

ACI Guía de configuración de VMM Integration

Esta guía pretende explicar la configuración necesaria para hacer la integración de ACI con vCenter. Además de mostrar los pasos a seguir para la configuración, se explicará cómo se realiza esta integración.

Introducción.

La integración de VMM en ACI permite una gestión conjunta y automática de la infraestructura de VMWare y la Fábrica de ACI. De manera general la integración permite que los EPGs asociados a un Dominio de VMM, sean configurados automáticamente como Portgroups dentro del DVS de VMWare. Una vez que a la Máquina virtual se les asigne el portgroup del EPG, la Fábrica descubre la misma y programa la VLAN asociada al EPG (Esta asociación puede ser dinámica o manual) en los Leafs que conecten al ESXi que hospeda a la Máquina Virtual. La integración se realiza a través del vCenter, lo cual implica que las configuraciones serán aplicadas en cualquier ESXi asociado al mismo.

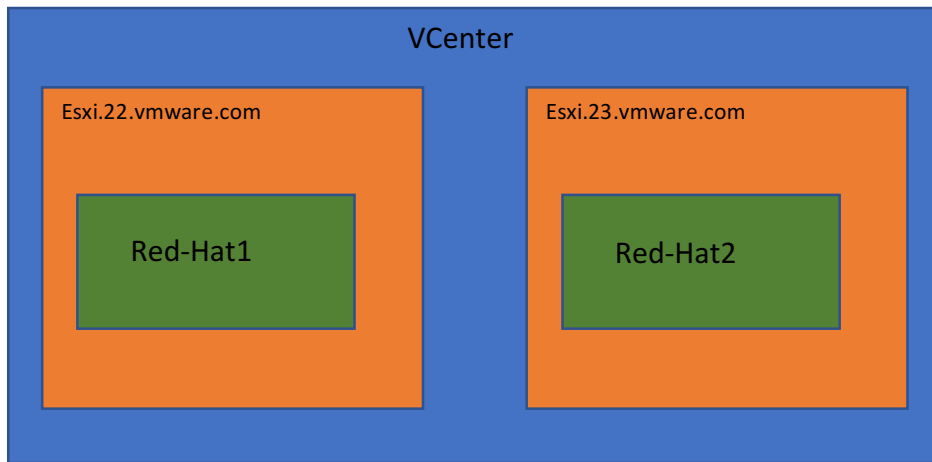
La gran diferencia entre la asociación de dominios físicos y de VMM en ACI consiste en que los dominios físicos requieren que definamos los puertos de acceso (individuales, Port-channels, vPCs) específicos que proveerán conectividad al EPG en cuestión, así como la asignación de la VLAN asociada. Por medio del dominio VMM, este proceso se automatiza, ya que la Fábrica descubre los ESXi por medio de protocolos de capa 2, como CDP o LLDP. La integración también permite a la Fábrica registrar las Máquinas virtuales asignadas a los EPGs, permitiendo conocer al ESXi que la hospeda y las vnic's asociadas.

Para tener la integración de VMM con ACI, hacemos el uso de 2 comunicaciones, Una entre el APIC y vCenter, la cual permite hacer llamadas al API de vcenter para la configuración del DVS y los portgroups y sincronizar el inventario entre ambos.

La segunda línea de comunicación se realiza entre los Leafs de la Fábrica y los Servidores ESXi que conectan a la misma. Esta comunicación es la que usa para descubrir Los diferentes ESXi, y así programar las VLANs apropiadas en los Leafs. La Fábrica utiliza el inventario obtenido en vCenter para hacer la programación.

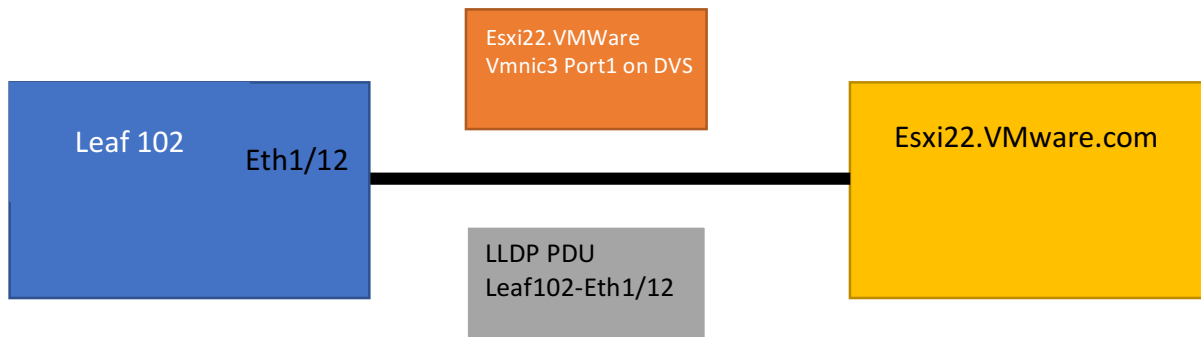
Ejemplo:

Vcenter reporta que la Máquina virtual **Red-Hat1** se encuentra hospedada en el Host **Esxi.22.vmware.com**



Ejemplo:

Mediante la información contenida en los PDUs de LLDP o CDP, La Fábrica sabrá la interfaz y el Leaf que se encuentra conectando al Uplink de ese ESXi, programando así la VLAN necesaria.



Es importante señalar que la comunicación siempre se realiza entre el APIC y el VCenter a través de sus interfaces de gestión (soporte para Inband y OOB) para las configuraciones y sincronización de inventario desde el APIC; La configuración hacia los ESXi la realiza el VCenter, no el APIC. El segundo canal de comunicación (entre los Leafs y los ESXi) no es usado para configuración de políticas, sirviendo únicamente para descubrir a los ESXi conectados a la fábrica, la configuración de las VLANs en los Leafs se realiza entre el APIC y los nodos.

La configuración requiere que ciertos pasos sean realizados por el Administrador del Apic o de Vcenter, pero de manera General la configuración se divide en dos aspectos:

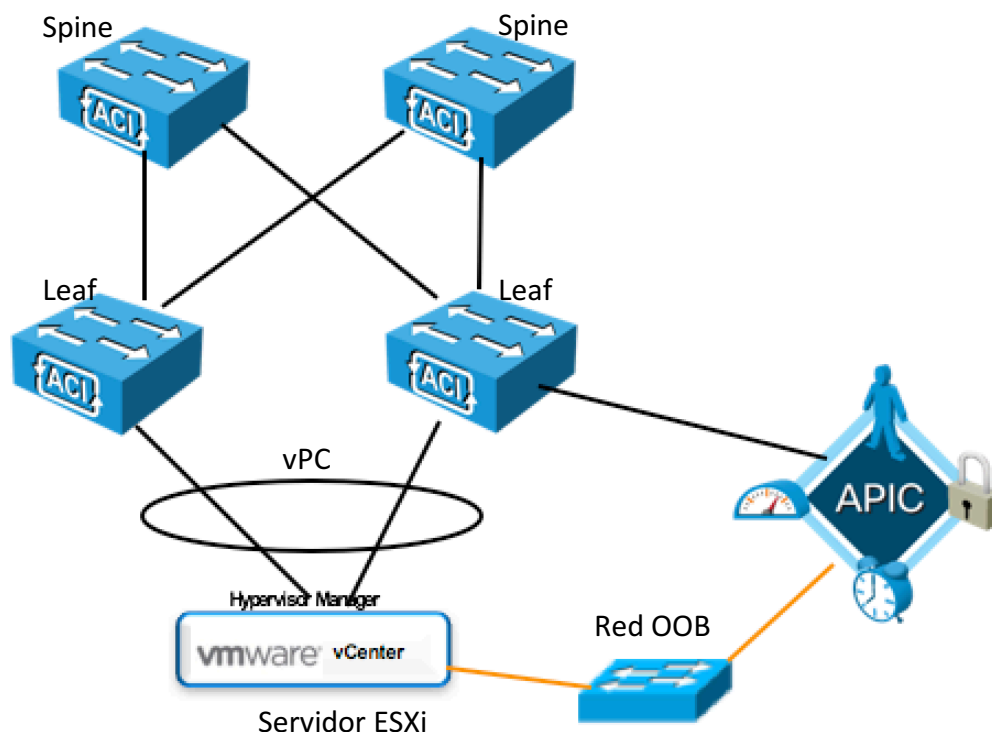
- Comunicación entre APIC y Vcenter, Gestión
- Comunicación entre Fábrica y los ESXi, Data Plane

La parte de Gestión permite la sincronización de Inventario entre el APIC y Vcenter, además de permitir la configuración del DVS y Portgroups desde el APIC. La parte de Data Plane es la que realiza el descubrimiento de los ESXi y permite que las VLANs sean programadas en los Leafs de la Fábrica.

Del lado de VMWare, la configuración necesaria incluye crear un Datacenter, añadir el/los ESXIs al DVS, definir los Uplinks del mismo en cada Host y realizar la asignación de los portgroups a las interfaces virtuales de las Máquinas Virtuales.

Configuración.

Vayamos a la configuración, la topología utilizada en este ejemplo es la siguiente:



La Fábrica de APIC se compondría de un par de Leafs en vPC, conectando a un Servidor UCS corriendo VMWare ESXi 6.0, dentro del Servidor también está operando la Máquina

Virtual de Vcenter. La comunicación de gestión entre el APIC y el Vcenter se logra a través de la red de OOB (Out-of-Band).

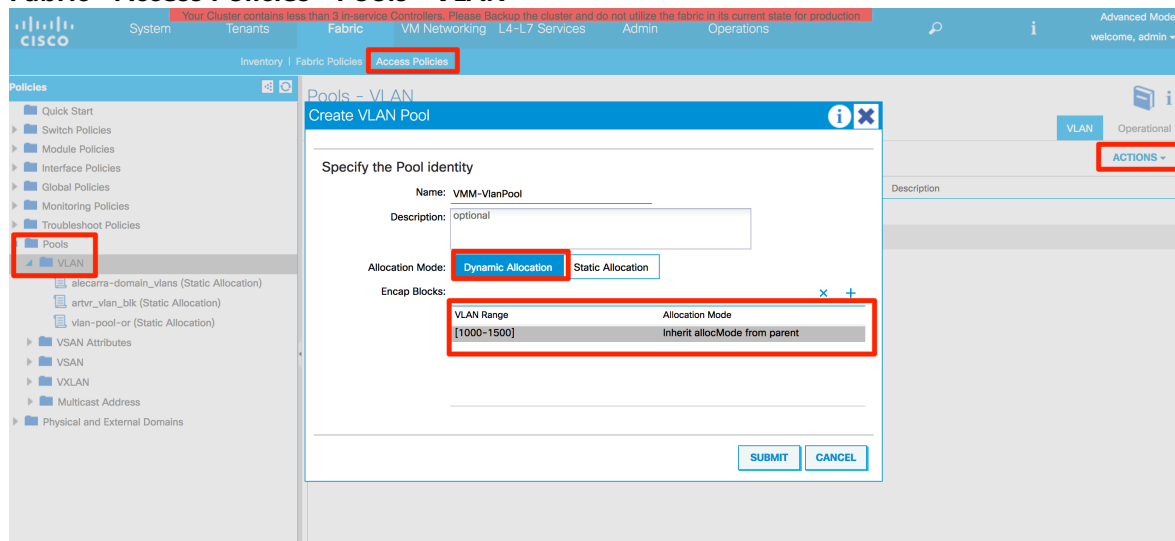
En primer lugar, realizaremos la configuración de Gestión, la cual provee la comunicación entre el APIC y el Vcenter para la configuración del DVS y la sincronización del inventario.

Definir un Vlan Pool

Este VLAN Pool indica las VLANs asignadas al DVS, las cuales son automáticamente asignadas a los EPGs (Portgroups en Vcenter) asociados al Dominio de VMM.

Para crear un VLAN Pool, tenemos que ir a:

Fabric->Access Policies->Pools->VLAN



La información necesaria es:

Name – Define El nombre del Pool

Allocation Mode – El modo de asignación, para integraciones de VMM significa si los EPGs son asignados a una VLAN de forma dinámica (Dynamic Allocation) o de manualmente (Static Allocation).

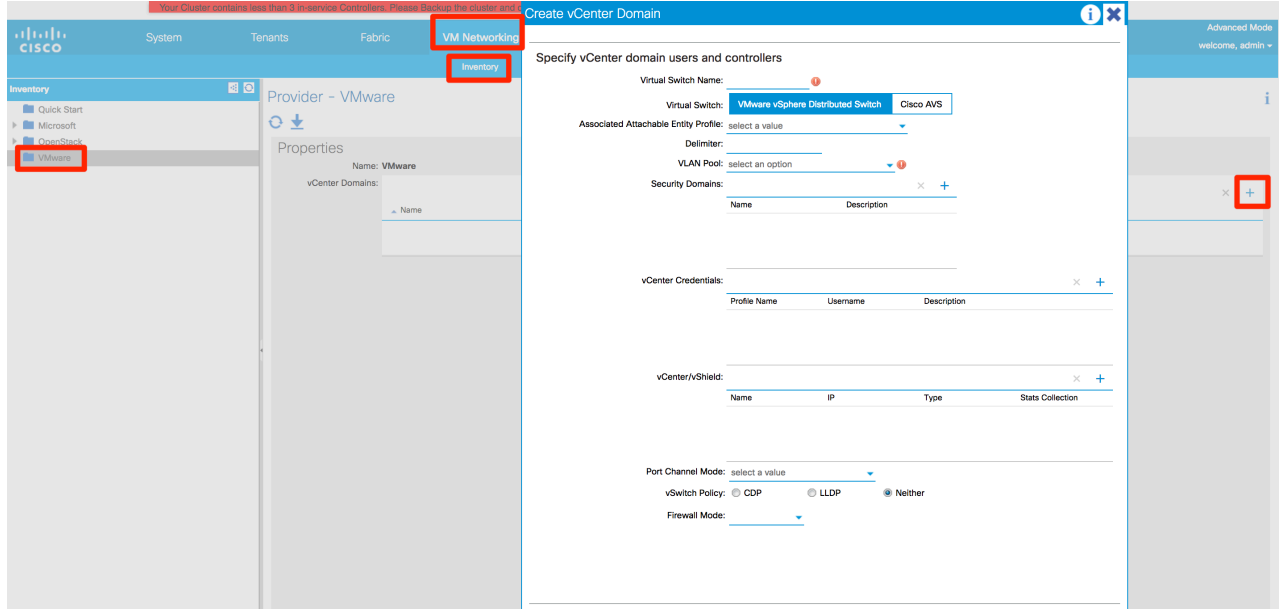
Encap Blocks – El o los bloques que contienen las VLANs de Pool, El Allocation mode puede ser heredado del Pool (Inherit allocMode from parent) o ser definido independientemente. Si el modo no es Inherit, éste tiene precedencia sobre el modo del Pool.

