

Configuración de la integración de dominios VM con ACI y UCS serie B

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Crear el dominio VM](#)

[Verifique que el DVS se haya creado en vCenter](#)

[Cree/verifique que CDP o LLDP estén habilitados en los vNIC de UCS](#)

[Configure las políticas de vSwitch en APIC para UCS B](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe los pasos de configuración necesarios para integrar una serie B de Cisco Unified Computing System (UCS) en un fabric de Application Centric Infrastructure (ACI) que aproveche la integración de dominios de Virtual Machine Manager (VM).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Un fabric ACI que consta de dos switches de columna y dos switches de hoja
- Un chasis UCS serie B con dos fabric interconnects
- Servidores blade UCS serie B con VMware ESXi
- Un controlador de infraestructura de políticas de aplicaciones (APIC)

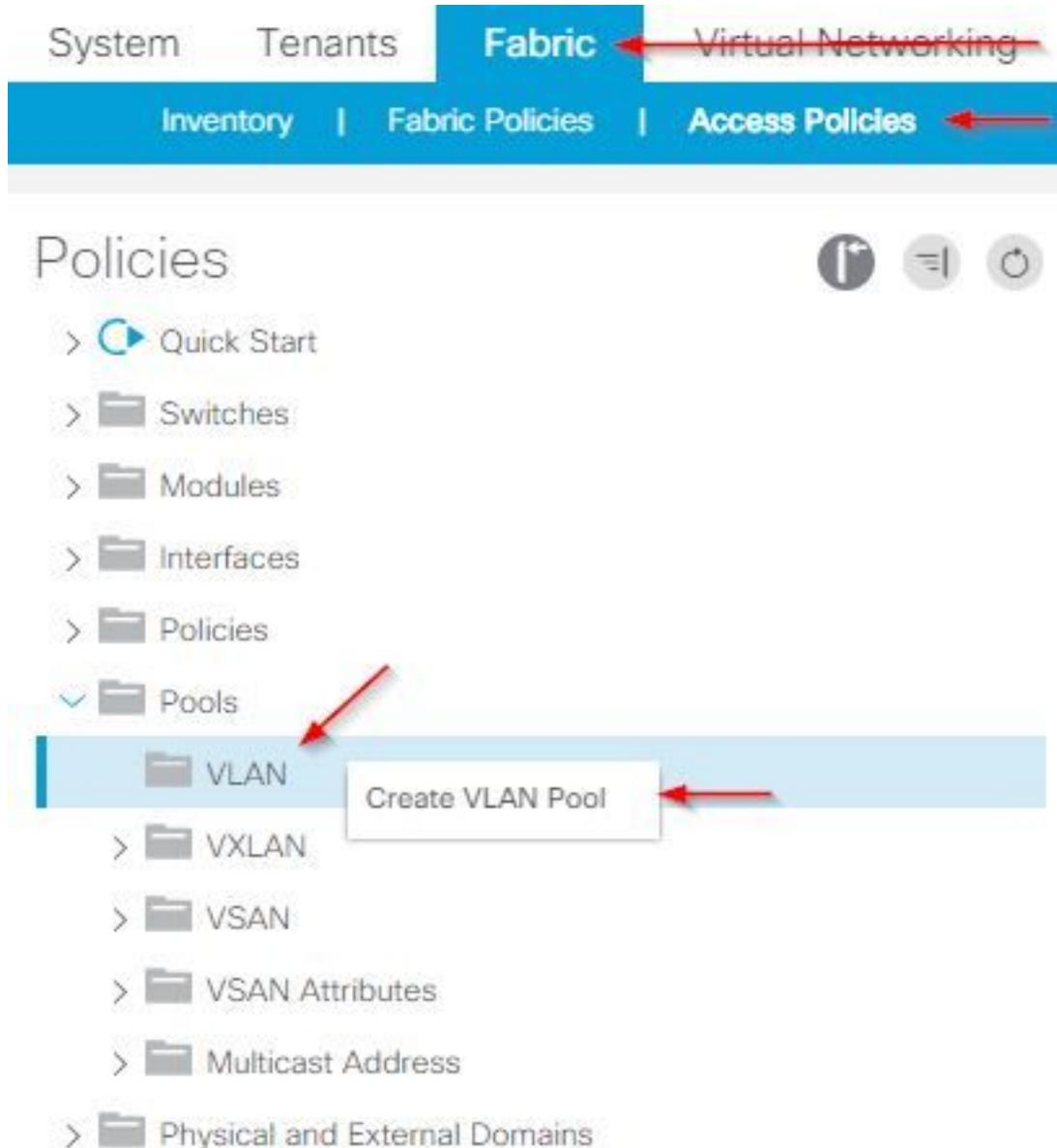
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Crear el dominio VM

La mayor parte de esta configuración es similar a la implementación de un dominio VM en cualquier hardware de servidor. Existen ciertas limitaciones para las que la solución temporal es configurar el APIC de una determinada manera. Estas configuraciones de solución temporal se describen específicamente en este procedimiento.

1. Cree un conjunto de VLAN dinámicas. Desde la interfaz de usuario APIC, elija Fabric > Access Policies > Pools > VLAN > Create VLAN Pool.



2. Cuando se abra la ventana Create VLAN Pool , ingrese esta información: Introduzca el nombre del conjunto en el campo Nombre.Haga clic en **Asignación dinámica**.Haga clic en el símbolo **Bloques de cierre (+)** más e introduzca el Intervalo de bloques de encapsulado en los campos Rango del cuadro de diálogo Crear rangos.Haga clic en **Asignación dinámica** para el campo Modo de asignación.Haga clic en **External** o **On the wire encapsulations**.Click OK.Haga clic en Submit (Enviar).

