

# Konfigurieren der VMM-Domänenintegration mit der ACI und der UCS B-Serie

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Erstellen der VMM-Domäne](#)

[Überprüfen Sie, ob der DVS in vCenter erstellt wurde.](#)

[Erstellen/Überprüfen der Aktivierung von CDP oder LLDP auf den UCS vNICs](#)

[Konfigurieren der vSwitch-Richtlinien auf dem APIC für UCS B](#)

[Überprüfen](#)

[Fehlerbehebung](#)

## Einführung

In diesem Dokument werden die Konfigurationsschritte beschrieben, die Sie zur Integration der Cisco Unified Computing System (UCS) B-Serie in eine ACI-Fabric (Application Centric Infrastructure) durchführen, die die Integration der Virtual Machine Manager (VMM)-Domäne ermöglicht.

## Voraussetzungen

### Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Hardware- und Softwareversionen:

- Eine ACI-Fabric, die aus zwei Spine-Switches und zwei Leaf-Switches besteht
- Ein Chassis der UCS B-Serie mit zwei Fabric Interconnects
- Blades der UCS B-Serie mit VMware ESXi
- Ein Application Policy Infrastructure Controller (APIC)

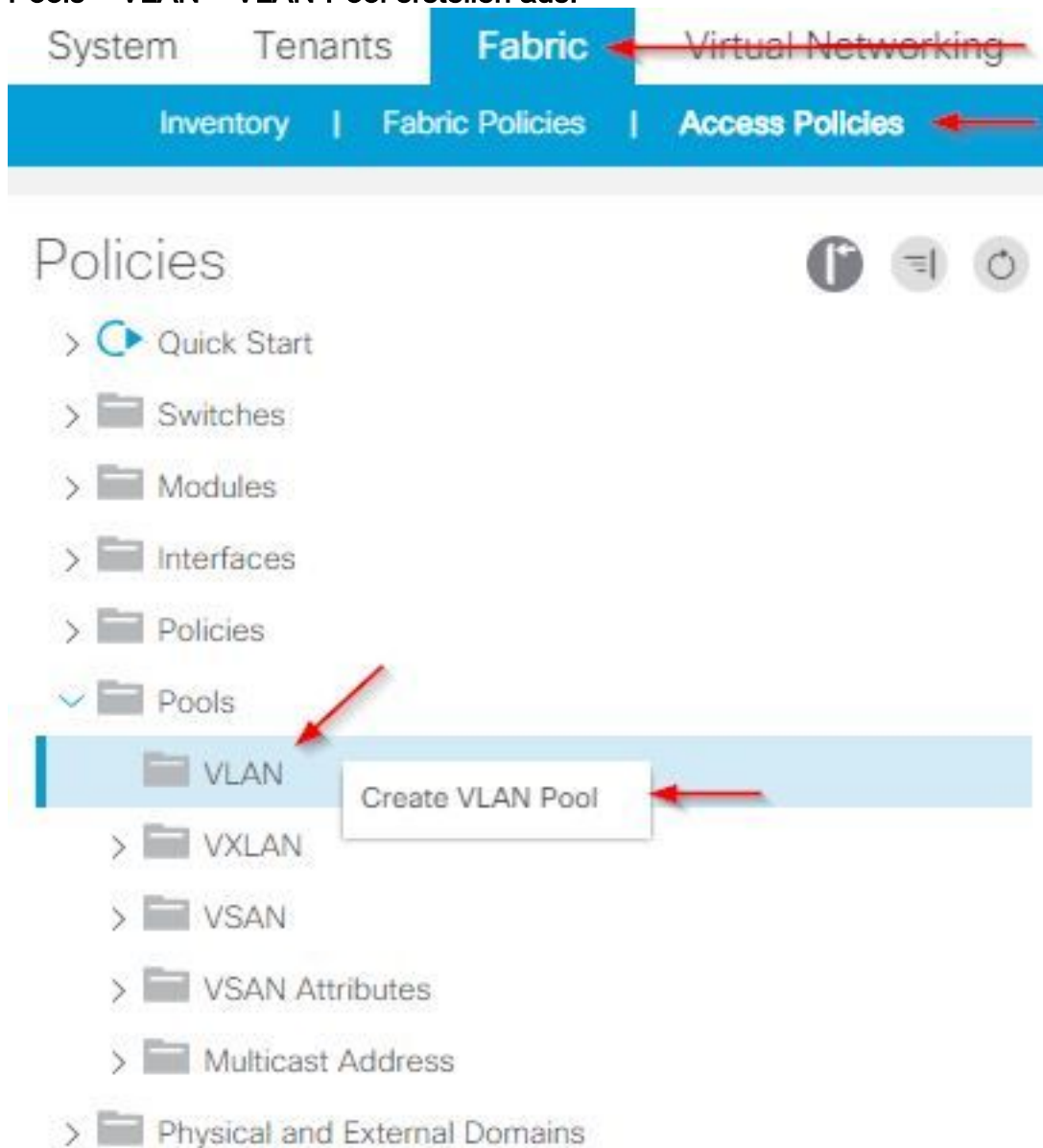
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

# Konfigurieren

## Erstellen der VMM-Domäne

Die meisten dieser Konfigurationen ähneln der Bereitstellung einer VMM-Domäne auf einer beliebigen Serverhardware. Es gibt gewisse Einschränkungen, für die die Lösung die Konfiguration des APIC auf eine bestimmte Art und Weise ist. Diese Workaround-Konfigurationen werden in diesem Verfahren speziell beschrieben.

