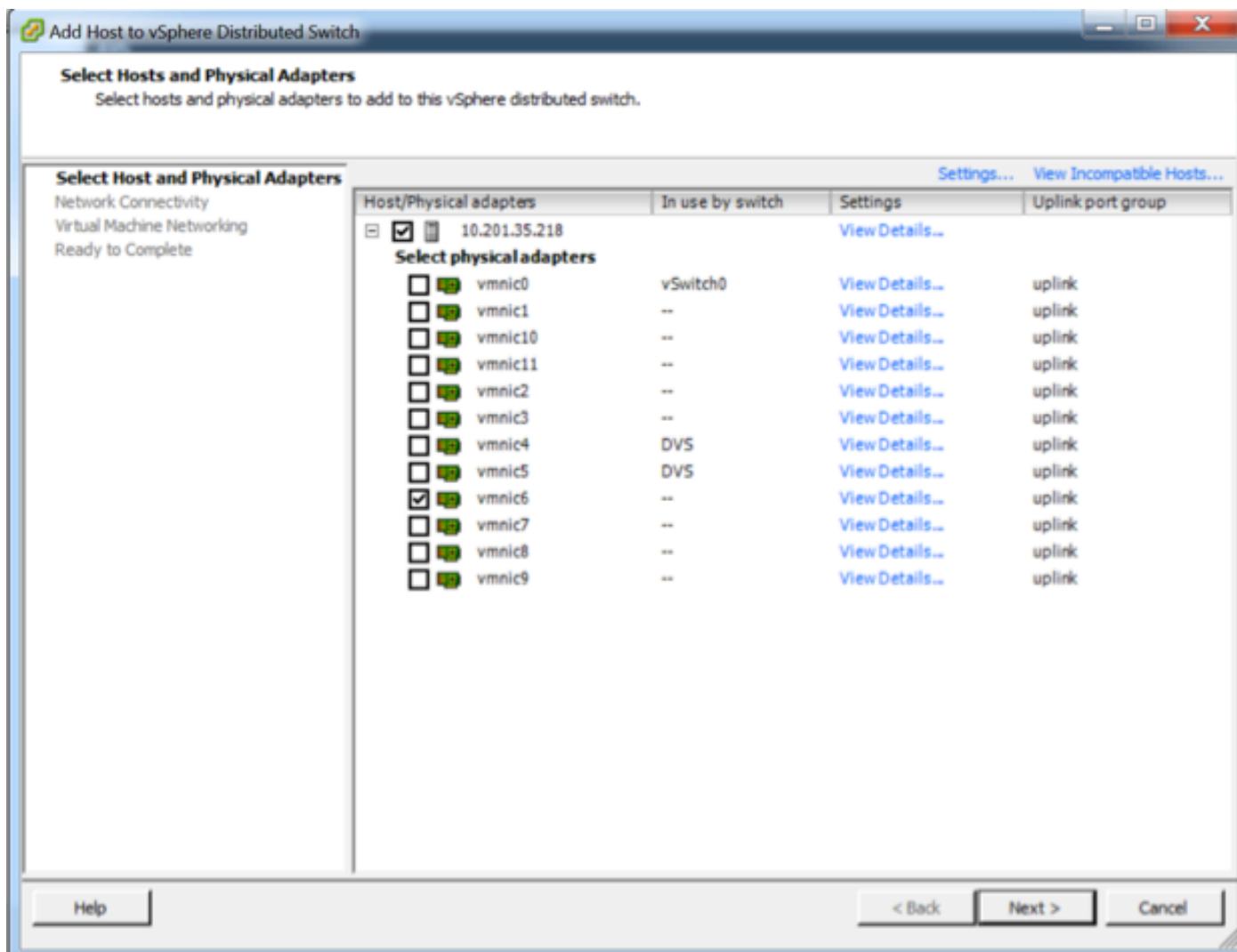
~ #

```

- Virtual Ethernet モジュール(VEM)が起動したら、AVSにホストを追加できます。

図に示すように、[Add Host to vSphere Distributed Switch]ダイアログボックスで、リーフスイッ

手に接続されている仮想NICポートを選択します（この例では、vmnic6のみを移動します）。



- [Next] をクリックします。
- [ネットワーク接続]ダイアログボックスで、[次へ]をクリックします
- [仮想マシンネットワーキング]ダイアログボックスで、[次へ]をクリックします
- [完了準備]ダイアログボックスで、[完了]をクリックします

注：複数のESXiホストを使用する場合は、すべてのホストでAVS/VEMを実行して、標準スイッチからDVSまたはAVSに管理できるようにする必要があります。

これでAVSの統合が完了し、L4-L7 ASAvの導入を続行する準備が整いました。

### ASAvの初期設定

- Cisco ASAvデバイスパッケージをダウンロードし、APICにインポートします。
- 図に示すように、[L4-L7 Services] > [Packages] > [Import Device Package]に移動します。



## Quick Start

## HELP

The **Packages** menu allows you to import L4-L7 device packages, which are used to define, configure, and monitor a network service balancer, context switch, SSL termination device, or intrusion prevention system (IPS). Device packages contain descriptions of the function and network connectivity information for each function. A network service device is deployed in the network by adding it to a service graph.

You can use the **Import a Device Package** wizard to import a device package for a function that you want to manage with APIC. We will walk you through configuring a service graph.

## Quick Start

## Import a Device Package

## Import Device Package

File Name:

BROWSE...

Device Types

SUBMIT

CLOSE

- すべてが正常に動作している場合、図に示すように、インポートされたデバイスパッケージが[L4-L7 Service Device Types]フォルダを展開していることがわかります。

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



General

Operational

Faults

History



ACTIONS ▾

## Properties

Vendor: CISCO

Model: ASA

Capabilities: GoThrough,GoTo

Major Version: 1.2

Minor Version: 4.8

Minimum Required Controller Version: 1.1

Logging Level: DEBUG ▾

Package Name: device\_script.py

Supported Protocols: |

Interface Labels:

▾ Name

cluster\_ctrl\_lk

external

failover\_lan

failover\_link

internal

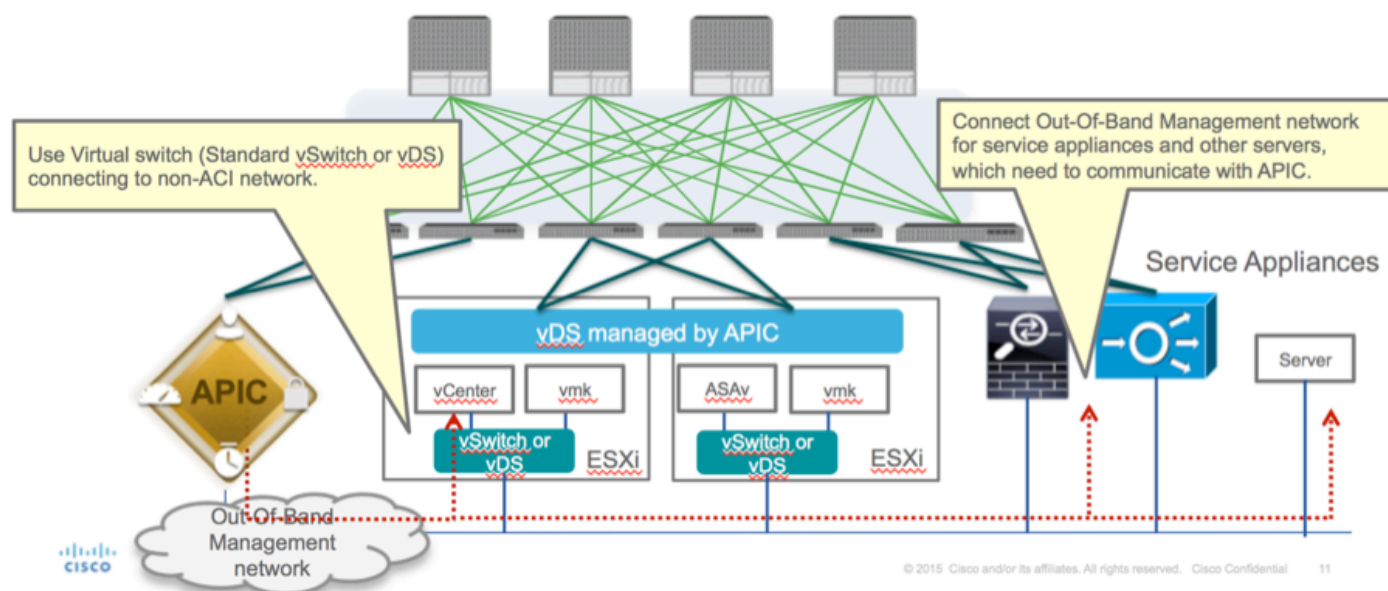
mgmt

utility

続行する前に、実際のL4-L7統合を実行する前に、インストールのいくつかの側面を決定する必要があります。

管理ネットワークには、インバンド管理とアウトオブバンド(OOB)の2種類があり、これらはASA v、ロードバランサなどの基本的なアプリケーションセントリックインフラストラクチャ(ACI)に含まれないデバイスの管理に使用できます。

この場合、ASA vのOOBは標準vSwitchを使用して展開されます。ペアメタルASAまたはその他のサービスアプライアンスやサーバの場合は、図に示すように、OOB管理ポートをOOBスイッチまたはネットワークに接続します。