Crear el Dominio de Vcenter

El siguiente paso es crear el dominio de Vcenter, el cual asocia al APIC, también define los parámetros de Red del DVS a configurar.

Para crear un VMM Domain, debemos ir a:

VM Networking->Inventory->VMWare->(+)



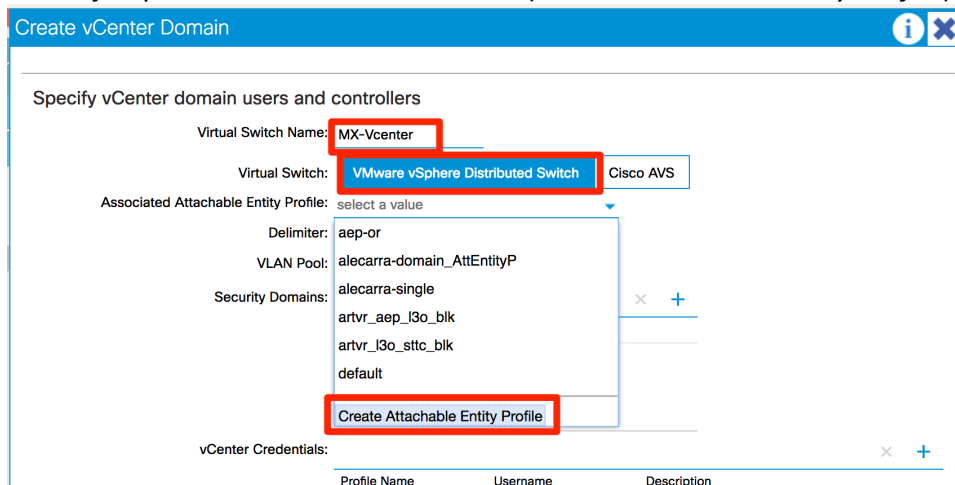
La pantalla de creación requiere la siguiente información:

Virtual Switch Name – Nombre del DVS, Con este nombre aparecerá en Vcenter.

Virtual Switch – Tipo de DVS a implementar, en nuestro Ejemplo la opción elegida es VMWare vSphere Distributed Switch la cuál configura un DVS de VMWare, la opción Cisco AVS funciona como Nexus1kV.

Associated Attachable Entity Profile(AAEP) – Esta política asocia el VLAN Pool creado, permitiendo asignar el AAEP a uno o más Policy groups (Usados para la parte de Data Plane)

En el ejemplo vamos a crear uno nuevo (*Create Attachable Entity Profile*):



La pantalla de creación del AAEP:

Create vCenter Domain

Create Attachable Access Entity Profile

STEP 1 > Profile

1. Profile 2. Association To Interfaces

Specify the name, domains and infrastructure encaps

Name: VMM-AEP

Description: optional

Enable Infrastructure VLAN:

EPG DEPLOYMENT (All Selected EPGs Will Be Deployed On All The Interfaces Associated.)

Application EPGs	Encap	Primary Encap	Mode
------------------	-------	---------------	------

La información requerida incluye:

Name – Nombre del AAEP de VMM, este nombre será el que podamos seleccionar cuando configuremos los Policy Groups.

Enable Infrastructure VLAN – Esta opción sólo es necesaria cuando se configura AVS, y VxLAN, ya que los ESXi funcionan como VTEPs a nivel de VxLAN y la VLAN de Infra es necesaria para terminar los túneles.

Una vez que tenemos creado el AAEP, falta asociar el VLAN Pool creado anteriormente.

Specify vCenter domain users and controllers

Virtual Switch Name: MX-Vcenter

Virtual Switch: VMware vSphere Distributed Switch Cisco AVS

Associated Attachable Entity Profile: VMM-AEP

Delimiter:

VLAN Pool: VMM-VlanPool(dynamic)

Security Domains:

Name	Description
------	-------------

La siguiente sección corresponde a las credenciales para autenticar el APIC con Vcenter, y también definen la localización de Vcenter (Datacenter).

Dentro de vCenter Credentials, agregamos una (+), la información requerida incluye:
Name – Nombre de la Política para referenciar.
Username – Nombre del usuario para autenticar.
Password – Contraseña asociada del usuario.

Create vCenter Credential

Specify account profile

Name: vCenterCredentials

Description: optional

Username: administrator@vsphere.local

Password:

Confirm Password:

OK CANCEL

vCenter Credentials:

Profile Name	Username	Description
--------------	----------	-------------

vCenter/vShield:

Name	IP	Type	Stats Collection
------	----	------	------------------

La siguiente parte es vCenter/vSwitch, la información requerida es:

Add vCenter/vShield Controller

Specify controller profile

Type: vCenter vCenter + vShield

vCenter Controller

Name: Mx-vCenter

Host Name (or IP Address): 10.88.247.30

DVS Version: DVS Version 6.0

Stats Collection: Disabled Enabled

Datacenter: MXC-DCPo1

Management EPG: select an option

Associated Credential: vCenterCredentials

OK CANCEL

vCenter/vShield:

Name	IP	Type	Stats Collection
------	----	------	------------------

Specify Controller Profile – Permite elegir un vCenter con módulos añadidos (vShield).

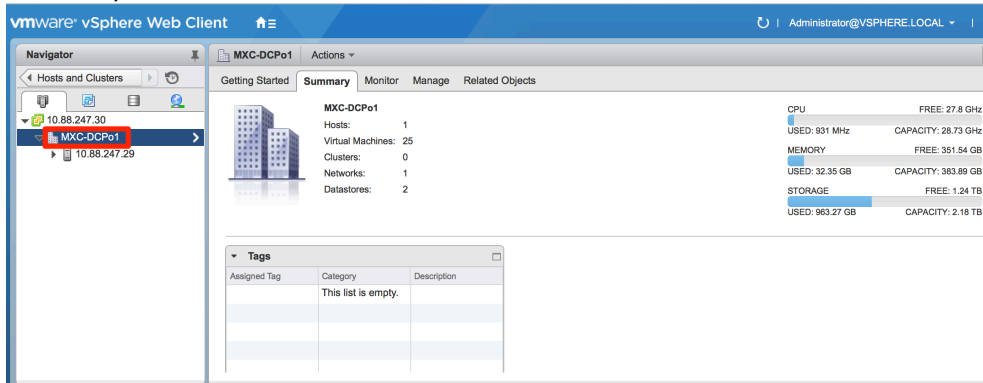
Name – Nombre de la Política, ID Local a la Fábrica.

Host name (or IP Address) – Definimos la dirección IP o FQDN del vCenter.

DVS Version – Define la version del DVS.

Stats Collection – Habilita poder obtener estadísticas de vCenter

Datacenter – Nombre del Datacenter dentro de vCenter, el nombre debe ser igual (Capital sensitive)



Management EPG – Indica la red de gestión a utilizar para comunicar vCenter y el APIC, las opciones incluyen Inband y Out-of-band. En caso de sólo tener configurado el OOB, no es necesario elegir alguna opción.

Associated Credential – Permite referenciar la política de credenciales creada anteriormente.

La siguiente parte define las características del Switch Virtual a configurarse en Vcenter. La información necesaria incluye:

Port Channel Mode:

vSwitch Policy: Static Channel - Mode On Neither

Firewall Mode:

Port Channel Mode – Esta opción define el tipo de modo a correr en el Port-channel, pudiendo elegir entre LACP activo o pasivo, y otros métodos de balanceo.

Port Channel Mode: select a value ▼

vSwitch Policy: CDP LLDP Neither

Firewall Mode: _____ ▼

vSwitch Policy – Define el protocolo de descubrimiento a utilizar, el cual es utilizado en el Dataplane. Las opciones son CDP, LLDP, o Ninguno. La opción a utilizar depende del soporte del Servidor (CDP es un protocolo propietario, no todo el Hardware lo soportará).

La política completa quedaría de la siguiente forma:

Create vCenter Domain
[i](#) [X](#)

Specify vCenter domain users and controllers

Virtual Switch Name: MX-Vcenter _____

Virtual Switch: VMware vSphere Distributed Switch Cisco AVS

Associated Attachable Entity Profile: VMM-AEP ▼ [+](#)

Delimiter: _____

VLAN Pool: VMM-VlanPool(dynamic) ▼ [+](#)

Security Domains: _____ × +

Name	Description

vCenter Credentials: _____ × +

Profile Name	Username	Description
vCenterCredentials	administrator@vsph...	

vCenter/vShield: _____ × +

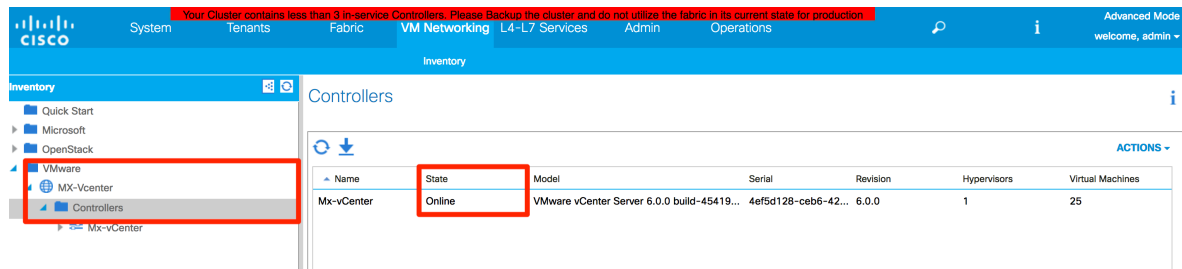
Name	IP	Type	Stats Collection
Mx-vCenter	10.88.247.30	vCenter	Disabled

Port Channel Mode: LACP Active ▼

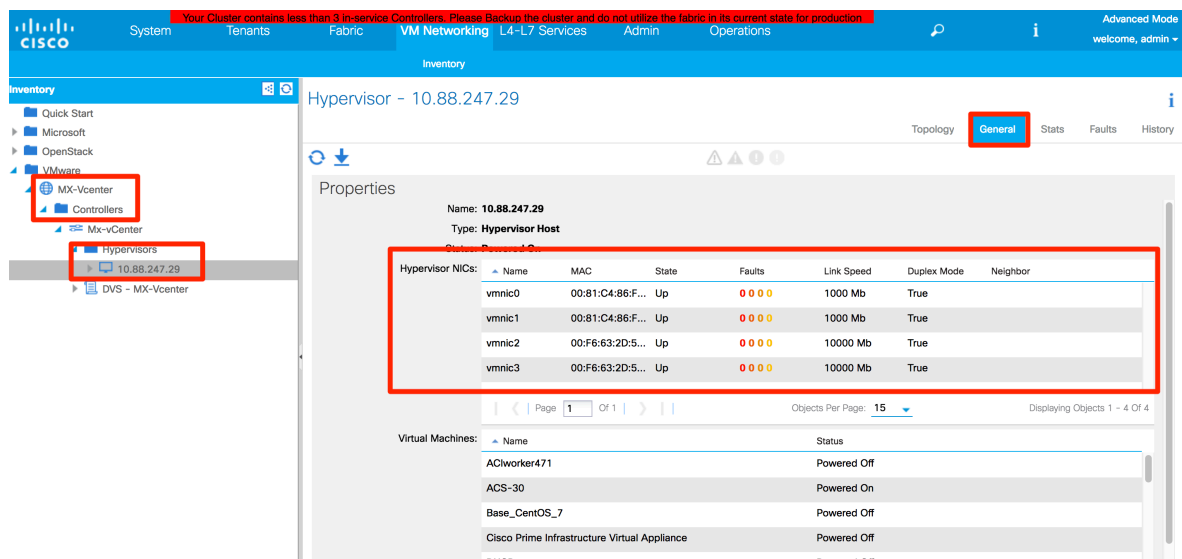
vSwitch Policy: CDP LLDP Neither

Firewall Mode: _____ ▼

Una vez que hayamos confirmado (submit) la política, podemos revisar el estado del Controlador de Vcenter bajo **VM Networking ->Inventory -> VMWare -> VMM Policy-> Controllers**, el cual debe aparecer como 'Online', de esta forma podemos confirmar que la comunicación APIC-Vcenter es correcta.



Expandiendo sobre el vCenter llegamos a la opción de los Hypervisores, eligiendo la vista General podemos ver el detalle de la información del Servidor, como las vmnics, y las Máquinas virtuales hospedadas en él mismo.



Crear y asignar las Políticas de Acceso para los Servidores ESXi.

La siguiente parte de la configuración comprende la comunicación de Data plane entre los Leafs y los Servidores ESXi. Estas son las políticas que permiten descubrir a los servidores en la Fábrica y poder programar las VLANs asociadas al Dominio VMM. La topología requiere configurar un dominio de vPC para conectar al Servidor ESXi en modo Dual-homed. La forma en que el o los Servidores se conectan a la Fábrica moldearán la configuración de los Uplinks del DVS, en términos generales tenemos Switch Dependent (SD) y Switch Independent (SI). El primero, SD, requiere configuración adicional en el DVS para coincidir con la configuración de la Red, por ejemplo, en un vPC la configuración de los Uplinks requerirá métodos de balanceo que soporten que el tráfico pueda esperarse en cualquier puerto. Por otro lado, el método SI no requiere conocer las características de la red, y requiere configuraciones en el DVS mas deterministas. Para conocer a detalle

cada método y los casos que aplica cada uno nos podemos referir a esta presentación de Cisco Live:

https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=6115

Configurar AAEP:

El Attachable Entity Profile es la política que funge como puente entre las configuraciones de Acceso a la Fábrica y la configuración del Tenant (EPG), nos permite configurar uno o más dominios (Físicos o Virtuales) a un rango de puertos específicos. En primer lugar, debemos crear un AAEP (**Fabric->Access Policies->Global Policies->Attachable Entity Profile**) y asignar el Dominio de VMM que se creó durante la configuración de VMM (No aparecerá listado junto con los dominios físicos, pero puede ser elegido para asociarlo a los AAEPs).