1. Erstellen Sie einen dynamischen VLAN-Pool. Wählen Sie in der APIC-Benutzeroberfläche **Fabric > Access Policies > Pools > VLAN > Create VLAN Pool (Fabric > Zugriffsrichtlinien > Pools > VLAN > VLAN-Pool erstellen aus.**



2. Wenn das Fenster Create VLAN Pool (VLAN-Pool erstellen) geöffnet wird, geben Sie folgende Informationen ein: Geben Sie im Feld Name den Namen des Pools ein. Klicken Sie auf **Dynamische Zuweisung**. Klicken Sie auf das Symbol **Encap Blocks (+)** und geben Sie den Blockbereich der Encap in die Felder Bereich des Dialogfelds Bereich erstellen ein. Klicken Sie im Feld Zuweisungsmodus auf **Dynamic Allocation** (Dynamische Zuweisung). Klicken Sie auf **Extern oder Auf den Kabelkapselungen**. Klicken Sie auf **OK**. Klicken Sie auf

Senden.

Create VLAN Pool

Specify the Pool identity

Name: Demo-pool

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: VLAN 100 - VLAN 199

Allocation Mode: Dynamic Allocation Inherit allocMode from parent Static Allocation

Role: External or On the wire encapsulations Internal

Cancel OK

Create VLAN Pool

Specify the Pool identity

Name: Demo-pool

Description: optional

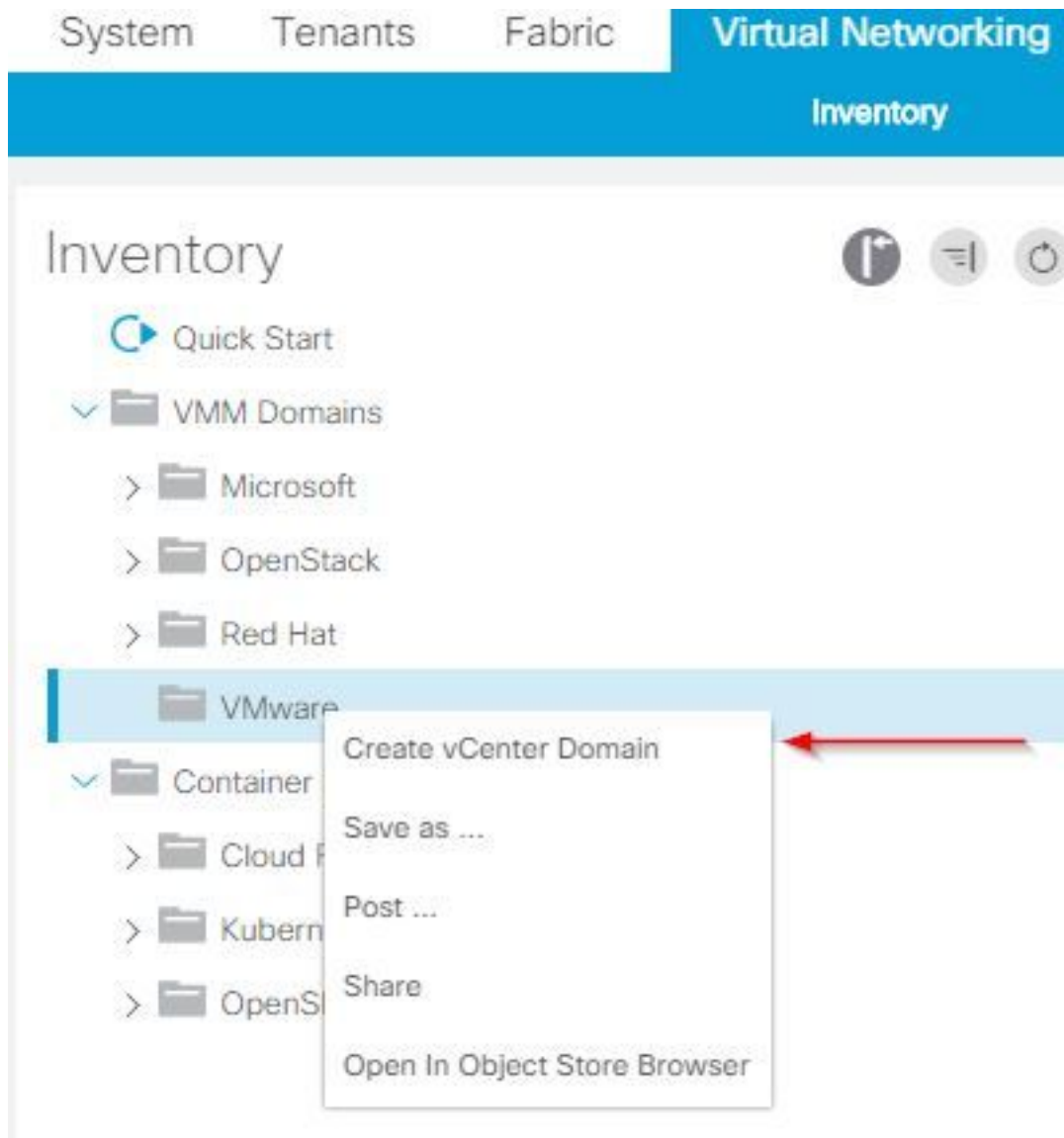
Allocation Mode: Dynamic Allocation Static Allocation

Encap Blocks:

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

Cancel Submit

3. Wählen Sie in der APIC-Benutzeroberfläche **Virtual Networking > VMM Domains > VMware > Create vCenter Domain** aus.



4. Wenn das Fenster Create vCenter Domain (vCenter-Domäne erstellen) angezeigt wird, geben Sie folgende Informationen ein: Geben Sie den Domänennamen im Feld Virtual Switch Name (Name des virtuellen Switches) ein. Klicken Sie auf **VMWare vSphere Distributed Switch**. Wählen Sie (ggf. erstellen) **Demo-AEP** aus der Dropdown-Liste Associated Attachable Entity Profile (Associated Attachable Entity-Profil) aus. Wählen Sie **Demo-Pool (dynamic)** aus der Dropdown-Liste VLAN Pool (VLAN-Pool) aus. Klicken Sie auf das **vCenter-Anmeldeinformationen (+)**-Pluszeichen, und geben Sie Ihre vCenter-Anmeldeinformationen im Dialogfeld Create vCenter Credential (vCenter-Anmeldeinformationen erstellen) ein. Klicken Sie auf **OK**. Klicken Sie auf **Senden**.

## Create vCenter Domain ? X

Specify vCenter domain users and controllers

Virtual Switch Name:

Virtual Switch: VMware vSphere Distributed Switch Cisco AVS Cisco AVE

Associated Attachable Entity Profile:

Delimiter:

Enable Tag Collection:

Access Mode: Read Only Mode Read Write Mode

Endpoint Retention Time (seconds):

VLAN Pool:

Security Domains:

Name	Description

vCenter Credentials:

Profile Name	Username	Description

Cancel
Submit

## Create vCenter Credential ? X

Specify account profile

Name:

Description:

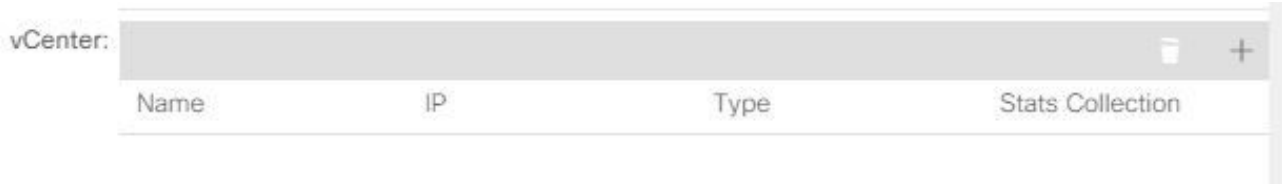
Username:

Password:

Confirm Password:

Cancel
OK

- Klicken Sie im Fenster Create vCenter Domain (vCenter-Domäne erstellen) auf das (+) Pluszeichen nach vCenter. Es kann erforderlich sein, einen Bildlauf nach unten durchzuführen, um es anzuzeigen. Geben Sie diese Informationen ein, wenn das Fenster Create vCenter Controller (vCenter-Controller erstellen) angezeigt wird:



Geben Sie den Hostnamen oder die IP-Adresse im Feld Hostname (oder IP-Adresse) ein. Wählen Sie **vCenter Default** aus der Dropdown-Liste DVS Version aus. Geben Sie den Namen des Rechenzentrums im Feld Datacenter ein. Wählen Sie **Demo-VMM-Creds** aus der Dropdown-Liste Associated Credential (Zugeordnete Anmeldeinformationen) aus. Klicken Sie auf **OK**. Klicken Sie auf **Senden**.

### Add vCenter Controller

Specify controller profile

vCenter Controller

Name:

Host Name (or IP Address):  ←

DVS Version:  ←

Stats Collection:  Disabled  Enabled

Datacenter:  ←

Management EPG:

Associated Credential:  ←

**Überprüfen Sie, ob der DVS in vCenter erstellt wurde.**

Im Fenster "Aktuelle Aufgaben" sollten einige neue Aufgaben angezeigt werden, und im vCenter-Server sollte ein Distributed Virtual Switch (DVS) hinzugefügt werden:

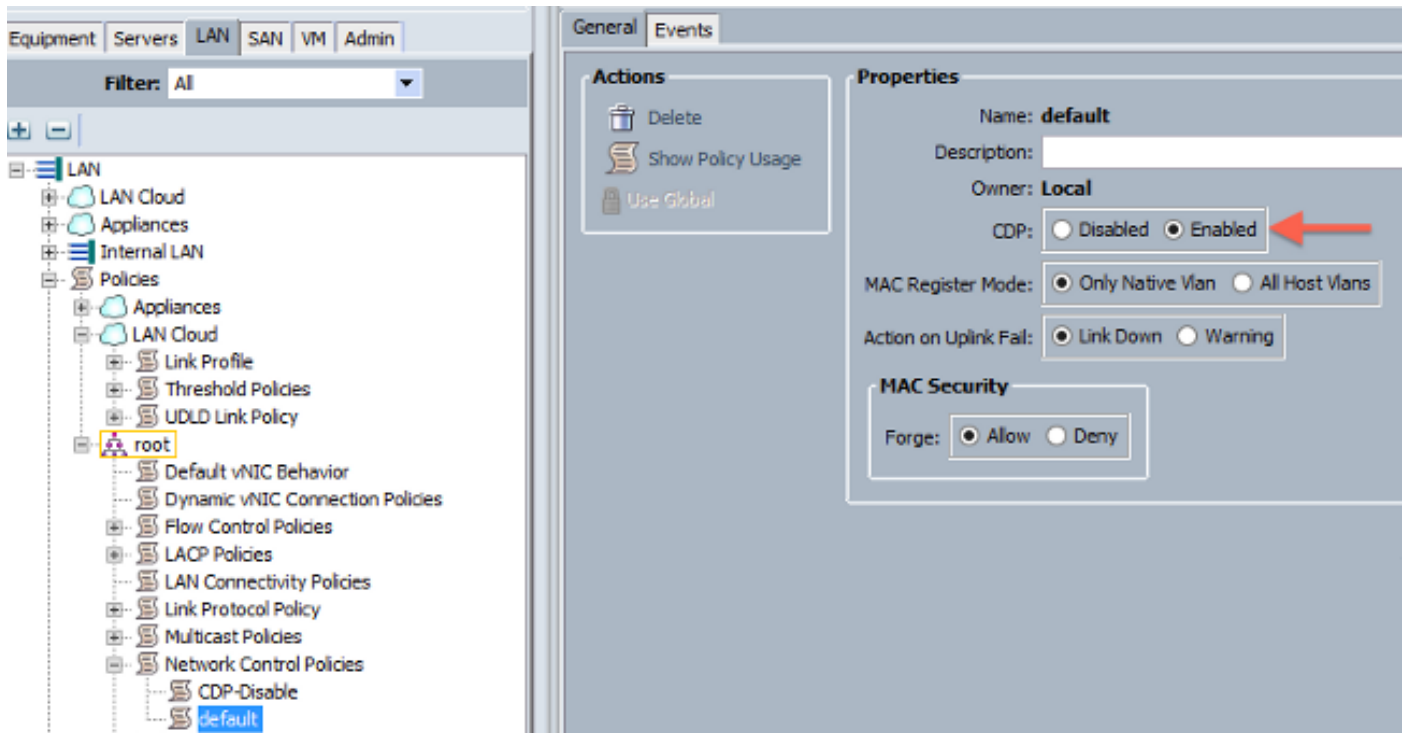
Recent Tasks						
Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Ti...
Create a vSphere Distributed Switch	Demo-VMM	Completed		root	JRISTAIN-VCE...	4/9/2015 10:38:57 AM
Create alarm	Demo-VMM	Completed		root	JRISTAIN-VCE...	4/9/2015 10:38:57 AM
Create alarm	Demo-VMM	Completed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



## Erstellen/Überprüfen der Aktivierung von CDP oder LLDP auf den UCS vNICs

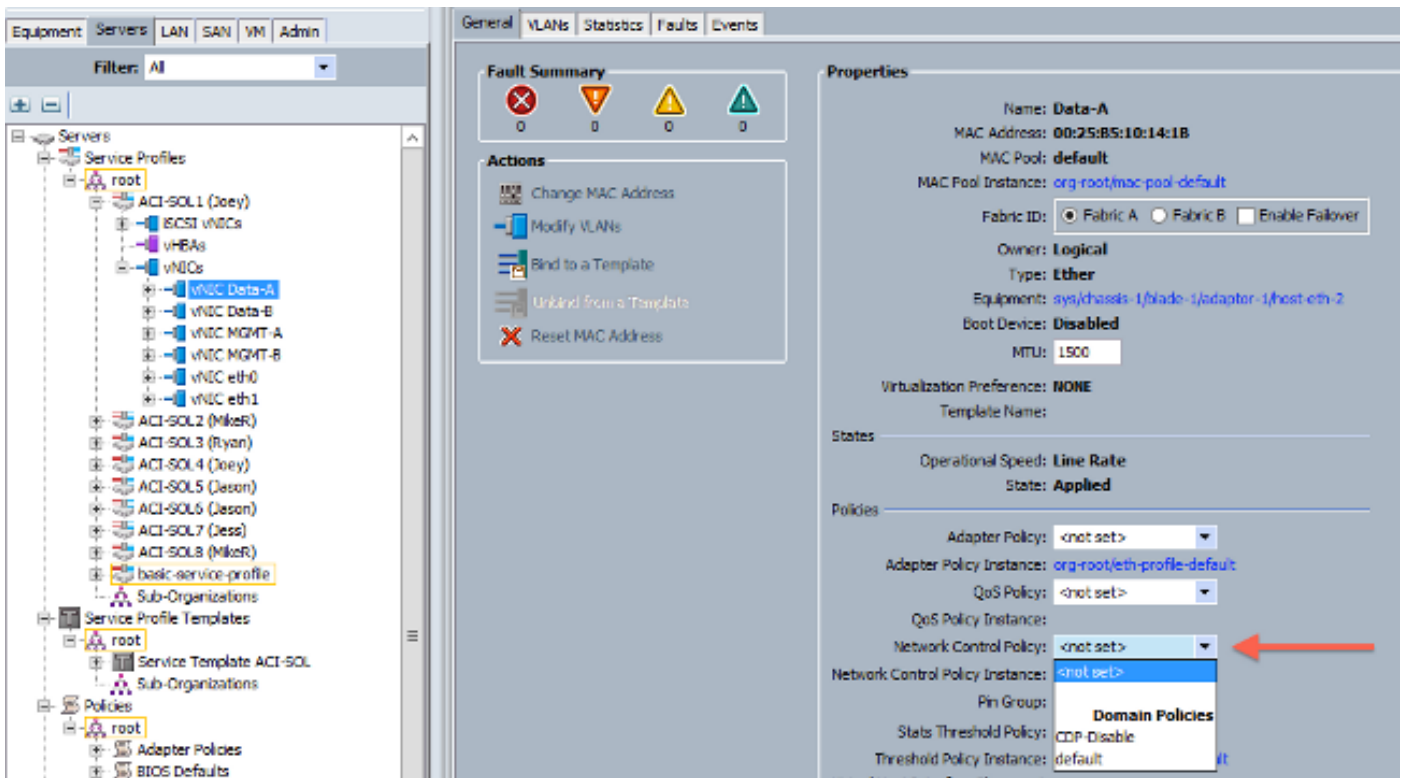
Wenn Sie UCS B in der ACI bereitstellen, können Sie das Discovery Protocol auswählen, das Sie zum Erkennen der Hosts verwenden möchten. In diesem Abschnitt erfahren Sie, wie Sie die einzelnen Typen im UCS Manager konfigurieren.

