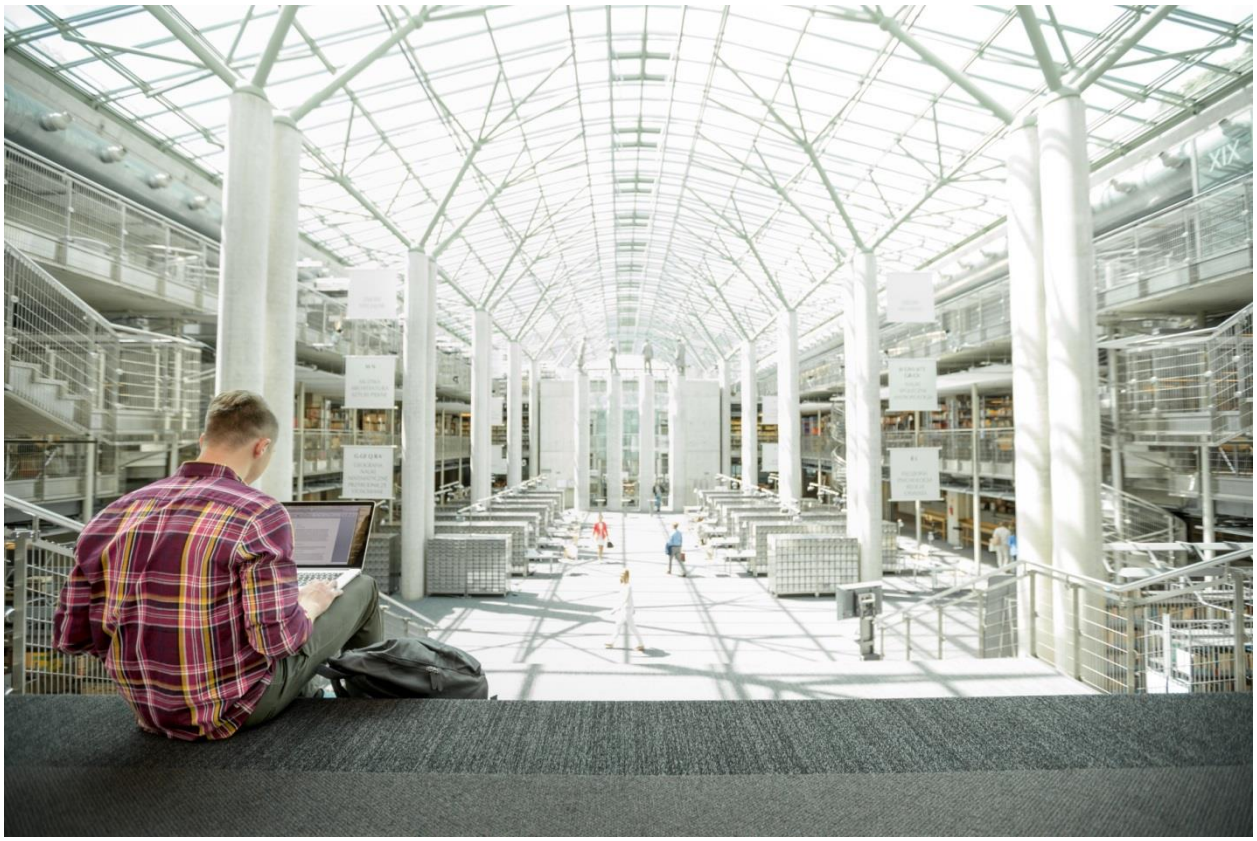


VersaStack Data Center with Cisco Application Centric Infrastructure

Deployment Guide for Cisco ACI and IBM FlashSystem V9000 and Storwize V7000 Unified with vSphere 6.0

Last Updated: September 30, 2016

About Cisco Validated Designs

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit

http://www.cisco.com/go/designzone.

Table of Contents

Executive Summary

Cisco Validated Designs (CVDs) deliver systems and solutions that are designed, tested, and documented to facilitate and improve customer deployments. These designs incorporate a wide range of technologies and products into a portfolio of solutions that have been developed to address the business needs of the customers and to guide them from design to deployment.

Customers looking to deploy applications using shared data center infrastructure face a number of challenges. A recurrent infrastructure challenge is to achieve the levels of IT agility and efficiency that can effectively meet the business objectives. Addressing these challenges requires having an optimal solution with the following key characteristics:

- **Availability**: Helps ensure applications and services availability at all times with no single point of failure
- **Flexibility**: Ability to support new services without requiring underlying infrastructure modifications
- **Efficiency**: Facilitate efficient operation of the infrastructure through re-usable policies
- **Manageability**: Ease of deployment and ongoing management to minimize operating costs
- **Scalability**: Ability to expand and grow with significant investment protection
- **Compatibility**: Minimize risk by ensuring compatibility of integrated components

Cisco and IBM have partnered to deliver a series of VersaStack solutions that enable strategic data center platforms with the above characteristics. VersaStack solution delivers an integrated architecture that incorporates compute, storage and network design best practices thereby minimizing IT risks by validating the integrated architecture to ensure compatibility between various components. The solution also addresses IT pain points by providing documented design guidance, deployment guidance and support that can be used in various stages (planning, designing and implementation) of a deployment.

The Cisco Application Centric Infrastructure (ACI) based VersaStack solution, covered in this CVD, delivers a converged infrastructure platform specifically designed for software defined networking (SDN) enabled data centers. The design showcases:

- ACI enabled Cisco Nexus 9000 switching architecture
- Cisco Unified Compute System (UCS) servers with Intel Broadwell processors
- Storage designs covering both IBM Storwize V7000 Unified and IBM FlashSystem V9000 storage systems
- VMware vSphere 6.0U1b hypervisor
- Cisco MDS Fibre Channel (FC) switches for SAN connectivity

Solution Overview

Introduction

VersaStack solution is a pre-designed, integrated and validated architecture for the data center that combines Cisco UCS servers, Cisco Nexus family of switches, Cisco MDS fabric switches and IBM Storwize and FlashSystem Storage Arrays into a single, flexible architecture. VersaStack is designed for high availability, with no single points of failure, while maintaining cost-effectiveness and flexibility in design to support a wide variety of workloads.

VersaStack design can support different hypervisor options, bare metal servers and can also be sized and optimized based on customer workload requirements. VersaStack design discussed in this document has been validated for resiliency (under fair load) and fault tolerance during system upgrades, component failures, and partial as well as complete loss of power scenarios.

VersaStack with ACI solution is designed to simplify the data center evolution to a shared cloud-ready infrastructure based on an application driven policy model. Cisco ACI integration with VersaStack platform delivers an application centric architecture with centralized automation that combines software flexibility with the hardware performance.

Audience

The intended audience of this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, partner engineering, and customers who want to take advantage of an infrastructure built to deliver IT efficiency and enable IT innovation.

Purpose of this document

This document provides step by step configuration and implementation guidelines for setting up VersaStack with ACI system. The following design elements distinguish this version of VersaStack from previous models:

- Validation of the Cisco ACI release 1.3 with IBM FlashSystem V9000 and IBM Storwize V7000 Unified
- Support for the Cisco UCS release 3.1 and Intel Broadwell based M4 servers
- Support for IBM software release 7.6.0.4 and IBM File Module software release 1.6.1
- Validation of IP-based storage design supporting both NFS and iSCSI based storage access
- Support for Fiber Chanel storage utilizing Cisco MDS 9148S
- Application design guidance for multi-tiered application using Cisco ACI application profiles and policies
- Support for application segregation utilizing ACI multi-tenancy
- Integration of Cisco ASA firewall appliance for enhanced application security

For more information on previous VersaStack models, please refer the VersaStack guides at:

http://www.cisco.com/c/en/us/solutions/enterprise/data-center-designs-cloud-computing/versastack-designs.html

Solution Design

Architecture

VersaStack with Cisco ACI architecture aligns with the converged infrastructure configurations and best practices as identified in the previous VersaStack releases. The system includes hardware and software compatibility support between all components and aligns to the configuration best practices for each of these components. All the core hardware components and software releases are listed and supported on both:

Cisco compatibility list:

http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html

IBM Interoperability Matrix:

http://www-03.ibm.com/systems/support/storage/ssic/interoperability.wss

The system supports high availability at network, compute and storage layers such that no single point of failure exists in the design. The system utilizes 10 and 40 Gbps Ethernet jumbo-frame based connectivity combined with port aggregation technologies such as virtual port-channels (vPC) for non-blocking LAN traffic forwarding. A dual SAN 8/16 Gbps environment provides redundant storage access from compute devices to the storage controllers.

Physical Topology

This VersaStack with Cisco ACI solution utilizes Cisco UCS platform with Cisco UCS B200 M4 half-width blades and Cisco UCS C220 M4 rack mount servers connected and managed through the Cisco UCS 6248UP Fabric Interconnects and integrated UCS manager. These high performance servers are configured as stateless compute nodes where VMware ESXi 6.0 U1b hypervisor is loaded using SAN (iSCSI and FC) boot. The boot disks to store the ESXi hypervisor image and configuration along with the block and file based datastores to host application virtual machines (VMs) are provisioned on the IBM storage devices.

As in the non-ACI designs of VersaStack, link aggregation technologies play an important role in VersaStack with ACI solution providing improved aggregate bandwidth and link resiliency across the solution stack. The IBM Storwize V7000 Unified File Modules, Cisco UCS, and Cisco Nexus 9000 platforms support active port channeling using 802.3ad standard Link Aggregation Control Protocol (LACP). In addition, the Cisco Nexus 9000 series features virtual Port Channel (vPC) capability which allows links that are physically connected to two different Nexus devices to appear as a single "logical" port channel. Each Cisco UCS FI is connected to both the Cisco Nexus 9372 leaf switches using virtual port-channel (vPC) enabled 10GbE uplinks for a total aggregate bandwidth of 40GBps. Additional ports can be easily added to the design for increased bandwidth. Each Cisco UCS 5108 chassis is connected to the FIs using a pair of 10GbE ports from each IO Module for a combined 40GbE uplink. Each of the Cisco UCS C220 servers connect directly into each of the FIs using a 10Gbps converged link for an aggregate bandwidth of 20Gbps per server.

To provide the storage system connectivity, this deployment guide covers two different storage connectivity options:

- **Option 1**: iSCSI based storage design validated for IBM FlashSystem V9000
- **Option 2**: FC and NFS based storage design validated for IBM Storwize V7000 Unified