Create VLAN Pool

Specify the Pool identity

Name:

Description: optional

Allocation Mode: Dynamic Allocation Static Allocation

Encap Blocks:

| VLAN Range | Allocation Mode | Role |
|------------|-----------------|------|
| | | |

Create Ranges

Specify the Encap Block Range

Type: VLAN

Range: -
Integer Value Integer Value

Allocation Mode: Dynamic Allocation Inherit allocMode from parent Static Allocation

Role: External or On the wire encapsulations Internal

Create VLAN Pool

Specify the Pool identity

Name:

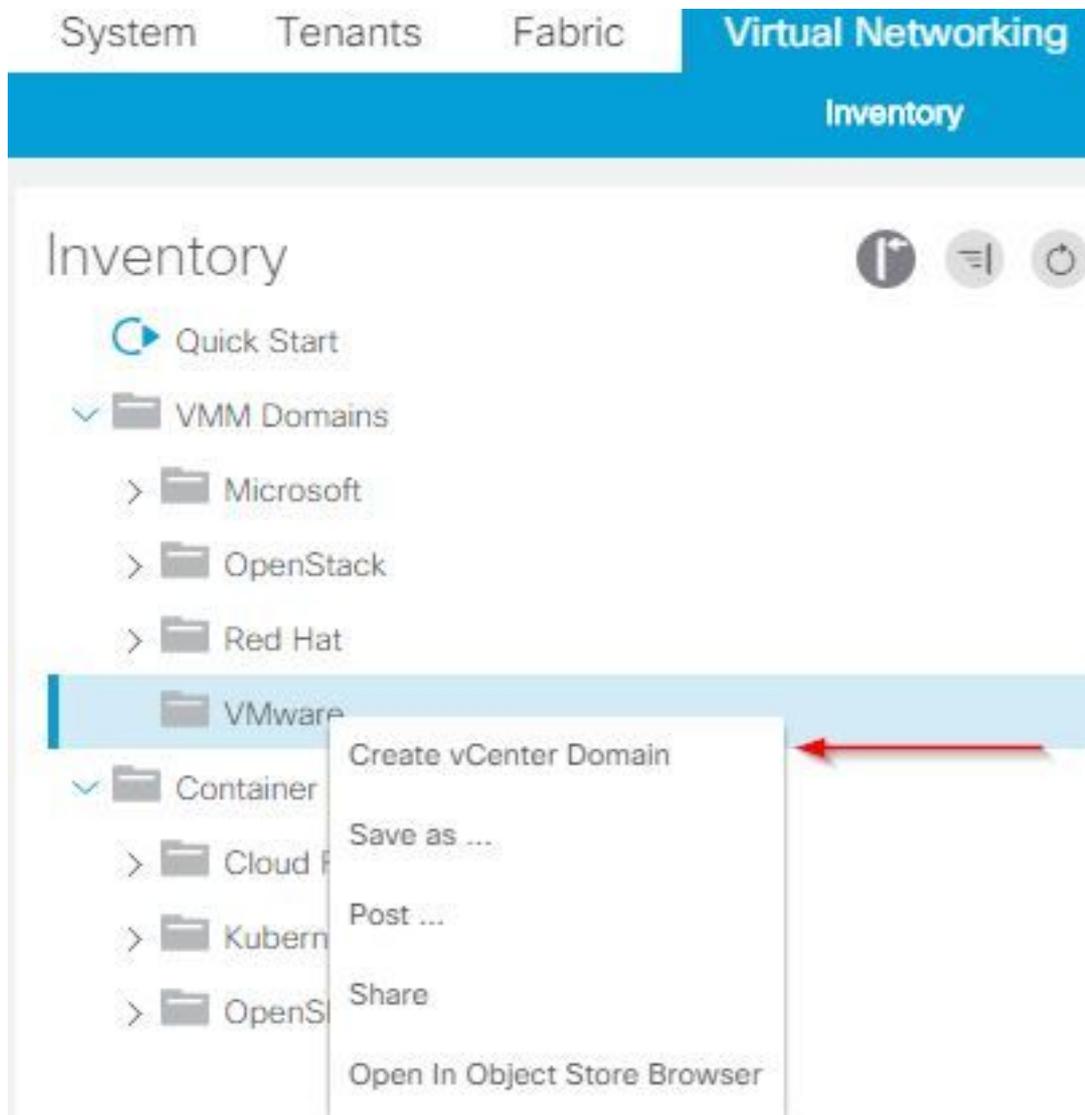
Description: optional

Allocation Mode: Dynamic Allocation Static Allocation

Encap Blocks:

| VLAN Range | Allocation Mode | Role |
|------------|-------------------------------|-------------------------------|
| [100-199] | Inherit allocMode from par... | External or On the wire en... |

3. Desde la interfaz de usuario de APIC, elija **Virtual Networking > VMware > Create vCenter**



Domain.

4. Cuando aparezca la ventana Create vCenter Domain (Crear dominio de vCenter), introduzca esta información: Introduzca el nombre de dominio en el campo Virtual Switch Name (Nombre del switch virtual). Haga clic en **VMWare vSphere Distributed Switch**. Elija (crear si es necesario) **Demo-AEP** de la lista desplegable Perfil de entidad adjunta asociado. Elija **Demo-Pool (Dynamic)** en la lista desplegable VLAN Pool. Haga clic en el símbolo **vCenter Credentials (+)** plus e introduzca la información de credenciales de vCenter en el cuadro de diálogo Create vCenter Credential (Crear credenciales de vCenter). Click OK. Haga clic en Submit (Enviar).