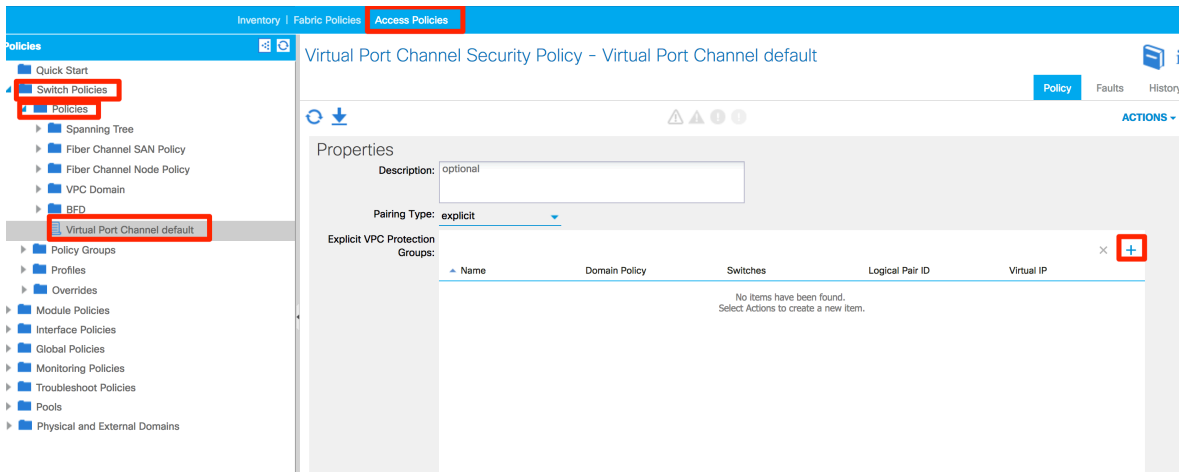
The screenshot displays the Cisco Fabric Manager interface for configuring an Attachable Access Entity Profile (VMM-AEP). The navigation tree on the left shows the path: Global Policies > Attachable Access Entity Profiles > VMM-AEP. The main configuration area shows the following details:

- Name: VMM-AEP
- Description: optional
- Enable Infrastructure VLAN:
- Domains (VMM, Physical or external) Associated to Interfaces:

Name	State
MX-Vcenter (Vmm-Vmware)	formed

Configurar el dominio de vPC.

El siguiente paso es configurar el dominio de vPC eligiendo el par de Switches que conectarán al Servidor. Esta política define los Switches en la Fábrica que actuarán como vPC peers. El Id del Dominio y los Switches deben ser únicos a través de toda la Fábrica. Para crear un dominio de vPC debemos ir a **Fabric->Access Policies->Switch Policies->Policies->Virtual Port Channel default** y crear un nuevo *Explicit VPC Protection Group*.



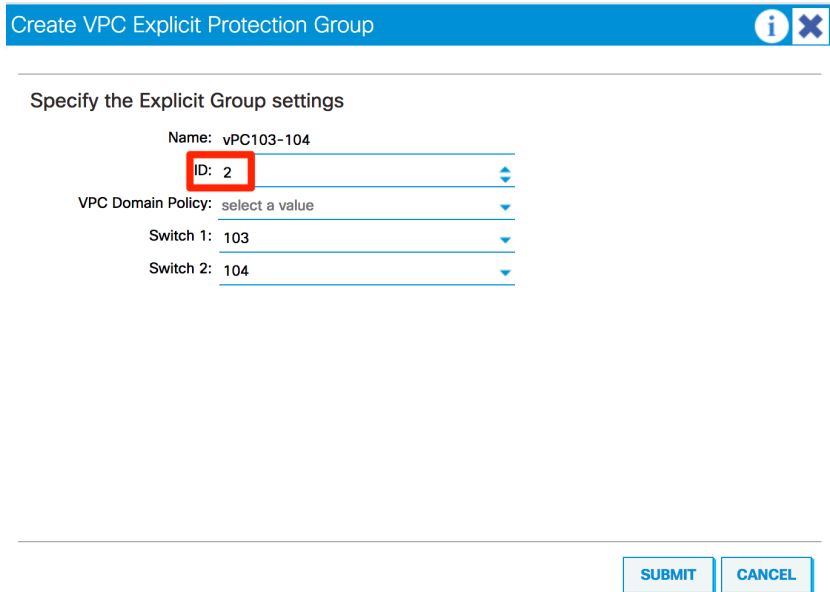
La información requerida para crear un nuevo Grupo incluye:

Name –Nombre del Grupo

ID – Este ID será usado para identificar al dominio de VPC que será configurado en los Switches.

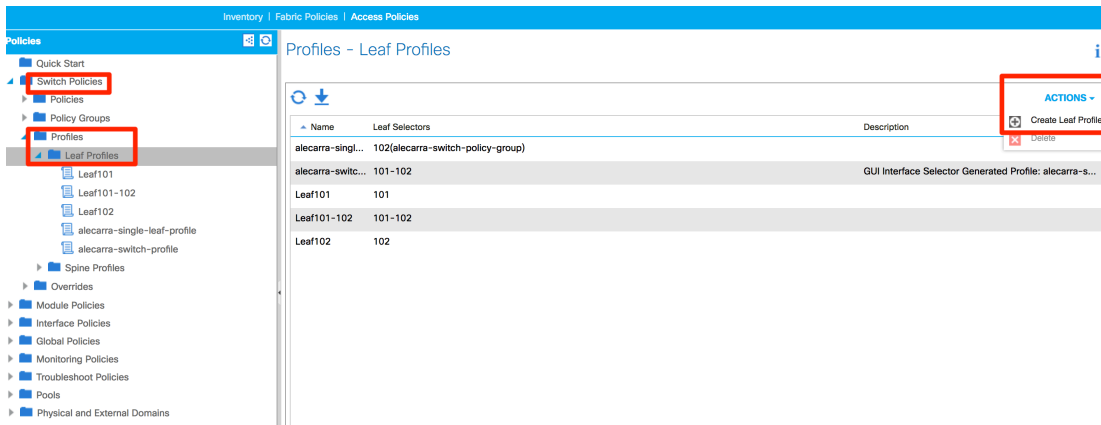
VPC Domain Policy – Permite personalizar parametros del dominio de VPC.

Switch 1, 2 – Despliega una lista para elegir al par de nodos que integrarán al dominio.



El siguiente paso será crear un Profile de Switch. Este objeto por un lado asocia a uno o más nodos de la Fábrica dentro de un bloque de Switches. Por el otro lado permite asociar uno o más Interface Profiles (Objeto que define un rango de puertos y su configuración), para ser aplicados a todos los Switches dentro del bloque. Ya que las Best Practices para uso de vPc dictan usar los mismos puertos en ambos pares, tener un Switch profile asociado a ambos VPC peers facilitará la configuración, ya que podemos configurar ambos Switches con el Profile común.

Los Switch profiles se encuentran en **Fabric->Access Policies->Switch Policies->Profiles->Leaf Profiles**, seleccionamos *Create Leaf Profile* para configurar un nuevo Profile.



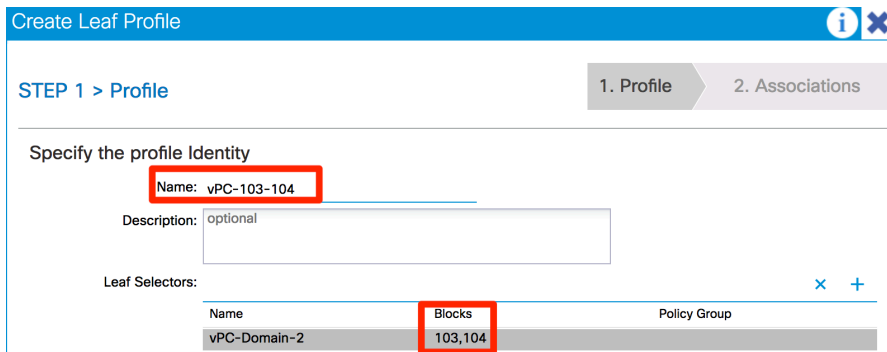
Para configurar un nuevo Switch Profile requerimos la siguiente información:

Name – Nombre del Profile.

Leaf Selectors – Añadimos un Selector al seleccionar el signo ‘+’

Name – Nombre del Leaf Selector

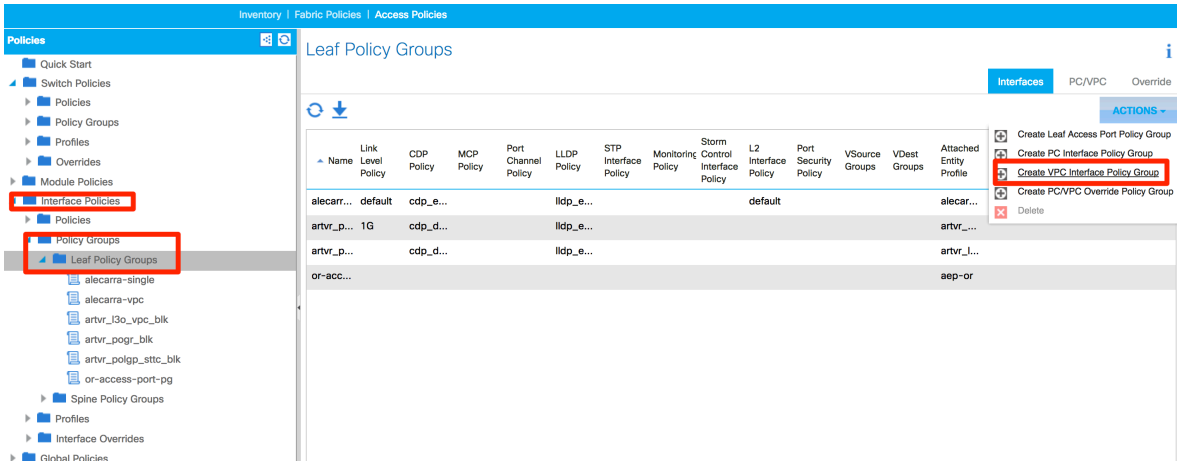
Blocks – Nos permite seleccionar uno o más Leafs de la Fábrica, en este caso elegimos los 2 Switches del vPC Domain.



Configurar el Interface Policy Group (VPC)

El siguiente paso es configurar el Policy group que usarán los puertos que conectarán al Servidor en el VPC. Un Policy Group es un objeto que agrupa una serie de Políticas comunes, para que puedan ser aplicadas como un todo, a uno o más puertos de Acceso en la Fábrica. Existen Policy groups de Access Port, Port-channel o VPC, dependiendo del tipo de conexión a realizar; En este caso configuraremos un Policy Group de VPC.

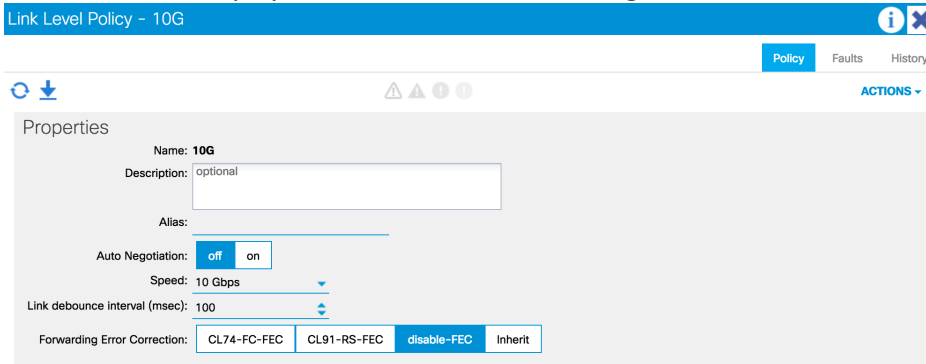
Los Policy Groups se encuentran en ***Fabric->Access Policies->Interface Policies->Policy Groups->Leaf Policy Groups***



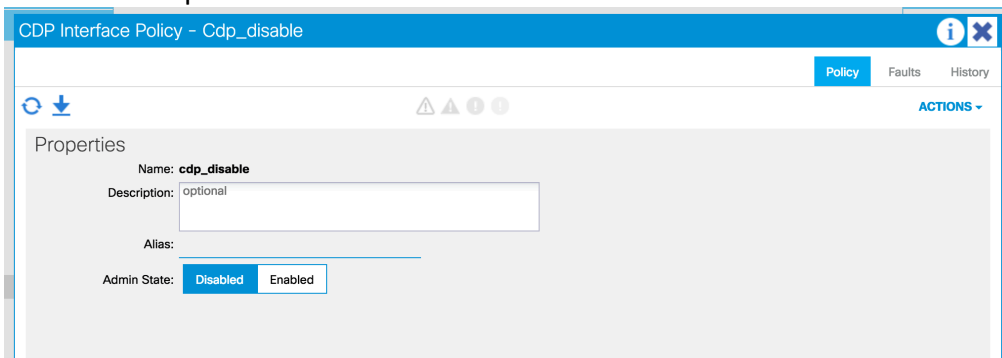
Como se mencionó, el Policy Group permite agrupar un conjunto de Políticas que serán aplicadas como un todo, dentro del Policy group debemos configurar los distintos parámetros de interfaz que serán aplicados, dentro de la información requerida se incluye:

Name – Nombre del Policy Group, Para casos de Port-channel o VPC, debemos crear un Policy Group por cada Port-channel o VPC que se quiera configurar.

Link Level – Configura la Velocidad y Duplex del puerto. En este caso elegimos Duplex full, Velocidad de 10Gps y deshabilitamos la auto negociación.



CPD Policy – Define la configuración de CDP en el Puerto (Habilitar o deshabilitar), en las políticas de VMM elegimos LLDP como el protocolo a usar, por lo cual la política asociada deshabilita el protocolo.



LLDP Policy – Configura el comportamiento de LLDP, ya que éste será el protocolo a utilizar, la política lo habilita.

