# Configure Dell VxRail and ACI VMM Integration

## Contents

## Introduction

This document describes how Cisco Application Centric Infrastructure (ACI) is configured for Virtual Machine Manager (VMM) with Dell VxRail servers.

## Background Information

ACI can integrate with a variety of physical servers that utilize VMWare vSphere. Dell VxRail is an answer to a "turn-key" hyper-converged infrastructure. Dell VxRail utilizes VMWare vSAN to replicate data across multiple physical servers. In reality, VxRail has no special features that distinguish it from other vendors that utilize VMWare vSAN replication technology.

A VxRail deployment can be completed with a nested vSphere server (vSphere VM installed on the VxRail cluster) or with an external vSphere server. In this document, it is assumed that vSphere and VxRail are already installed. The processes to implement VMWare and Cisco VMM integration are not dependent on where in the infrastructure the vSphere server resides. The only network requirement is IP reachability to the vSphere server and Link Layer Discovery Protocol (LLDP) network discovery with the Dell VxRail ESXi servers.

Specifics to the VxRail deployment are not covered within this document. Please reference appropriate Dell documentation or technical support on how to deploy VxRail. This guide focuses on the network aspects of a pre-installed VxRail server cluster.

## vSphere Preparation

In a typical VxRail deployment, the VxRail installer creates a new VMware Distributed Switch (VDS) that the VxRail ESXi hosts are attached to. This VDS has several VM Port Groups (VLANs) and VMkernel interfaces (IP addresses).

**VxRail Default VMWare Port Groups**

| Name | Purpose |
| --- | --- |
| Management Network | ESXi Management Network |
| Virtual SAN | Replication Network for VSAN |
| vSphere vMotion | vMotion |
| VxRail Management | The isolated network used for VxRail node discovery |