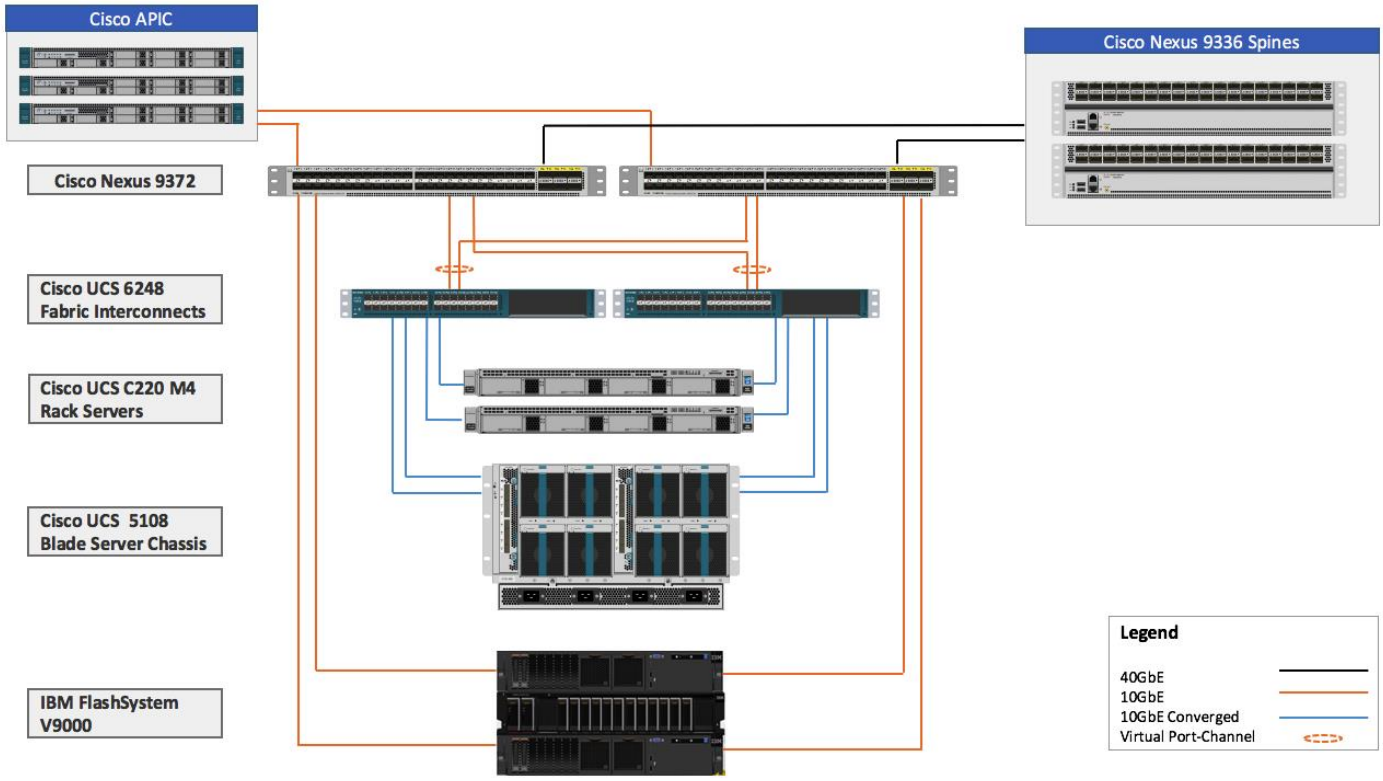
While both IBM FlashSystem V9000 and IBM Storwize V7000 Unified support iSCSI and FC connectivity, the storage connectivity models presented in this design guide are only intended to provide a reference connectivity model. All the possible storage connectivity designs on different controllers are not covered.

iSCSI based storage design with IBM FlashSystem V9000

IBM FlashSystem V9000 based VersaStack design option is shown in Figure 1 below. This design utilizes an all-IP based storage access model where IBM FlashSystem V9000 is connected directly to the Cisco Nexus 9372 leaf switches without requiring Fiber based switching infrastructure*. A10GbE port from each IBM FlashSystem V9000 controller is connected to each of the two Nexus 9372 leaf switches providing an aggregate bandwidth of 40Gbps.

* Fibre Channel switching infrastructure is required for IBM V9000 controller and storage enclosure connectivity

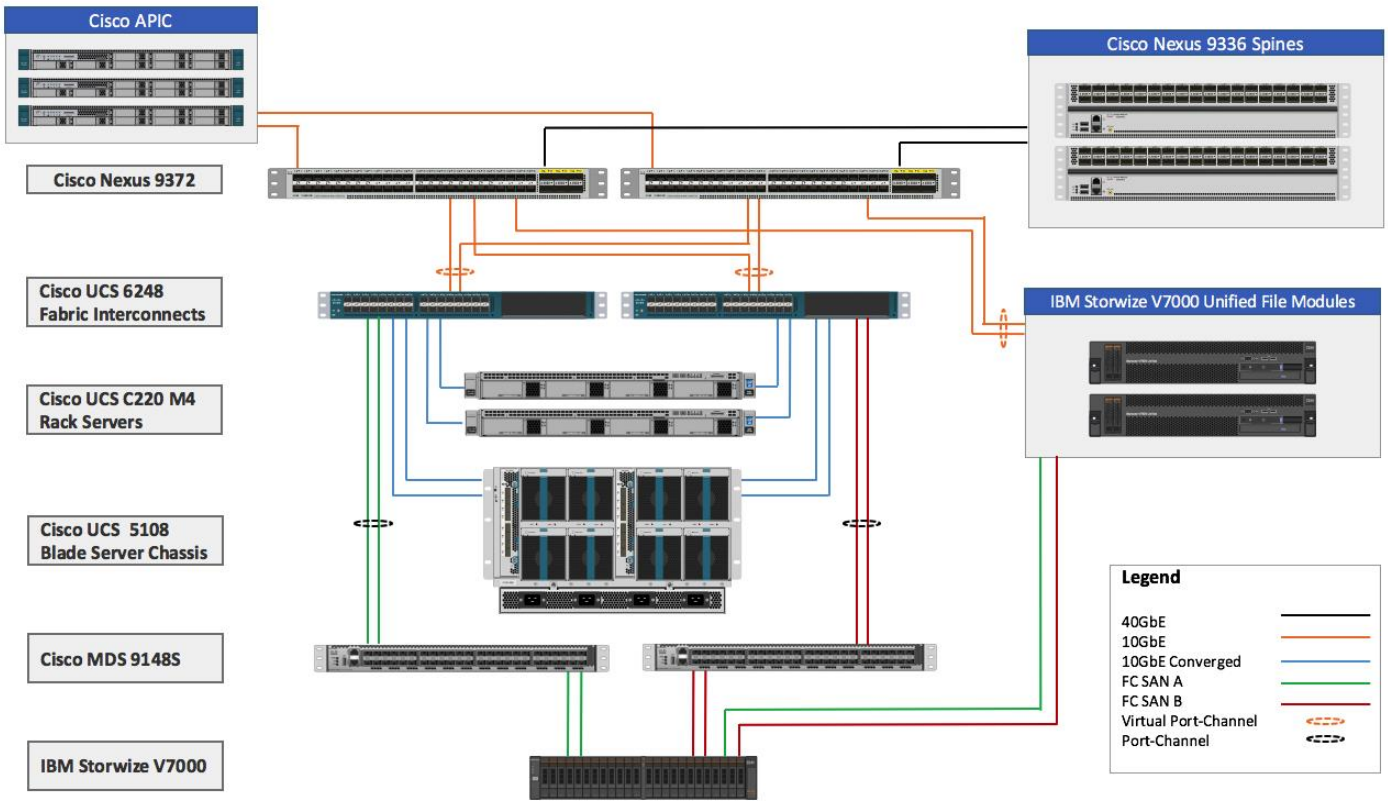
Figure 1 iSCSI based storage design with IBM FlashSystem V9000



FC and NFS based storage design with IBM Storwize V7000 Unified

IBM Storwize V7000 unified based VersaStack design option is shown in Figure 2 below. This design utilizes an FC based storage access model where IBM Storwize V7000 controller is connected to the Cisco UCS Fabric Interconnects through a dedicated Cisco MDS 9148S based redundant FC fabric. This design also covers NFS based storage connectivity by utilizing IBM Storwize V7000 Unified File Modules. The IBM Storwize V7000 Unified File Modules are connected to the Cisco Nexus 9372 leaf switches using 10GbE connectivity as shown below.

Figure 2 FC and NFS based storage design with IBM Storwize V7000 Unified



The reference architecture covered in this document leverages:

- One Cisco UCS 5108 Blade Server chassis with 2200 Series Fabric Extenders (FEX)
- Two* Cisco UCS B200-M4 Blade Servers
- Two* Cisco UCS C220-M4 Rack-Mount Servers
- Two Cisco UCS 6248UP Fabric Interconnects (FI)
- Three Cisco Application Policy Infrastructure Controllers (APIC-M2)
- Two Cisco Nexus 9336 ACI Spine Switches
- Two Cisco Nexus 9372 ACI leaf Switches
- Two Cisco MDS 9148S Fabric Switches
- One dual node IBM FlashSystem V9000
- One dual controller IBM Storwize V7000 Unified
- Two IBM Storwize V7000 Unified File Modules
- VMware vSphere 6.0 update 1b
- Cisco Application Virtual Switch (AVS) **

* The actual number of servers in customer environment will vary.

** This deployment guide covers both VMware Virtual Distributed Switch (VDS) and Cisco AVS.

This document guides customers through the low-level steps for deploying the base architecture. These procedures cover everything from physical cabling to network, compute and storage device configurations.

For detailed information regarding the design of VersaStack, see:
http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/versastack_aci_vmw6_design.html

Software Revisions

Table 1 below outlines the hardware and software versions used for the solution validation. It is important to note that Cisco, IBM, and VMware have interoperability matrices that should be referenced to determine support for any specific implementation of VersaStack. See the following links for more information:

- IBM System Storage Interoperation Center
- Cisco UCS Hardware and Software Interoperability Tool

Table 1 Hardware and software revisions

Layer	Device	Image	Comments
Compute	Cisco UCS Fabric Interconnects 6200 Series, Cisco UCS B200 M4, Cisco UCS C220 M4	3.1(1g)	Includes the Cisco UCS-IOM 2208XP, Cisco UCS Manager, and Cisco UCS VIC 1340
	Cisco ESXi eNIC Driver	2.3.0.7	Ethernet driver for Cisco VIC
	Cisco ESXi fnic Driver	1.6.0.25	FCoE driver for Cisco VIC
Network	Cisco Nexus Switches	11.3(2f)	iNXOS
	Cisco APIC	1.3(2f)	ACI release
	Cisco MDS 9148S	6.2(13b)	FC switch firmware version
Storage	IBM FlashSystem V9000	7.6.0.4	Software version
	IBM Storwize V7000 Unified	7.6.0.4	Software version
	IBM Storwize V7000 Unified File Modules	1.6.1	Software version
Software	VMware vSphere ESXi	6.0 update1b	Software version
	VMware vCenter	6.0 update 1b	Software version
	Cisco AVS	5.2(1)SV3(1.25)	Software version

Configuration Guidelines

This document provides details for configuring a fully redundant, highly available configuration. Therefore, appropriate references are provided to indicate the component being configured at each step, such as 01 and 02 or A and B. For example, the Cisco UCS fabric interconnects are identified as FI-A or FI-B. This document is intended to enable customers

and partners to fully configure the customer environment and during this process, various steps may require the use of customer-specific naming conventions, IP addresses, and VLAN schemes, as well as record appropriate MAC addresses.

This document covers network (ACI), compute (UCS), virtualization (VMware) and related storage configurations (host to storage system connectivity). For basic setup of IBM V7000 and IBM V9000 systems, the document will refer to existing IBM V7000 and IBM V9000 VersaStack documentation.

Physical Infrastructure

The information in this section is provided as a reference for cabling the equipment in an ACI with VersaStack environment. To simplify the cabling requirements, both IBM V9000 base iSCSI design covered in Figure 1 and IBM V7000 unified based FC/NFS design covered in Figure 2 is broken down into network, compute and storage related physical connectivity and shown below.

This document assumes that the out-of-band management ports are plugged into an existing management infrastructure at the deployment site. These interfaces will be used in various configuration steps.

Customers can choose interfaces and ports of their liking but failure to follow the exact connectivity shown in figures below will result in changes to the deployment procedures because specific port locations are used in various configuration steps

ACI Network Connectivity

Figure 3 and Table 3 provide physical connectivity details of the Cisco ACI network.