The screenshot shows the configuration page for an LLDP Interface Policy named 'lldp_enable'. The page has a blue header with the title 'LLDP Interface Policy - Lldp_enable' and a close button. Below the header, there are tabs for 'Policy', 'Faults', and 'History'. The main content area is titled 'Properties' and contains the following fields:

- Name:** lldp_enable
- Description:** optional
- Alias:** (empty text field)
- Receive State:** Disabled (radio button), Enabled (radio button)
- Transmit State:** Disabled (radio button), Enabled (radio button)

Port channel Policy – Esta política sólo está disponible cuando el Policy group representa a un Port-channel o VPC. Define el comportamiento a nivel de Etherchannel, nos permite elegir un protocolo para el mismo, como LACP, así como el comportamiento en caso de failover, número mínimo y máximo de enlaces, etc. En este caso elegimos LACP como el protocolo a utilizar, los demás parámetros los dejamos con su valor default.

The screenshot shows the configuration page for a Port Channel Policy named 'lACP-Active'. The page has a blue header with the title 'Port Channel Policy - LACP-Active' and a close button. Below the header, there are tabs for 'Policy', 'Faults', and 'History'. The main content area is titled 'Properties' and contains the following fields:

- Name:** lACP-active
- Description:** optional
- Alias:** (empty text field)
- Mode:** LACP Active (dropdown menu)
- Control:**
 - Fast Select Hot Standby Ports
 - Graceful Convergence
 - Load Defer Member Ports
 - Suspend Individual Port
- Minimum Number of Links:** 1 (with up/down arrows and a note: 'Not Applicable for FEX PC/VPC')
- Maximum Number of Links:** 16 (with up/down arrows and a note: 'Not Applicable for FEX PC/VPC')

At the bottom of the configuration area, there are two buttons: 'CHECK ALL' and 'UNCHECK ALL'. At the very bottom of the page, there are three buttons: 'SHOW USAGE', 'SUBMIT', and 'CLOSE'.

Attachable Entity Profile – Asocia el AAEP que integra el Dominio VMM, permite programar las VLANs dentro de los Leafs.

Una vez creadas las diversas políticas y asociando el AAEP, el Policy group queda de la siguiente manera:

Create VPC Interface Policy Group i X

Specify the Policy Group identity

Name: vPC-ESXi
Description: optional

Link Level Policy: 10G 🔗
CDP Policy: cdp_disable 🔗
MCP Policy: select a value ▼
LLDP Policy: lldp_enable 🔗
STP Interface Policy: select a value ▼
L2 Interface Policy: select a value ▼
Port Security Policy: select a value ▼
Egress Data Plane Policing Policy: select a value ▼
Ingress Data Plane Policing Policy: select a value ▼
Priority Flow Control Policy: select a value ▼
Fiber Channel Interface Policy: select a value ▼
Slow Drain Policy: select a value ▼
Port Channel Policy: lacp-active 🔗
Attached Entity Profile: VMM-AEP 🔗

Connectivity Filters: × +

Switch IDs	Interfaces
------------	------------

El Policy group configurado establece un VPC de 10Gps en full dúplex, quita la auto negociación, habilita LLDP y remueve CDP, utiliza LACP para establecer el etherchannel y permite configurar las VLANs dentro del Dominio de VMM.

Configurar el Interface Profile

El siguiente paso es aplicar el Policy Group a los puertos de acceso. Esto se logra mediante un Interface Profile, un objeto que asocia un grupo de uno o más puertos a un Polcy group. Los Interface Profiles se encuentran en Fabric->Access Policies->Interface Policies->Profiles->Leaf Profiles.

Inventory | Fabric Policies | **Access Policies**

Policies

- Quick Start
- Switch Policies
 - Policies
 - Policy Groups
 - Profiles
 - Overrides
- Module Policies
- Interface Policies**
 - Policies
 - Policy Groups
 - Profiles
 - Leaf Profiles**
 - alecarras-single
 - alecarras-vpc
 - artvr_ip_13o_bik
 - artvr_ip_sttc_bik
 - int-profile2-or

Leaf Selector Profiles

Name	Interface Selectors	Description
type: Interfaces		
alecarras-single	1/9	
alecarras-vpc	1/1	
artvr_ip_13o_bik	1/3	
artvr_ip_sttc_bik	1/1	
int-profile2-or	1/16, 1/5	

ACTIONS

- Create Leaf Interface Profile**
- Create FEX Profile
- Delete

Al crear un nuevo Profile (**Create Leaf Interface Profile**) requerimos ingresar la siguiente información:

Name – Nombre del Interface Profile

Interface Selectors – Permite configurar varios bloques de puertos, cada uno asignado a un Policy Group.

Create Leaf Interface Profile



Specify the profile Identity

Name: vPC-ESXi

Description: optional

Interface Selectors:



Name	Type
------	------

Name – Nombre del Port Selector

Interface IDs – Elige el número de puerto o puertos, los esquemas válidos se describen debajo.

Connected to FEX – Identifica si los puertos elegidos son parte de un FEX.

Interface Policy groups – Asocia el Policy Group al o los puertos dentro del Bloque.

Create Access Port Selector



Specify the selector identity

Name: Port17

Description: optional

Interface IDs: 1/17

valid values: All or Ranges. For Example:
1/13,1/15 or 2/22-2/24, 2/16-3/16

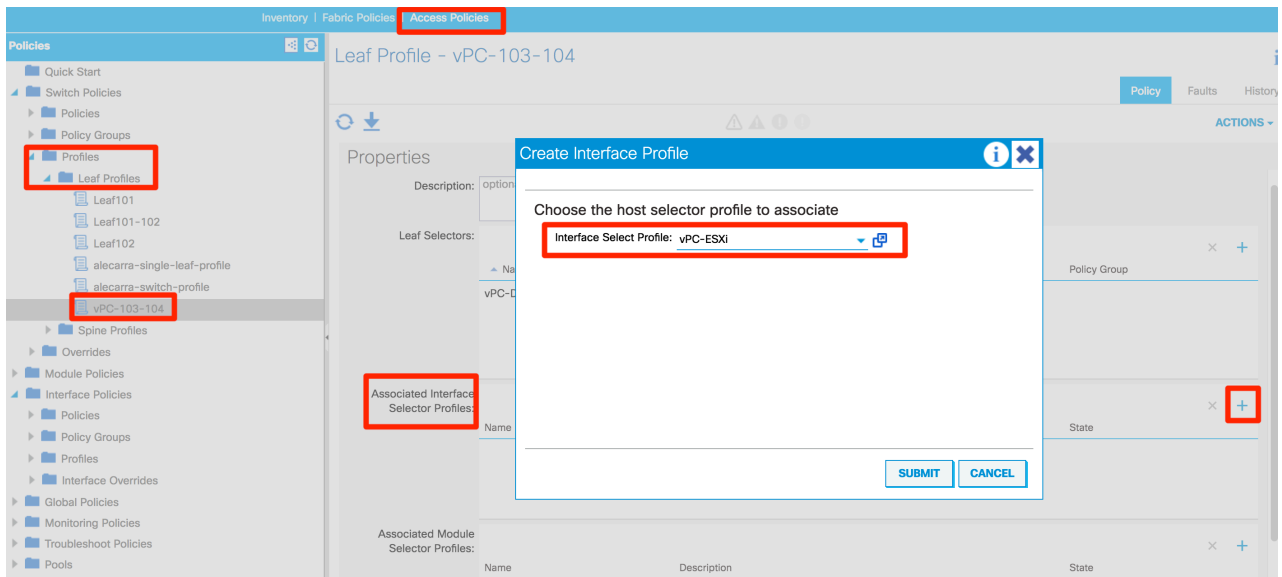
Connected To Fex:

Interface Policy Group: vPC-ESXi

Asignar el Interface Profile al Switch Profile

El último paso de configuración de Acceso es asociar el Interface Profile al Switch Profile, esta configuración asigna la configuración de las interfaces seleccionadas en el Interface Profile a los Switches dentro del Switch Profile. Este caso el Interface Profile tiene la interfaz 1/17, y el Switch Profile tiene los Nodos 103 y 104. Así que estamos aplicando el Policy Group de vPC al puerto Eth1/17 en los Switches 103 y 104.

Para hacer esto basta con Elegir el Switch Profile (**Fabric->Access Policies->Switch Policies->Profiles->Leaf Profiles**) y agregar el Interface Profile. (+ Sobre Associated Interface Selector Profiles)



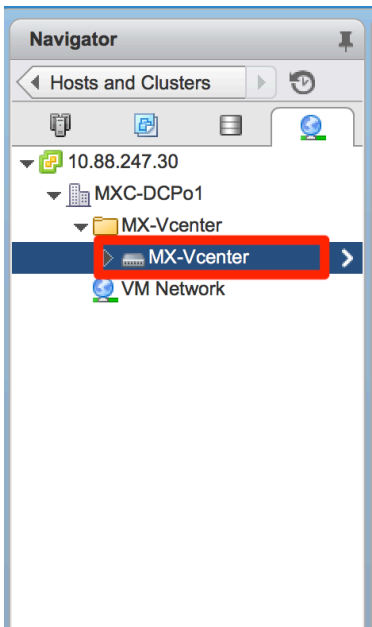
Cabe mencionar que ninguna VLAN será programada en este punto en el Switch, la configuración únicamente permite que las VLANs dentro del Pool definido puedan ser asignadas a los puertos asignados al Policy Group. Las VLANs serán programadas bajo 2 criterios, que sean asignadas a algún EPG por medio del Dominio VMM y que la Fábrica reciba tráfico de la VLAN desde el puerto asignado.

En este punto la configuración de ACI está completa. Los siguientes pasos se realizan del lado de VMWare, en específico en el VCenter.

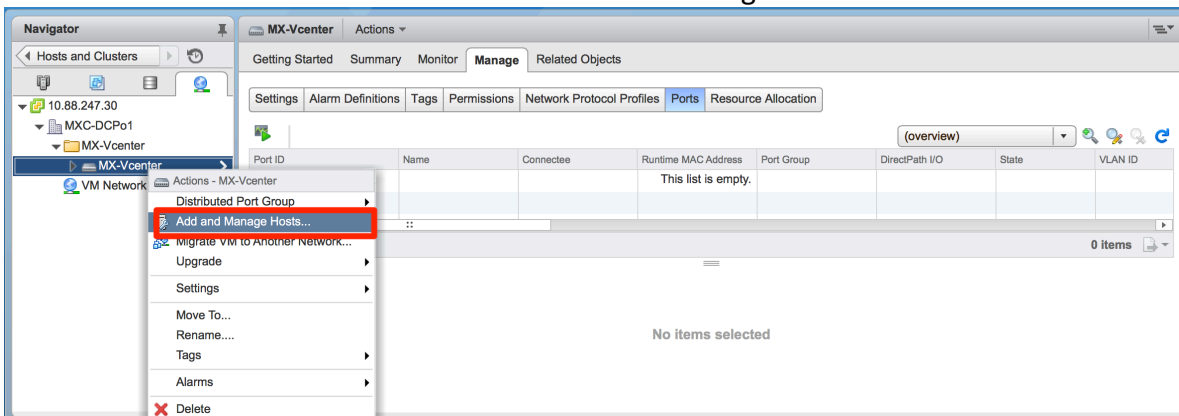
Agregar los Servidores ESXi al DVS creado y configurar los Uplinks del mismo.

El siguiente paso es agregar el o los Servidores ESXi al DVS creado por ACI, posteriormente debemos asignar los Uplinks en cada uno de los Servidores agregados. El acceso de los Servidores se configuró dentro de las Políticas de Acceso a la Fábrica.

Para esto debemos entrar al VCenter. En la vista de Networking expandimos el Datacenter, y la Carpeta creada por el APIC; veremos entonces al DVS creado:



Con el clic derecho debemos seleccionar “Add and Manage Hosts...”



Seleccionamos "Add Hosts" y hacemos clic en Next:

Add and Manage Hosts

1 Select task

Select a task to perform on this distributed switch.

- Add hosts**
Add new hosts to this distributed switch.
- Manage host networking**
Manage networking of hosts attached to this distributed switch.
- Remove hosts**
Remove hosts from this distributed switch.
- Add host and manage host networking (advanced)**
Add new hosts and manage networking of hosts already attached to this distributed switch. Use this option to unify the network configuration of new and existing hosts.

Dentro de la Lista de Servidores, seleccionamos al o los Servidores para agregar y hacemos clic en Next:

Add and Manage Hosts

2 Select hosts

Select hosts to add to this distributed switch.

+ New hosts... | X Remove

Host	Host Status
(New) 10.88.247.29	Connected

Dentro de las tareas a realizar debemos seleccionar Manage Physical Adapters, y hacer Clic en Next:

Add and Manage Hosts

3 Select network adapter tasks

Select the network adapter tasks to perform.

- Manage physical adapters**
Add physical network adapters to the distributed switch, assign them to uplinks, or remove existing ones.
- Manage VMkernel adapters**
Add or migrate VMkernel network adapters to this distributed switch, assign them to distributed port groups, configure VMkernel adapter settings, or remove existing ones.
- Migrate virtual machine networking**
Migrate VM network adapters by assigning them to distributed port groups on the distributed switch.
- Manage advanced host settings**
Set the number of ports per legacy host proxy switch.