When VxRail is deployed, the names of the default port group can have numbers appended to the end of them. The appended numbers can be safely removed.
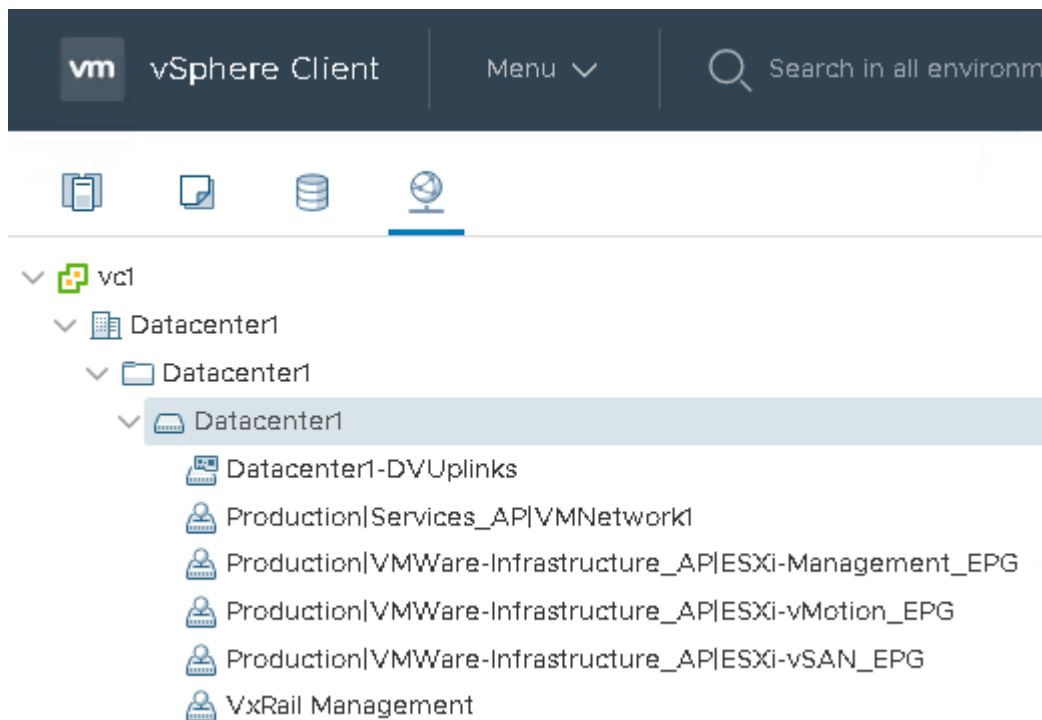
VxRail Distributed Switch:
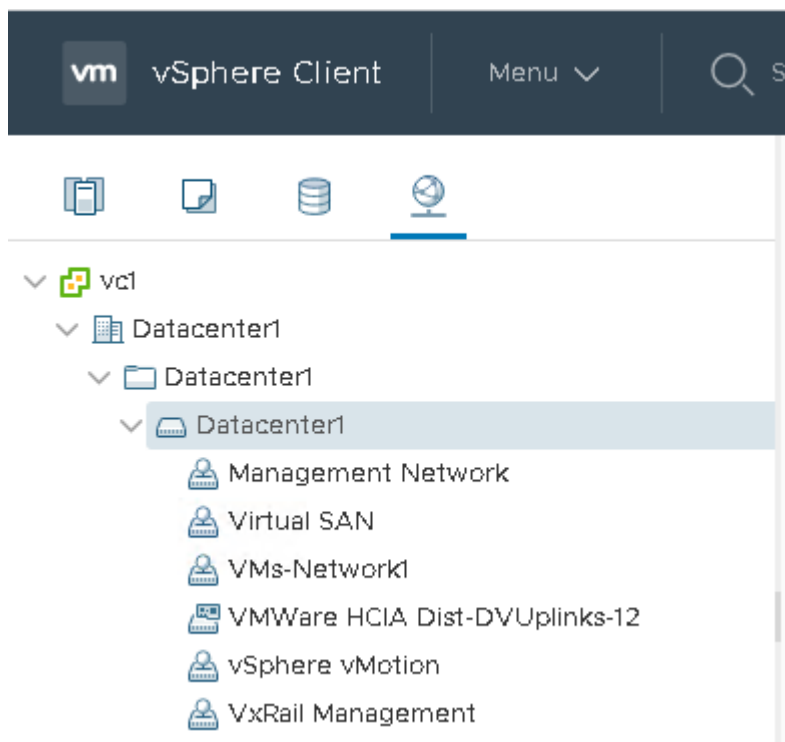


## Rename VMWare Port Groups

For VMM-integrated VMWare domains, when ACI creates a port group inside vSphere, ACI names the port group with a specific format: tenant|application|epgACI .

> **Note**: It is typically recommended to use the default, but this is not required. A custom port group name can be chosen when an EPG is deployed to vSphere if desired. If this approach is chosen, then great care must be taken that the EPGs are deployed with the exact port group names within the VMWare dvSwitch. If a custom ACI name is required, refer to Custom EPG Name Configuration and Cisco ACI in the Cisco ACI Virtualization Guide located on Cisco.com.

This document assumes that the default ACI name is used. In order to begin VxRail and ACI VMM integration, the default VMWare port groups must be renamed to match the default ACI name scheme. The only exception to this is the VxRail Management port group; this port group is not renamed to ACIâ€™s default because certain VxRail node addition scripts look for this port group name.

Example of VxRail Distributed Switch with Renamed Port Groups:



The first step of VxRail and ACI VMM integration is to standardize the name convention of default port groups.

By default, VxRail creates the VMWare Distributed Switch at the root of the Datacenter folder structure. To comply with the ACI name and expected folder structure, the VMWare administrator must create a folder named the same as the VMWare data center and move the VMWare distributed switch into the newly created folder. This move must not impact services, but changes must be executed within a scheduled maintenance window.

The data center, Network Folder, and dvSwitch must all have the same name. The various dvPortGroups are named as per the ACI tenant and EPG names.