Figure 3 Physical Connectivity - ACI Network

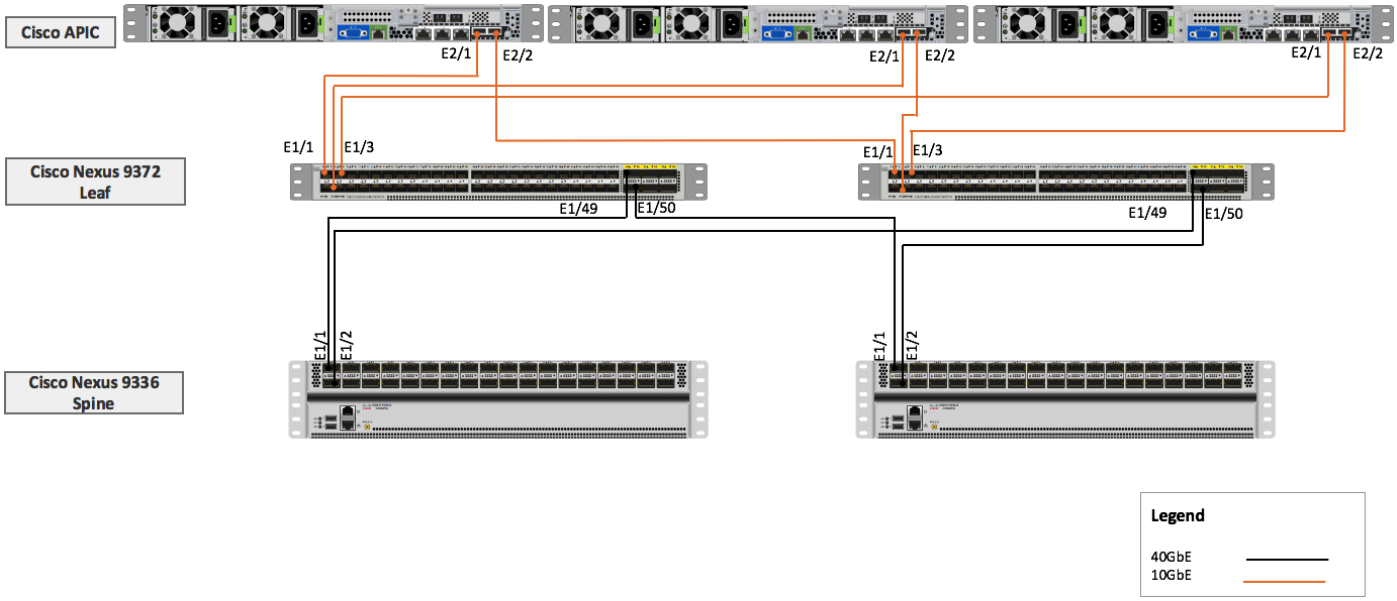


Table 2 – ACI Network Connectivity

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco APIC 1 -3	Mgmt./CIMC	GbE	Existing OOB Mgmt. Switch	Any
Cisco APIC 1 -3	Eth1/1	GbE	Existing OOB Mgmt. Switch	Any

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco APIC 1 -3	Eth1/2	GbE	Existing OOB Mgmt. Switch (select a different switch for redundancy)	Any
Cisco Nexus 9372 (A and B)	Mgmto	GbE	Existing OOB Mgmt. Switch	Any
Cisco Nexus 9372 A	Eth1/1	10GbE	Cisco APIC 1	Eth2/1
Cisco Nexus 9372 A	Eth1/2	10GbE	Cisco APIC 2	Eth2/1
Cisco Nexus 9372 A	Eth1/3	10GbE	Cisco APIC 3	Eth2/1
Cisco Nexus 9372 B	Eth1/1	10GbE	Cisco APIC 1	Eth2/2
Cisco Nexus 9372 B	Eth1/2	10GbE	Cisco APIC 2	Eth2/2
Cisco Nexus 9372 B	Eth1/3	10GbE	Cisco APIC 3	Eth2/2
Cisco Nexus 9372 A	Eth1/49	40GbE	Cisco Nexus 9336 A	Eth1/1
Cisco Nexus 9372 A	Eth1/50	40GbE	Cisco Nexus 9336 B	Eth1/1
Cisco Nexus 9372 B	Eth1/49	40GbE	Cisco Nexus 9336 A	Eth1/2
Cisco Nexus 9372 B	Eth1/50	40GbE	Cisco Nexus 9336 B	Eth1/2

IBM V9000 based iSCSI connectivity design

For physical connectivity details of an IP only iSCSI based connectivity design, Figure 4 through Figure 6 show Cisco UCS and IBM V9000 connectivity to the Cisco ACI infrastructure.

Figure 4 Cisco UCS connectivity for IBM V9000 based iSCSI design

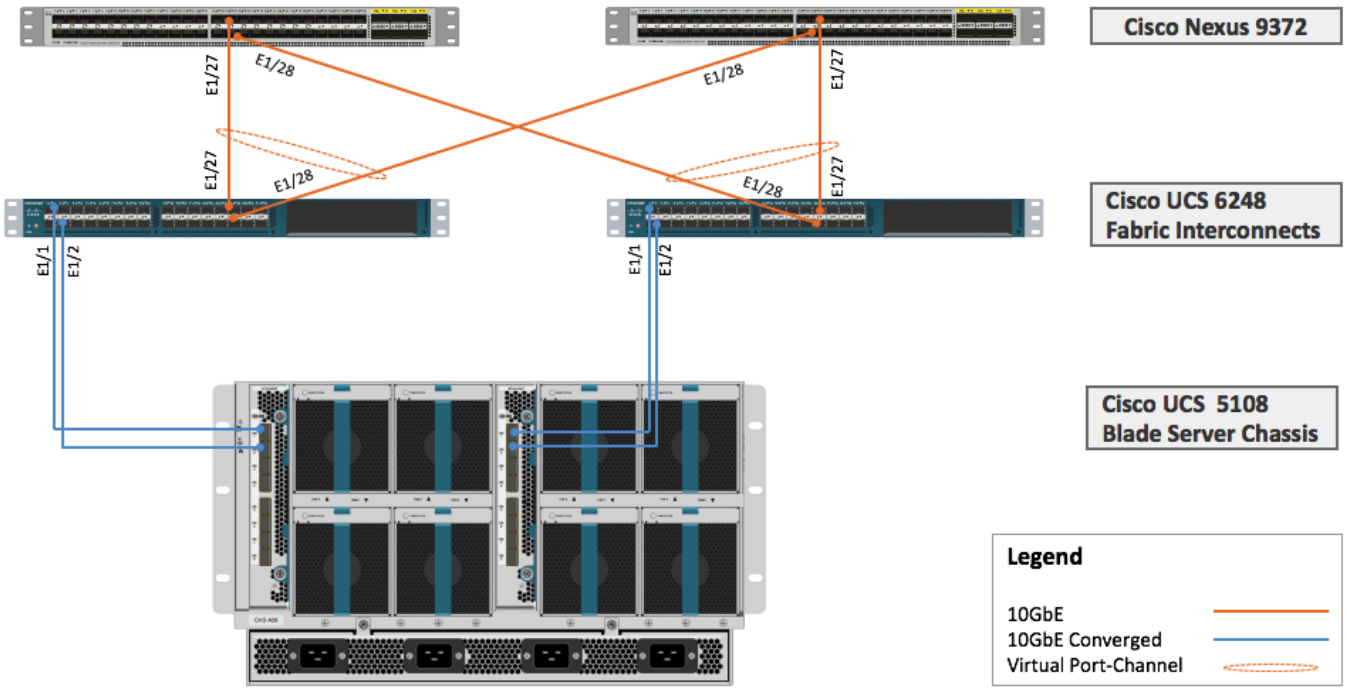


Table 3 UCS connectivity for iSCSI design

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric Interconnect A	Eth1/1	10GbE	Cisco UCS Chassis FEX A	IOM 1/1
Cisco UCS Fabric Interconnect A	Eth1/2	10GbE	Cisco UCS Chassis FEX A	IOM 1/2
Cisco UCS Fabric Interconnect A	Eth1/27	10GbE	Cisco Nexus 9372 A	Eth1/27
Cisco UCS Fabric Interconnect A	Eth1/28	10GbE	Cisco Nexus 9372 B	Eth1/28
Cisco UCS Fabric Interconnect B	Eth1/1	10GbE	Cisco UCS Chassis FEX B	IOM 1/1
Cisco UCS Fabric Interconnect B	Eth1/2	10GbE	Cisco UCS Chassis FEX B	IOM 1/2
Cisco UCS Fabric Interconnect B	Eth1/28	10GbE	Cisco Nexus 9372 A	Eth1/28
Cisco UCS Fabric Interconnect B	Eth1/27	10GbE	Cisco Nexus 9372 B	Eth1/27

Figure 5 Cisco UCS C-Series server connectivity to UCS Fabric Interconnects

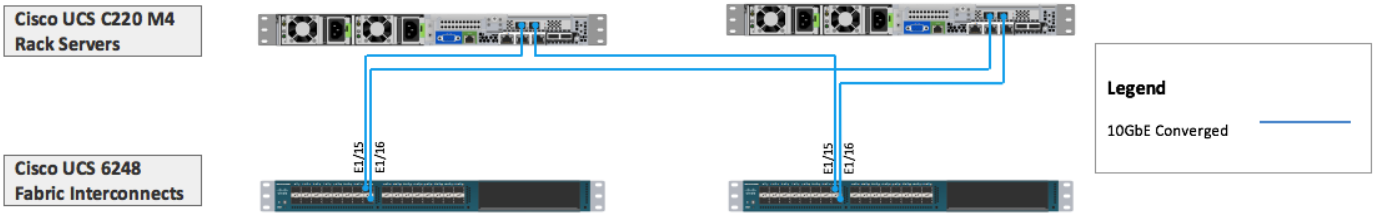


Table 4 Cisco UCS C-Series connectivity to UCS Fabric Interconnects

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS C220-M4 1	Port 1	10GbE	Cisco UCS Fabric A	Eth1/15
Cisco UCS C220-M4 1	Port 2	10GbE	Cisco UCS Fabric B	Eth1/15
Cisco UCS C220-M4 2	Port 1	10GbE	Cisco UCS Fabric A	Eth1/16
Cisco UCS C220-M4 2	Port 2	10GbE	Cisco UCS Fabric B	Eth1/16

Figure 6 IBM V9000 connectivity for iSCSI design

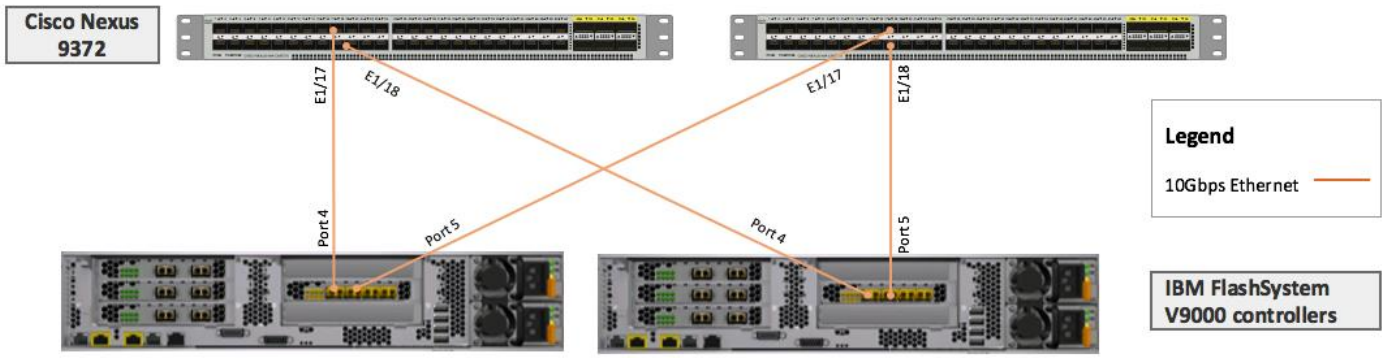


Table 5 IBM V9000 connectivity for iSCSI design

Local Device	Local Port	Connection	Remote Device	Remote Port
IBM V9000 Controller A	Port 4	10GbE	Cisco Nexus 9372 A	Eth1/17
IBM V9000 Controller A	Port 5	10GbE	Cisco Nexus 9372 B	Eth1/17
IBM V9000 Controller B	Port 4	10GbE	Cisco Nexus 9372 A	Eth1/18
IBM V9000 Controller B	Port 5	10GbE	Cisco Nexus 9372 B	Eth1/18

IBM V7000 based FC/NFS connectivity design

For physical connectivity details of an FC/NFS based connectivity design, Figure 7 through Figure 9 show Cisco UCS and IBM V7000 connectivity to the ACI infrastructure.