Sample distributed switch

Manage VMkernel adapters

VMkernel port group

VMkernel ports

vmk

Uplink port group

Uplink

vnic

Manage physical adapters

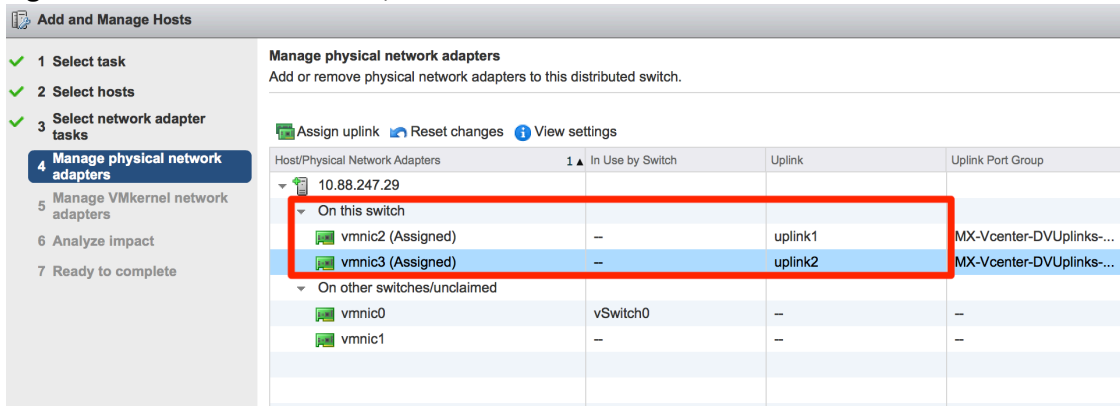
VM port group

Virtual Machines

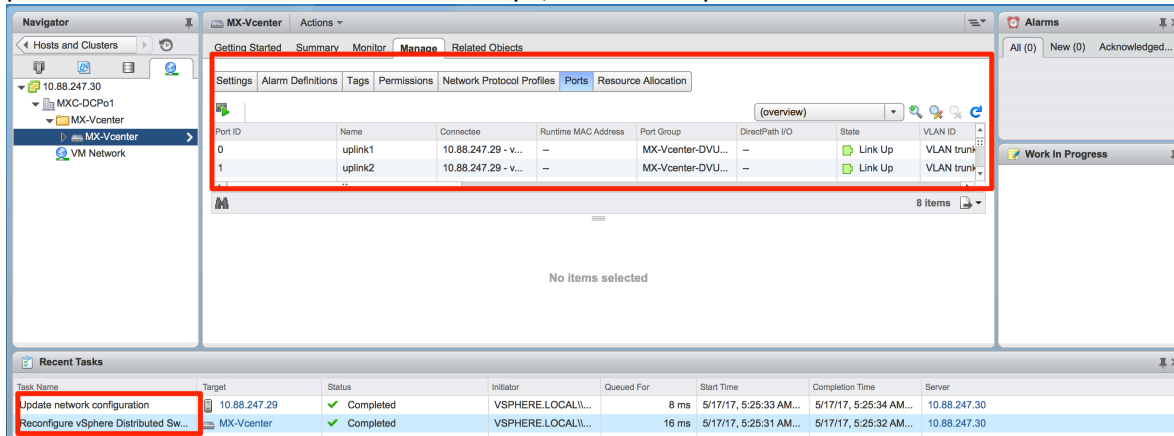
vm

Una vez en la tarea de "Manage physical network adapters" seleccionamos los adaptadores físicos que fungirán como Uplinks, en este caso, El servidor ESXi se conecta a

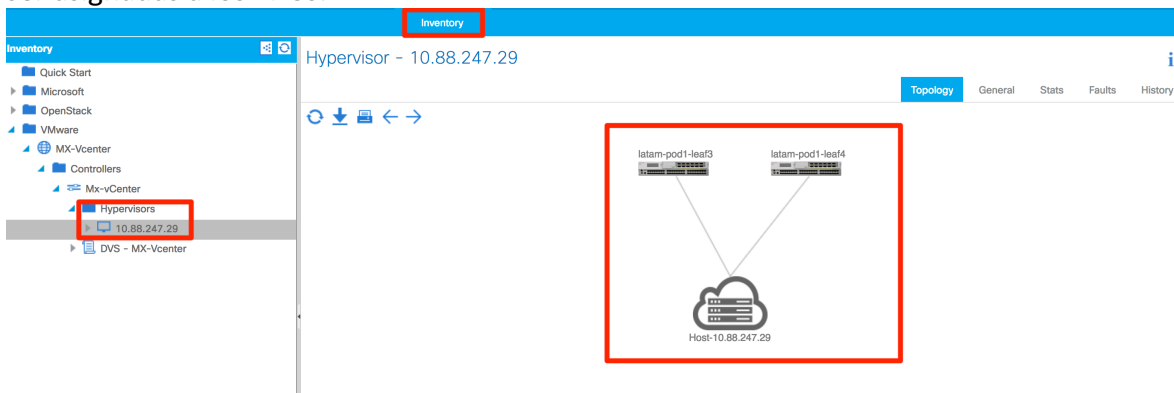
un VPC, así que asignamos los vmnic2 y vmnic3 como Uplinks del DVS, dejamos las siguientes tareas como están, hasta alcanzar “Finish”:



Una vez que completamos la configuración podemos ver los Uplinks dentro del Switch, los puertos deben mostrarse como “Link up”, indicando que el enlace se encuentra activo:



Si revisamos el Inventario de la integración VMM en ACI, expandiendo el Vcenter y seleccionando al Servidor, podremos ver la forma en que conecta a la Fábrica. En este punto la Fábrica conoce que el servidor se encuentra conectado a ella por medio del protocolo de Descubrimiento definido (LLDP o CDP), las VLANs se encuentran listas para ser asignadas a los EPGs:



Ejemplo de configuración de EPGs con VMM:

La configuración referente a la Integración está completa. La siguiente parte es crear los EPGs y asignar las Máquinas virtuales a los Portgroups generados de éstos en Vcenter. Ya que los Endpoints serán aprendidos por las interfaces ya asignadas para conectar a los ESXi, y como la Fábrica descubre dinámicamente donde se conecta cada ESXi, Basta con agregar el Dominio VMM creado al EPG para activar la creación del Portgroup y programar a los Leafs para que esperen tráfico en el EPG.

En el ejemplo a utilizar vamos a configurar un par de EPGs bajo un mismo Bridge Domain y VRF. Posterior a esto vamos a realizar diferentes configuraciones para mostrar el comportamiento de la Fábrica.

Creamos un Tenant con una VRF y creamos un Bridge Domain (BD). Dentro del BD configuramos una Subnet, 192.168.1.1/24, en este caso configuraremos a la Fábrica como el Gateway del EPG.

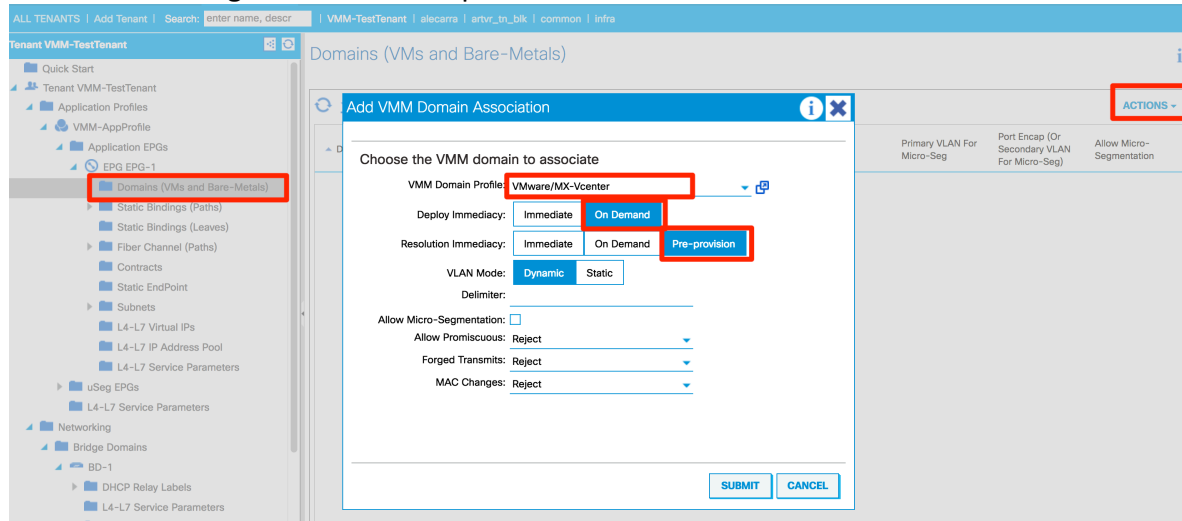
The screenshot shows the configuration for Bridge Domain - BD-1. The 'Subnets' table is highlighted with a red box:

Gateway Address	Scope	Primary IP Address	Virtual IP	Subnet Control
192.168.1.1/24	Private to VRF	False	False	

Creamos un Application Profile y dentro de él un EPG. Al EPG lo asociamos al BD antes creado.

The screenshot shows the configuration for EPG - EPG-1. The 'Bridge Domain' field is highlighted with a red box, showing 'VMM-TestTenant/BD-1'.

Dentro del EPG elegimos Domains y dentro de *Actions* elegimos “Add VMM Domain Association” la siguiente ventana aparece:



La información requerida para añadir el Dominio VMM incluye:

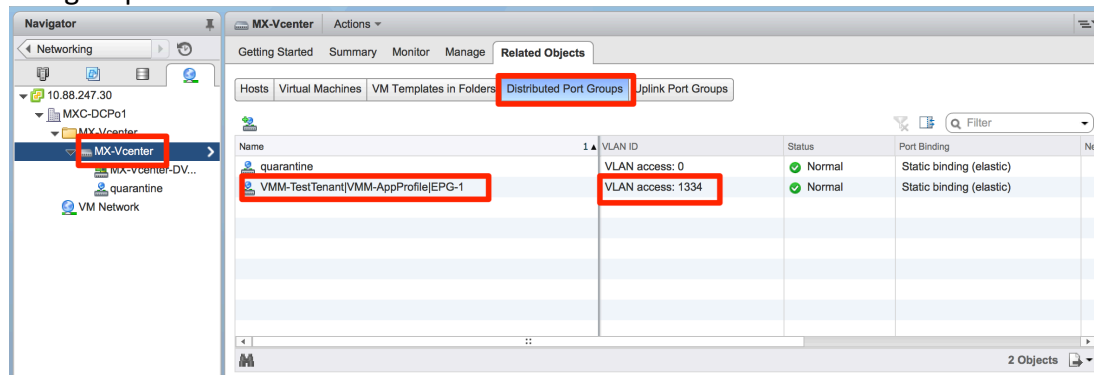
VMM Domain Profile – Define el Dominio VMM a utilizar. En este caso el dominio que creamos, MX-Vcenter.

Deploy immediacy – Define el comportamiento de la Fábrica una vez que las políticas son descargadas del Apic al Leaf. Tenemos las opciones **Immediate**, la cual programa las políticas en Hardware en cuanto son descargadas, y **On Demand**(default) la cual programa las políticas hasta que la fábrica recibe el primer paquete, ayudando a optimizar el espacio en Hardware. Para el ejemplo seleccionamos *On Demand*.

Resolution immediacy – Especifica si las políticas referentes a Contratos y Filtros se aplican de manera inmediata (**Immediate**), cuando se tenga un Hypervisor conectado y generando tráfico (**On Demand**) o si las políticas son configuradas en el Switch antes de tener el Hypervisor conectado, pre-provisionando la configuración (**Pre-provision**). En este caso elegimos *Pre-provision*.

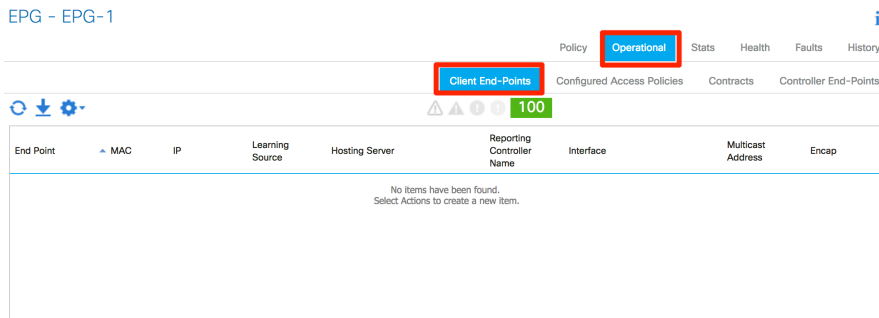
VLAN Mode – Nos permite elegir la Vlan asignada para el EPG (**Static**) manualmente dentro del Pool, o dejar que la asignación sea Dinámica dentro del mismo (**Dynamic**), para el ejemplo elegiremos *Dynamic*.

Una vez que hagamos *Submit* del dominio, podremos ver que el DVS tiene un nuevo Portgroup.



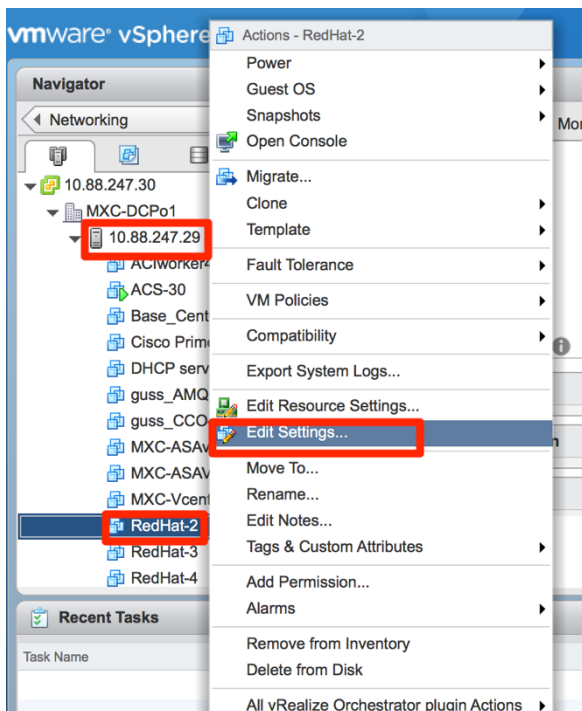
Como observamos, el nombre del *Portgroup* se genera conjuntando el Nombre del *Tenant*, del *Application Profile* y del *EPG*, en la información del *Portgroup* vemos la VLAN que fue asignada por el Apic (1334).