Cisco Discovery Protocol (CDP) ist auf der virtuellen UCS-Netzwerkschnittstellenkarte (vNIC) standardmäßig deaktiviert, da CDP deaktiviert ist. Um CDP zu aktivieren, können Sie entweder die Standard-Netzwerksteuerungsrichtlinie ändern oder eine neue Richtlinie mit aktiviertem CDP erstellen. Wenden Sie diese Richtlinie dann auf jede vNIC in jedem Serviceprofil an. In diesem Beispiel wird die standardmäßige Netzwerksteuerungsrichtlinie geändert, da alle Serviceprofile diese standardmäßig verwenden:



Wenn Sie eine andere Richtlinie verwenden, stellen Sie sicher, dass Sie diese Richtlinie den vNICs in jedem Serviceprofil hinzufügen:





In Version 2.2(4b) und höher unterstützt das UCS das Link Layer Discovery Protocol (LLDP) von den Fabric Interconnects bis hin zu den Blades. Dies bedeutet, dass Sie LLDP auch verwenden können, um die Hosts in vCenter und der Fabric zu erkennen, wenn Sie diese Version oder eine spätere Version ausführen. Die Konfiguration entspricht der oben beschriebenen Konfiguration, Sie aktivieren jedoch LLDP in beide Richtungen:



**Create Network Control Policy**

Name:

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

## Konfigurieren der vSwitch-Richtlinien auf dem APIC für UCS B

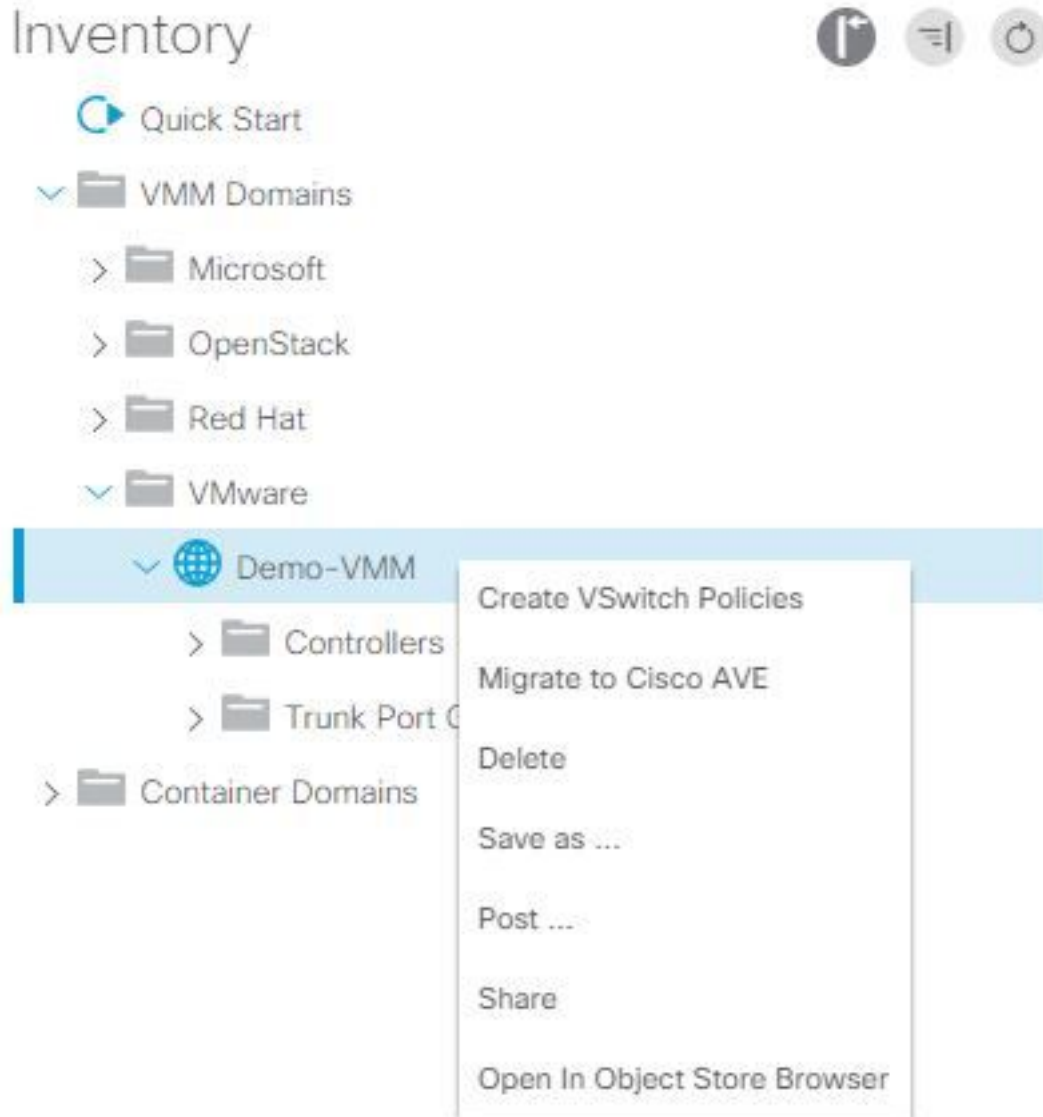
Auf dem DVS wird standardmäßig LLDP verwendet. Dies ist für alle Server geeignet, die LLDP unterstützen. Die Blades der UCS B-Serie unterstützen jedoch nur LLDP auf UCSM-Version 2.2(4b) und höher. Aus diesem Grund kann ESXi LLDP-Informationen nur dann an den APIC melden, wenn Sie sich im richtigen Code befinden.