Create vCenter Domain

Specify vCenter domain users and controllers

Virtual Switch Name: Demo-VMM

Virtual Switch: VMware vSphere Distributed Switch Cisco AVS Cisco AVE

Associated Attachable Entity Profile: Demo-AEP

Delimiter:

Enable Tag Collection:

Access Mode: Read Only Mode Read Write Mode

Endpoint Retention Time (seconds): 0

VLAN Pool: Demo-pool(dynamic)

Security Domains:

| Name | Description |
|------|-------------|
|------|-------------|

vCenter Credentials:

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

Cancel Submit

Create vCenter Credential

Specify account profile

Name: Demo-VMM-Creds

Description: optional

Username: root

Password:

Confirm Password:

Cancel OK

5. Haga clic en el encabezado (+) más por vCenter de la ventana Create vCenter Domain (Crear dominio de vCenter); puede que sea necesario desplazarse hacia abajo para verlo. Introduzca esta información cuando aparezca la ventana Create vCenter Controller:

vCenter:

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

Introduzca el nombre de host o la dirección IP en el campo Nombre de host (o Dirección IP). Elija **vCenter Default** en la lista desplegable Versión DVS. Introduzca el nombre del Data Center en el campo Data Center. Elija **Demo-VM-Creds** en la lista desplegable Credencial asociada. Click OK. Haga clic en Submit (Enviar).

Add vCenter Controller

Specify controller profile

vCenter Controller

Name: Demo-vCenter

Host Name (or IP Address): 192.168.100.50

DVS Version: vCenter Default

Stats Collection: Disabled Enabled

Datacenter: jristain

Management EPG: select an option

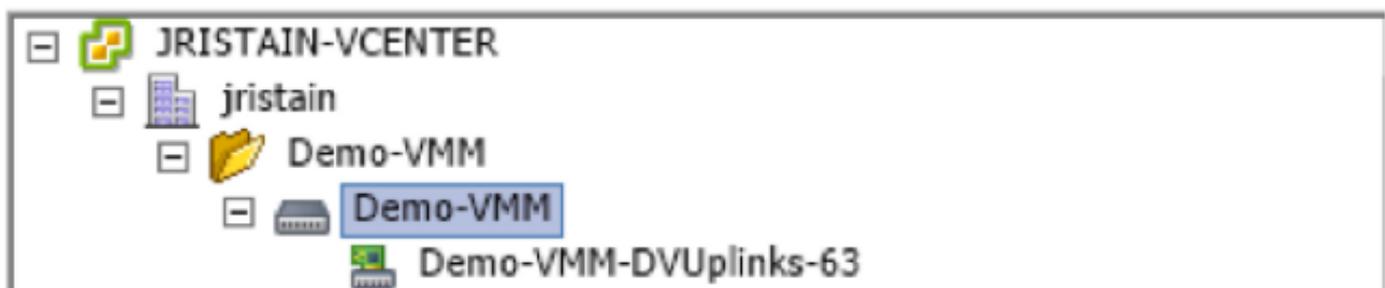
Associated Credential: Demo-VMM-Creds

Cancel OK

Verifique que el DVS se haya creado en vCenter

Debería ver algunas tareas nuevas en la ventana Tareas recientes y la adición de un switch virtual distribuido (DVS) en el servidor vCenter:

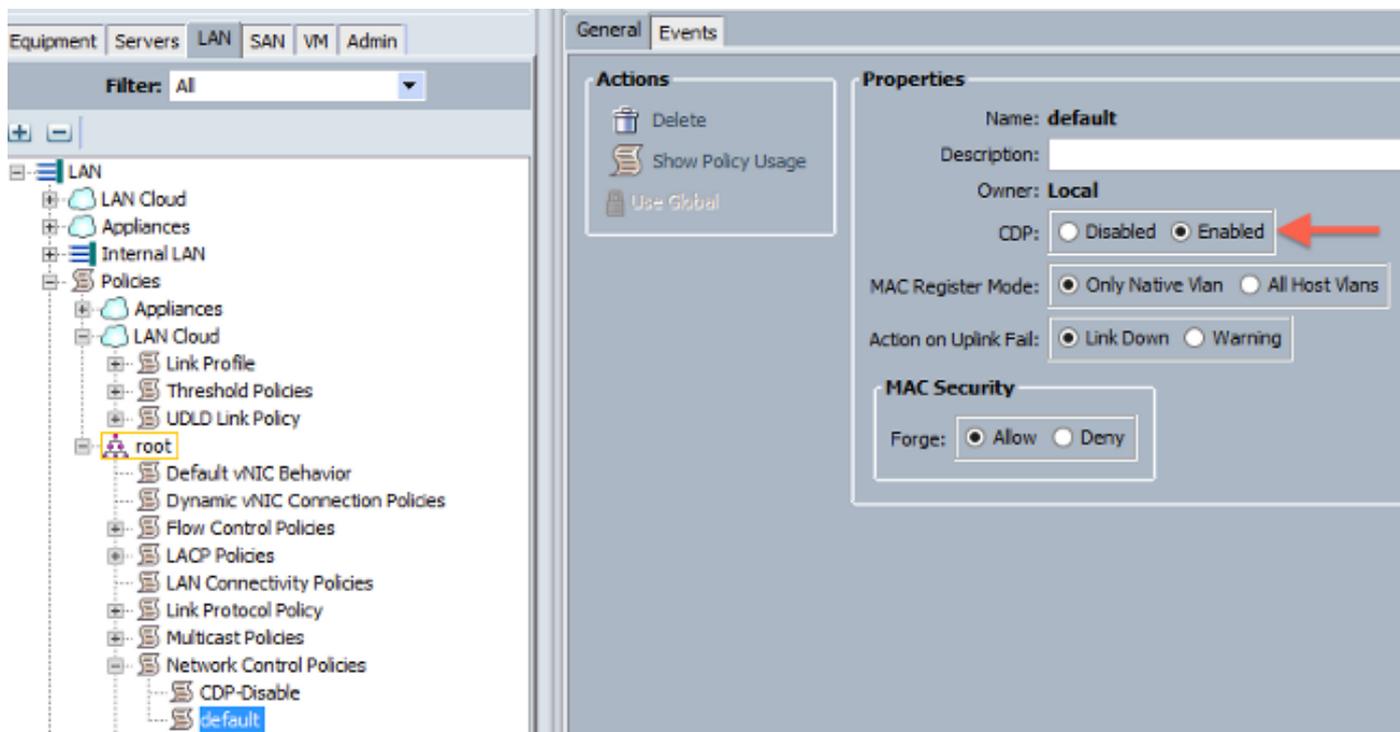
| Recent Tasks | | | | | | | |
|-------------------------------------|----------|-----------|---------|--------------|-----------------|-----------------------|--|
| Name | Target | Status | Details | Initiated by | vCenter Server | Requested Start Ti... | |
| Create a vSphere Distributed Switch | Demo-VMM | Completed | | root | JRISTAIN-VCE... | 4/9/2015 10:38:57 AM | |
| Create alarm | Demo-VMM | Completed | | root | JRISTAIN-VCE... | 4/9/2015 10:38:57 AM | |
| Create alarm | Demo-VMM | Completed | | root | JRISTAIN-VCE... | 4/9/2015 10:38:56 AM | |
| Create folder | jristain | Completed | | root | JRISTAIN-VCE... | 4/9/2015 10:38:56 AM | |