ASA v OOB管理ポート管理接続は、ESXiアップリンクポートを使用してOOB経由でAPICと通信する必要があります。vNICインターフェイスをマッピングする場合、Network adapter1は常にASA vのManagement0/0インターフェイスと一致し、残の残はNetwork adapter2から開始します。

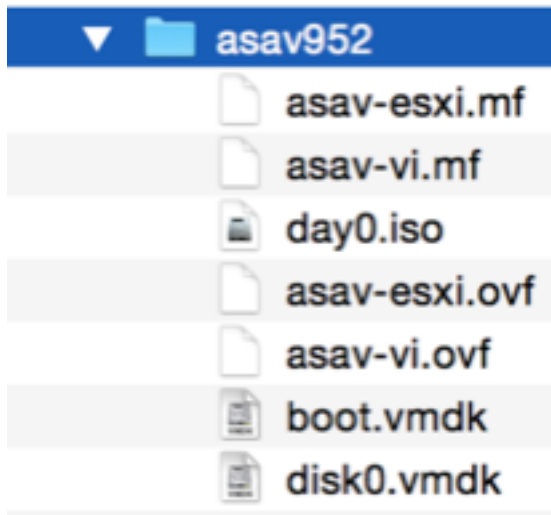
表2に、ネットワークアダプタIDとASA vインターフェイスIDの対応を示します。

表 2

Network Adapter ID	ASA v 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

- [File] > [Deploy OVF (Open Virtualization Format) Template]のウィザードを使用して、ASA v VMを展開します
- スタンドアロンESX ServerまたはvCenterにasav-viを使用する場合はasav-esxiを選択します。この場合、vCenterが使用されます。





- インストールウィザードに進み、利用規約に同意します。ウィザードの途中で、ホスト名、管理、IPアドレス、ファイアウォールモード、ASA vに関するその他の特定の情報など、いくつかのオプションを決定できます。ASA vにはOOB管理を使用することを忘れないでください。この場合は、VMネットワーク（標準スイッチ）を使用している間はインターフェイス Management0/0を維持する必要があり、インターフェイスGigabitEthernet0-8がデフォルトのネットワークポートです。

**Source**

Select the source location.

**Source**

OVF Template Details

Name and Location

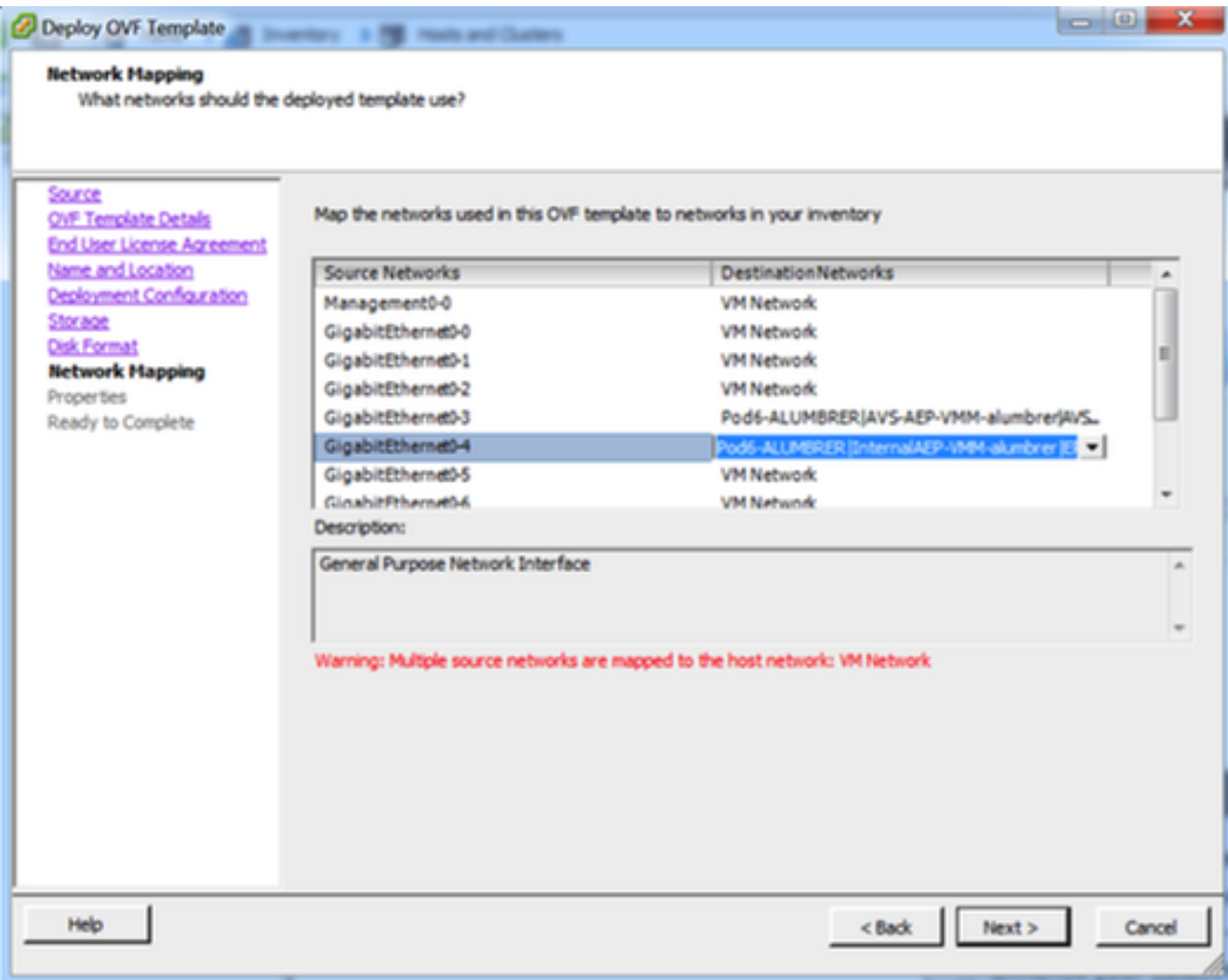
Storage

Disk Format

Ready to Complete

Deploy from a file or URL

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.



Deploy OVF Template

**Properties**  
Customize the software solution for this deployment.

[Source](#)  
[OVF Template Details](#)  
[End User License Agreement](#)  
[Name and Location](#)  
[Deployment Configuration](#)  
[Storage](#)  
[Disk Format](#)  
[Network Mapping](#)  
**Properties**  
Ready to Complete

**Deployment Type**  
**Type of deployment**  
Select the type of ASA v host to install. When an HA type deployment is selected, the additional HA Properties below should also be filled in.  
Standalone

**Hostname**  
**Hostname**  
Host name for this system. A hostname must start and end with a letter or digit and have as interior characters only letters, digits, or a hyphen.  
ASAv-w-AVS

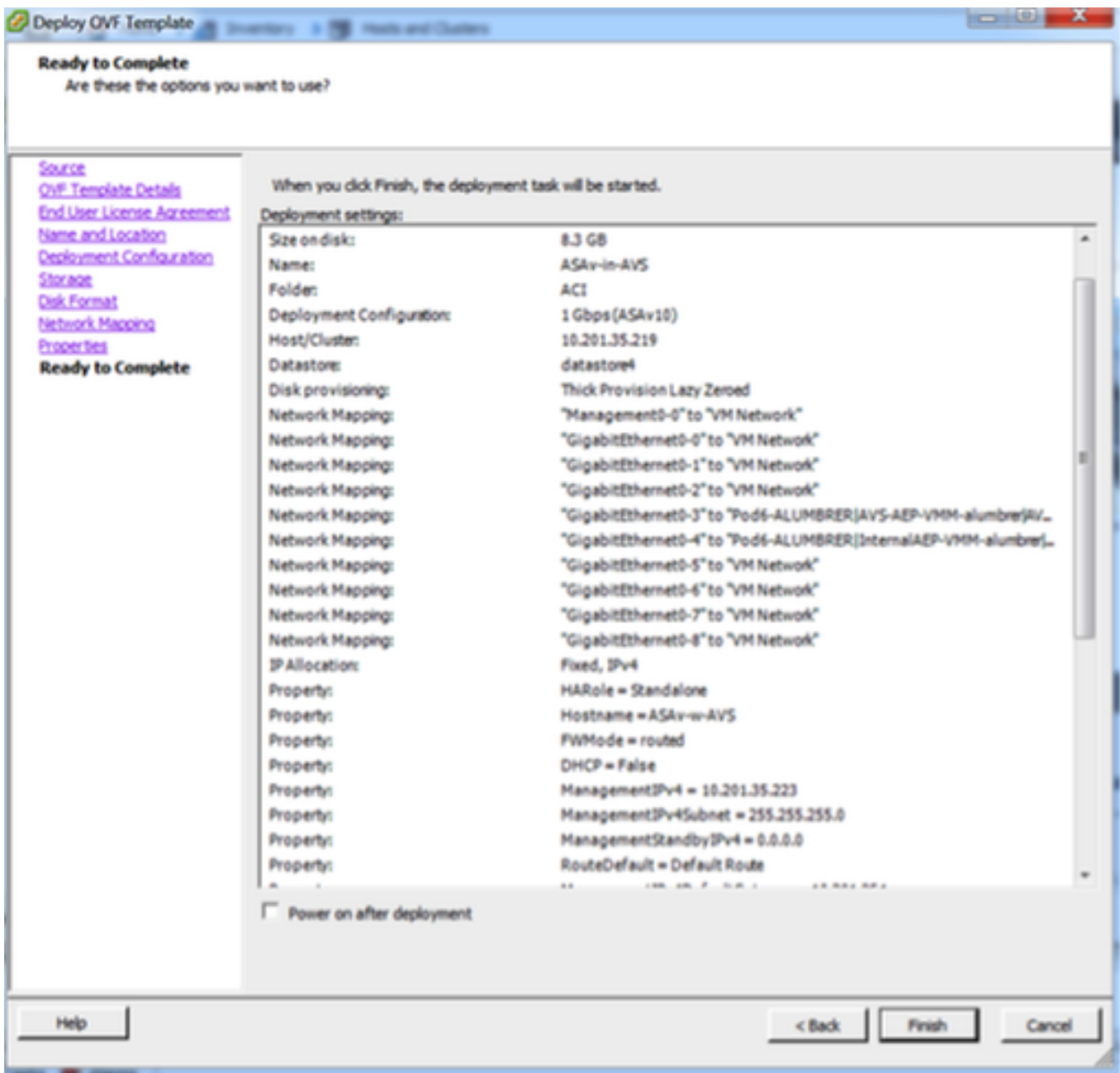
**Firewall Properties**  
**Firewall Mode**  
Select the Firewall Mode  
routed

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

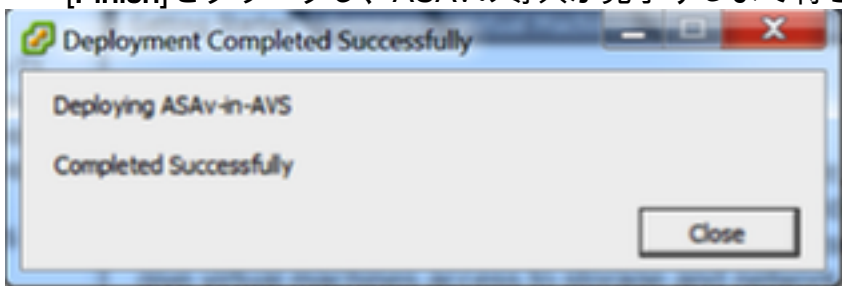
**Management IP Address**  
Enter the Management IPv4 Address. For HA-type deployments, this property specifies the Management IPv4 address of the Active HA host.  
10 . 201 . 35 . 223

**Management IP Subnet Mask**

Help < Back Next > Cancel



- [Finish]をクリックし、ASAvの導入が完了するまで待ちます



- ASAv VMの電源をオンにし、コンソールからログインして初期設定を確認します。