Figure 7 UCS connectivity for IBM 7000 based FC/NFS design

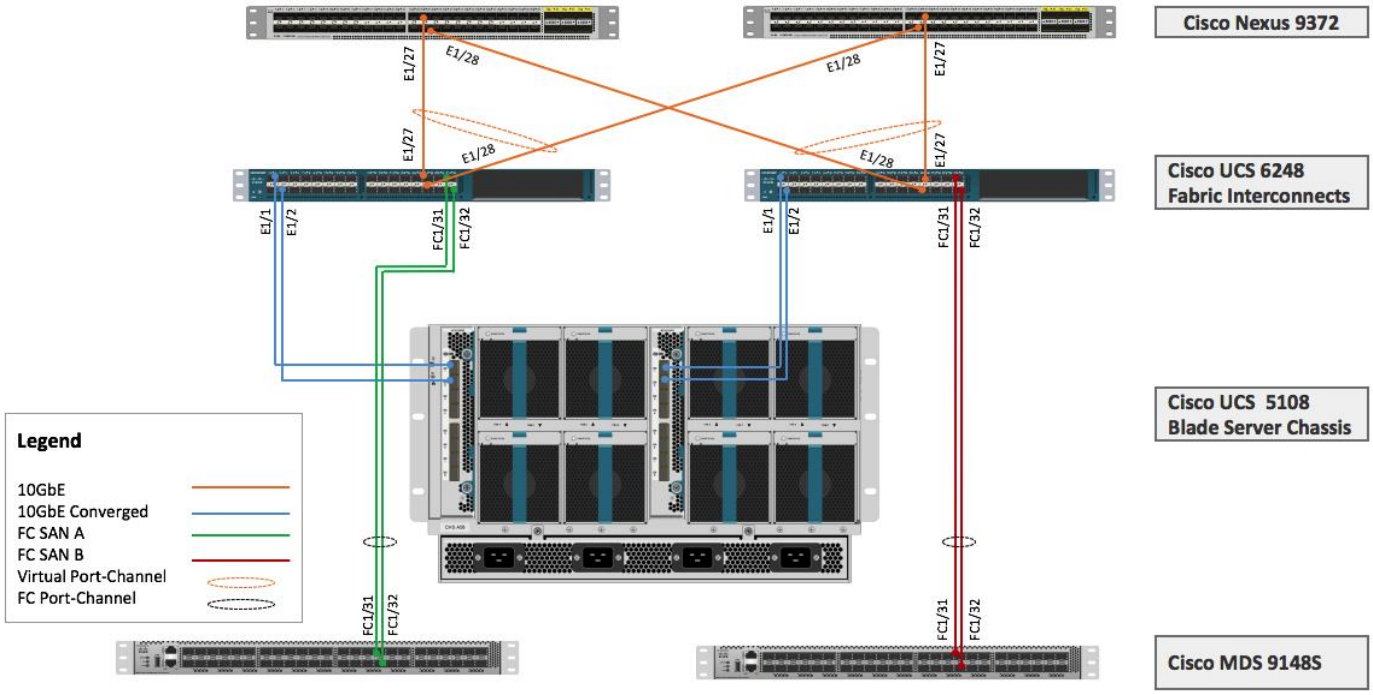


Table 6 Cisco UCS connectivity for IBM V7000 Unified (FC and NFS)

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric Interconnect A	Eth1/1	10GbE	Cisco UCS Chassis FEX A	IOM 1/1
Cisco UCS Fabric Interconnect A	Eth1/2	10GbE	Cisco UCS Chassis FEX A	IOM 1/2
Cisco UCS Fabric Interconnect A	Eth1/27	10GbE	Cisco Nexus 9372 A	Eth1/27
Cisco UCS Fabric Interconnect A	Eth1/28	10GbE	Cisco Nexus 9372 B	Eth1/28
Cisco UCS Fabric Interconnect A	FC1/31	8Gbps	Cisco MDS 9148S A	FC1/31
Cisco UCS Fabric Interconnect A	FC1/32	8Gbps	Cisco MDS 9148S A	FC1/32
Cisco UCS Fabric Interconnect B	Eth1/1	10Gbs	Cisco UCS Chassis FEX B	IOM 1/1
Cisco UCS Fabric Interconnect B	Eth1/2	10GbE	Cisco UCS Chassis FEX B	IOM 1/2
Cisco UCS Fabric Interconnect B	Eth1/28	10GbE	Nexus 9372 A	Eth1/28
Cisco UCS Fabric Interconnect B	Eth1/27	10GbE	Nexus 9372 B	Eth1/27

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric Interconnect B	FC1/31	8Gbps	Cisco MDS 9148S B	FC1/31
Cisco UCS Fabric Interconnect B	FC1/32	8Gbps	Cisco MDS 9148S B	FC1/32

Figure 8 IBM V7000 connectivity for FC storage access

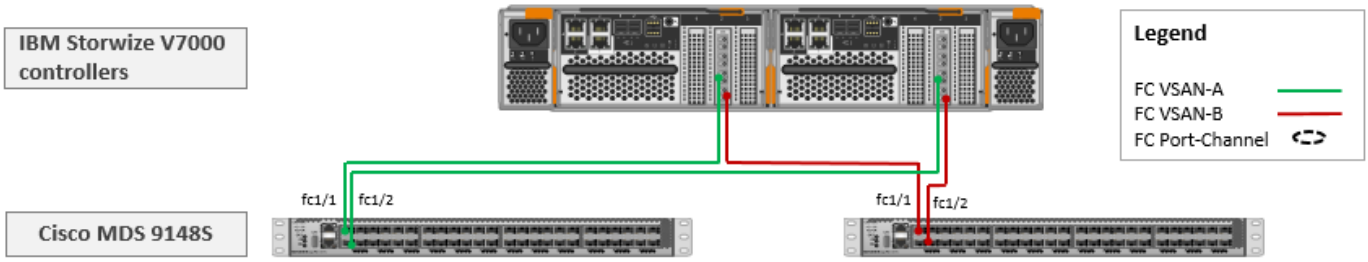


Table 7 IBM V7000 connectivity for FC storage access

Local Device	Local Port	Connection	Remote Device	Remote Port
IBM V7000 Node 1	Port 3	8Gbps	Cisco MDS 9148S A	FC1/1
IBM V7000 Node 1	Port 4	8Gbps	Cisco MDS 9148S A	FC1/2
IBM V7000 Node 2	Port 3	8Gbps	Cisco MDS 9148S B	FC1/1
IBM V7000 Node 2	Port 4	8Gbps	Cisco MDS 9148S B	FC1/2

Figure 9 IBM V7000 Unified File Module connectivity

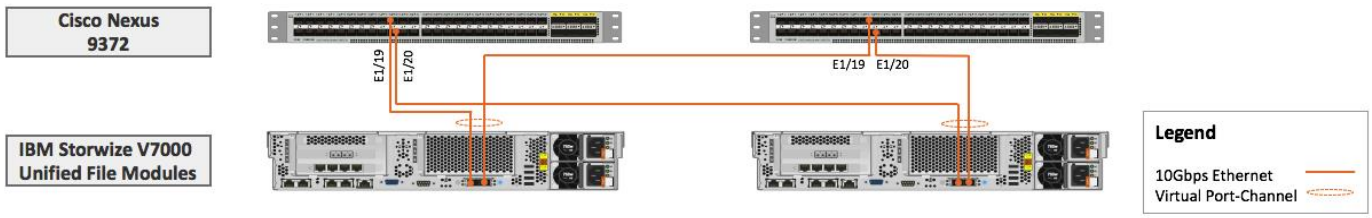


Table 8 IBM V7000 Unified File Module connectivity

Local Device	Local Port	Connection	Remote Device	Remote Port
IBM V7000 Unified File Module 1	Port 1	10GbE	Cisco Nexus 9372 A	Eth1/19
IBM V7000 Unified File Module 1	Port 2	10GbE	Cisco Nexus 9372 B	Eth1/20
IBM V7000 Unified File Module 2	Port 1	10GbE	Cisco Nexus 9372 A	Eth1/19

Local Device	Local Port	Connection	Remote Device	Remote Port
IBM V7000 Unified File Module 2	Port 2	10GbE	Cisco Nexus 9372 B	Eth1/20

Initial Storage Configuration

Storage System Base Configurations

Cisco and IBM have collaborated to deliver a number of VersaStack CVDs covering initial setup and base configuration of both IBM FlashSystem V9000 and IBM Storwize V7000 Unified. This deployment guide covers setting up the network and storage configuration used in the VersaStack with ACI design after the initial storage system setup has been performed. Refer to the following deployment guides on www.cisco.com for setting up a new IBM systems including setting up Cisco MDS switches for storage system component connectivity.

IBM Flash System V9000 Base configuration:

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/Versastack_vmw6_flash.html#_Toc449475184

IBM Storwize V7000 Unified Base Configuration:

http://www.cisco.com/c/dam/en/us/td/docs/unified_computing/ucs/UCS_CVDs/Versastack_n9k_vmw55.pdf

IBM FlashSystem V9000 iSCSI configuration (iSCSI storage access setup only)

Cisco UCS configuration requires information about the iSCSI IQNs on IBM V9000. Therefore, as part of the initial storage configuration, iSCSI ports are configured on IBM v9000

Two 10G ports from each of the IBM FlashSystem V9000 nodes are connected to each of Nexus 9372 Leaf switches. These ports are configured as shown in Table 9:

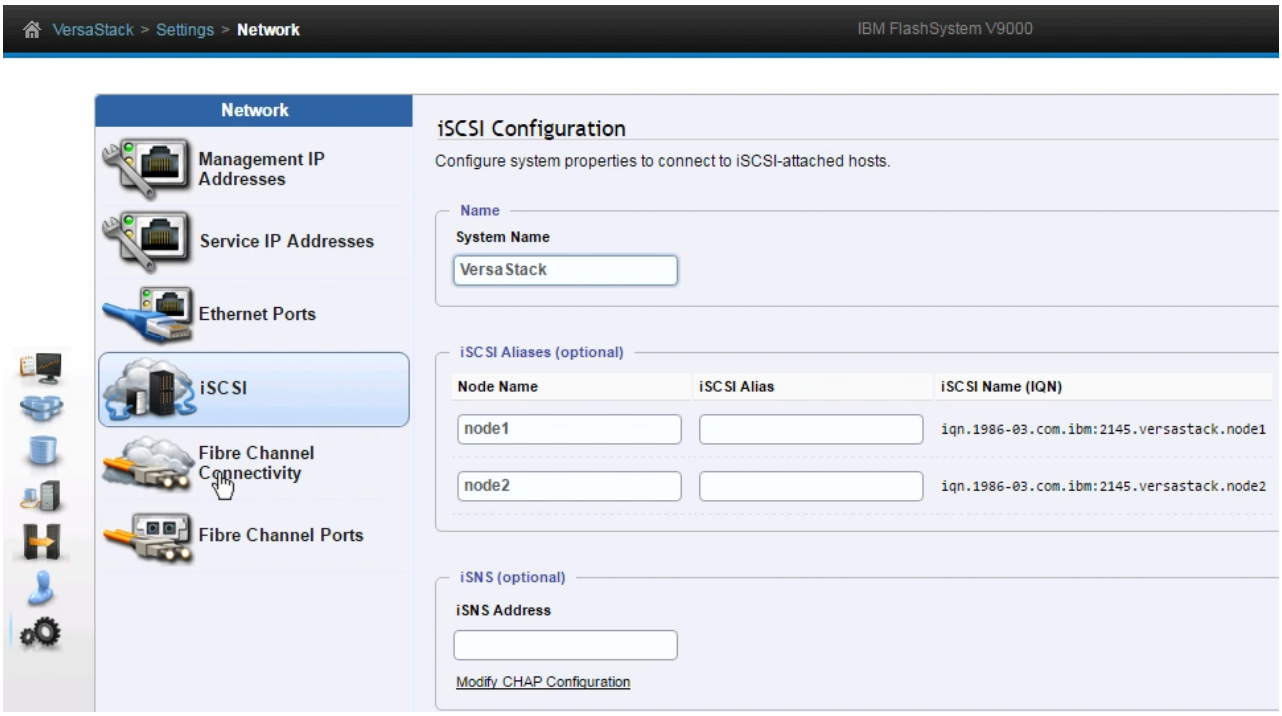
Table 9 IBM FlashSystem V9000 iSCSI interface configuration

System	Port	Path	VLAN	IP address	Gateway
Node 1	4	iSCSI-A	3031	192.168.181.251/24	192.168.181.254
Node 1	5	iSCSI-B	3041	192.168.182.251/24	192.168.182.254
Node 2	4	iSCSI-A	3031	192.168.181.252/24	192.168.181.254
Node 2	5	iSCSI-B	3041	192.168.182.252/24	192.168.182.254

To configure the IBM V9000 system for iSCSI storage access, complete the following steps:

1. Log into the IBM V9000 GUI and navigate to Settings > Network.
2. Click the iSCSI icon 

and enter the system and node names as shown:



3. Note the resulting iSCSI Name (IQN) in the Table 10 to be used later in the configuration procedure

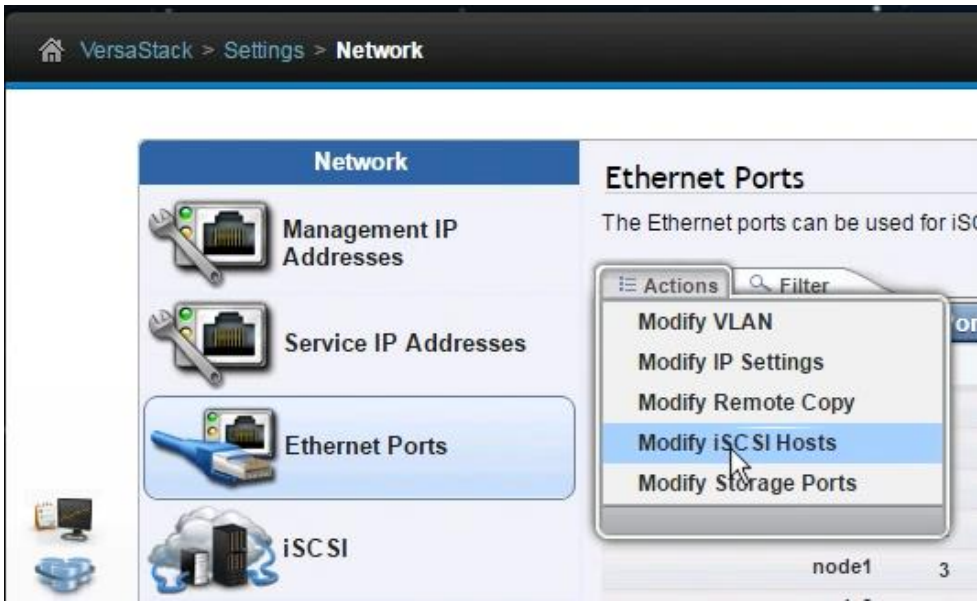
Table 10 IBM FlashSystem V9000 IQN

Node	IQN
Node 1	
Node 2	

4. Click the **Ethernet Ports** icon 

.

5. Click Actions and choose Modify iSCSI Hosts.

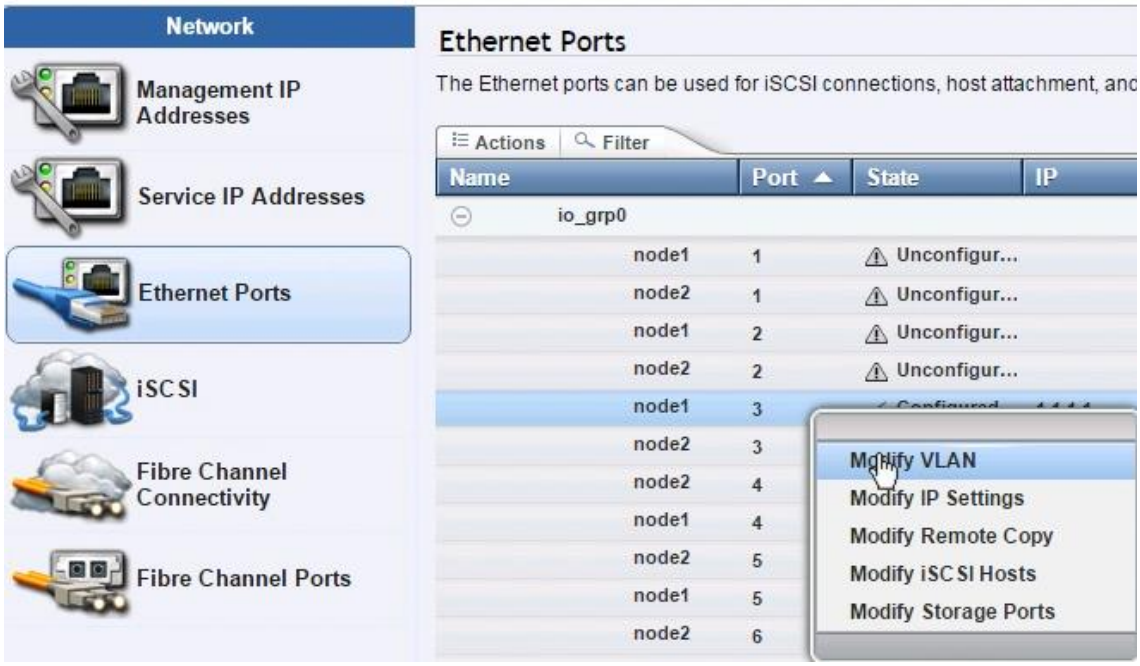


6. Make sure IPv4 iSCSI hosts field is set to enable – if not, change the setting to Enabled and click **Modify**.

7. If already set, click **Cancel** to close the configuration box.
8. For each of the four ports listed in Table 9, repeat the steps 9 – 17.
9. Right-click on the appropriate port and choose **Modify IP Settings**.
10. Enter the IP address, Subnet Mask and Gateway information in Table 9 (gateway will be configured later during ACI set-up).

11. Click **Modify**.

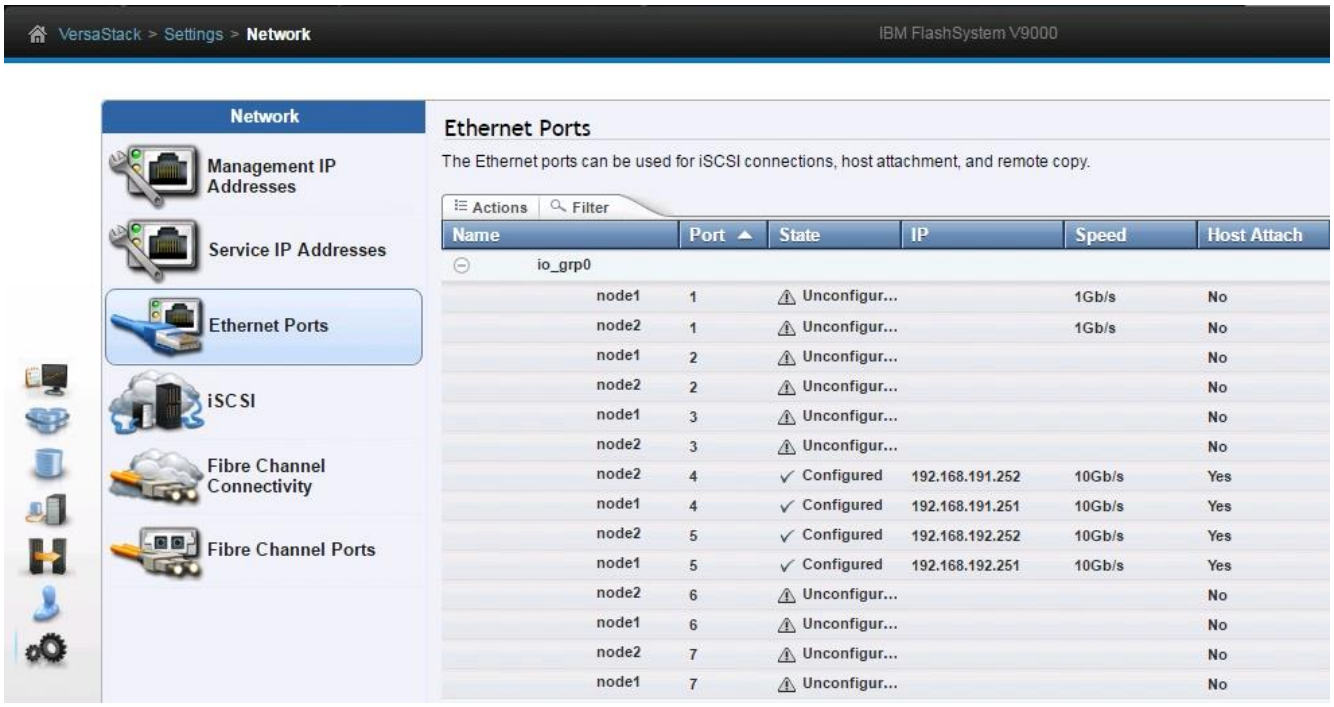
12. Right-click on the newly updated port and choose **Modify VLAN**.



13. Check the check box to Enable VLAN.

14. Enter the appropriate VLAN from Table 9.

15. Keep the Apply change to the failover port too check box checked.
16. Click **Modify**.
17. Repeat the steps for all for iSCSI ports listed in Table 9.
18. Verify all four ports are configured as shown below.



This completes the initial configuration of the IBM systems. The next section covers the Cisco UCS configuration.

Server (UCS) Configuration

This section covers the Cisco UCS setup for VersaStack infrastructure with ACI design. This section includes setup for both iSCSI SAN boot and iSCSI LUN access for IBM V9000 as well as FCoE boot and FCoE LUN access for IBM V7000.

If a customer environment does require implementing some of the storage protocols covered in this deployment guide, the relevant configuration sections can be skipped.

Table 11 shows various VLANs, VSANs and subnets used to setup infrastructure (Foundation) tenant to provide connectivity between core elements of the design.

Table 11 Infrastructure (Foundation) Tenant Configuration

VLAN Name	VLAN	Subnet
IB-MGMT	111	192.168.160.0/22
Infra-iSCSI-A	3030	192.168.181.0/24
infra-iSCSI-B	3040	192.168.182.0/24
Infra-NFS	3050	192.168.180.0/24
vMotion	3000	192.168.179.0/24
Native-2	2	N/A
VDS Pool	1101-1120	Multiple – Tenant Specific
AVS-Infra	4093	N/A
VSAN-A	101	N/A
VSAN-B	102	N/A

Cisco UCS Initial Configuration

This section provides detailed procedures for configuring the Cisco Unified Computing System (Cisco UCS) for use in a VersaStack environment. The steps are necessary to provision the Cisco UCS C-Series and B-Series servers and should be followed precisely to avoid improper configuration.

Cisco UCS 6248 A

To configure the Cisco UCS for use in a VersaStack environment, complete the following steps:

1. Connect to the console port on the first Cisco UCS 6248 fabric interconnect.

```
Enter the configuration method. (console/gui) ? console

Enter the setup mode; setup newly or restore from backup.(setup/restore)? setup

You have chosen to setup a new Fabric interconnect? Continue? (y/n): y

Enforce strong password? (y/n) [y]: y

Enter the password for "admin": <password>

Confirm the password for "admin": <password>
```

```
Is this Fabric interconnect part of a cluster(select 'no' for standalone)?
(yes/no) [n]: y

Which switch fabric (A/B)[]: A

Enter the system name: <Name of the System>

Physical Switch Mgmt0 IP address: <Mgmt. IP address for Fabric A>

Physical Switch Mgmt0 IPv4 netmask: <Mask>

IPv4 address of the default gateway: <Default GW for the mgmt. IP >

Cluster IPv4 address: <Cluster Mgmt. IP address>

Configure the DNS Server IP address? (yes/no) [n]: y

DNS IP address: <DNS IP address>

Configure the default domain name? (yes/no) [n]: y

Default domain name: <DNS Domain Name>

Join centralized management environment (UCS Central)? (yes/no) [n]: n

Apply and save configuration (select 'no' if you want to re-enter)? (yes/no): Y
```

2. Wait for the login prompt to make sure that the configuration has been saved.

Cisco UCS 6248 B

To configure the second Cisco UCS Fabric Interconnect for use in a VersaStack environment, complete the following steps:

1. Connect to the console port on the second Cisco UCS 6248 fabric interconnect.

```
Enter the configuration method. (console/gui) ? console

Installer has detected the presence of a peer Fabric interconnect. This

Fabric interconnect will be added to the cluster.  Continue (y|n)? y

Enter the admin password for the peer Fabric interconnect: <Admin Password>

Physical switch Mgmt0 IP address: < Mgmt. IP address for Fabric B>

Apply and save the configuration (select 'no' if you want to re-enter)?

(yes/no): y
```

2. Wait for the login prompt to make sure that the configuration has been saved.

Cisco UCS Software Upgrade

Log in to Cisco UCS Manager

To log in to the Cisco Unified Computing System (UCS) environment, complete the following steps:

1. Open a web browser and navigate to the Cisco UCS 6248 fabric interconnect cluster address.

2. Under HTML, click the **Launch UCS Manager link** to launch the Cisco UCS Manager HTML5 User Interface.
3. When prompted, enter admin as the user name and enter the administrative password.
4. Click **Login** to log in to Cisco UCS Manager.
5. Respond to the pop-up on Anonymous Reporting and click **OK**.