## User Account with Minimum VMware vCenter Privileges

When you configure a service accountâ€™s VMware vCenter privileges, you allow the APIC to send VMware API commands to VMware vCenter for the creation of the port groups. This also allows ACI to relay all necessary alerts and gather VM information and inventory. Accounts can be Active Directory-integrated or local vCenter Single Sign On (SSO) credentials.

Refer to Cisco ACI Virtualization Guide on Cisco.com for specific permissions needed for this integration.

Assign this service account permissions to the VxRail ESXi cluster and dvSwitch, at a minimum.

> **Warning**: With ACI to VxRail integration it is critical to create an ACI dedicated service account for each VxRail cluster (not necessarily the VMWare cluster, but VxRail/vSAN cluster - which

must have a 1:1 relationship). This is because if there is ever a future desire to remove ACI and VxRail integration, the VMWare administrator must first remove the service account's permission from vCenter and then the ACI administrator remove the VMM Domain from ACI. This makes it so ACI cannot delete the VMWare distributed Switch (because ACI no longer has permission to do so) when the ACI VMM domain is deleted. If this dissociation is performed, it is also recommended to ensure that the account does not have an active login to vCenter at the time of ACI VMM domain deletion.

## dvSwitch Discovery Protocol Configuration

VMWare Distributed switches can use LLDP or CDP for the next-hop switch discovery protocol, but not both. Identify what the discovery protocol is for the default VMWare VxRail dvSwitch and ensure it is configured for "Both" under operation. This allows for proper neighbor discovery within ACI and ESXi.

To find this, the VMWare administrator can right-click on the VMWare dvSwitch and navigate to Settings > Edit Settings > Advanced . The Discovery Protocol can easily be identified, and the Operation can be changed to Both if not already set. Document the discovery protocol configured, as it is needed later in ACI.

Additionally, the VxRail VMWare dvSwitch version must be identified and documented under the dvSwitch Summary informational menu.

# ACI Configuration

Once the VMWare network objects have been named as per the ACI name standards it is time to begin the ACI read-only integration. The read-only integration tracks the standard ACI VMM-integration procedure, but with the only exception that the domain can be created as Read-Only.

## ACI Access Policy Configuration

The first step within ACI is to create the various standard ACI policy objects that are required when you create a new domain in ACI. Because the Virtual Domain is tied to a physical VxRail cluster that already exists and there can be some overlap between physical objects and virtual objects. For example, the Interface Policy Groups (IPGs) used for the physical ESXi connections are probably configured as a physical domain. This must not be changed.

One thing that is needed is to ensure that these IPGs have the necessary CDP or LLDP policies applied. Generally, LLDP and CDP can both be enabled on these IPGs, which is the recommended approach herein. However, it is critical that the aforementioned dvSwitch discovery policy is enabled within the IPG so that proper host discovery policy occurs between VMWare and ACI.

Take note of the AEP that is referenced within the IPG. Since VxRail is deployed as a cluster there must be, but it is not required, a dedicated AEP for this VxRail cluster. This AEP is later referenced by the VMWare domain that is to be created in future sections of this document.

### Dynamic VLAN Pool

VMWare VMM domains require that a Dynamic VLAN pool be used. If the current VxRail VLAN pool is not dynamic, then a new pool needs to be created and migrated to. It is possible to have a static range of VLANs within a Dynamic VLAN pool, which is the case in a migration scenario. These static VLANs are

vMotion, ESXi Management, VxRail Management, and vSAN. All other VM-based port groups can be dynamically assigned, but they can be static.

The document does not cover migration from a Static VLAN pool to a Dynamic VLAN pool. Please contact Cisco TAC for assistance.

## Create VMware VMM Domain without Controllers

Within ACI, under Virtual Networking, and then VMWare: select VMWare and select Create vCenter domain. When you create the domain, the Virtual Switch Name must match the name of the previously modified VMWare Distributed Switch. Ensure the names are the same. Additionally, ensure that the â€œAccess Modeâ€� is changed from Read Write Mode to Read Only Mode.