```

?
interface Management0/0
 management-only
 nameif management
 security-level 0
 ip address 10.201.35.223 255.255.255.0
?
ftp mode passive
pager lines 23
mtu management 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
route management 0.0.0.0 0.0.0.0 10.201.35.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
<--- More --->_

```

- 図に示すように、一部の管理設定はすでにASAvファイアウォールにプッシュされています。adminユーザ名とパスワードを設定します。このユーザ名とパスワードは、ASAにログインして設定するためにAPICによって使用されます。ASAはOOBネットワークに接続でき、APICに到達できる必要があります。

```
username admin password <device_password> encrypted privilege 15
```

```

ASA-v-w-AUS(config)# username admin password C1sc0123 privilege 15
ASA-v-w-AUS(config)# wr mem
Building configuration...
Cryptochecksum: d491b980 86fa522f 6f937baf b5bfb318

7977 bytes copied in 0.250 secs
[OK]
ASA-v-w-AUS(config)# ping 10.201.35.211
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.201.35.211, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
ASA-v-w-AUS(config)# _

```

さらに、グローバルコンフィギュレーションモードでhttp serverを有効にします。

```
http server enable
```

```
http 0.0.0.0 0.0.0.0 management
```

APICでのASAv統合のためのL4-L7:

- ACI GUIにログインし、サービスグラフを展開するテナントをクリックします。ナビゲーションペインの下部にある[L4-L7 services]を展開し、[L4-L7 Devices]を右クリックし、[Create L4-L7 devices]をクリックしてウィザードを開きます



- この実装では、次の設定が適用されます。

- マネージモード

- ファイアウォールサービス

- 仮想デバイス

- 単一ノードでAVSドメインに接続

- ASAvモデル

- ルーテッドモード(GoTo)

- 管理アドレス ( Mgmt0/0インターフェイスに割り当てられた以前のアドレスと一致する必要があります )

- APICとしてHTTPSを使用するデフォルトでは、最もセキュアなプロトコルを使用してASAvと通信します

Create L4-L7 Devices i x

STEP 1 > General 1. General 2. Device Configuration

Please select device package and enter connectivity information.

### General

Managed:

Name: ASAv-AVS-Routed

Service Type: Firewall

Device Type:  PHYSICAL  VIRTUAL

VMM Domain: AVS

Mode:  Single Node  HA Cluster

Device Package: CISCO-ASA-1.2

Model: ASAv

Function Type:  GoThrough  GoTo

### Device 1

Management IP Address: 10.201.35.3 Management Port: https

VM: vCenterController/ASAv-in-AVS

Device Interfaces:

Name	VNIC	Path (Only For Route Peering)
GigabitEthernet0/0	Network adapter 2	Node-102/MAC_Pinning
GigabitEthernet0/1	Network adapter 3	Node-102/MAC_Pinning

### Cluster

Management IP Address: 10.201.35.3 Management Port: https

Cluster Interfaces:

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

### Connectivity

APIC to Device:  Out-Of-Band

Management Connectivity:  In-Band

### Credentials

Username: admin

Password: .....

Confirm Password: .....

- 導入を成功させるには、デバイスインターフェイスとクラスタインターフェイスを正しく定義することが重要です

最初の部分では、前のセクションで示した表2を使用して、ネットワークアダプタIDと使用するASAvインターフェイスIDを正しく一致させます。パスは、ファイアウォールインターフェイスの出入りを可能にする物理ポート、ポートチャネル、またはVPCを指します。この場合、ASAはESXホスト内に配置され、両方のインターフェイスの入出力が同じです。物理アプライアンスでは、ファイアウォール(FW)の内部と外部は異なる物理ポートになります。

2つ目の部分では、クラスタインターフェイスを常に例外なく定義する必要があります ( クラスタHAを使用していない場合でも )。これは、オブジェクトモデルがmlfインターフェイス ( デバイ

スパッケージのメタインターフェイス)、Lifインターフェイス(外部、内部、内部など)とCif(具体的なインターフェイス)。L4-L7の具体的なデバイスは、デバイスクラス設定で設定する必要があり、この抽象化は論理デバイスと呼ばれます。論理デバイスは、コンクリートデバイス上の具体的なインターフェイスにマッピングされた論理インターフェイスを有する。

この例では、次の関連付けが使用されます。

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

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

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

The screenshot displays the configuration for 'ASAv-AVS-Routed'. In the 'General' section, the 'Managed' checkbox is checked, and the 'MVM Domain' is set to 'AVS'. The 'Function Type' is set to 'GoThrough'. In the 'Device 1' section, the 'Management Port' is 443, and the 'VM Name' is 'ASAv-Is-AVS'. The 'Interfaces' table is as follows:

Name	vNIC	Path (Only For Route Peering)
GigabitEthernet0/1	Network adapter 3	Node-102/MAC_Pinning, Nod...
GigabitEthernet0/2	Network adapter 4	Node-102/MAC_Pinning

The 'Cluster' section shows the following interfaces:

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

注：フェールオーバー/HAの導入では、GigabitEthernet 0/8がフェールオーバーインターフェイスとして事前設定されています。

デバイスの状態が安定しており、機能プロファイルとサービスグラフテンプレートを導入する準備が整っている必要があります

#### サービスグラフ寺

まず、ASAvの機能プロファイルを作成します。その前に、図に示すように、機能プロファイルグループを作成し、そのフォルダの下にL4-L7サービス機能プロファイルを作成する必要があります。

Create L4-L7 Services Function Profile Group

Specify the information about the Function Profile Group

Name: FunProfGroup

Description:

SUBMIT CANCEL

Tenant Pod9-ALUMBRER

L4-L7 Services Function Profile Group - FunProfGroup

General Faults History

Properties

Name: FunProfGroup

Description:

Service Function Profiles:

Name	Associated Function	Description
No items have been found. Select Actions to create a new item.		

DELETE Create L4-L7 Services Function Profile Save as ... Post ...

- ドロップダウンメニューから[WebPolicyForRoutedMode Profile]を選択し、ファイアウォールのインターフェイスの設定に進みます。以降の手順はオプションであり、後で実装または変更できます。これらの手順は、サービスグラフの再利用可能またはカスタム化の方法に応じて、導入のいくつかの段階で実行できます。

この演習では、ルーテッドファイアウォール (GoToモード) では、各インターフェイスに一意的IPアドレスが必要です。標準のASA設定には、インターフェイスのセキュリティレベルもあります (外部インターフェイスのセキュリティは低く、内部インターフェイスのセキュリティは高くなります)。必要に応じて、インターフェイスの名前を変更することもできます。この例では、デフォルトを使用します。

- [Interface Specific Configuration]を展開し、IPアドレスx.x.x.x/y.y.y.yまたはx.x.x.x/yyの次の形式でServerIntのIPアドレスとセキュリティレベルを追加します。ClientIntインターフェイスのプロセスを繰り返します。

## Create Function Profile

Name: FunProf-ASA  
Description: optional

Copy Existing Profile Parameters:

Profile: CISCO-ASA-1.2/WebPolicyForRoutedMode

Features and Parameters

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

Basic Parameters **All Parameters**

Folder/Param	Name	Value	Mandatory	Locked	Shared
Device Config	Device				
Bridge Group Interface					
Interface Related Configuration	externallif			false	false
Access Group	ExtAccessGroup			false	
IPv6 Enforce EUI-64					
Interface Specific Configur...	externallICfg			false	
IPv4 Address Configur...					
IPv4 Address	ipv4_address	192.168.10.1/24			
IPv4 Standby Address					
IPv6 Address Configura...					
IPv6 Link Local Address...					

UPDATE RESET CANCEL

SUBMIT CANCEL

注：デフォルトのアクセスリスト設定を変更し、独自の基本テンプレートを作成することもできます。デフォルトでは、RoutedModeテンプレートにはHTTPおよびHTTPSのルールが含まれます。この演習では、許可された外部アクセスリストにSSHとICMPが追加されます

。

## Create Function Profile

Name: FunProf-ASA  
Description: optional

Copy Existing Profile Parameters:

Profile: CISCO-ASA-1.2/WebPolicyForRoutedMode

Features and Parameters

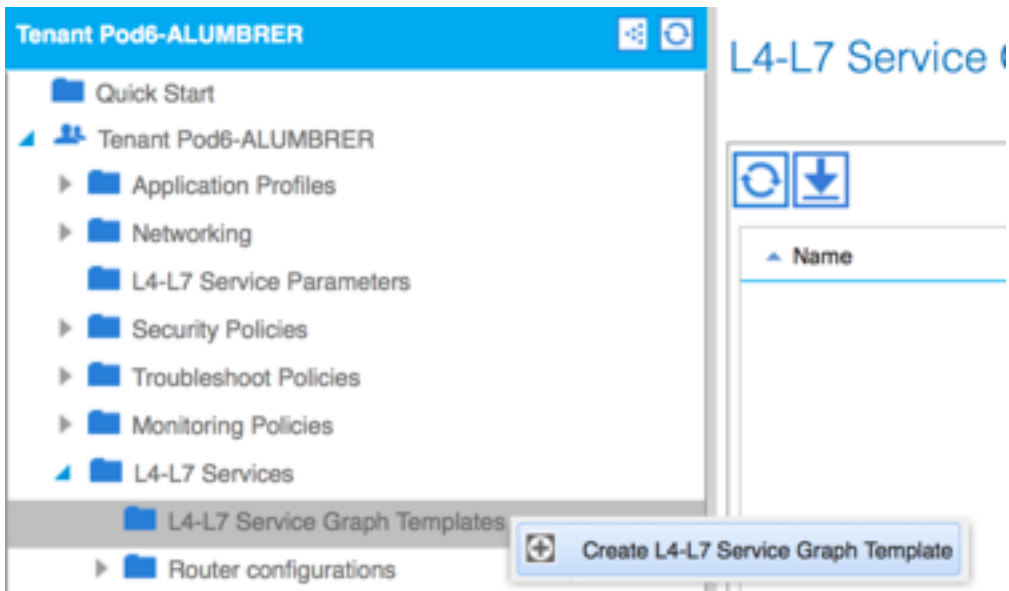
In order to auto apply new values to the parameters of existing graph instance when users modify function profiles, the name of top folder must be ended with -Default.

Basic Parameters **All Parameters**

Folder/Param	Name	Value	Mandatory	Locked	Shared
Destination Service	destination_service				
High Port					
Low Port	low_port	22		false	
Operator	operator	eq		false	
ICMP					
Logging					
Protocol					
Source Address					
Source Service					
Action	action	permit		false	
Order	order	30		false	

SUBMIT CANCEL

- 次に、[送信]をクリックします
- ここで、サービスグラフテンプレートを作成します





- デバイスクラスタを右側にドラッグアンドドロップして、コンシューマとプロバイダーの関係を形成し、[ルーテッドモード(Routed Mode)]と以前に作成した機能プロファイルを選択します。

Graph Name:

Graph Type:  Create A New One  Clone An Existing One


**Consumer**





ASA