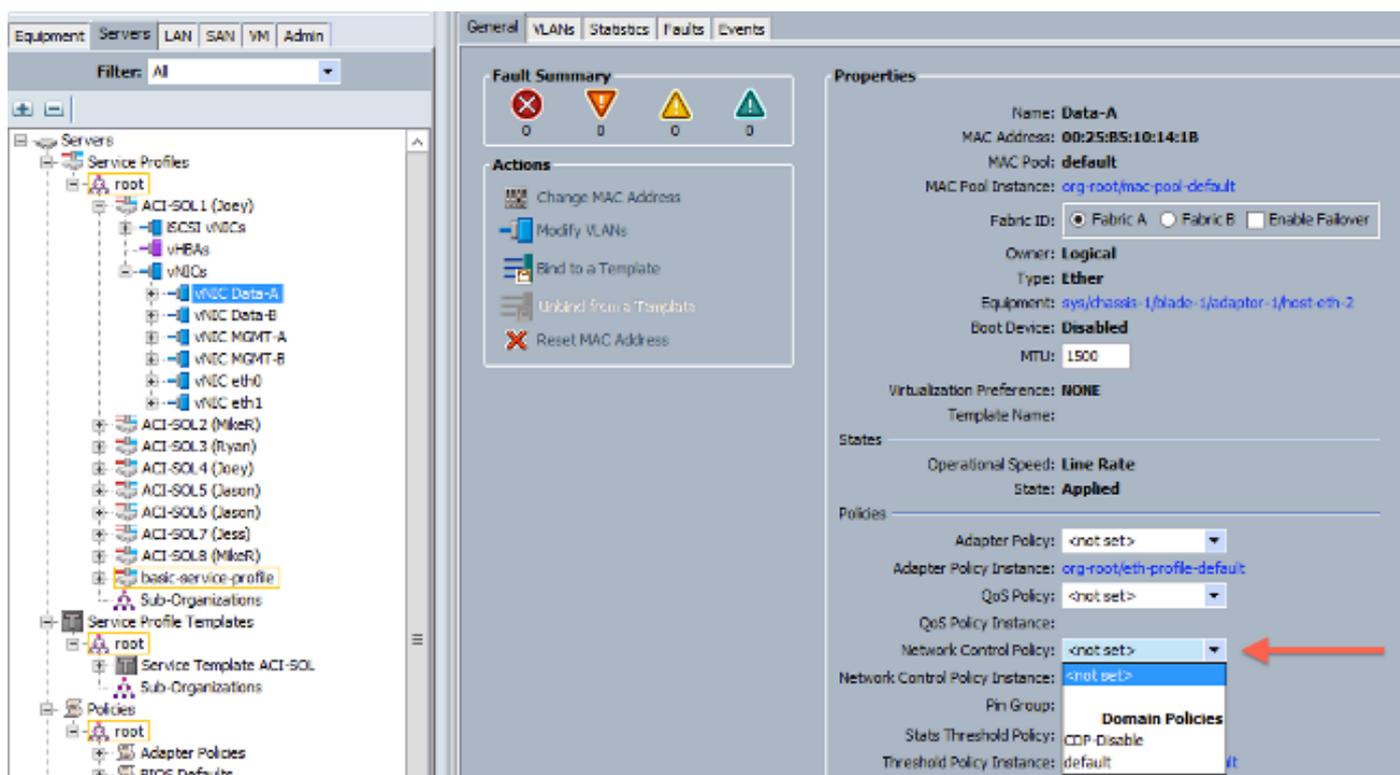
Cree/verifique que CDP o LLDP estén habilitados en los vNIC de UCS

Al implementar UCS B en ACI, puede elegir el protocolo de detección que desea utilizar para descubrir los hosts. En esta sección se explica cómo configurar cada tipo en UCS Manager.