El *Portgroup* no está asignado a ninguna Máquina Virtual, por lo cual de momento no tenemos ningún *Endpoint* dentro del mismo (vista *Operational*):

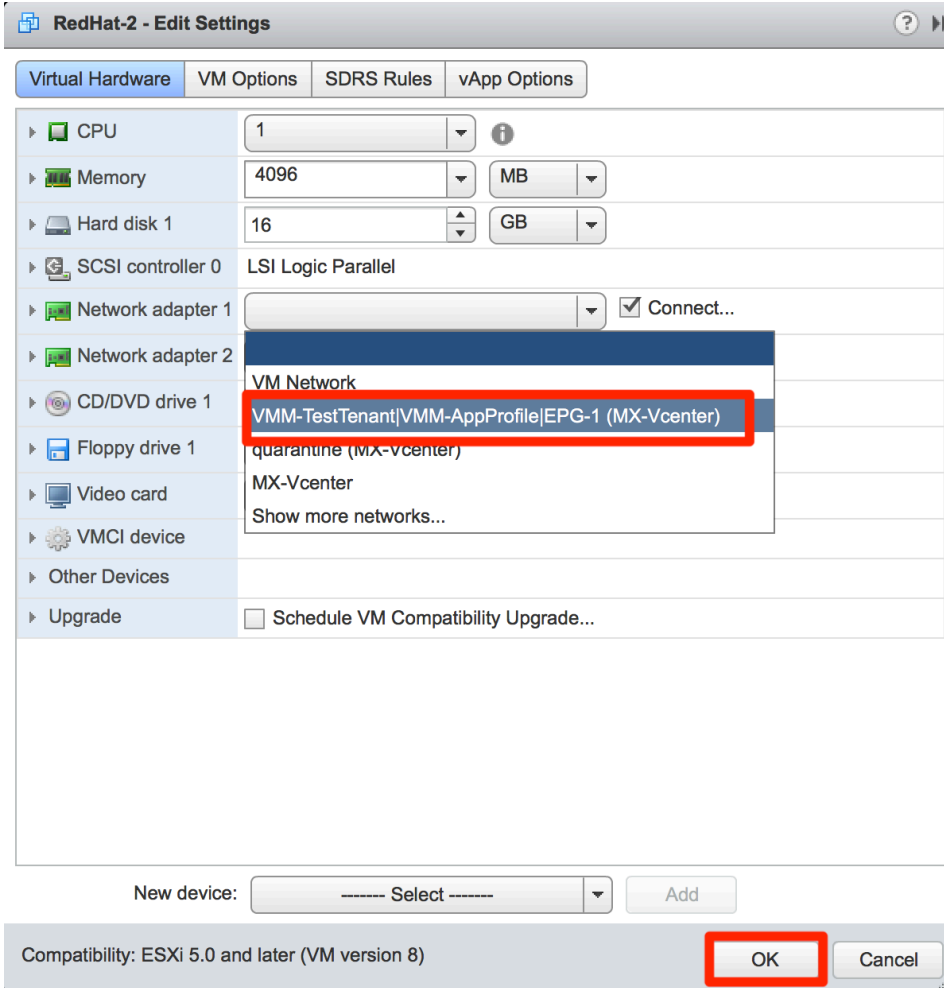


Asignar vnics de Máquinas Virtuales a los *Portgroups*.

Como siguiente paso vamos a tomar una Máquina Virtual en Vcenter y procederemos a asignarle el *Portgroup* del *EPG* a alguna de sus interfaces Virtuales. En la vista de *Hosts and Clusters* expandimos el *Host* en cuestión y elegimos la Máquina virtual, en este caso la llamada *RedHat-2*, damos clic derecho y elegimos *Edit Settings...*



Dentro de las opciones elegimos alguno de los Network Adapters y expandimos la selección, elegimos el Portgroup creado para el EPG-1, hacemos clic en Ok para confirmar:



Una vez que aplicamos los cambios, podremos ver la Máquina virtual en la vista *Operational* del EPG. Cabe destacar que el *Learning Source* será **vmm**, esto indica que el Endpoint fue aprendido mediante la sincronización de inventarios entre el Apic y Vcenter.

EPG - EPG-1

Policy **Operational** Stats Health Faults History

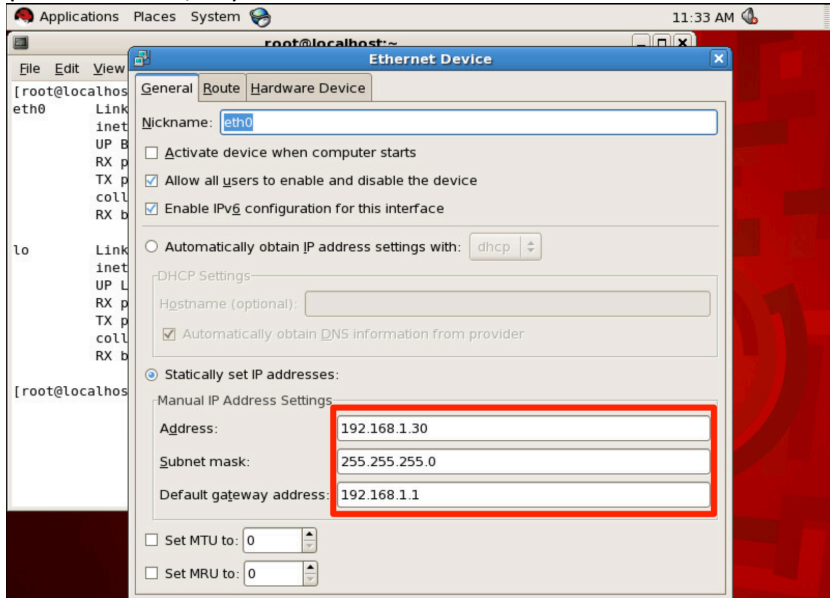
Client End-Points Configured Access Policies Contracts Controller End-Points

100

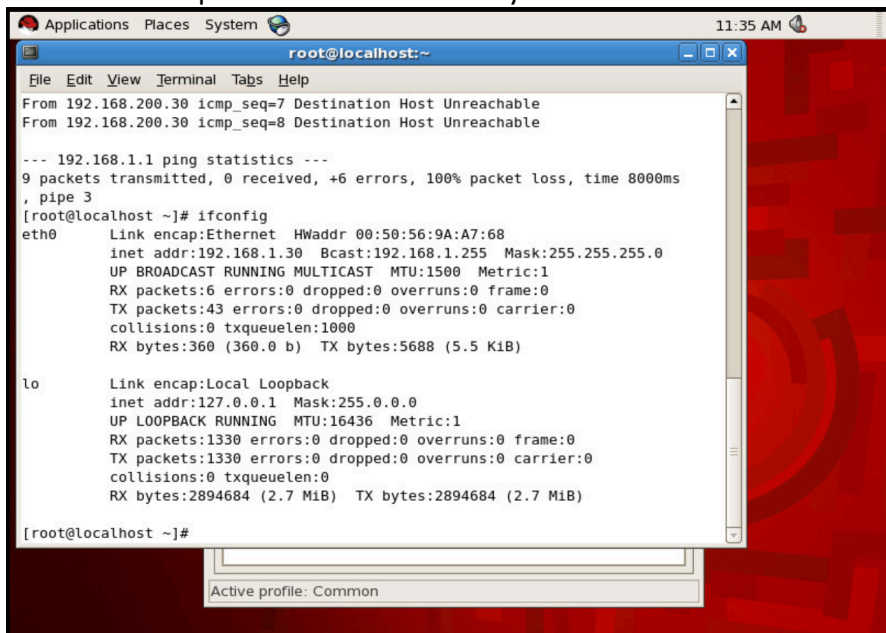
End Point	MAC	IP	Learning Source	Hosting Server	Reporting Controller Name	Interface	Multicast Address	Encap
RedHat-2	00:50:56:9A:...	---	vmm	10.88.247.29	Mx-vCenter	Pod-1/Node-103-104/vPC-E...	---	vlan-1334

Probar conectividad de la Máquina Virtual

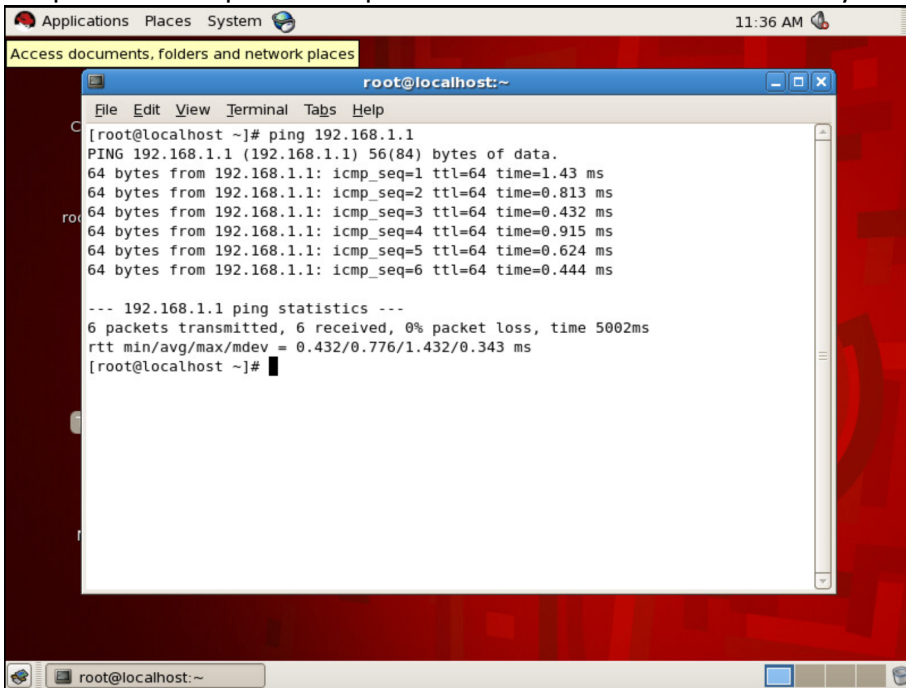
Como siguiente paso vamos a configurar la Máquina virtual, definiendo la información IP. Mediante una consola a la Máquina virtual elegimos las opciones de Red y modificamos la información de Direccionamiento IP, colocando una IP del segmento definido en el BD (192.1268.1.1/24):



Confirmamos que la información se haya actualizado:



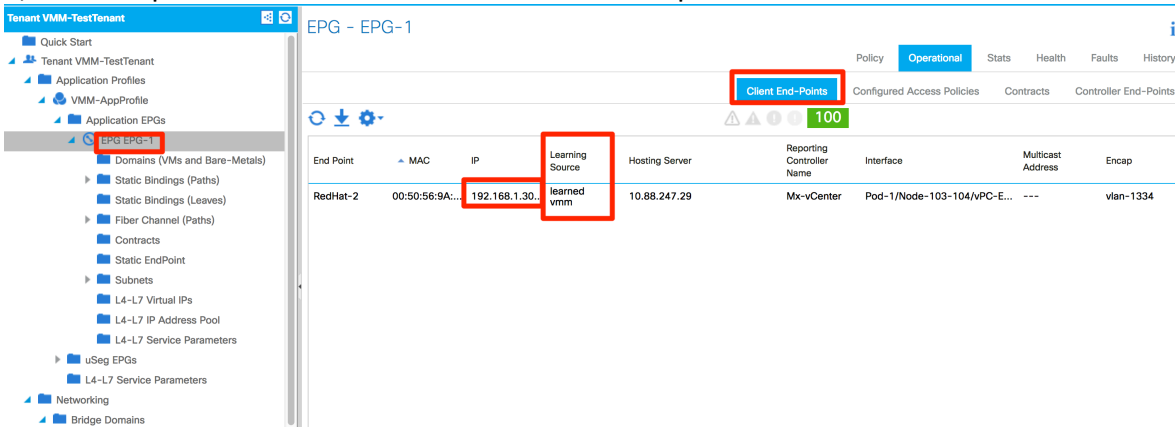
Después de esto podremos probar conectividad hacia el Gateway:



```
root@localhost:~# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data:
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=1.43 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.813 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.432 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.915 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=0.624 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=0.444 ms

--- 192.168.1.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5002ms
rtt min/avg/max/mdev = 0.432/0.776/1.432/0.343 ms
root@localhost ~]#
```

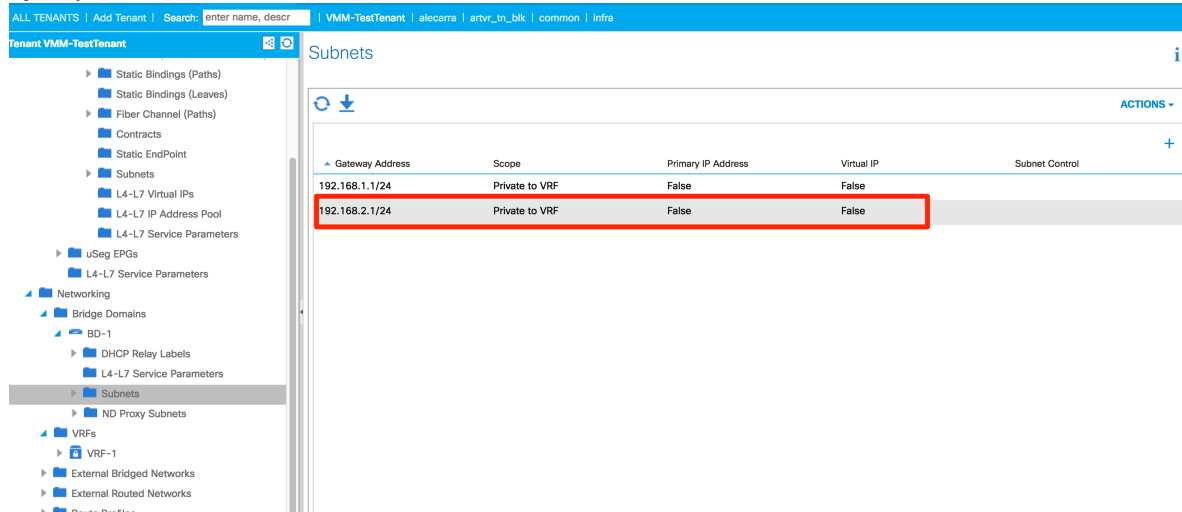
Una vez que la Fábrica haya recibido tráfico desde la Máquina virtual, la vista *Operational* del EPF mostrara un segundo valor debajo de *Learning Source*, **learned**. Este valor indica que la Máquina virtual ha generado tráfico en la fábrica. Ya que el BD tiene activado Capa 3, también podemos ver la información IP de la Máquina virtual:



End Point	MAC	IP	Learning Source	Hosting Server	Reporting Controller Name	Interface	Multicast Address	Encap
RedHat-2	00:50:56:9A:...	192.168.1.30	learned vmm	10.88.247.29	Mx-vCenter	Pod-1/Node-103-104/vPC-E...	---	vlan-1334

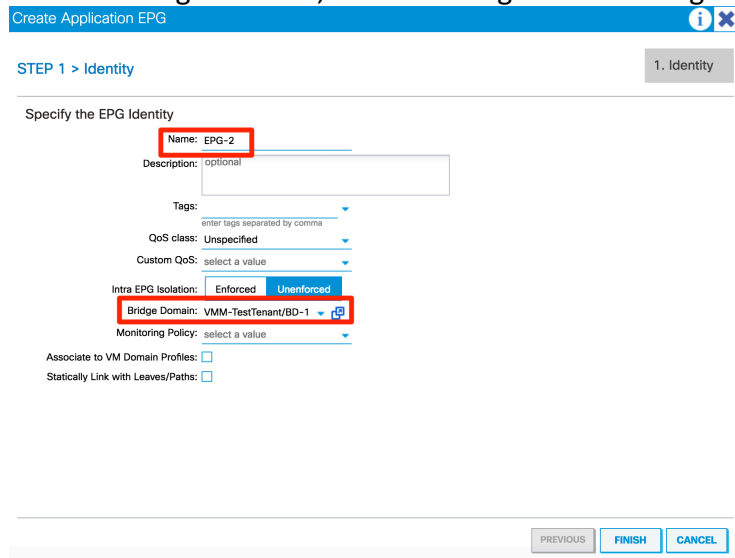
Configuración de un segundo EPG.