**Provider**



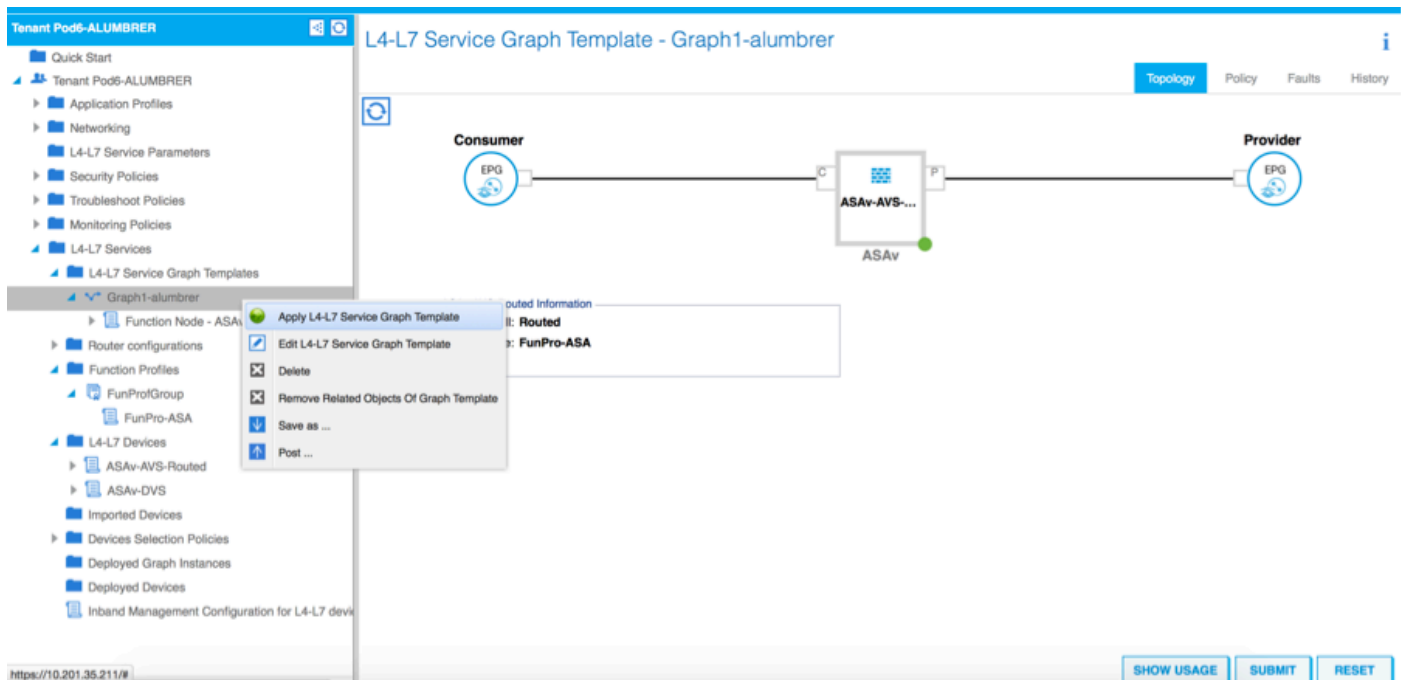
Please drag a device from devices table and drop it here to create a service node.

ASAv-AVS-Routed Information

Firewall:  Routed  Transparent

Profile:  

- テンプレートの障害をチェックします。テンプレートは再利用可能になるように作成され、特定のEPGなどに適用する必要があります。
- テンプレートを適用するには、右クリックして[Apply L4-L7 Service Graph Template]を選択します



- どのEPGがコンシューマ側とプロバイダー側になるかを定義します。この演習では、AVS-EPG2がコンシューマ（クライアント）であり、AVS-EPG1がプロバイダー（サーバ）です。フィルタは適用されないことに注意してください。これにより、ファイアウォールは、このウィザードの最後のセクションで定義されたアクセスリストに基づいてすべてのフィルタリングを実行できます。
- [Next] をクリックします。

## STEP 1 > Contract

1. Contract 2. Graph

### Config A Contract Between EPGs

EPGs Information

Consumer EPG / External Network: Pod6-ALUMBRER/AVS-AEP-VMM

Provider EPG / External Network: Pod6-ALUMBRER/AVS-AEP-VMM

Contract Information

Contract:  Create A New Contract  Choose An Existing Contract Subject

Contract Name: EPG2-to-EPG1

No Filter (Allow All Traffic):

Pod6-ALUMBRER/AVS-AEP-VMM-alumbrer/epg-AVS-EPG1

Pod6-ALUMBRER/InternalAEP-VMM-alumbrer/epg-EPG-Internal-alumbrer

Pod6-ALUMBRER/VRF1-alumbrer/AnyEPG

Pod6-ALUMBRER/VRF2/AnyEPG

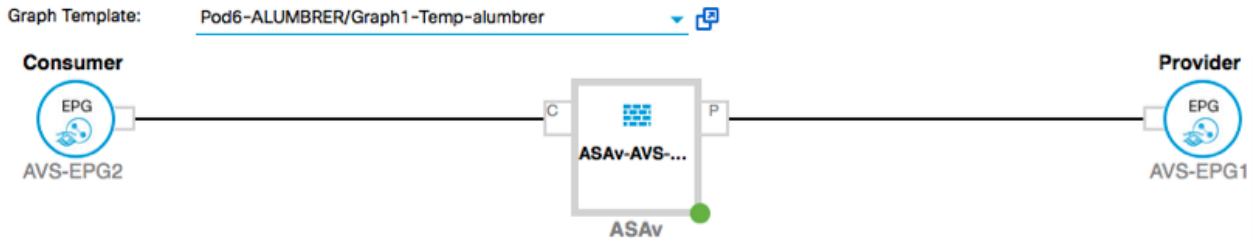
Pod6-ALUMBRER/L3Out-N3K2/L3Net

PREVIOUS NEXT CANCEL

- 各EPGのBD情報を確認します。この場合、EPG1はIntBD DBのプロバイダーであり、EPG2はBD ExtBDのコンシューマです。EPG1はファイアウォールインターフェイス ServerIntに接続し、EPG2はインターフェイス ClientIntに接続します。両方のFWインターフェイスが各EPGのDGになるため、トラフィックは常にファイアウォールを通過するように強制されます。



- [Next] をクリックします。



ASAv-AVS-Routed Information

Firewall: routed  
Profile: FunPro-ASA

Consumer Connector

Type:  General  Route Peering

BD: Pod6-ALUMBRER/ExtBD-alubrер

Cluster Interface: ClientInt

Provider Connector

Type:  General  Route Peering

BD: Pod6-ALUMBRER/IntBD-alubrер

Cluster Interface: ServerInt

PREVIOUS NEXT CANCEL

- [Config Parameters]セクションで[All Parameters]をクリックし、更新または設定が必要なREDインジケータがあるかどうかを確認します。図に示す出力では、アクセスリストの順序が間違っていることがわかります。これは、show ip access-list Xで表示される回線順序と同じです。

STEP 3 > ASAv-AVS-Routed Parameters

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

config parameters for the selected device

Profile Name: FunPro-ASA

Required Parameters All Parameters

Folder/Param	Name	Value	Write Domain
Access List	access-list-inbound		
Access Control Entry	ICMP		
Access Control Entry	SSH2		
Access Control Entry	SSH		
Destination Address			
Destination Service	destination_service		
ICMP			
Logging			
Protocol	protocol		
Source Address			
Source Service			
Action	action	permit	
Order	order	100	select asa domain
Access Control Entry			
Access Control Entry			

UPDATE RESET CANCEL

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

PREVIOUS FINISH CANCEL

- 先に定義した機能プロファイルから割り当てられたIPアドレスを確認することもできます。必要に応じて情報を変更する可能性が高くなります。すべてのパラメータを設定したら、図

に示すように[Finish]をクリックします。

STEP 3 > ASA-VS-Routed Parameters

1. Contract 2. Graph 3. ASA-VS-Routed Parameters

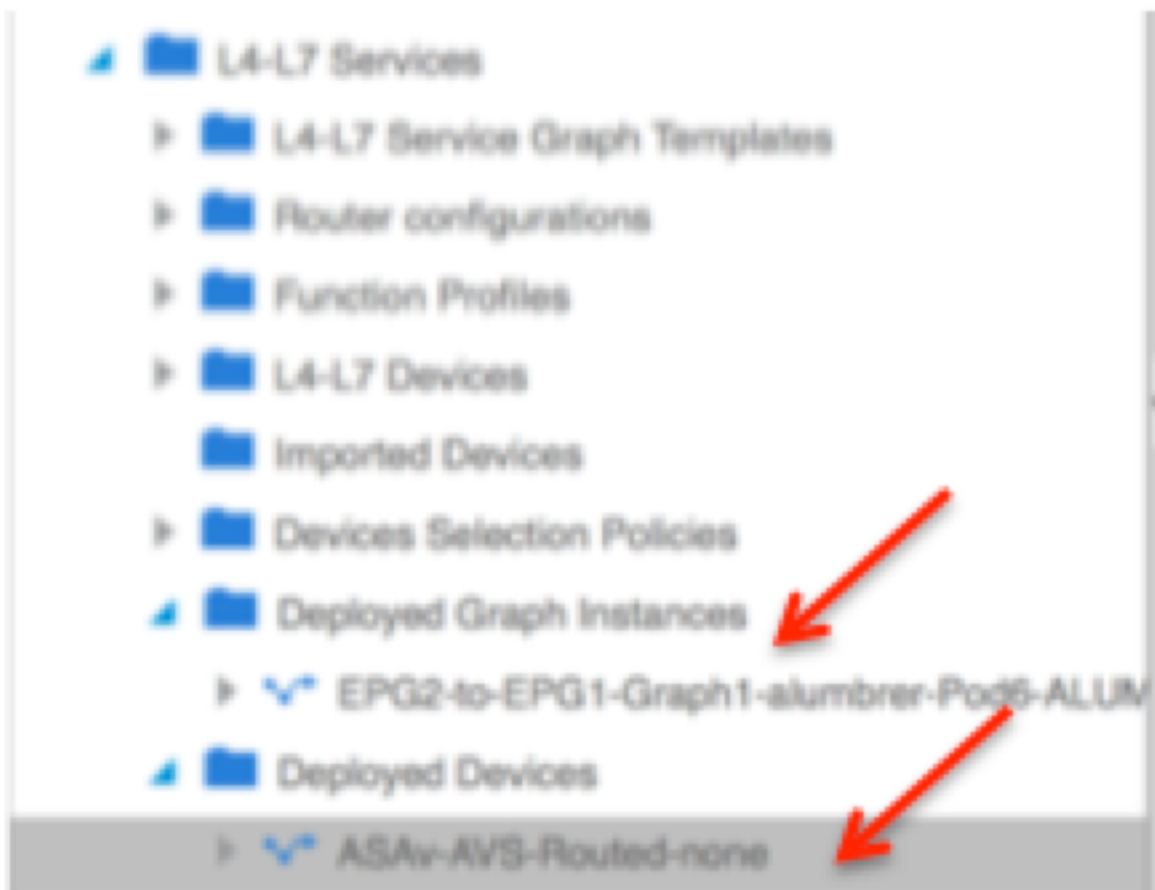
config parameters for the selected device

Profile Name: FunProf-ASA

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

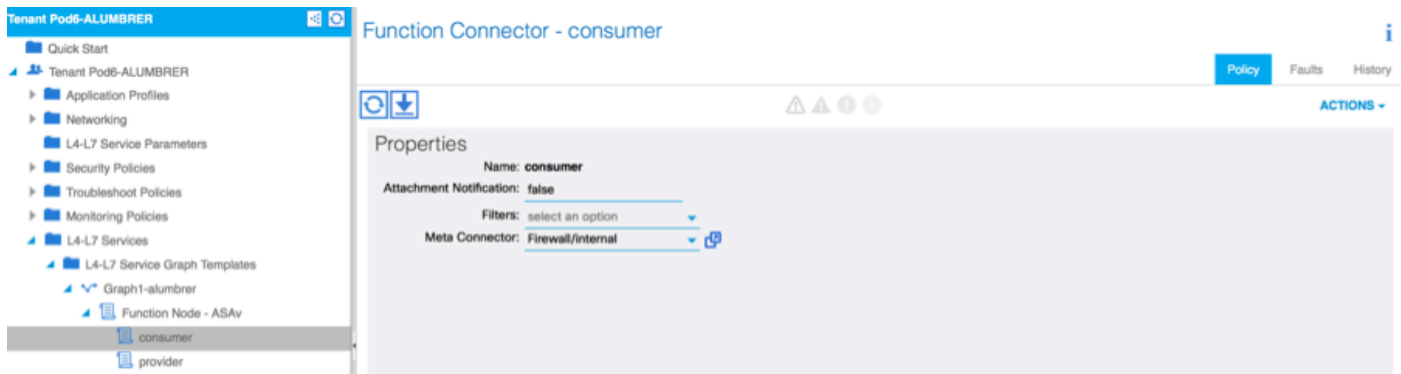
RED indicators parameters needed to be updated and GREEN indicates parameters will be submitted to the provider EPG.

- 問題がなければ、新しい展開済みデバイスとグラフインスタンスが表示されます。

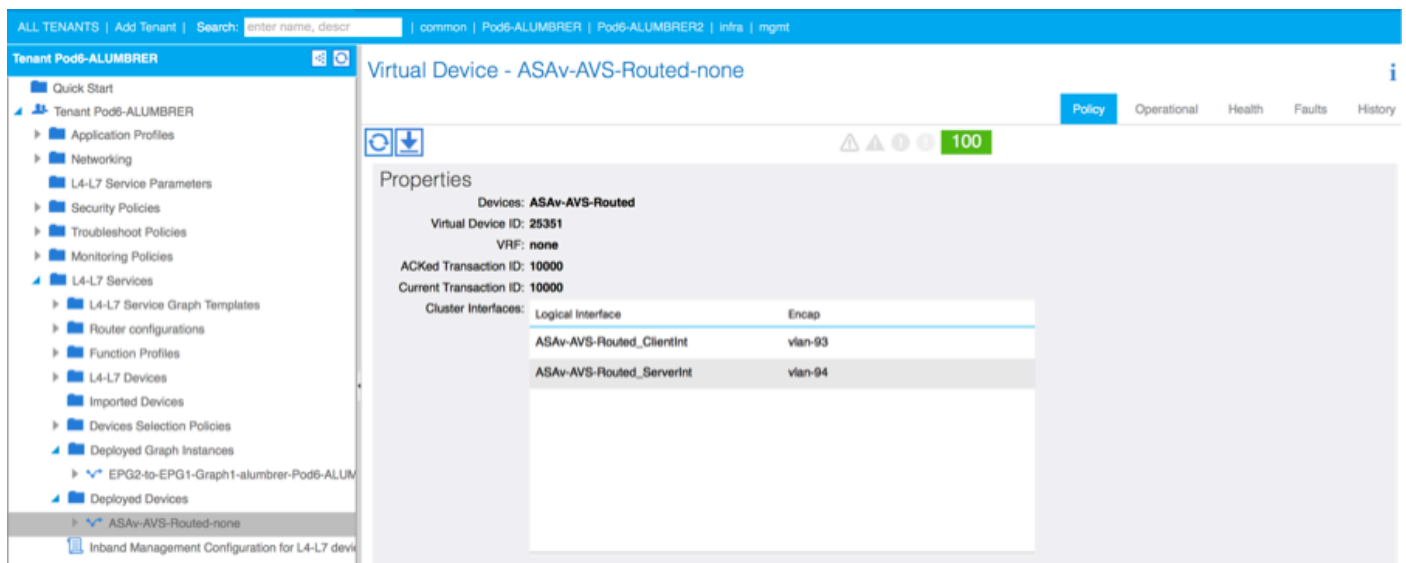


## 確認

- サービスグラフを作成した後で確認すべき重要な点の1つは、コンシューマ/プロバイダー関係が適切なメタコネクタで作成されていることです。[Function Connector Properties]で確認します。



注：ファイアウォールの各インターフェイスには、AVSダイナミックプールからencap-vlanが割り当てられます。障害がないことを確認します。



- 次に、ASAvにプッシュされた情報も確認できます

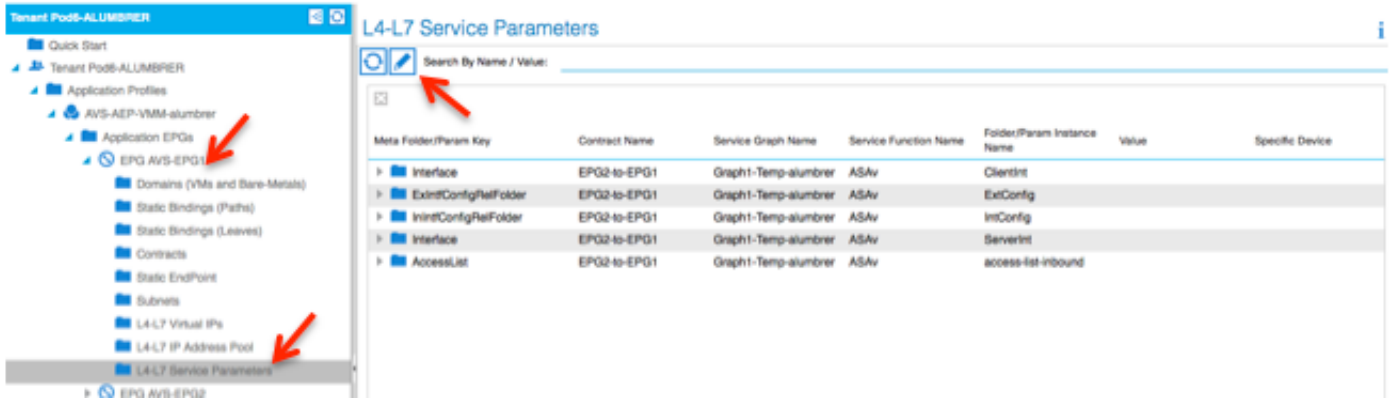
```