### Create the vCenter Domain



## Deploy EPGs to Newly Created VMM Domain

At this point, the very basic VMM domain has been created, but there has not been a VMWare credential or controller created. Because the dvSwitch already exists in vCenter, the EPGs must first be deployed to the empty VMM domain. Navigate to Tenants, and deploy the newly created VMM domain to every EPG that currently exists in VxRAIL. At a minimum, these networks must exist within a VxRail cluster: ESXi Management, Virtual SAN, vMotion, and VxRail Management.

Deploy these EPGs with a static port encapsulation and reutilize the VLAN that is already on the EPG for the static path. Essentially, this process makes a copy of the EPGâ€™s configuration from the VxRailâ€™s

physical domain configuration to the VMM configuration. It is also recommended, for most situations, that Pre-provision is selected as the Resolution Immediacy for these VxRail infrastructure networks.

**Deploy EPGs to the VMM Domain**
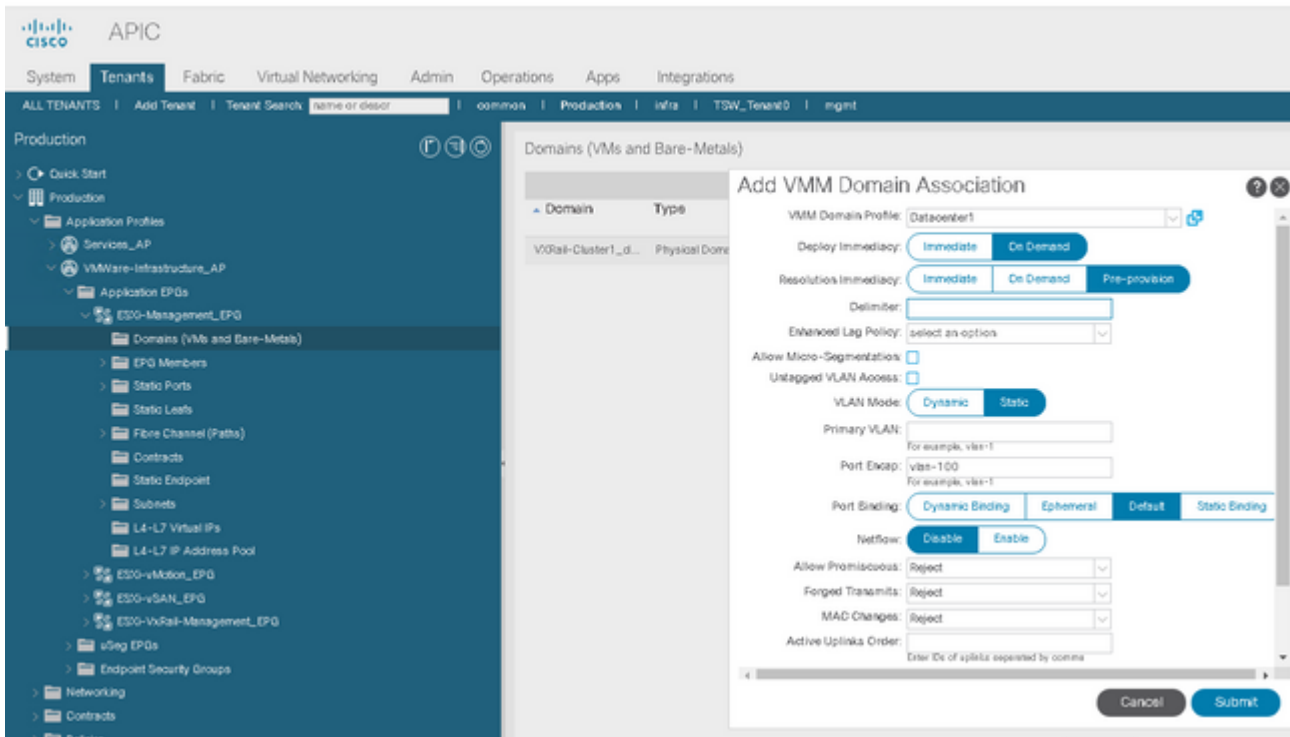


If you do not use the default ACI name convention for VMWare port groups then ensure that the custom port-group names match what is currently used in vCenter. One example of this can be the VxRail Management Network.