La siguiente prueba será configurar un segundo EPG asociado al Dominio VMM creado. En primera instancia vamos a configurar una segunda Subnet para fungir como Gateway para el segundo EPG. La subred a utilizar será 192.168.2.1/24, en escenarios diferentes la nueva subred puede ser configurada dentro de un segundo BD, o como en nuestro ejemplo dentro del mismo BD. En este caso, ambos EPGs serán asociados al mismo BD.



Gateway Address	Scope	Primary IP Address	Virtual IP	Subnet Control
192.168.1.1/24	Private to VRF	False	False	
192.168.2.1/24	Private to VRF	False	False	

Al crear el segundo EPG, EPG-2 los asignamos al Bridge Domain ya configurado.



STEP 1 > Identity

Specify the EPG Identity

Name: EPG-2

Description: optional

Tags: enter tags separated by comma

QoS class: Unspecified

Custom QoS: select a value

Intra EPG Isolation: Enforced Unenforced

Bridge Domain: VMM-TestTenant/BD-1

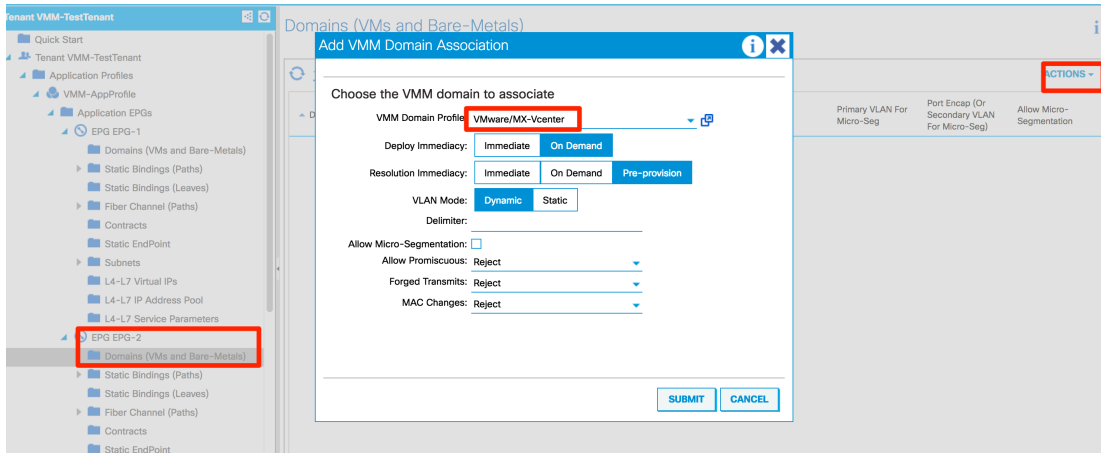
Monitoring Policy: select a value

Associate to VM Domain Profiles:

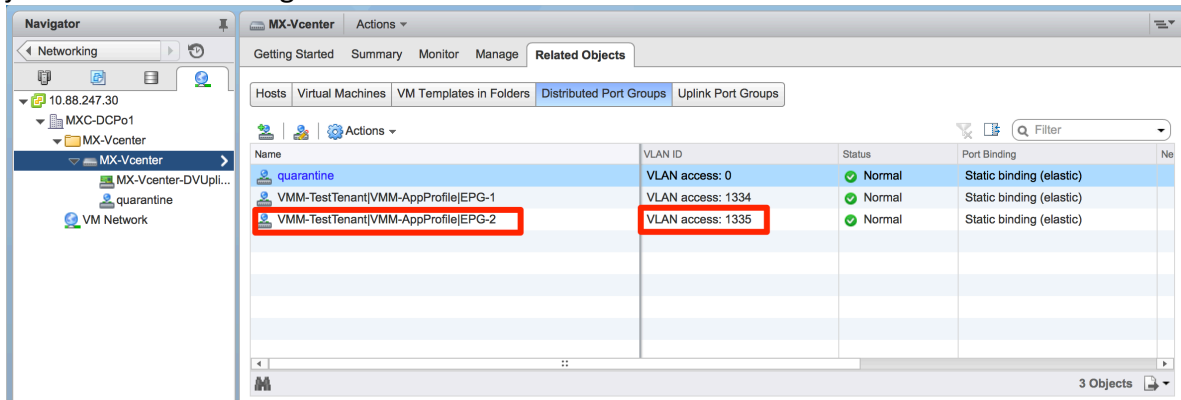
Statically Link with Leaves/Paths:

PREVIOUS FINISH CANCEL

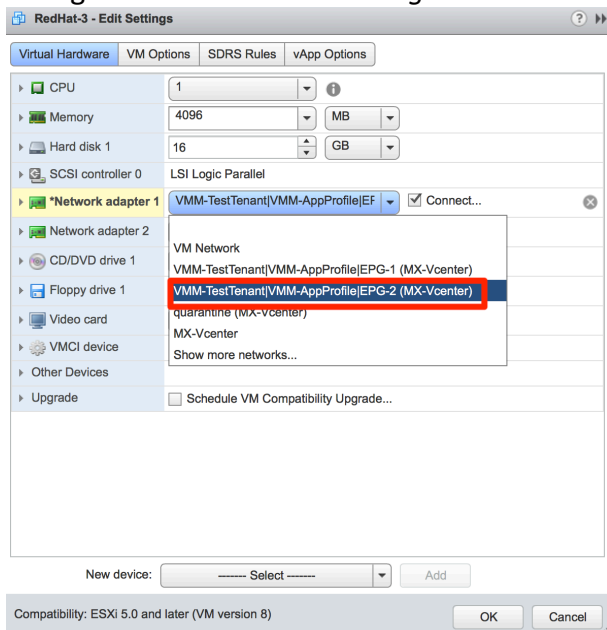
Para el segundo EPG repetiremos el paso de asignar el Dominio VMM, eligiendo opciones igual para el modo de *Resolution* y *Deploy*.



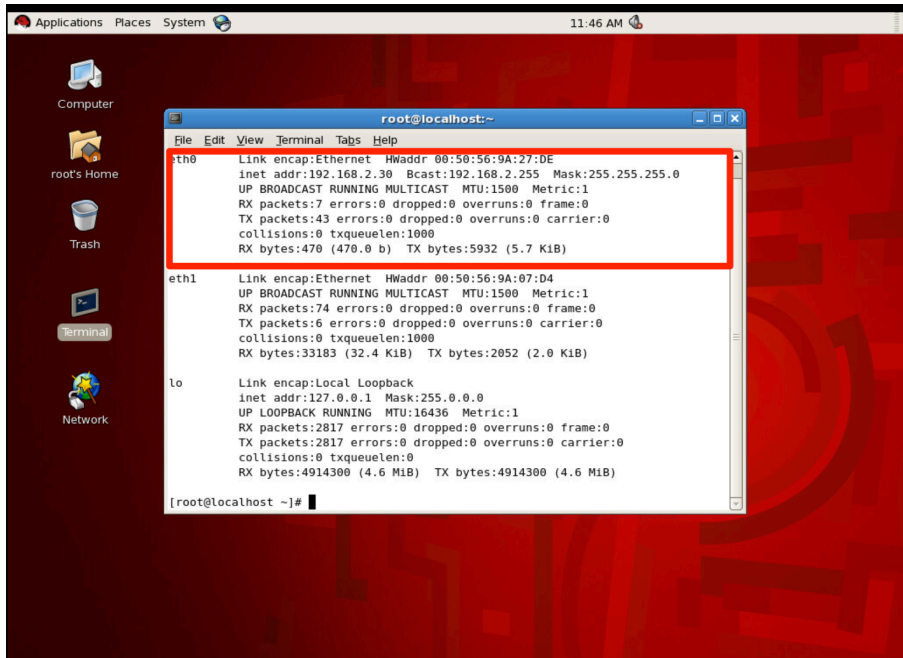
Al tener el Dominio VMM asociado al EPG, un segundo Portgroup aparecerá en el DVS, junto con la VLAN asignada:



Utilizaremos la Máquina Virtual llamada RedHat-3 para ser asignada al Portgroup. Los pasos son los mismos; Eligiendo con clic derecho a la Máquina virtual accedemos a la configuración desde *Edit Settings...*

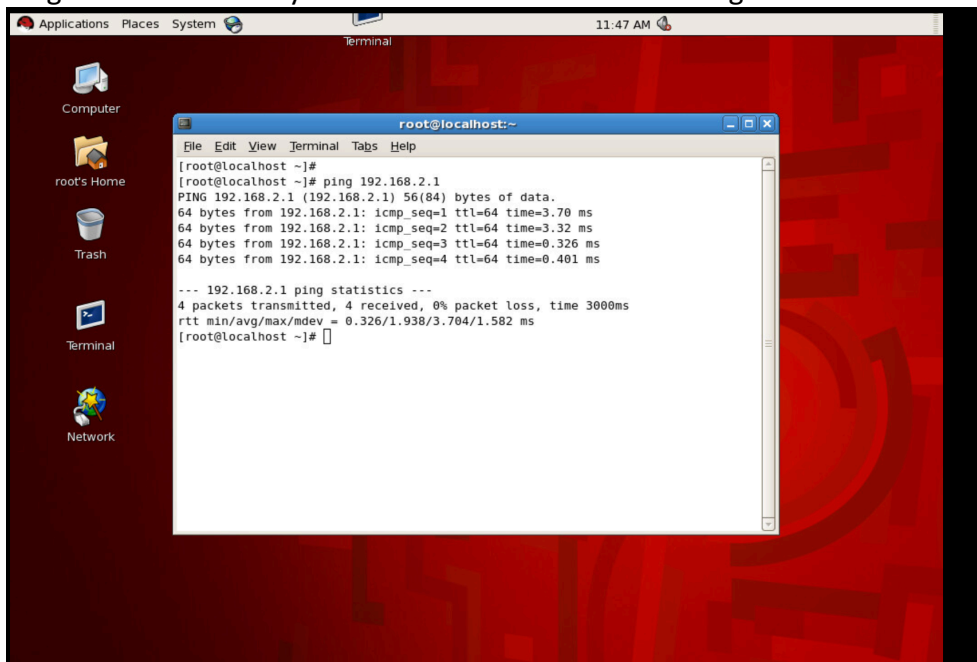


De igual forma configuramos la Dirección IP de la segunda Máquina Virtual, asignando una IP dentro de la nueva Subred.



```
root@localhost:~  
File Edit View Terminal Tabs Help  
eth0  Link encap:Ethernet  HWaddr 00:50:56:9A:27:DE  
      inet addr:192.168.2.30  Bcast:192.168.2.255  Mask:255.255.255.0  
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
      RX packets:7 errors:0 dropped:0 overruns:0 frame:0  
      TX packets:43 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:1000  
      RX bytes:470 (470.0 b)  TX bytes:5932 (5.7 KiB)  
  
eth1  Link encap:Ethernet  HWaddr 00:50:56:9A:07:D4  
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
      RX packets:74 errors:0 dropped:0 overruns:0 frame:0  
      TX packets:6 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:1000  
      RX bytes:33183 (32.4 KiB)  TX bytes:2052 (2.0 KiB)  
  
lo    Link encap:Local Loopback  
      inet addr:127.0.0.1  Mask:255.0.0.0  
      UP LOOPBACK RUNNING  MTU:16436  Metric:1  
      RX packets:2817 errors:0 dropped:0 overruns:0 frame:0  
      TX packets:2817 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:0  
      RX bytes:4914300 (4.6 MiB)  TX bytes:4914300 (4.6 MiB)  
  
[root@localhost ~]#
```

Pings hacia el Gateway confirman la conectividad del segundo EPG hacia la Fábrica.



```
root@localhost:~  
File Edit View Terminal Tabs Help  
[root@localhost ~]# ping 192.168.2.1  
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data:  
64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=3.70 ms  
64 bytes from 192.168.2.1: icmp_seq=2 ttl=64 time=3.32 ms  
64 bytes from 192.168.2.1: icmp_seq=3 ttl=64 time=0.326 ms  
64 bytes from 192.168.2.1: icmp_seq=4 ttl=64 time=0.401 ms  
  
--- 192.168.2.1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3000ms  
rtt min/avg/max/mdev = 0.326/1.938/3.704/1.582 ms  
[root@localhost ~]#
```

La información operacional del EPG-2 confirma que estamos recibiendo tráfico desde la Máquina virtual RedHat-3

EPG - EPG-2

Policy **Operational** Stats Health Faults History

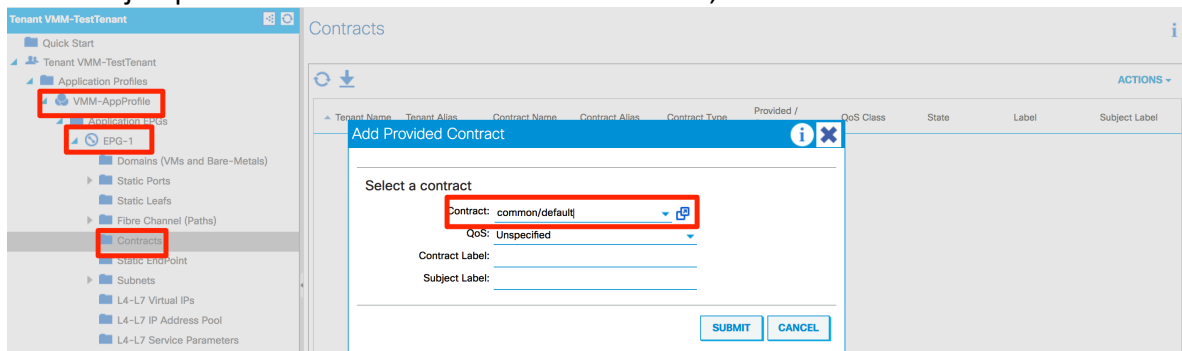
Client End-Points Configured Access Policies Contracts Controller End-Points