ASAv-w-AUS# show interface ip brief
Interface                               IP-Address      OK? Method Status      Prot
ocol
GigabitEthernet0/0                      192.168.10.1   YES manual  up          up
GigabitEthernet0/1                      172.16.1.1     YES manual  up          up
GigabitEthernet0/2                      unassigned     YES unset   administratively down up
GigabitEthernet0/3                      unassigned     YES unset   administratively down up
GigabitEthernet0/4                      unassigned     YES unset   administratively down up
GigabitEthernet0/5                      unassigned     YES unset   administratively down up
GigabitEthernet0/6                      unassigned     YES unset   administratively down up
GigabitEthernet0/7                      unassigned     YES unset   administratively down up
GigabitEthernet0/8                      unassigned     YES unset   administratively down up
Management0/0                           10.201.35.223 YES CONFIG  up          up
ASAv-w-AUS# show run access-list
access-list access-list-inbound extended permit tcp any any eq www
access-list access-list-inbound extended permit tcp any any eq https
access-list access-list-inbound extended permit tcp any any eq ssh
access-list access-list-inbound extended permit icmp any any
ASAv-w-AUS#

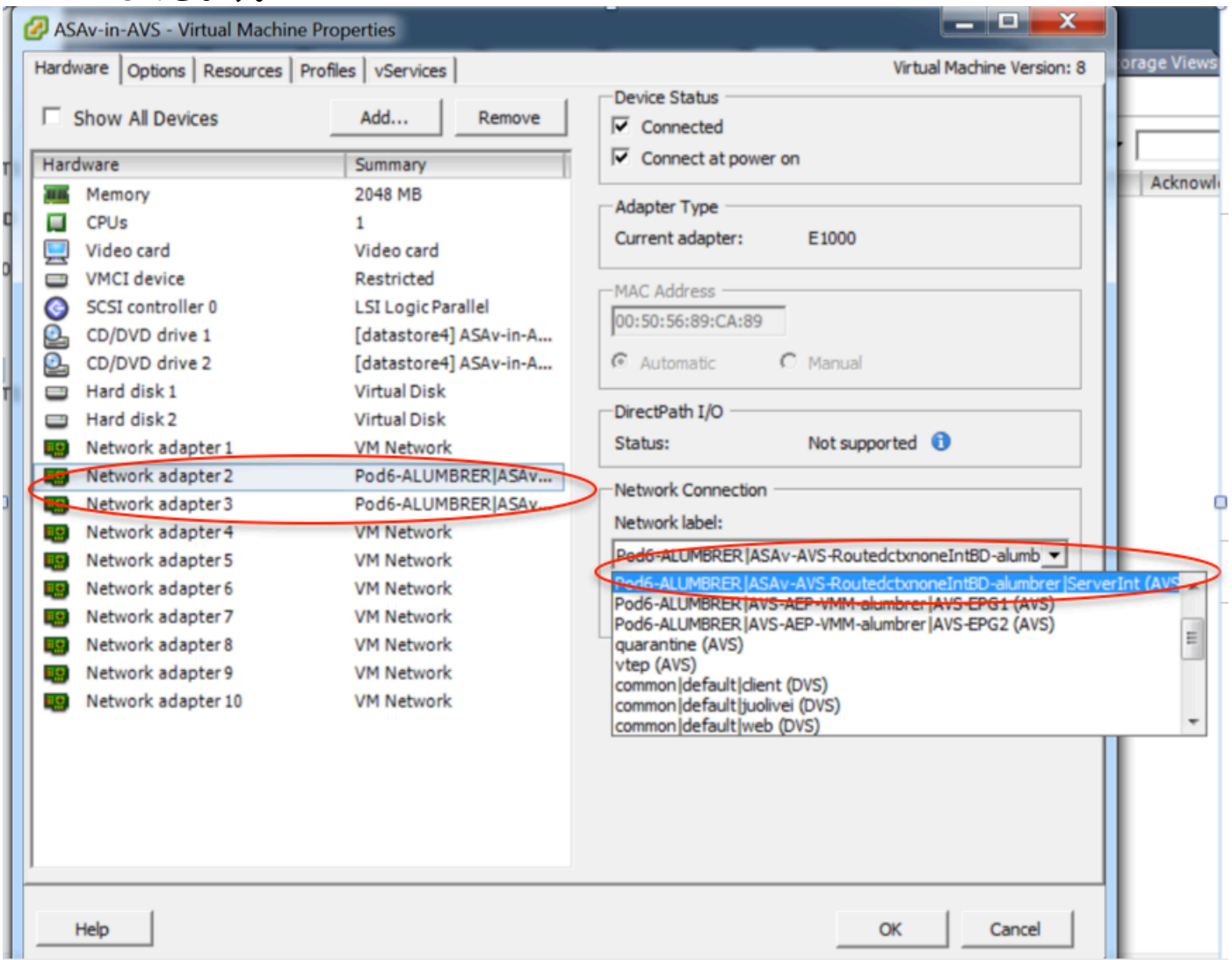
```

- 新しい契約がEPGの下に割り当てられます。今後、アクセスリストに何らかの変更を加える必要がある場合は、プロバイダーEPGのL4-L7サービスパラメータを変更する必要があります

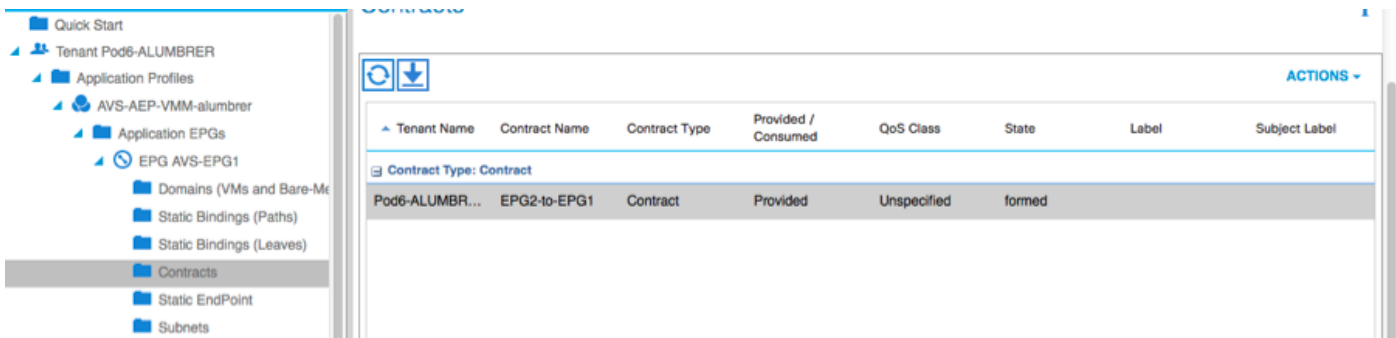
。



- vCenterでは、シャドウEPGが各FWインターフェイスに割り当てられていることを確認することもできます。



このテストでは、2つのEPGを標準契約と通信させ、これら2つのEPGは異なるドメインと異なるVRFにあるため、これらの間のルート漏出は以前に設定されています。これにより、FWが2つのEPG間でルーティングとフィルタリングを設定するときに、サービスグラフを挿入した後に少し簡素化されます。EPGおよびBDで以前に設定したDGは、契約と同じように削除できます。L4-L7によってプッシュされた契約だけがEPGの下に残ります。



標準の契約が削除されると、トラフィックがASAを通過していることを確認できます。クライアントがサーバに要求を送信するたびに、show access-listコマンドでルールのヒットカウントが増加します。