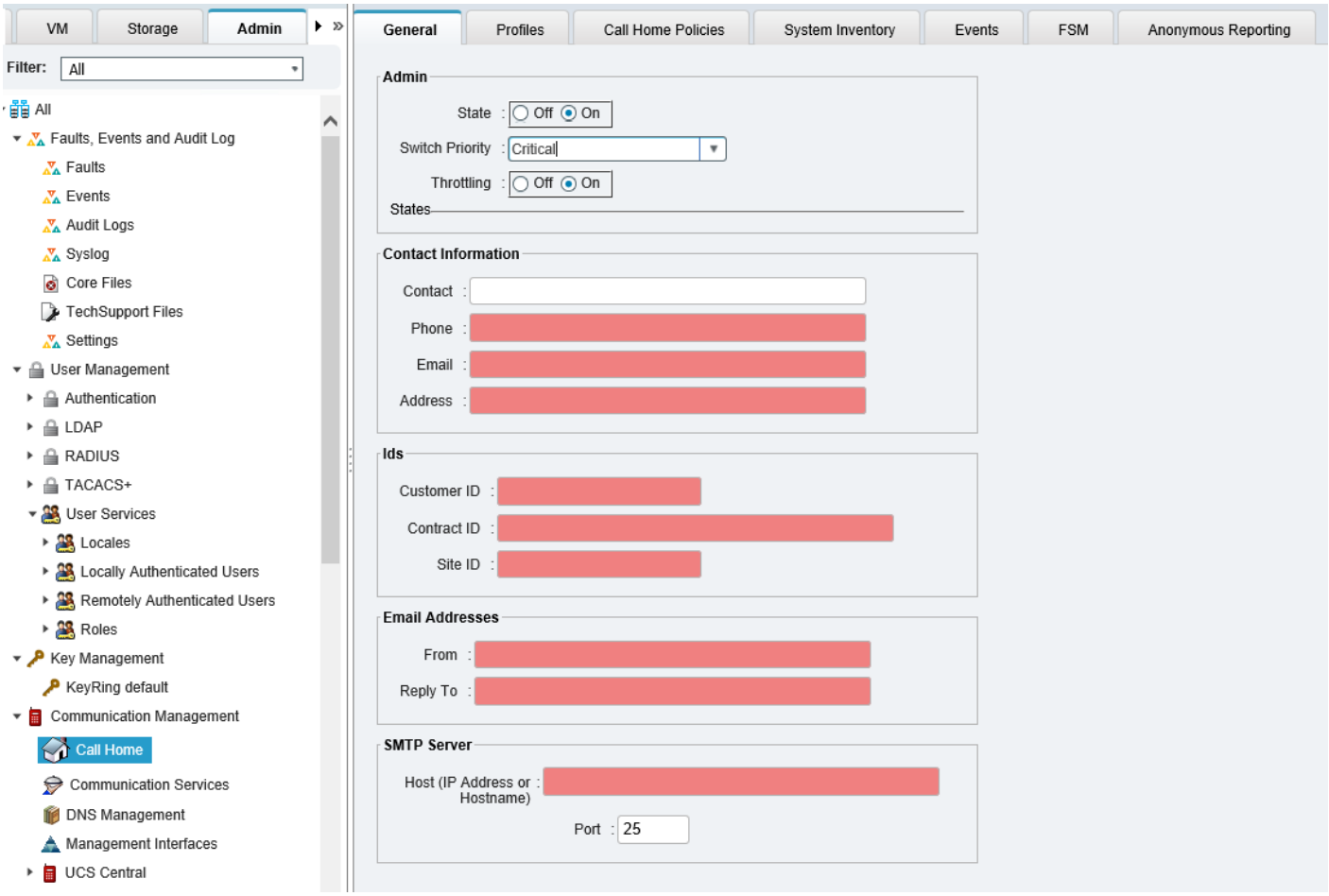
Upgrade Cisco UCS Manager Software to Version 3.1(1g)

This document assumes the use of Cisco UCS 3.1(1g). To upgrade the Cisco UCS Manager software and the UCS 6248 Fabric Interconnect software to version 3.1(1g), refer to Cisco UCS Manager Install and Upgrade Guides.

Configure Cisco UCS Call Home

It is highly recommended by Cisco to configure Call Home in UCSM. Configuring Call Home will accelerate resolution of support cases. To configure Call Home, complete the following steps:

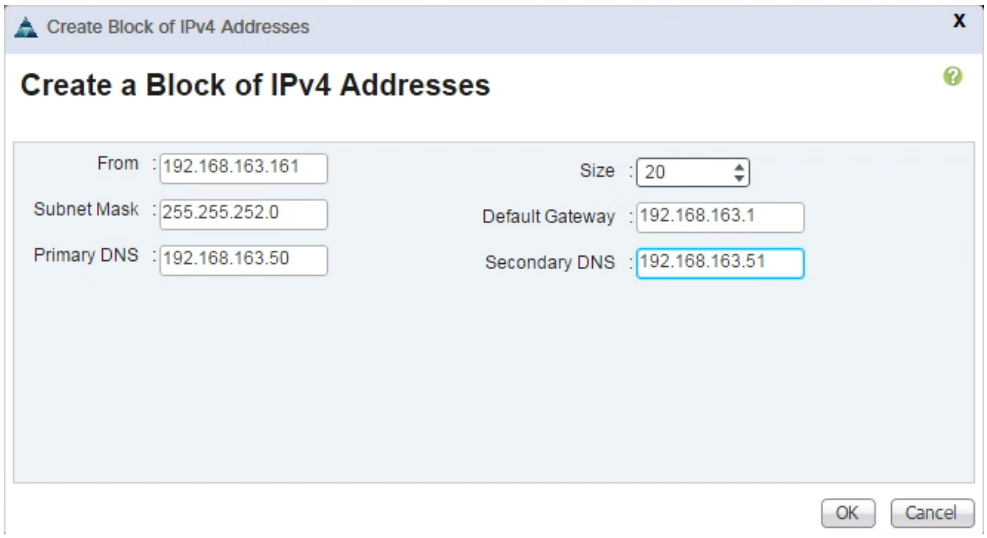
1. In Cisco UCS Manager, click the **Admin** tab in the navigation pane.
2. Select All > Communication Management > Call Home.
3. Change the State to **On**.
4. Fill in all the fields according to your Management preferences and click **Save Changes** and **OK** to complete configuring Call Home.



Add Block of Management IP Addresses for KVM Access

To create a block of IP addresses for out of band (mgmto) server Keyboard, Video, Mouse (KVM) access in the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the **LAN** tab in the navigation pane.
2. Expand Pools > root > IP Pools.
3. Right-click IP Pool ext-mgmt and choose **Create Block of IPv4 Addresses**.
4. Enter the starting IP address of the block, the number of IP addresses required, and the subnet and gateway information. Click **OK**.



This block of IP addresses should be in the out of band management subnet.

5. Click **OK**.
6. Click **OK** in the confirmation message.

Synchronize Cisco UCS to NTP

To synchronize the Cisco UCS environment to the NTP server, complete the following steps:

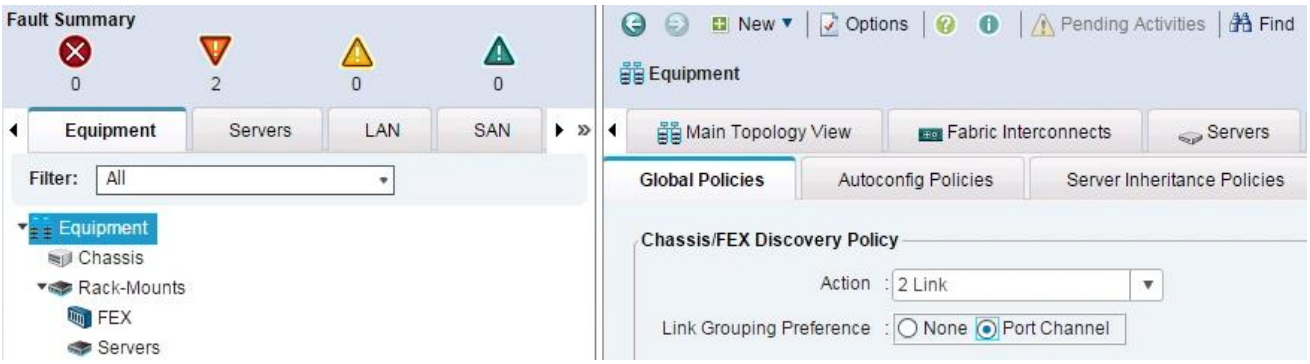
1. In Cisco UCS Manager, click the **Admin** tab in the navigation pane.
2. Select All > Timezone Management > Timezone.
3. In the Properties pane, select the appropriate time zone in the Timezone menu.
4. Click **Save Changes**, and then click **OK**.
5. Click Add NTP Server.
6. Enter <NTP Server IP Address> and click **OK**.
7. Click **OK**.

Edit Chassis Discovery Policy

Setting the discovery policy simplifies the addition of B-Series Cisco UCS chassis and of additional fabric extenders for further C-Series connectivity. To modify the chassis discovery policy, complete the following steps:

1. In Cisco UCS Manager, click the **Equipment** tab in the navigation pane and select Equipment from the list in the left pane.
2. In the right pane, click the **Policies** tab.

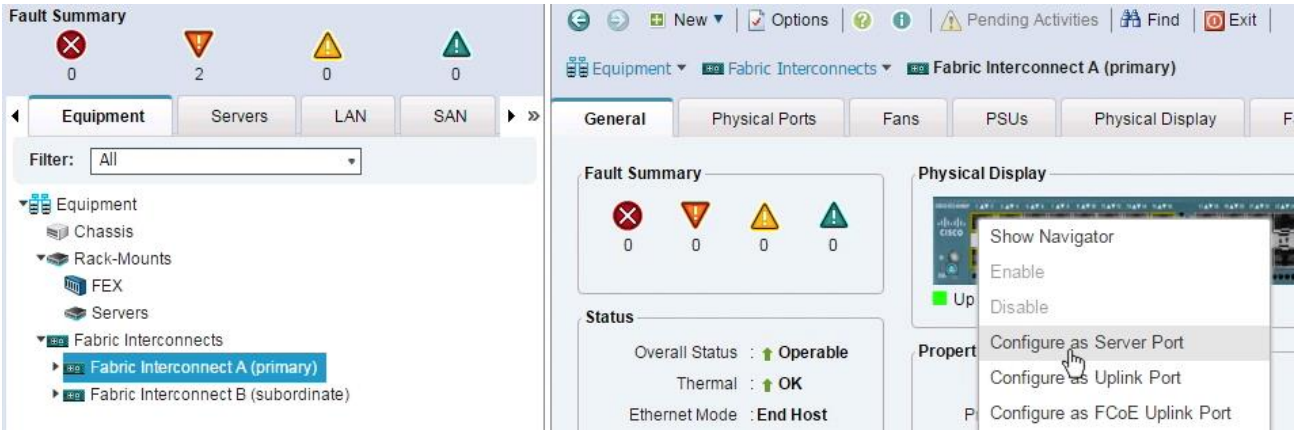
3. Under Global Policies, set the Chassis/FEX Discovery Policy to match the minimum the number of uplink ports that are cabled between any chassis IOM or fabric extender (FEX) and the fabric interconnects.
4. Set the Link Grouping Preference to Port Channel.
5. Click Save Changes.
6. Click **OK**.