**Specify Custom EPG Name**
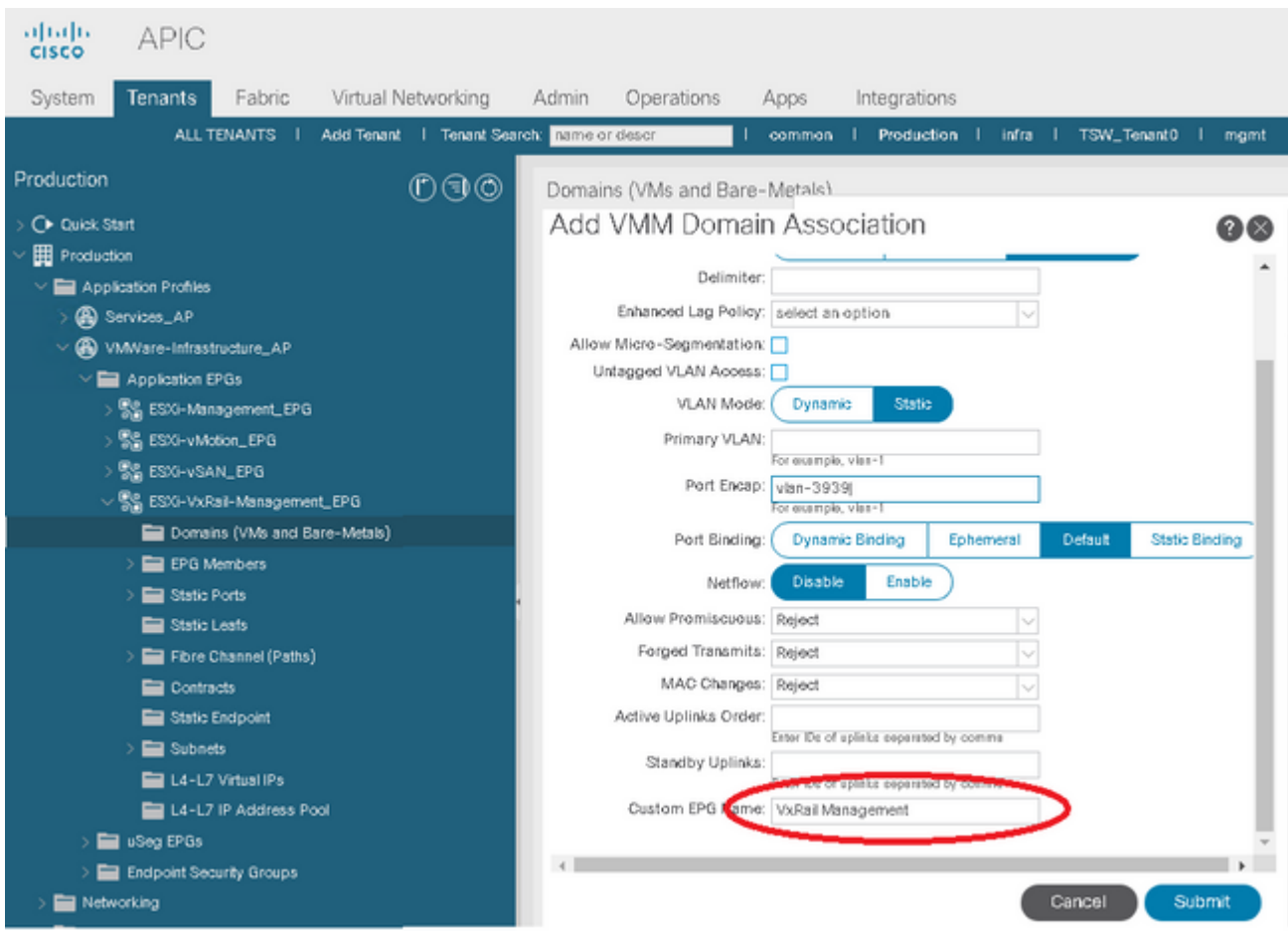
**Note**: When EPGs are deployed to a Read-Only VMM domain there can be multiple ACI F0565 Faults for the VMM Domain. This is normal for a Read-Only domain and can safely be ignored.