```

ASA-v-w-AUS#
ASA-v-w-AUS# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
  alert-interval 300
access-list access-list-inbound; 4 elements; name hash: 0xcb5bd6c7
access-list access-list-inbound line 1 extended permit tcp any any eq www (hitcnt=0) 0xc873a747
access-list access-list-inbound line 2 extended permit tcp any any eq https (hitcnt=0) 0x48bedbdd
access-list access-list-inbound line 3 extended permit tcp any any eq ssh (hitcnt=4) 0x532fd57a
access-list access-list-inbound line 4 extended permit icmp any any (hitcnt=4) 0xe4b5a75d
ASA-v-w-AUS#
  
```

リーフでは、クライアントとサーバのVMおよびASAvインターフェイスに対してエンドポイントを学習する必要があります

```

leaf2# show endpoint
Legend:
  0 - peer-attached      H - vtep                a - locally-aged      S - static
  V - vpc-attached      p - peer-aged          L - local              M - span
  s - static-arp        B - bounce
+-----+-----+-----+-----+-----+
| VLAN/ | Encap | MAC Address | MAC Info/ | Interface |
| Domain | VLAN | IP Address | IP Info | |
+-----+-----+-----+-----+-----+
Pod6-ALUMBREER:VRF1-alumbreer
14/Pod6-ALUMBREER:VRF1-alumbreer
30          vxlan-14778359  5897.bda4.f9bc L          eth1/13
          vxlan-98    0050.5689.f008 L          eth1/7
Pod6-ALUMBREER:VRF1-alumbreer
25          vxlan-98    192.168.10.10 L          po4
          vxlan-94    0050.5689.ca89 L
Pod6-ALUMBREER:VRF1-alumbreer
mgmt:inb
21          vxlan-94    192.168.10.1 L
          vxlan-94    192.168.2.11 S
Pod6-ALUMBREER:VRF2
26          vxlan-97    0050.5689.3fca L          eth1/7
          vxlan-97    172.16.1.10 L
Pod6-ALUMBREER:VRF2
          vxlan-93    0050.5689.e7dd L          po4
          vxlan-93    172.16.1.1 L
overlay-1
          vxlan-93    10.0.104.93 L
overlay-1
13          vxlan-93    10.0.96.67 L          FW
          vxlan-16777209 0050.5677.18a5 H          interface
          vxlan-16777209 10.0.32.93 H          (ServerInt)
overlay-1
13          vxlan-16777209 0050.5660.ddab H          po4
          vxlan-16777209 10.0.32.64 H
  
```

VEMに接続された両方のファイアウォールインターフェイスを参照してください。



## ESX-1

```
~ # vemcmd show port vlan
```

LTL	VSM Port	Admin	Link	State	Cause	PC-LTL	SGID	ORG	svcpath	Type	Vem Port
22	Eth1/5	UP	UP	FWD	-	1040	4	0	0		vmnic4
23	Eth1/6	UP	UP	FWD	-	1040	5	0	0		vmnic5
50		UP	UP	FWD	-	0	4	0	0		vmk1
51		UP	UP	FWD	-	0	4	0	0		ASAv-in-AVS.eth1
52		UP	UP	FWD	-	0	4	0	0		ASAv-in-AVS.eth2
1040	Po1	UP	UP	FWD	-	0	0	0	0		

## ESX-2

```
~ # vemcmd show port vlan
```

LTL	VSM Port	Admin	Link	State	Cause	PC-LTL	SGID	ORG	svcpath	Type	Vem Port
24	Eth1/7	UP	UP	FWD	-	1040	6	0	0		vmnic6
50		UP	UP	FWD	-	0	6	0	0		vmk1
51		UP	UP	FWD	-	0	6	0	0		Client1-AVS.eth0
52		UP	UP	FWD	-	0	6	0	0		Server1-AVS.eth0
1040	Po1	UP	UP	FWD	-	0	0	0	0		

```
~ #
```

最後に、送信元EPGと宛先EPGのPCタグがわかっている場合は、リーフレベルでもファイアウォールルールを確認できます。

### EPG1

Name	Description	State	Issues	QoS	Encap	PC Tag
AVS-EPG1		applied		Unspecified		17
EPG-Internal-almubrer		applied		Unspecified		32772

### EPG2

Name	Description	State	Issues	QoS	Encap	PC Tag
AVS-EPG2		applied		Unspecified		5476

フィルタIDをリーフのPCタグと一致させて、FWルールを確認できます。



```
leaf2# show zoning-rule | grep '17\|5476'
```

4141	17	32775	default	enabled	2916352	permit	src_dst_any(5)
4142	32775	17	default	enabled	2916352	permit	src_dst_any(5)
4139	5476	49156	14	enabled	2555904	permit	src_dst_any(5)
4140	49156	5476	14	enabled	2555904	permit	src_dst_any(5)

```
leaf2#
```

注：EPG PCTags/Sclassは直接通信しません。通信は、L4-L7サービスグラフの挿入によって作成されたシャドウEPGを介して中断または結合されます。

サーバへの通信クライアントが動作します。

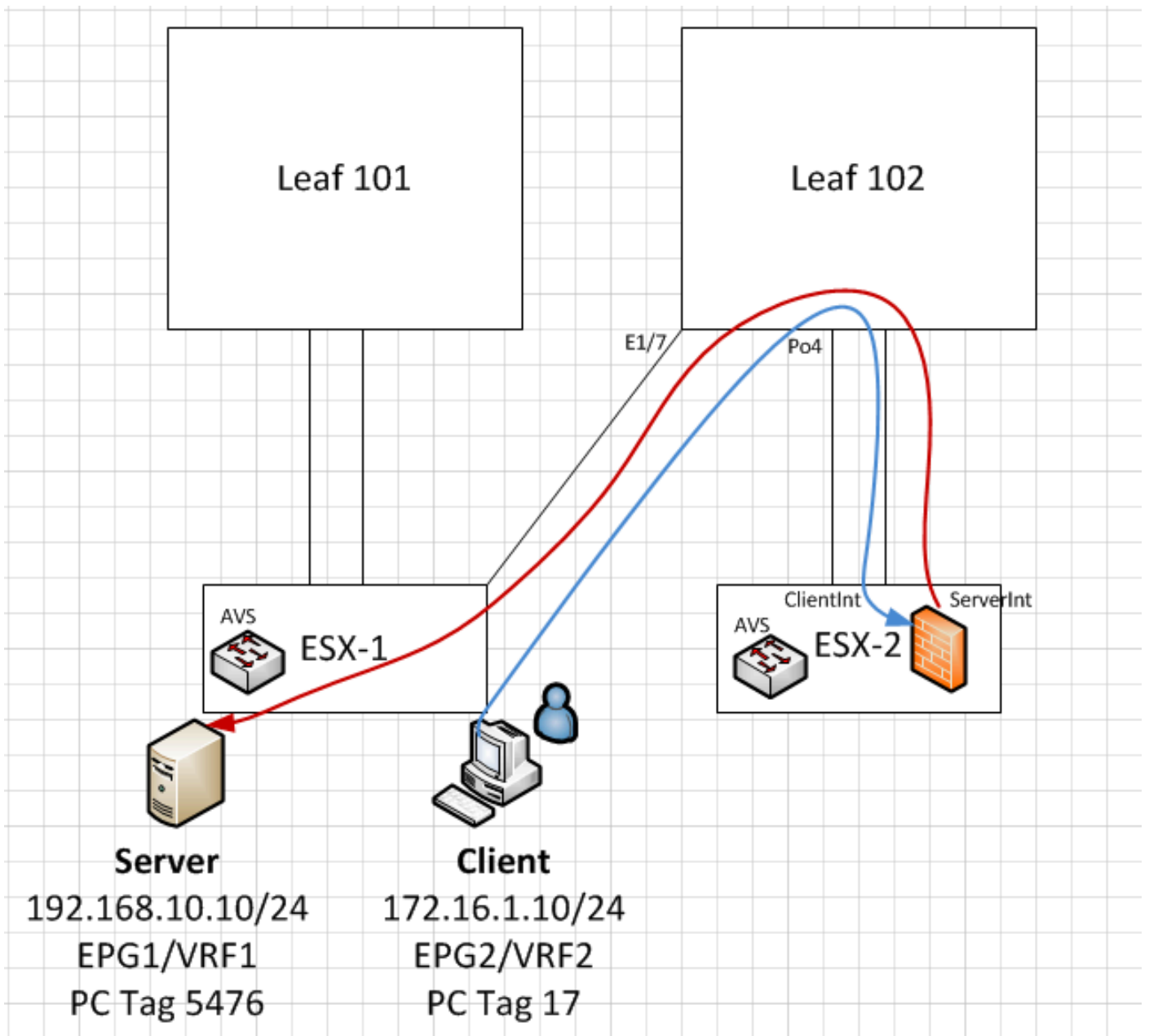
```
cisco@cisco-UbuntuClient:~$ ifconfig
eth1      Link encap:Ethernet  HWaddr 00:50:56:89:3f:ca
          inet addr:172.16.1.10  Bcast:172.16.1.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe89:3fca/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:346596 errors:0 dropped:97 overruns:0 frame:0
          TX packets:533034 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:33670388 (33.6 MB)  TX bytes:42734068 (42.7 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:170350 errors:0 dropped:0 overruns:0 frame:0
          TX packets:170350 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:18739044 (18.7 MB)  TX bytes:18739044 (18.7 MB)

cisco@cisco-UbuntuClient:~$ ssh 192.168.10.10
cisco@192.168.10.10's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