De forma predeterminada, Cisco Discovery Protocol (CDP) está desactivado en la tarjeta de interfaz de red virtual (vNIC) de UCS porque la política de control de red predeterminada tiene CDP desactivado. Para habilitar CDP, puede modificar la política de control de red predeterminada o crear una nueva con CDP habilitado. A continuación, aplique esa política a cada vNIC en cada perfil de servicio. En este ejemplo, se modifica la política de control de red predeterminada, ya que todos los perfiles de servicio lo utilizan de forma predeterminada:



Si utiliza una política diferente, asegúrese de agregar esa política a las vNIC en cada perfil de servicio:



En la versión 2.2(4b) y posteriores, UCS admite protocolo de detección de capa de enlace (LLDP) desde los Fabric Interconnects hasta los blades. Esto significa que también puede utilizar LLDP para detectar los hosts en vCenter y el fabric si ejecuta esta versión o posterior. La configuración es exactamente la misma que la anterior, pero usted habilitaría LLDP en ambas direcciones:

Create Network Control Policy

Name: **LLDP-Enable**

Description:

CDP: Disabled Enabled

MAC Register Mode: Only Native Vlan All Host Vlans

Action on Uplink Fail: Link Down Warning

MAC Security

Forge: Allow Deny

LLDP

Transmit: Disabled Enabled

Receive: Disabled Enabled

OK Cancel

Configure las políticas de vSwitch en APIC para UCS B

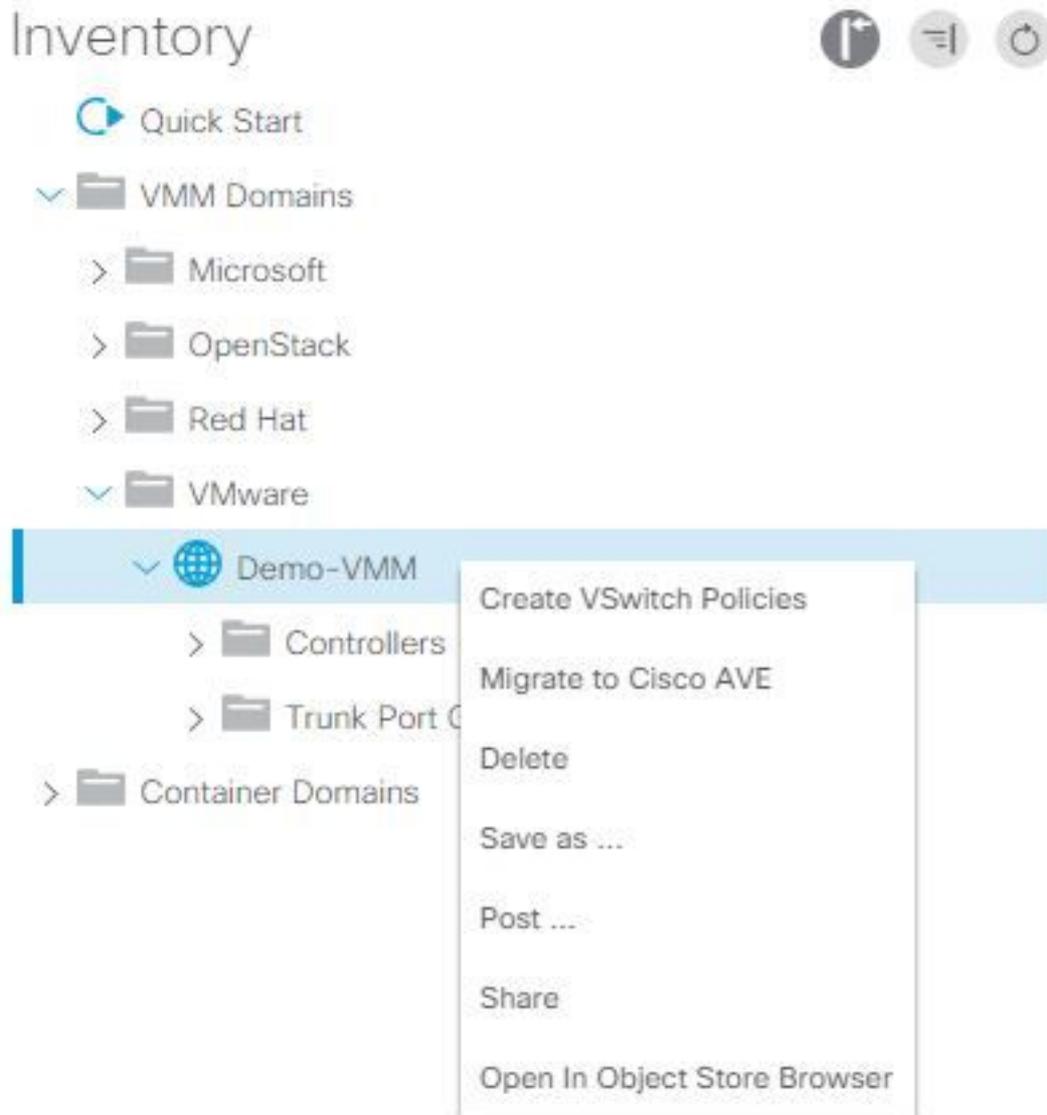
De forma predeterminada en el DVS, el protocolo de detección utilizado es LLDP. Esto está bien para cualquier servidor que admita LLDP, pero los blades de la serie B de UCS solamente admiten LLDP en la versión 2.2(4b) de UCSM y posteriores. Debido a esto, ESXi no puede informar la información LLDP al APIC, a menos que esté en el código correcto.

Como alternativa a LLDP, utilice CDP para detectar los hosts. Para que el DVS utilice CDP, configure una política vSwitch en el dominio de VM que tenga CDP habilitado y LLDP inhabilitado.