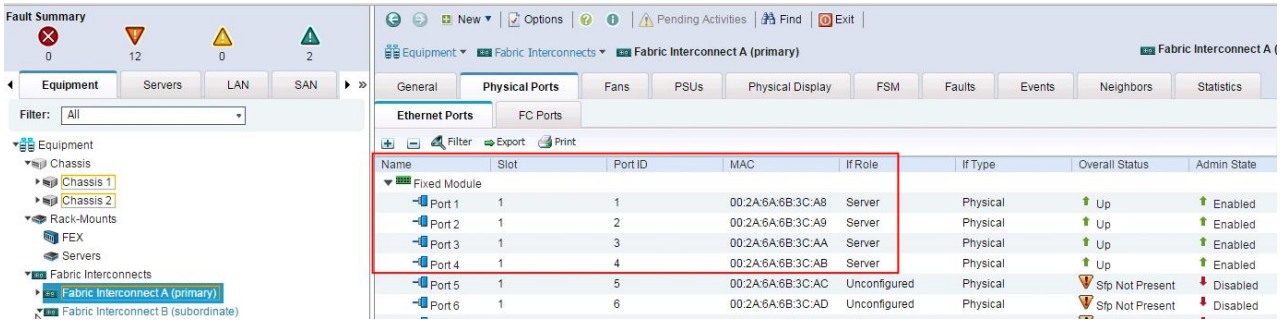
Enable Server and Uplink Ports

To enable server and uplink ports, complete the following steps:

1. In Cisco UCS Manager, click the **Equipment** tab in the navigation pane.
2. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module.
3. Expand Fixed Module.
4. Expand and select **Ethernet Ports**.
5. Select the ports that are connected to the Cisco UCS 5108 chassis and UCS C-Series servers, one by one, right-click and select **Configure as Server Port**.



6. Click **Yes** to confirm server ports and click **OK**.
7. Verify that the ports connected to the UCS 5108 chassis and C-series servers are now configured as Server ports by selecting **Fabric Interconnect A** in the left and **Physical Ports** tab in the right pane.



8. Select the ports that are connected to the Cisco Nexus 9372 leaf switches, one by one, right-click and select **Configure as Uplink Port**.

9. Click **Yes** to confirm uplink ports and click **OK**.

10. Verify that the uplink ports are now configured as Network ports by selecting **Fabric Interconnect A** in the left and **Physical Ports** tab in the right pane.

11. Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.

12. Repeat steps 3-10 to configure server and uplink ports on Fabric Interconnect B.

Acknowledge Cisco UCS Chassis and FEX

When the UCS FI ports are configured as server ports, UCS chassis is automatically discovered and may need to be acknowledged. To acknowledge all Cisco UCS chassis, complete the following steps:

1. In Cisco UCS Manager, click the **Equipment** tab in the navigation pane.

2. Expand **Chassis** and select each chassis that is listed.

3. Right-click each chassis and select **Acknowledge Chassis**.

4. Click **Yes** and then click **OK** to complete acknowledging the chassis.

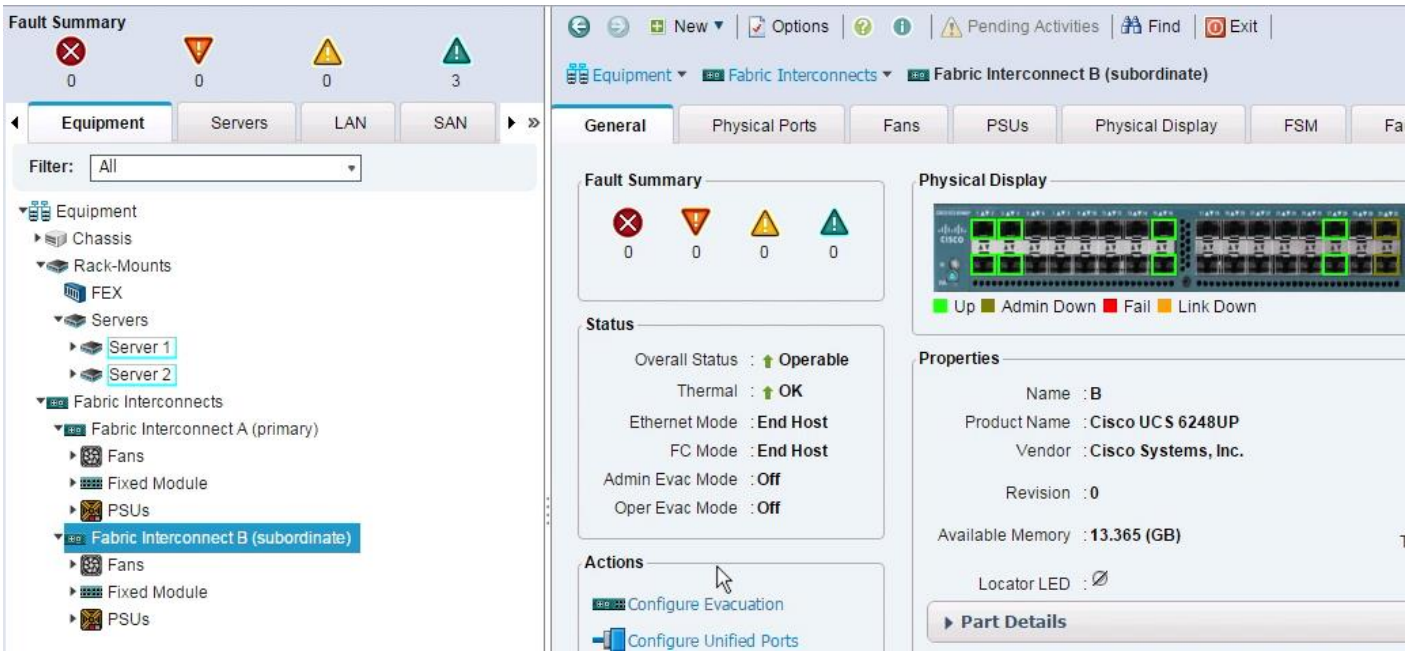
If Cisco Nexus 2232PP FEXes are part of the configuration, expand Rack-Mounts and FEX and acknowledge the FEXes one by one.

Enable Fibre Channel Ports (IBM V7000 Unified Only)

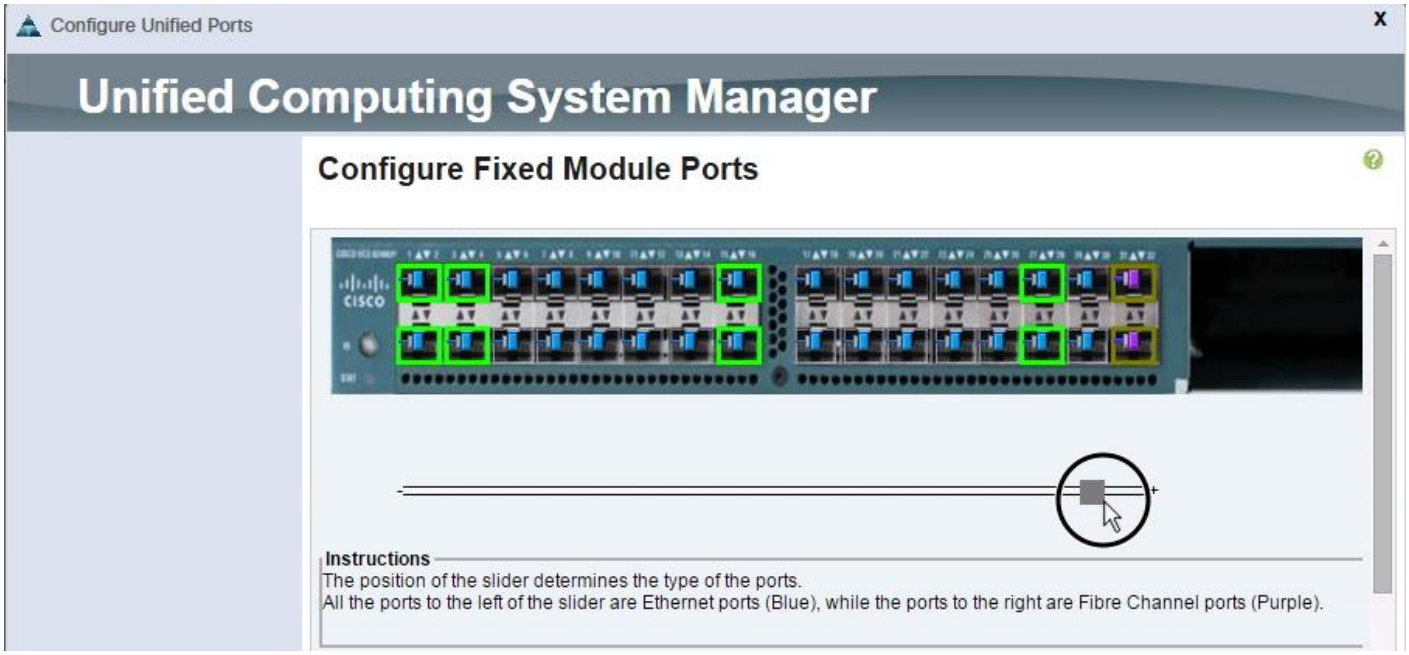
To enable FC uplink ports, complete the following steps.

This step requires a reboot. To avoid an unnecessary switchover, configure the subordinate Fabric Interconnect first.

1. In the **Equipment** tab, select the Fabric Interconnect B (subordinate FI in this example), and in the Actions pane, select **Configure Unified Ports**, and click **Yes** on the splash screen.



2. Slide the lever to change the ports 31-32 to Fiber Channel. Click Finish followed by Yes to the reboot message. Click **OK**.



3. When the subordinate has completed reboot, repeat the procedure to configure FC ports on primary Fabric Interconnect. As before, the Fabric Interconnect will reboot after the configuration is complete.

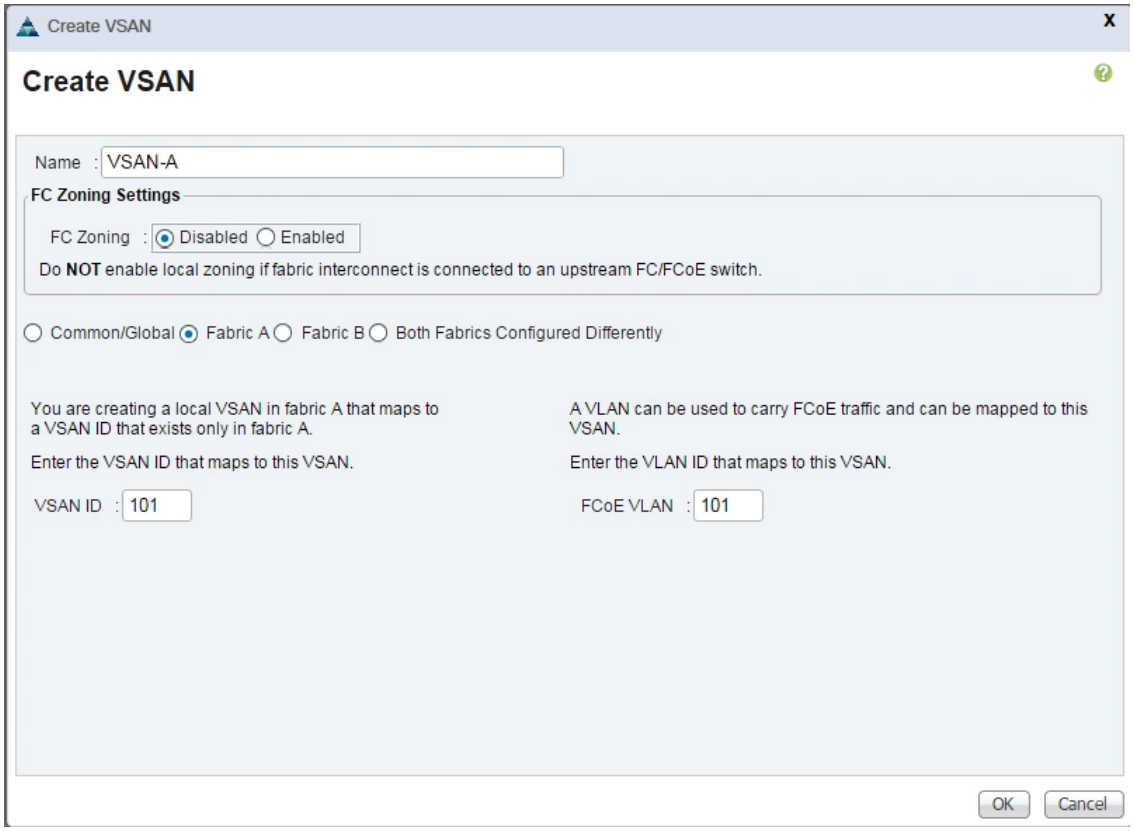
Create VSAN for the Fibre Channel Interfaces