Verwenden Sie als Alternative zu LLDP CDP, um die Hosts zu erkennen. Damit der DVS CDP verwenden kann, konfigurieren Sie eine vSwitch-Richtlinie auf der VMM-Domäne, für die CDP aktiviert und LLDP deaktiviert ist.

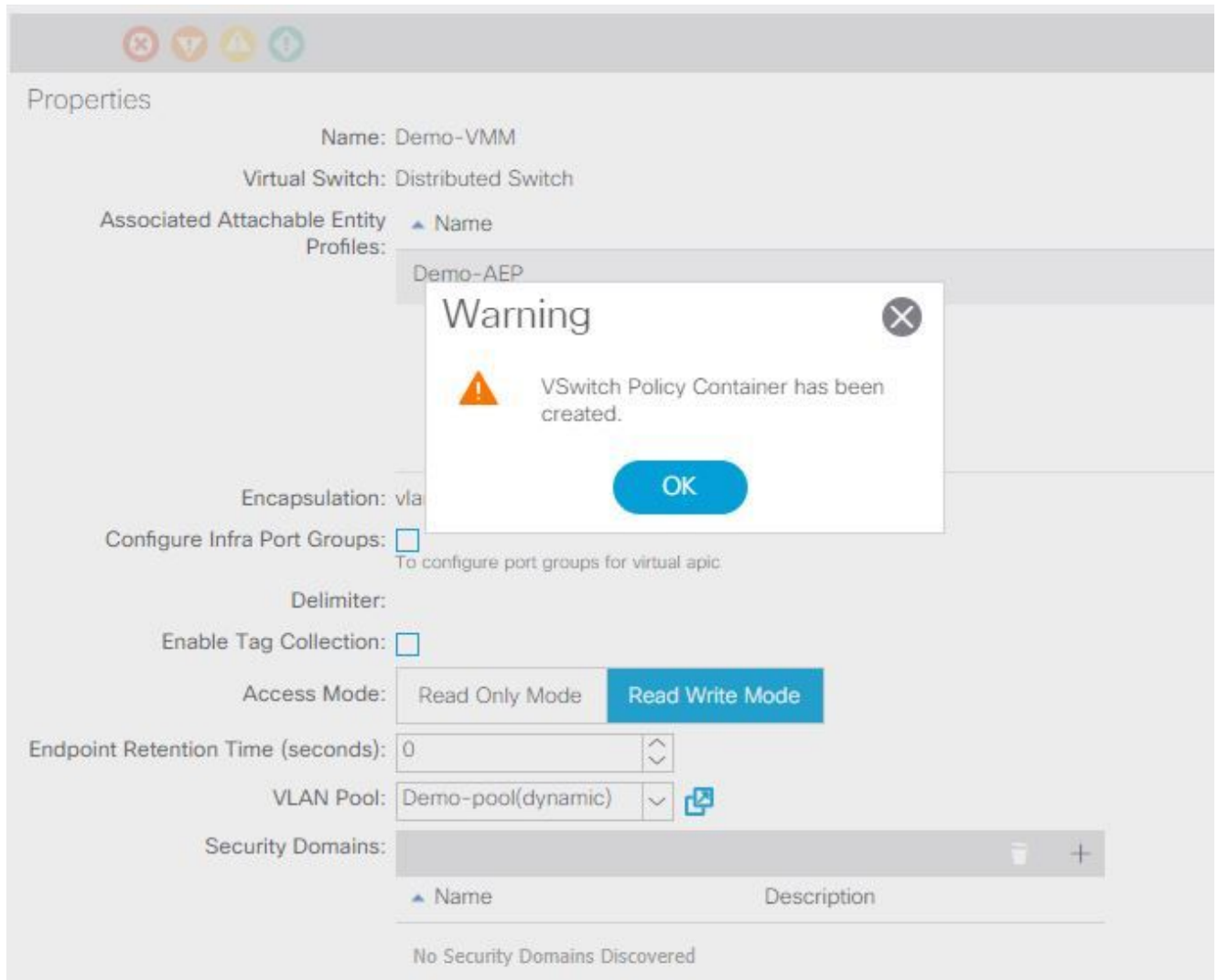
Darüber hinaus wird bei der Verwendung der UCS B-Serie nur der auf dem ursprünglichen virtuellen Port basierende Lastenausgleichsmechanismus unterstützt. Wenn Sie eine **MAC-Pinning**-Richtlinie konfigurieren, werden die Portgruppen programmiert, diesen Mechanismus zu verwenden. Dies ist sehr wichtig, um Paketverluste zu vermeiden.

1. Wählen Sie in der APIC-Benutzeroberfläche **Virtual Networking > VMM Domains > VMware**

> Configured Domain > Create VSwitch Policies aus.