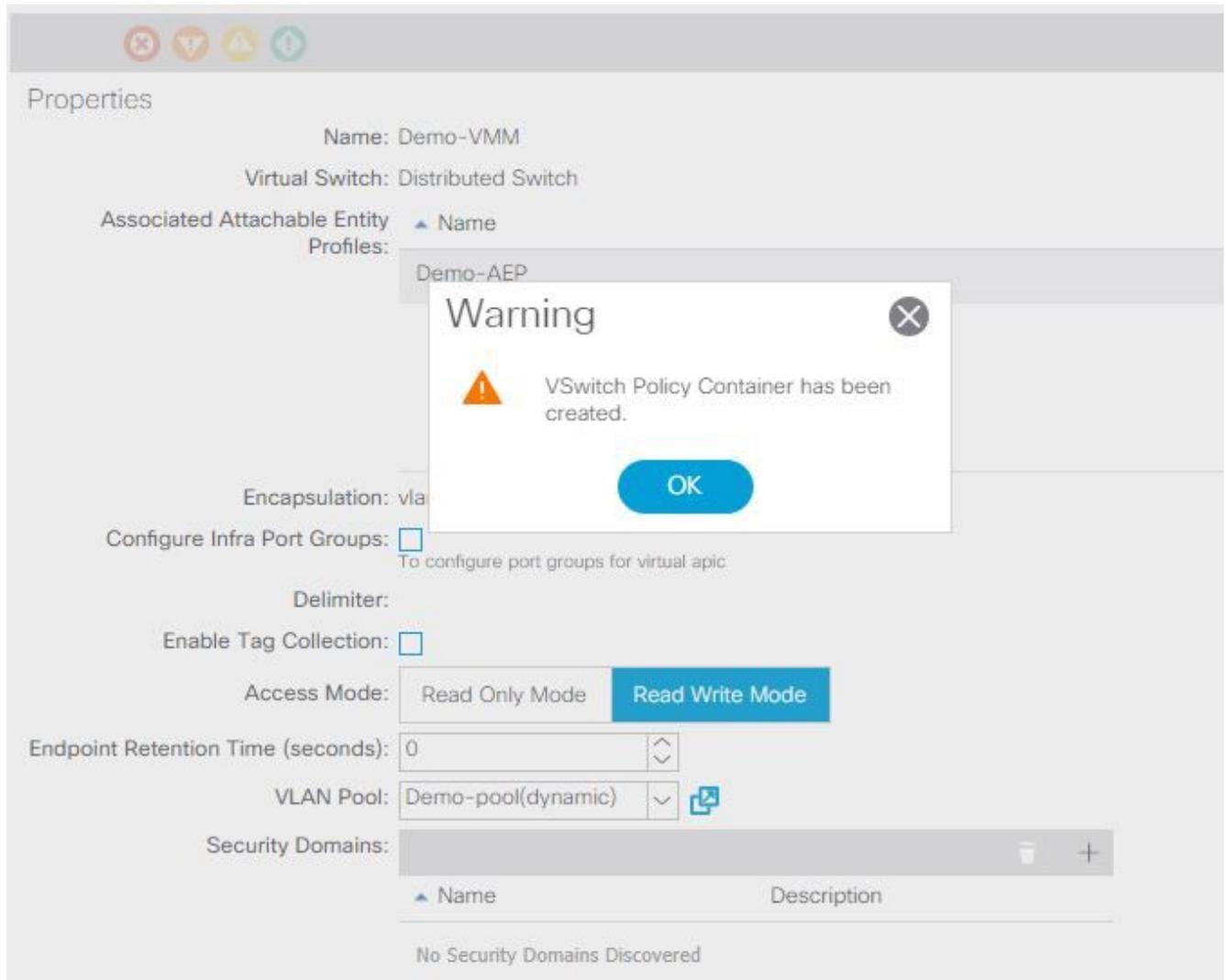
Junto con esto, el único mecanismo de balanceo de carga soportado cuando se utiliza la serie B de UCS es Route Based on Originating Virtual Port . Si configura una política **mac-pinning**,

programa los grupos de puertos para utilizar este mecanismo. Esto es muy importante para evitar la pérdida de paquetes.

1. Desde la interfaz de usuario de APIC, elija **Virtual Networking > VMware > Dominio Configurado > Crear Políticas de VSwitch**.



2. En este momento, se mostrará una advertencia para avisarle de que se ha creado una política de VSwitch predeterminada.