## Create vCenter Credentials and Controller

Once the VMM domain has been created and all the EPGs select the Controllers menu object to create the vCenter Credential. This credential must be the same one(s) that were granted access to vCenter in previous steps.

After the credential has been created, create the vCenter Controller. When you create the vCenter controller ensure that the DVS Version matches the dvSwitch in vCenter. Use the previously created service account for the credential.

At this point, ACI can see the ESXi hypervisors and any VMs attached to the dvSwitch port groups.

Completed Read Only integration:
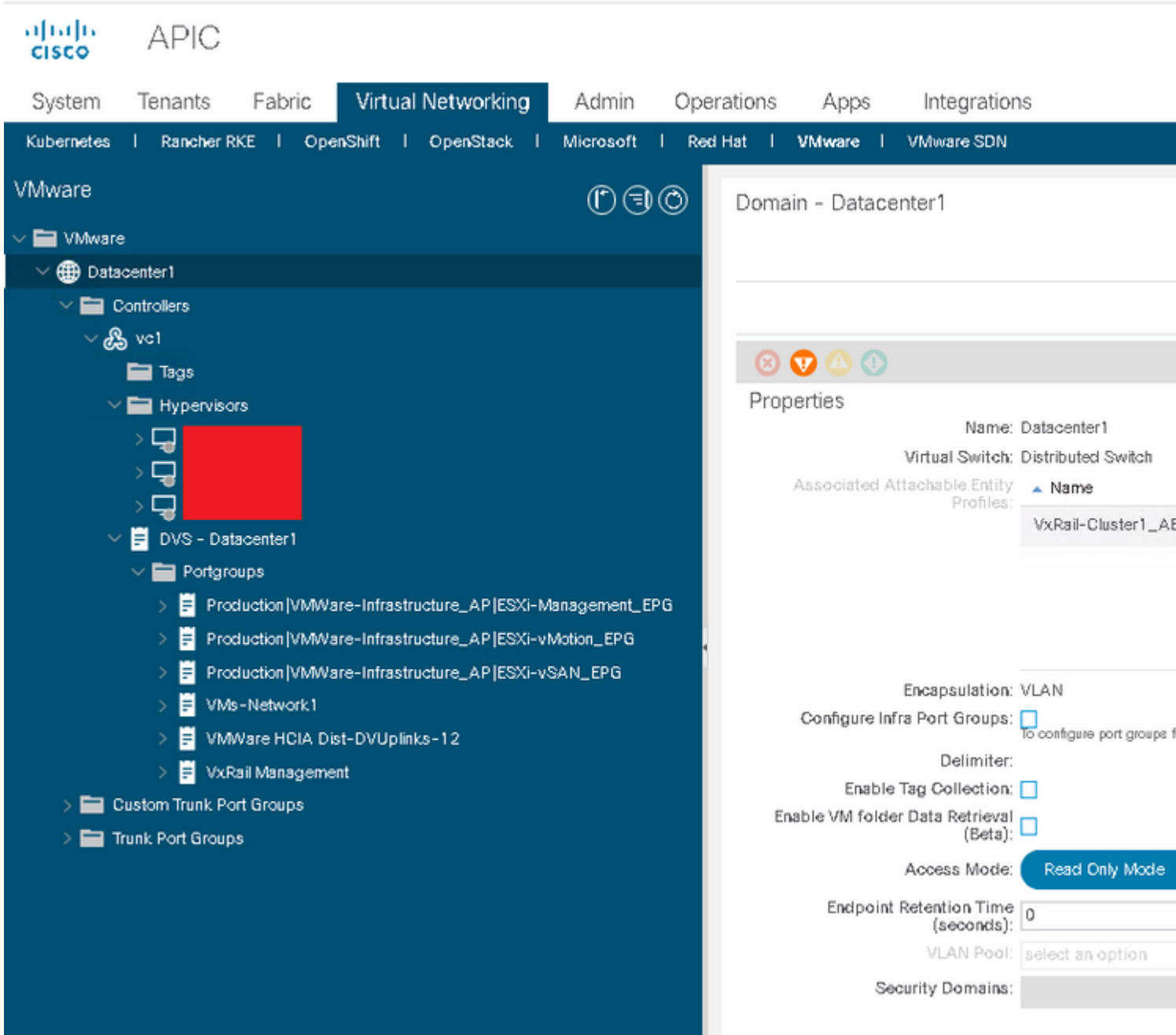
## Specify vSwitch Network Policies