2. Zu diesem Zeitpunkt wird eine Warnung angezeigt, dass eine Standard-VSwitch-Richtlinie erstellt wurde.

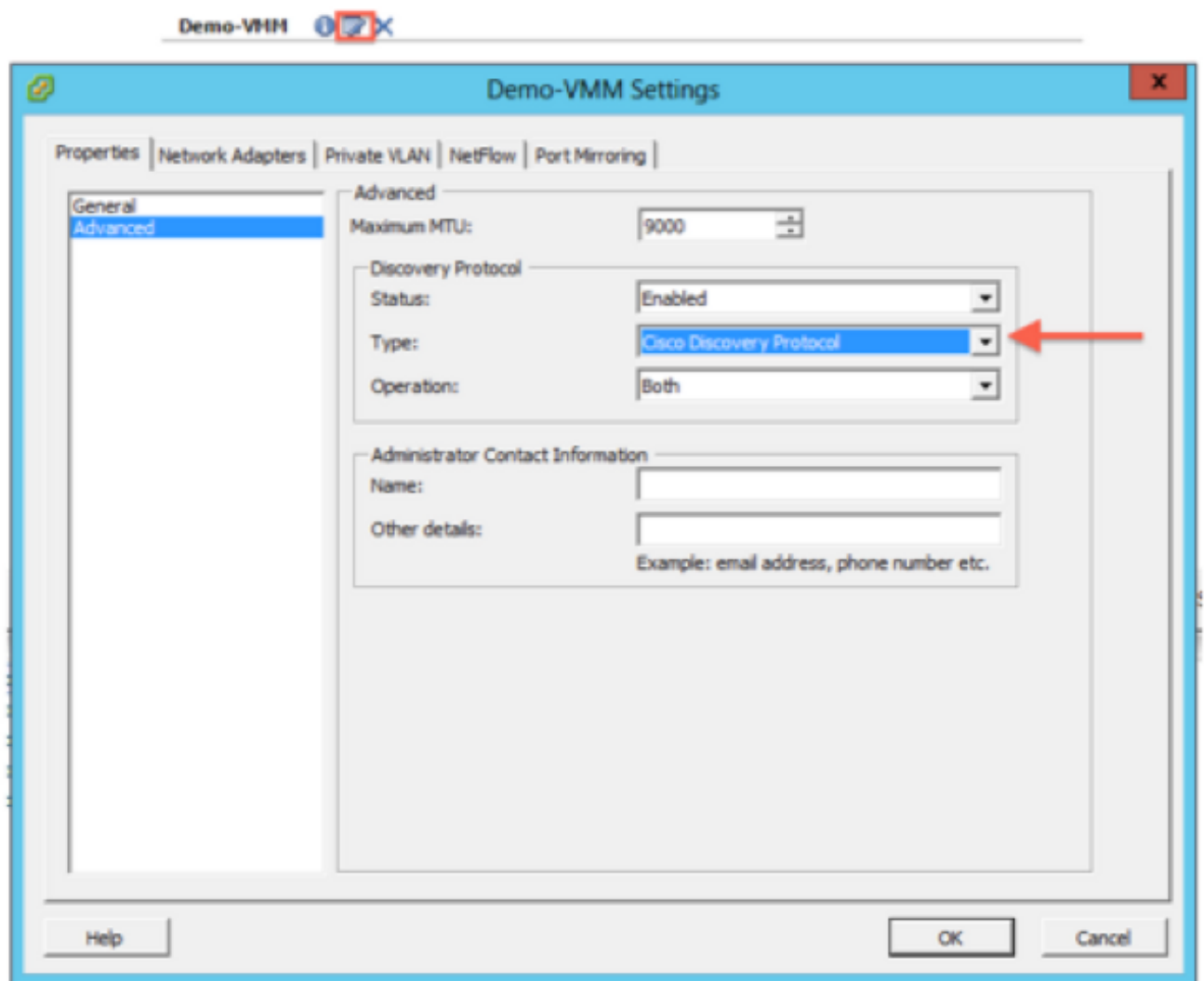


3. Akzeptieren Sie die Warnmeldung, und navigieren Sie zur Registerkarte **Vswitch Policy** unter der VMM Domain: Wählen oder erstellen Sie eine **CDP-Richtlinie**, in der **CDP aktiviert ist**. Wählen Sie eine **Port-Channel-Richtlinie** mit aktiviertem **MAC-Pinning-Modus** aus, oder erstellen Sie diese. Wählen oder erstellen Sie eine **LLDP-Richtlinie**, in der **CDP deaktiviert ist**. Klicken Sie auf **Senden**. **Hinweis:** Wenn Sie mit UCSM 2.2(4b) oder höher arbeiten und LLDP verwenden möchten, können Sie LLDP in dieser vSwitch-Richtlinie aktivieren, da das UCS dies unterstützt. Dieses Beispiel gilt nur für UCSM-Versionen, die LLDP nicht unterstützen, oder wenn CDP gewünscht ist. Wenn sowohl LLDP als auch CDP aktiviert sind, hat LLDP **Priorität**.