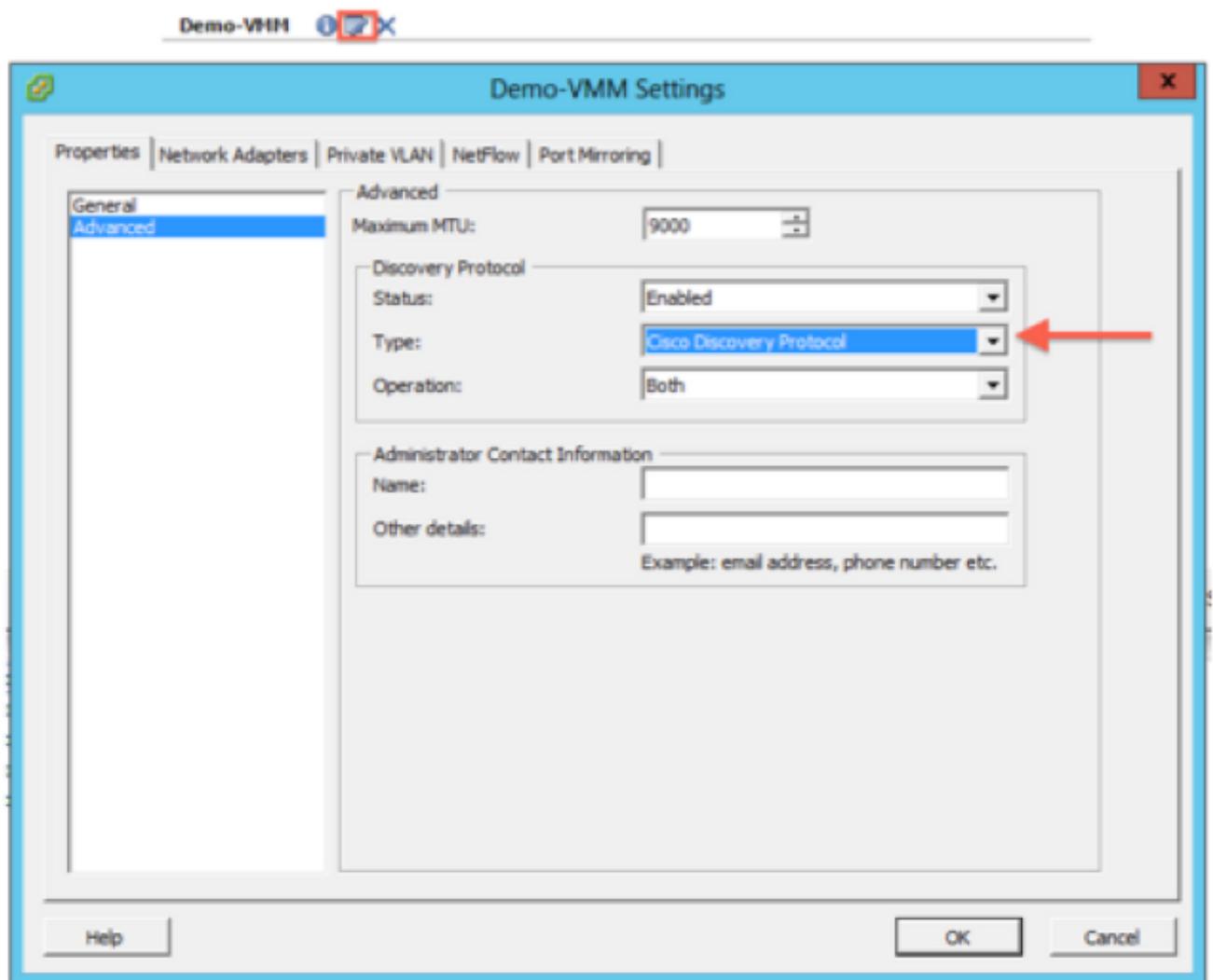


3. Acepte el mensaje de advertencia y navegue a la ficha **Política de Vswitch** bajo el Dominio de VM: Elija o cree una **política CDP** donde **CDP está habilitado**. Elija o cree una **política de canal de puerto** con el modo de clics seleccionado. Elija o cree una **política LLDP** donde **CDP está inhabilitado**. Haga clic en Submit (Enviar). **Nota:** Si está en UCSM 2.2(4b) o posterior y desea utilizar LLDP, puede activar LLDP en esta política de vSwitch ya que UCS lo admite. Este ejemplo es sólo para las versiones UCSM que no soportan LLDP, o si se desea CDP. Si tanto LLDP como CDP están habilitados, LLDP toma prioridad.

Domain - Demo-VMM



Después de hacer clic en **Enviar**, puede ver que el DVS se ha reconfigurado en el vCenter:



También puede verificar que los vmnics vean la información CDP de Fabric Interconnect:

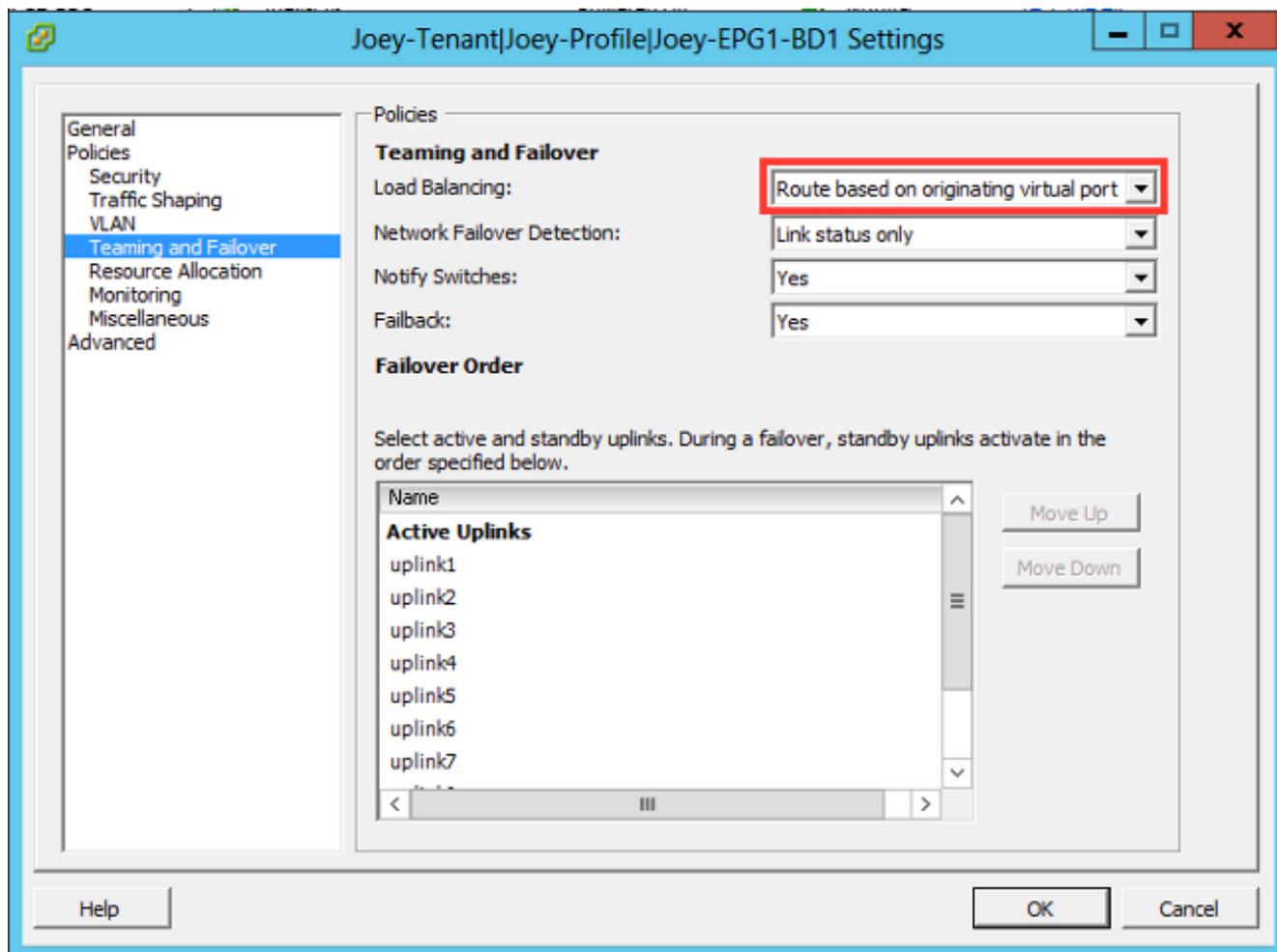
The screenshot shows a Cisco Discovery Protocol window with the following properties:

| | |
|---------------------|------------------------------------|
| Version: | 2 |
| Timeout: | 0 |
| Time to live: | 129 |
| Samples: | 1517 |
| Device ID: | aci-sol-calo-ucsb-A(SS118220541) |
| IP Address: | 14.2.104.23 |
| Port ID: | Vethernet813 |
| Software Version: | Cisco Nexus Operating System (...) |
| Hardware Platform: | UCS-FI-6248UP |
| IP Prefix: | 0.0.0.0 |
| IP Prefix Length: | 0 |
| VLAN: | 1 |
| Full Duplex: | Disabled |
| MTU: | 1500 |
| System Name: | aci-sol-calo-ucsb-A |
| System OId: | 1.3.6.1.4.1.9.12.3.1.3.1062 |
| Management Address: | 14.2.104.23 |
| Location: | snmplocation |

Peer Device Capability Enabled

| | |
|----------------------|-----|
| Router: | No |
| Transparent Bridge: | No |
| Source Route Bridge: | No |
| Network Switch: | Yes |
| Host: | No |
| IGMP: | Yes |
| Repeater: | No |

4. Verifique que la "Ruta basada en el puerto virtual de origen" esté programada en los grupos de puertos. Haga clic con el botón derecho del ratón en un grupo de puertos en la ficha Networking y edite la configuración para verificar esto:



Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Después de realizar estos cambios, vCenter debe notificar al APIC acerca de la información CDP. Para verificar esto, verifique el inventario del dominio de VM.

Desde la interfaz de usuario de APIC, elija Virtual Networking > Inventory > VMware > Domain > Controllers > vCenter > Hypervisors > Hypervisor > General para ver la ventana Propiedades.

System Tenants Fabric **Virtual Networking** L7 Services Admin Operations Apps

Inventory

Inventory

- Quick Start
- VMM Domains
 - Microsoft
 - OpenStack
 - Red Hat
 - VMware
 - Demo-VMM (Domain)
 - Controllers
 - Demo-vCenter (vCenter)
 - Hypervisors
 - 14.2.169.19 (Hypervisor)
 - 14.2.169.20
 - DVS - Demo-VMM
 - Trunk Port Groups
 - Container Domains
 - Cloud Foundry
 - Kubernetes
 - OpenShift

Hypervisor - 14.2.169.19

Topology General Stats Faults History

Properties

Name: 14.2.169.19
 Type: Hypervisor Host
 Status: Powered On

Hypervisor NICs:

| Name | MAC | State | Faults | Link Speed | Duplex Mode | Neighbor |
|--------|------------|-------|--------|------------|-------------|----------|
| vmnic0 | EC:BD:1... | Up | 0000 | 1000 Mb | True | |
| vmnic1 | EC:BD:1... | Down | 0000 | unknown | Unknown | |
| vmnic2 | 04:62:7... | Up | 0000 | 10000 Mb | True | |
| vmnic3 | 04:62:7... | Up | 0000 | 10000 Mb | True | |

Virtual Machines:

| Name | Status |
|--------------------------|-------------|
| ASAv(rrangelth) | Powered Off |
| ASAv-transparent | Powered Off |
| ASAv-vmv | Powered Off |
| ASAv1-trans-inside-host | Powered Off |
| ASAv1-trans-outside-host | Powered Off |

Neighbors:

| Management Address | Interface Name | Proto | Neighbor ID |
|---|----------------|-------|-------------|
| No items have been found. Select Actions to create a new item. | | | |

En este momento, puede cambiar los parámetros de red de VM para agregar el adaptador al grupo de puertos adecuado y probar la conectividad. Los ping deben tener éxito. Si los pings no son exitosos, verifique que todos los ajustes en vCenter y en el APIC sean correctos para la detección de vecinos CDP.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.