At a minimum, you must set the dvSwitch discovery policies before you elevate the VMM Domain to Read Write. VxRail systems are typically configured as trunks with no port channels, so this might not be necessary. Specify an LLDP and CDP policy. Ensure that these policies align, as close as possible, with how the VMWare dvSwitch is configured. Specify the MTU policy; 9000 is recommended. Enhanced Network LAG policies are typically not used in VxRail deployments.

Select Submit when completed.

**vSwitch Network Policy Configuration**
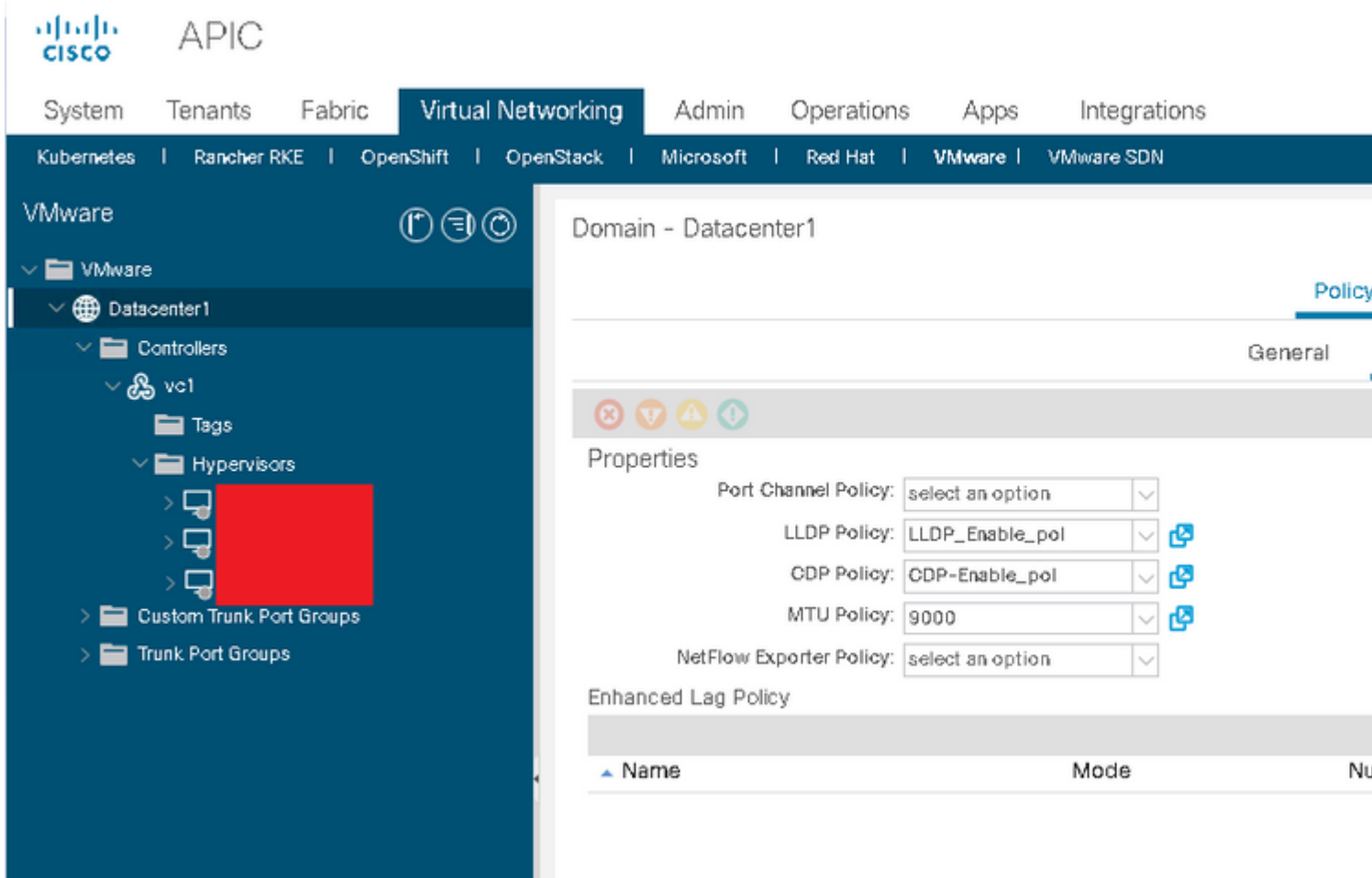
## Promote VMM Domain to Read Write

**Warning**: Prior to the promotion of the VMM domain from Read Only to Read Write, it is recommended that a complete vCenter backup be taken. It is also recommended to export the dvSwitch from the VMWare vCenter UI. Lastly, it is recommended that an ACI snapshot be taken.

**Warning**: When you change the Access Mode to Read Write Mode, ensure that you choose a VLAN Pool before you select Submit. It is recommended to double-check that the VLANs used by the dvPort-Group exist in this pool.

**Warning**: A VMM Domain can only be changed from Read Only Mode to Read Write Mode once. It cannot be changed from Read Write to Read Only. To revert to Read Only the domain needs to be deleted and recreated (or restored from a backup/snapshot).