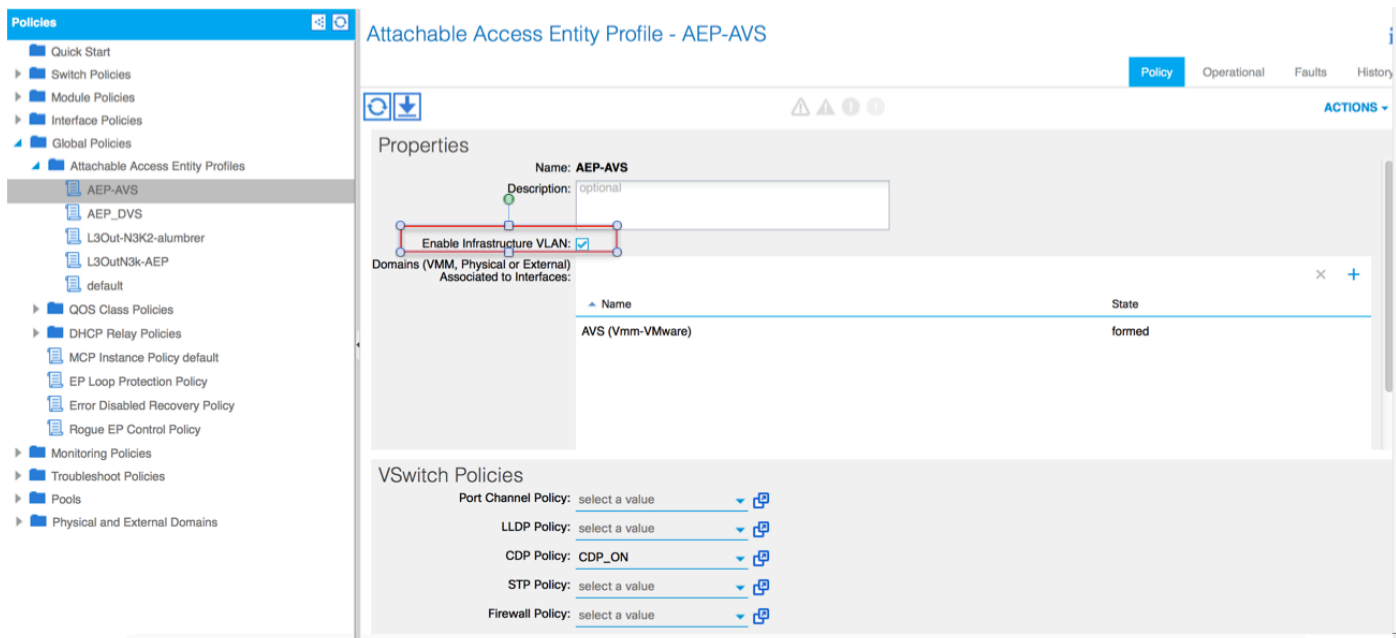
Last login: Mon Feb  1 10:14:11 2016 from 172.16.1.10
cisco@cisco-UbuntuClient:~$ $
```



## トラブルシューティング

VTEPアドレスが割り当てられていない

AEPで[Infrastructure Vlan]がチェックされていることを確認します。



## サポートされていないバージョン

VEMのバージョンが正しいことを確認し、適切なESXi VMWareシステムをサポートします。

```

~ # 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とファブリック通信が機能しない

- Check VEM status

```
vem status
```

- Try reloading or restating the VEM at the host:

```
vem reload
```

```
vem restart
```

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

```

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

```

```
--- 10.0.0.30 ping statistics ---
```

```
3 packets transmitted, 0 packets received, 100% packet loss
```

If ping fails, check:

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

```

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

```

```

Management Network IPv4 10.201.35.219 255.255.255.0 10.201.35.255 e4:aa:5d:ad:06:3e 1500 65535
true STATIC vmk0 Management Network IPv6 fe80::e6aa:5dff:fead:63e 64 e4:aa:5d:ad:06:3e 1500
65535 true STATIC, PREFERRED vmk1 160 IPv4 10.0.32.65 255.255.0.0 10.0.255.255 00:50:56:6b:ca:25
1500 65535 true STATIC vmk1 160 IPv6 fe80::250:56ff:fe6b:ca25 64 00:50:56:6b:ca:25 1500 65535
true STATIC, PREFERRED ~ # - Also on the host, verify if DHCP requests are sent back and forth:
~ # tcpdump-uw -i vmk1 tcpdump-uw: verbose output suppressed, use -v or -vv for full protocol
decode listening on vmk1, link-type EN10MB (Ethernet), capture size 96 bytes 12:46:08.818776 IP
truncated-ip - 246 bytes missing! 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request
from 00:50:56:6b:ca:25 (oui Unknown), length 300 12:46:13.002342 IP truncated-ip - 246 bytes
missing! 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 00:50:56:6b:ca:25
(oui Unknown), length 300 12:46:21.002532 IP truncated-ip - 246 bytes missing! 0.0.0.0.bootpc >
255.255.255.255.bootps: BOOTP/DHCP, Request from 00:50:56:6b:ca:25 (oui Unknown), length 300
12:46:30.002753 IP truncated-ip - 246 bytes missing! 0.0.0.0.bootpc > 255.255.255.255.bootps:
BOOTP/DHCP, Request from 00:50:56:6b:ca:25 (oui Unknown), length 300

```

この時点で、ESXiホストとリーフの間のファブリック通信が正しく動作していないと判断できます。一部の検証コマンドは、リーフ側でチェックして根本原因を特定できます。

```
leaf2# show cdp ne
```

```

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

```

Device-ID	Local Intrfce	Hldtme	Capability	Platform	Port ID
AVS:localhost.localdomainmain	Eth1/5	169	S I s	VMware ESXi	vmnic4
AVS:localhost.localdomainmain	Eth1/6	169	S I s	VMware ESXi	vmnic5
N3K-2 (FOC1938R02L)	Eth1/13	166	R S I s	N3K-C3172PQ-1	Eth1/13

```
leaf2# show port-c sum
```

```

Flags: D - Down          P - Up in port-channel (members)
       I - Individual    H - Hot-standby (LACP only)
       s - Suspended     r - Module-removed
       S - Switched      R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
       F - Configuration failed

```

```

-----
Group Port-      Type      Protocol  Member Ports
Channel
-----
5      Po5 (SU)    Eth      LACP      Eth1/5 (P)  Eth1/6 (P)

```

Po5を介して接続されたESXiで使用される2つのポートがあります

```
leaf2# show vlan extended
```

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

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

上記の出力から、インフラストラクチャVLANが許可されていないか、ESXiホスト(1/5-6)に接続するアップリンクポートを通過しないことが確認できます。これは、インターフェイスポリシーまたはスイッチポリシーがAPICで設定されている設定が誤っていることを示します。

両方をチェックします。

[Access Policies] > [Interface Policies] > [Profiles Access Policies] > [Switch Policies] > [Profiles]

この場合、図に示すように、インターフェイスプロファイルが誤ったAEP (DVSに使用される古いAEP) に接続されています。

Access Port Policy Group - AVS-102\_1-ports-7\_PolGrp

Policy | Faults | History

Properties

Name: AVS-102\_1-ports-7\_PolGrp

Description: optional

Label:

Link Level Policy: 1GigAuto

CDP Policy: CDP\_ON

MCP Policy: select a value

LLDP Policy: LLDP\_ON

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

Connectivity Filters:

Switch IDs | Interfaces

SHOW USAGE | SUBMIT | CLOSE

AVSに対して正しいAEPを設定すると、リーフの適切なアンリンクを通じてインフラストラクチャVLANが表示されます。

leaf2# show vlan extended

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

VLAN	Type	Vlan-mode	Encap
-----			

```
13 enet CE vxlan-16777209, vlan-3967
19 enet CE vxlan-14680064, vlan-150
22 enet CE vxlan-16383902
26 enet CE vxlan-15531929, vlan-200
27 enet CE vlan-11
28 enet CE vlan-14
36 enet CE vxlan-15662984
```

and Opflex connection is reestablished after restarting the VEM module:

```
~ # vem restart
stopDpa
VEM SwISCSI PID is
Warn: DPA running host/vim/vimuser/cisco/vem/vemdpa.213997
Warn: DPA running host/vim/vimuser/cisco/vem/vemdpa.213997
watchdog-vemdpa: Terminating watchdog process with PID 213974

~ # vemcmd show opflex
Status: 0 (Discovering)
Channel0: 14 (Connection attempt), Channel1: 0 (Discovering)
Dvs name: comp/prov-VMware/ctrlr-[AVS]-vCenterController/sw-dvs-129
Remote IP: 10.0.0.30 Port: 8000
Infra vlan: 3967
FTEP IP: 10.0.0.32
Switching Mode: unknown
Encap Type: unknown
NS GIPO: 0.0.0.0

~ # vemcmd show opflex
Status: 12 (Active)
Channel0: 12 (Active), Channel1: 0 (Discovering)
Dvs name: comp/prov-VMware/ctrlr-[AVS]-vCenterController/sw-dvs-129
Remote IP: 10.0.0.30 Port: 8000
Infra vlan: 3967
FTEP IP: 10.0.0.32
Switching Mode: LS
Encap Type: unknown
NS GIPO: 0.0.0.0
```

## 関連情報

アプリケーション仮想スイッチのインストール

[シスコ『Cisco Application Virtual Switch Installation Guide, Release 5.2\(1\)SV3\(1.2\)』](#)

VMwareを使用したASAの導入

[シスコ『Cisco Adaptive Security Virtual Appliance\(ASA\)クイックスタートガイド』、9.4](#)

Cisco ACIおよびCisco AVS

[シスコ『Cisco ACI Virtualization Guide, Release 1.2\(1i\)』](#)

シスコアプリケーションセントリックインフラストラクチャを使用したサービスグラフ設計ホワイトペーパー

[シスコアプリケーションセントリックインフラストラクチャを使用したサービスグラフ設計ホワイトペーパー](#)