100

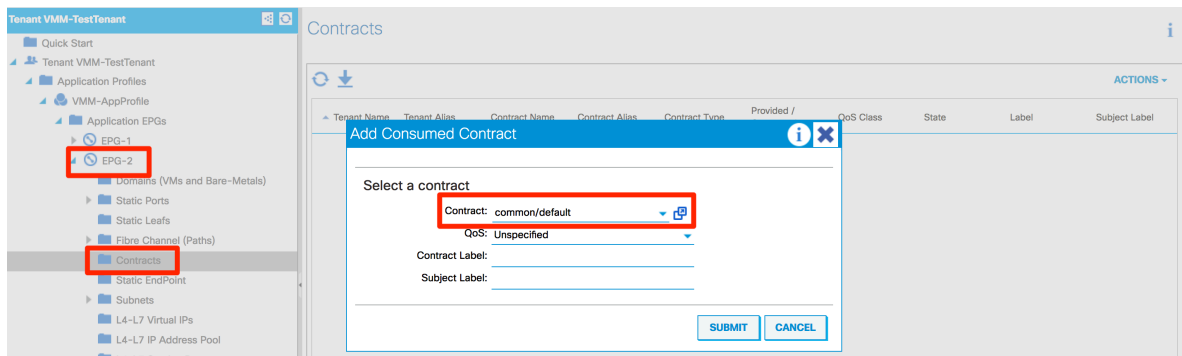
End Point	MAC	IP	Learning Source	Hosting Server	Reporting Controller Name	Interface	Multicast Address	Encap
RedHat-3	00:50:56:9...	10.20.30.4, 192.168.2.30	learned vmm	10.88.247.29	Mx-vCenter	Pod-1/Node-103-104/vP...	---	vlan-1335

Ya que las Máquinas virtuales corresponden a diferentes EPGs, requerimos un Contrato para que la comunicación entre ambos sea permitida. Para este ejemplo utilizaremos el contrato *Common/default*, este contrato puede ser visto como un *permit any any*, es decir, este contrato permite cualquier tipo de tráfico entre el *Consumer* y *Provider*. Estos dos términos definen la dirección en la que esperamos el flujo de comunicación. Un *Consumer* es el origen de tráfico, al consumir un servicio. El *Provider* es el destino, proveyendo el servicio.

En este ejemplo el EPG-1 será el *Provider* del Contrato, es decir el destino del tráfico.

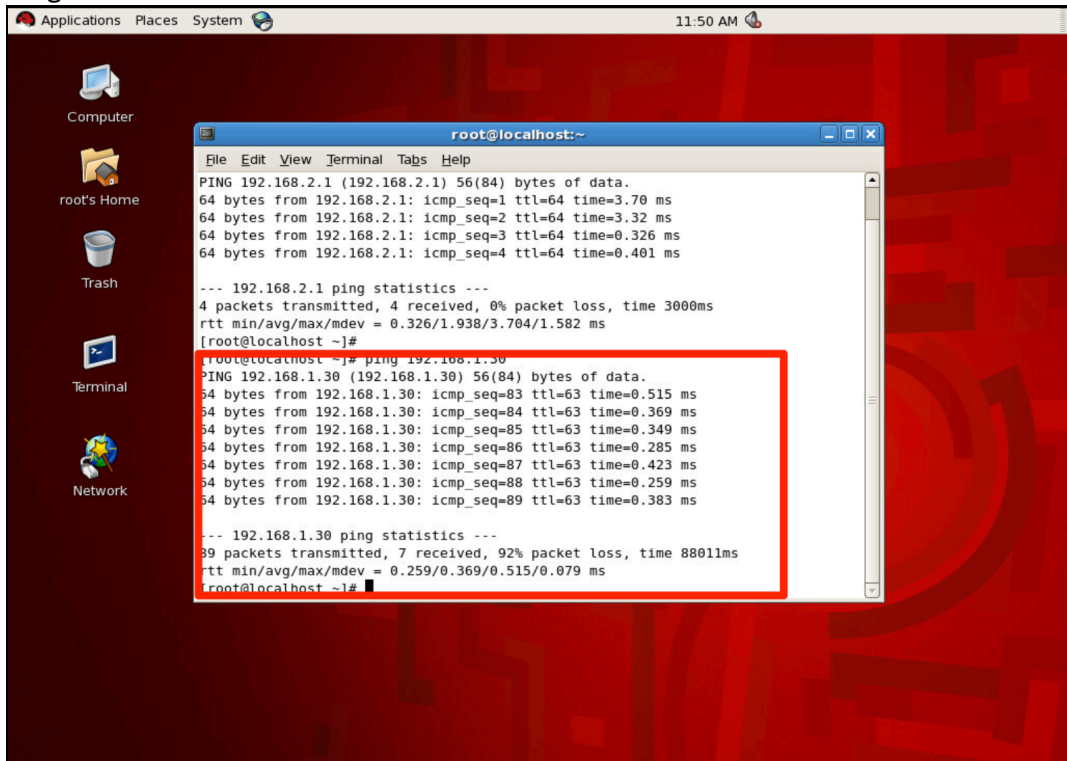


El EPG-2 será el *Consumer* del contrato, iniciando el tráfico. Es importante señalar que, para tener un tráfico totalmente bidireccional, ambos EPGs deben proveer y consumir el Contrato entre ellos.



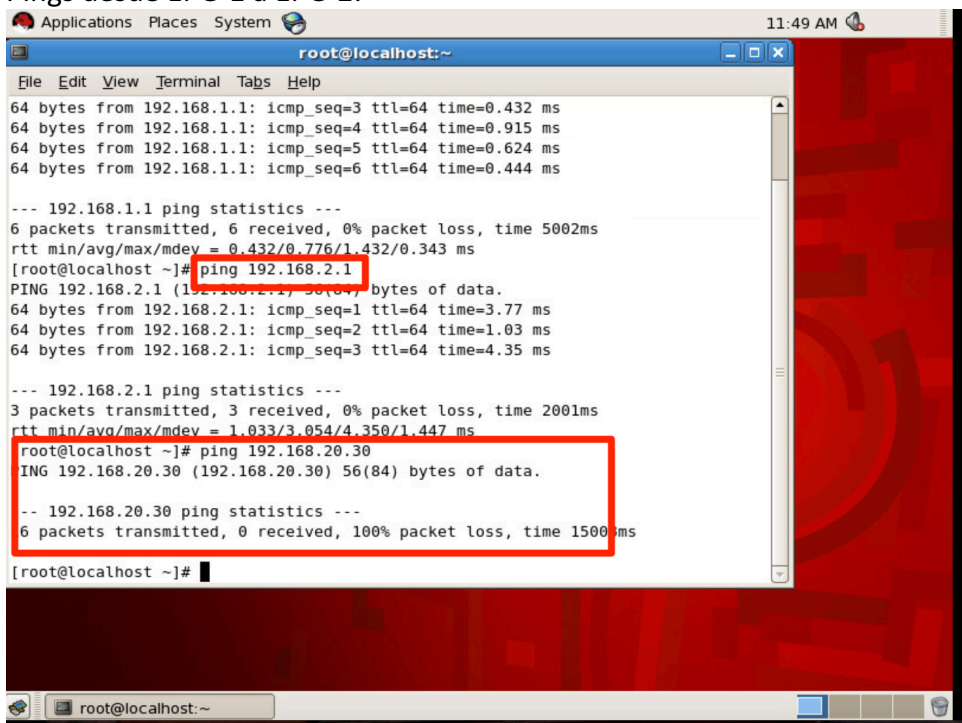
Una vez que aplicamos el contrato, los pings son permitidos desde el Consumer (EPG-2) al Provider(EPG-1).

Ping desde EPG-2 a EPG-1:



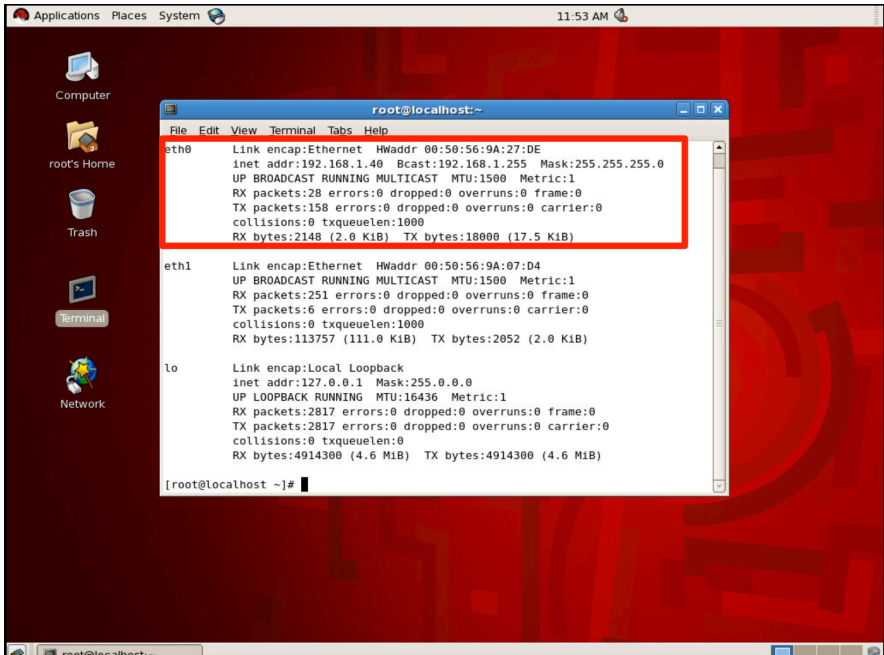
```
root@localhost:~  
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.  
64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=3.70 ms  
64 bytes from 192.168.2.1: icmp_seq=2 ttl=64 time=3.32 ms  
64 bytes from 192.168.2.1: icmp_seq=3 ttl=64 time=0.326 ms  
64 bytes from 192.168.2.1: icmp_seq=4 ttl=64 time=0.401 ms  
  
--- 192.168.2.1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3000ms  
rtt min/avg/max/mdev = 0.326/1.938/3.704/1.582 ms  
[root@localhost ~]#  
root@localhost ~]# ping 192.168.1.30  
PING 192.168.1.30 (192.168.1.30) 56(84) bytes of data.  
64 bytes from 192.168.1.30: icmp_seq=83 ttl=63 time=0.515 ms  
64 bytes from 192.168.1.30: icmp_seq=84 ttl=63 time=0.369 ms  
64 bytes from 192.168.1.30: icmp_seq=85 ttl=63 time=0.349 ms  
64 bytes from 192.168.1.30: icmp_seq=86 ttl=63 time=0.285 ms  
64 bytes from 192.168.1.30: icmp_seq=87 ttl=63 time=0.423 ms  
64 bytes from 192.168.1.30: icmp_seq=88 ttl=63 time=0.259 ms  
64 bytes from 192.168.1.30: icmp_seq=89 ttl=63 time=0.383 ms  
  
--- 192.168.1.30 ping statistics ---  
89 packets transmitted, 7 received, 92% packet loss, time 88011ms  
rtt min/avg/max/mdev = 0.259/0.369/0.515/0.079 ms  
root@localhost ~]#
```

Pings desde EPG-1 a EPG-2:

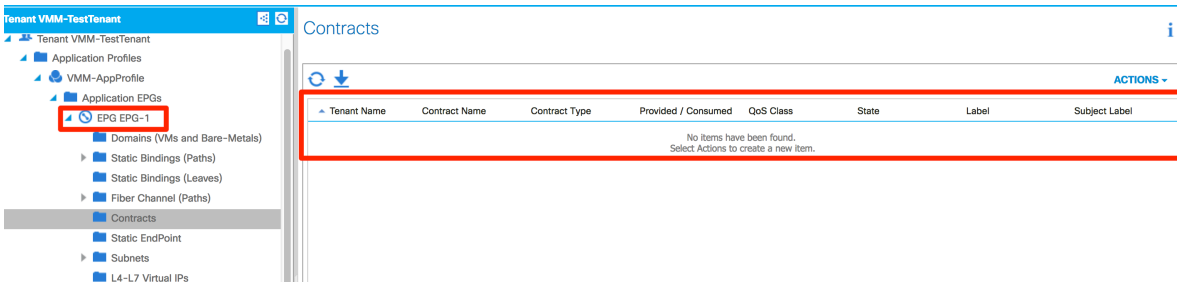


```
root@localhost:~  
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.432 ms  
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.915 ms  
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=0.624 ms  
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=0.444 ms  
  
--- 192.168.1.1 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5002ms  
rtt min/avg/max/mdev = 0.432/0.776/1.432/0.343 ms  
[root@localhost ~]# ping 192.168.2.1  
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.  
64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=3.77 ms  
64 bytes from 192.168.2.1: icmp_seq=2 ttl=64 time=1.03 ms  
64 bytes from 192.168.2.1: icmp_seq=3 ttl=64 time=4.35 ms  
  
--- 192.168.2.1 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2001ms  
rtt min/avg/max/mdev = 1.033/3.054/4.350/1.447 ms  
root@localhost ~]# ping 192.168.20.30  
PING 192.168.20.30 (192.168.20.30) 56(84) bytes of data.  
  
--- 192.168.20.30 ping statistics ---  
6 packets transmitted, 0 received, 100% packet loss, time 1500ms  
[root@localhost ~]#
```

La siguiente prueba será remover los Contratos y la segunda Subred configurada, 192.168.2.1/24. Colocaremos a ambas Máquinas virtuales en la misma subred, configurando la dirección IP 192.168.1.40/24, teniendo el mismo Gateway en ambos casos.



Los contratos se eliminan de ambos EPGs:



Aun cuando ambas Máquinas virtuales se encuentran en la misma subred y dominio de Capa 2, las políticas de ACI se interponen y no permiten la comunicación. Ya que cada Máquina se encuentra en diferente EPG, sin un contrato no será posible comunicarlos.