To promote the VMM Domain from Read Only Mode to Read Write Mode change the Access Mode and ensure a VLAN Pool is selected. Select  Submit   when complete. It is unlikely for this step to cause traffic disruption, but perform any maintenance within a maintenance window. At this point, EPGs can be deployed directly from ACI into VMWareâ€™s dvSwitch.

Promote VMM domain to Read Write:

Domain - Datacenter1

General     VSwitch Policy     Faults     History
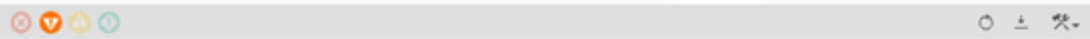
Properties

Name: Datacenter1
Virtual Switch: Distributed Switch
Associated Attachable Entity
Profiles:       ▲ Name
                VxRail-Cluster1_AEP

Encapsulation: vlan
Configure Infra Port Groups: ☐
                             To configure port groups for virtual epic
Delimiter:
Enable Tag Collection: ☐
Enable VM folder Data Retrieval
(Beta): ☐
                                            1
Access Mode:    Read Only Mode   **Read Write Mode**
Endpoint Retention Time          2
(seconds):     0
VLAN Pool:     VMWare_pool(dynamic)  ▼
                                                          3
Security Domains:                              🗑  +

                                    Show Usage    Reset    **Submit**