Domain - Demo-VMM



Wenn Sie auf **Senden** klicken, sehen Sie, dass der DVS im vCenter neu konfiguriert wird:



Sie können auch überprüfen, ob die vmnics CDP-Informationen von Fabric Interconnect sehen:

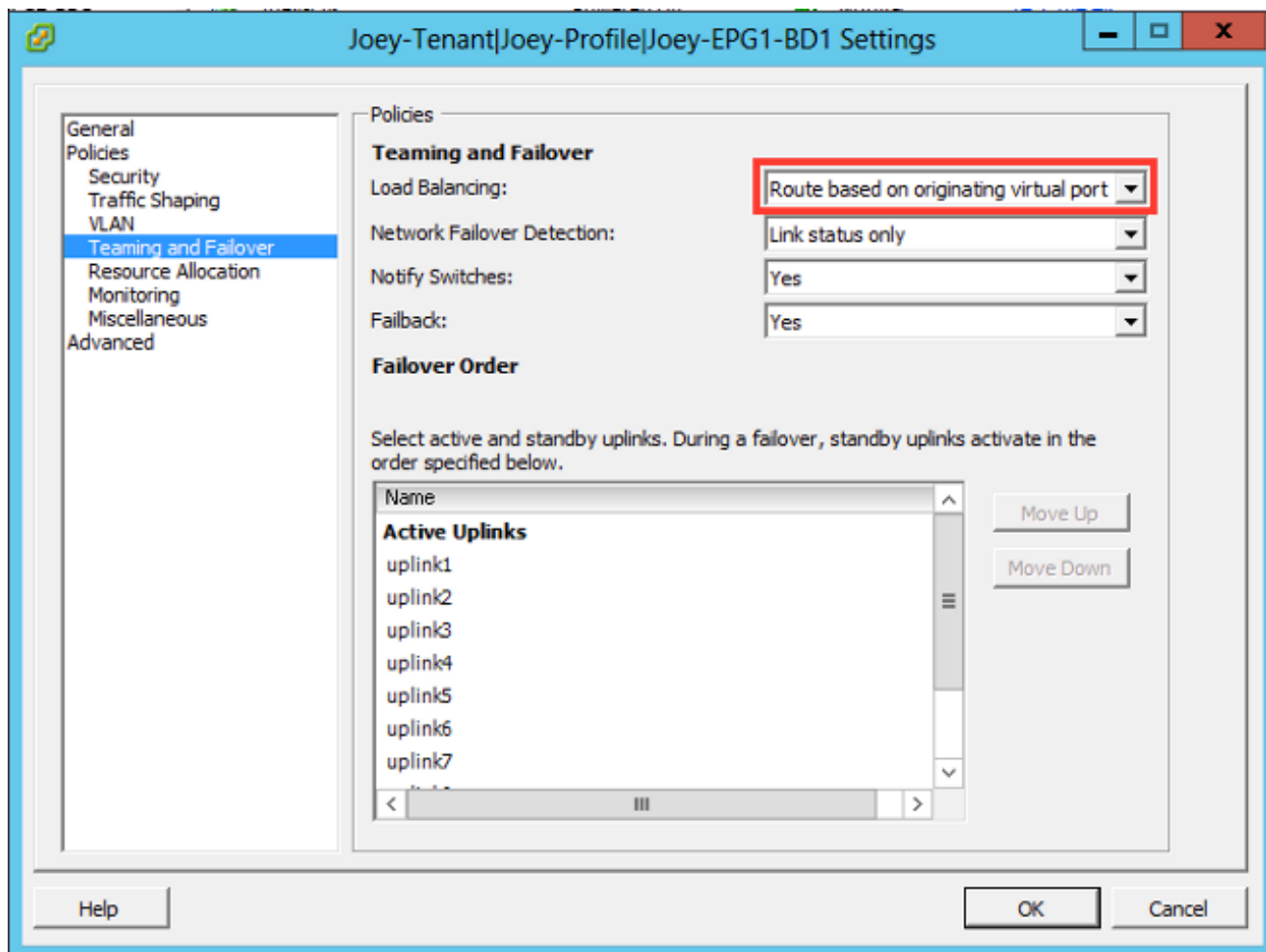
The screenshot shows a Cisco Discovery Protocol window with the following properties:

Version:	2
Timeout:	0
Time to live:	129
Samples:	1517
Device ID:	aci-sol-calo-ucsb-A(SSI18220541)
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. Vergewissern Sie sich, dass "Route based on origine virtual port" auf den Portgruppen programmiert ist. Klicken Sie mit der rechten Maustaste auf eine Port-Gruppe auf der Registerkarte Netzwerk, und bearbeiten Sie die Einstellung, um Folgendes zu überprüfen:



## Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Nachdem diese Änderungen vorgenommen wurden, sollte der APIC vom vCenter über die CDP-Informationen benachrichtigt werden. Überprüfen Sie dazu den Bestand der VMM-Domäne.

Wählen Sie in der APIC-Benutzeroberfläche **Virtual Networking > Inventory > VMM Domains > VMware > Domain > Controllers > vCenter > Hypervisors > Hypervisor > General** aus, um das Eigenschaftensfenster anzuzeigen.

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	0 0 0 0	1000 Mb	True	
vmnic1	EC:BD:1...	Down	0 0 0 0	unknown	Unknown	
vmnic2	04:62:7...	Up	0 0 0 0	10000 Mb	True	
vmnic3	04:62:7...	Up	0 0 0 0	10000 Mb	True	

Virtual Machines:

Name	Status
ASAv(rrangelth)	Powered Off
ASAv-transparent	Powered Off
ASAv-vmm	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.			

An diesem Punkt können Sie Ihre VM-Netzwerkeinstellungen ändern, um den Adapter der richtigen Portgruppe hinzuzufügen und die Verbindung zu testen. Pings sollten erfolgreich sein. Wenn Pings nicht erfolgreich sind, überprüfen Sie, ob alle Einstellungen in vCenter und im APIC für die CDP-Nachbareerkennung korrekt sind.

## Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.