To configure the necessary virtual storage area networks (VSANs) for FC uplinks for the Cisco UCS environment, follow these steps:

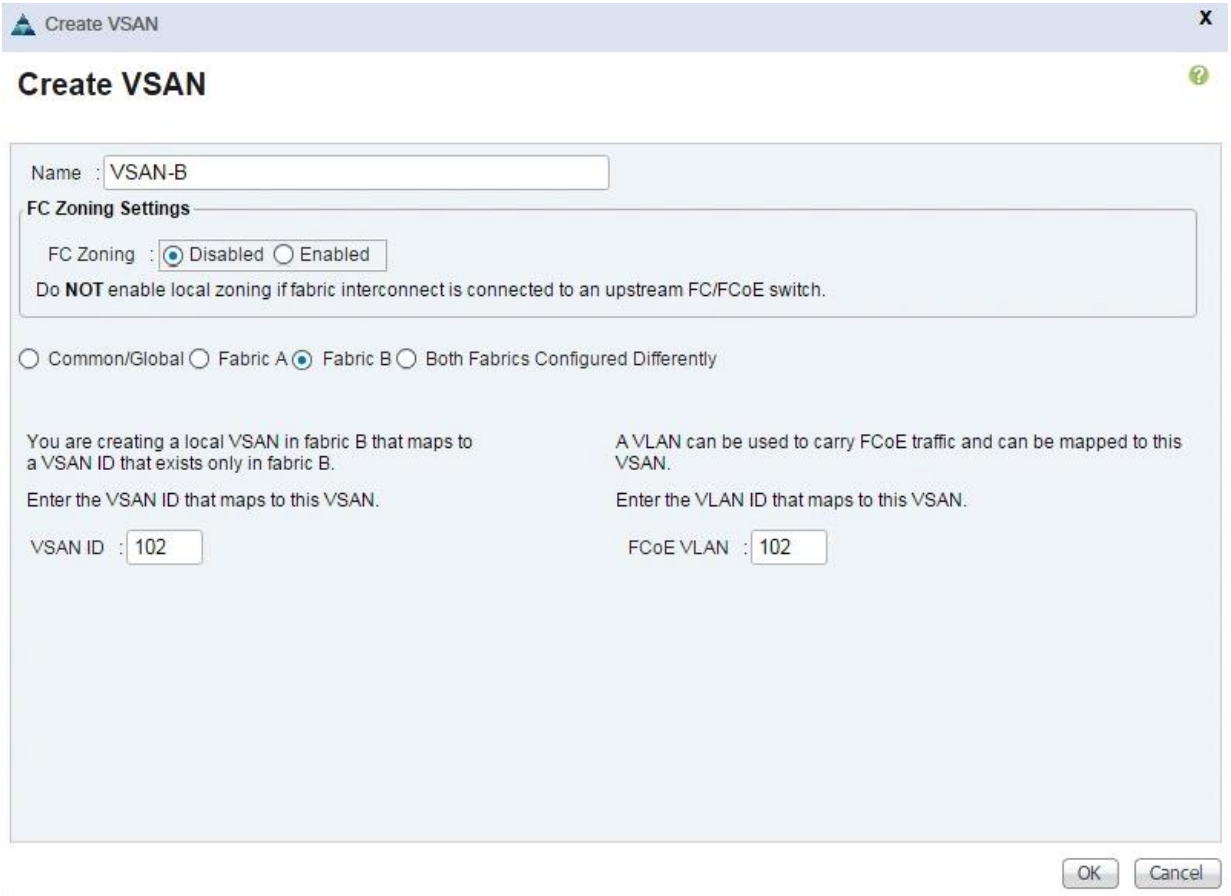
1. In Cisco UCS Manager, click the **SAN** tab in the navigation pane.

2. Expand the SAN > SAN Cloud and select Fabric A.

3. Right-click VSANs and choose **Create VSAN**.
4. Enter VSAN-A as the name of the VSAN for fabric A.
5. Keep the Disabled option selected for FC Zoning.
6. Click the Fabric A radio button.
7. Enter 101 as the VSAN ID for Fabric A.
8. Enter 101 as the FCoE VLAN ID for fabric A. Click **OK** twice.



9. In the **SAN** tab, expand SAN > SAN Cloud > Fabric-B.
10. Right-click VSANs and choose **Create VSAN**.
11. Enter VSAN-B as the name of the VSAN for fabric B.
12. Keep the Disabled option selected for FC Zoning.
13. Click the Fabric B radio button.
14. Enter 102 as the VSAN ID for Fabric B. Enter 102 as the FCoE VLAN ID for Fabric B. Click **OK** twice.

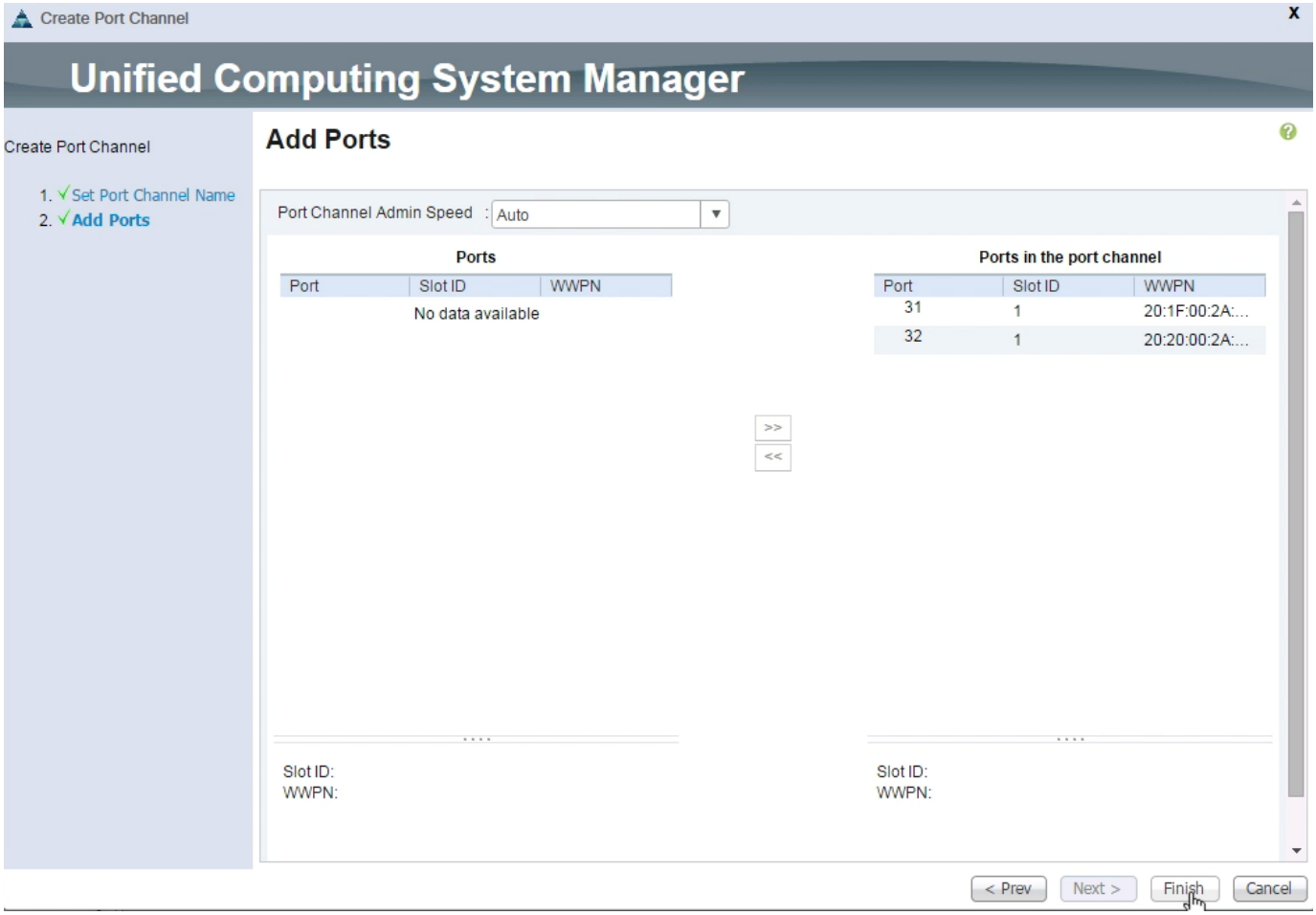


Create Port Channels for the Fibre Channel Interfaces

To configure the necessary port channels for the Cisco UCS environment, complete the following steps:

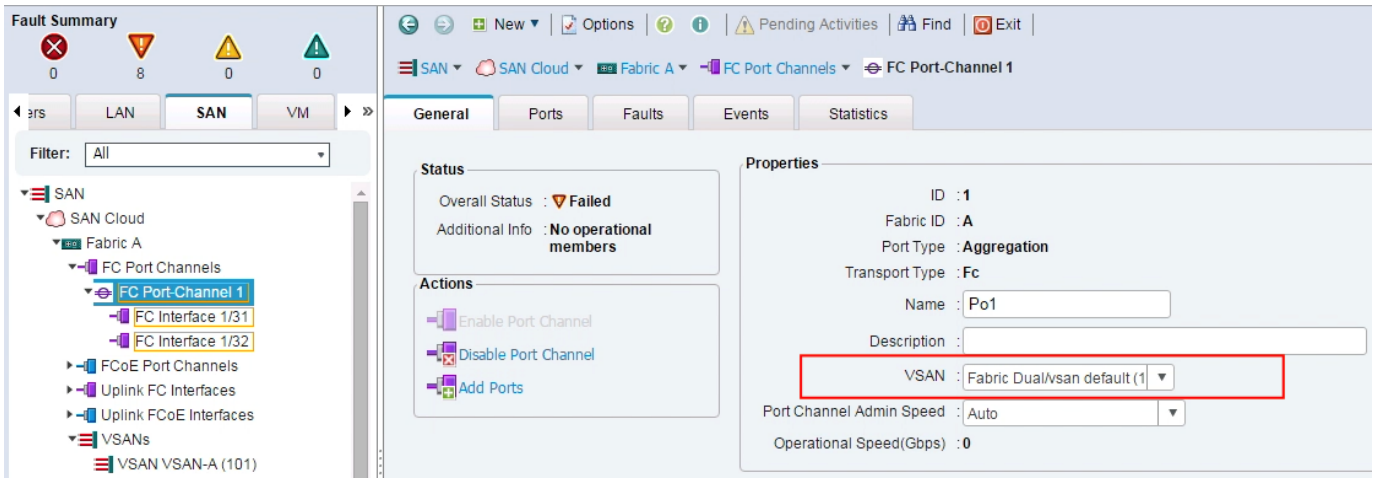
Fabric-A

1. In the navigation pane, under **SAN** > **SAN Cloud**, expand the Fabric A tree.
2. Right-click FC Port Channels and choose **Create Port Channel**.
3. Enter 1 for the port channel ID and Po1 for the port channel name.
4. Click **Next** then choose ports 31 and 32 and click **>>** to add the ports to the port channel. Click **Finish**.



5. Click **OK**.

6. Select FC Port-Channel 1 from the menu in the left pane and from the VSAN drop-down field, select VSAN 101 in the right pane.



7. Click **Save Changes** and then click **OK**.

Fabric-B

1. Click the **SAN** tab. In the navigation pane, under **SAN** > **SAN Cloud**, expand the Fabric B.
2. Right-click FC Port Channels and choose **Create Port Channel**.
3. Enter 2 for the port channel ID and Po2 for the port channel name. Click **Next**.
4. Choose ports 31 and 32 and click **>>** to add the ports to the port channel.
5. Click **Finish**, and then click **OK**.
6. Select FC Port-Channel 2 from the menu in the left pane and from the VSAN drop-down field, select VSAN 102 in the right pane.
7. Click **Save Changes** and then click **OK**.

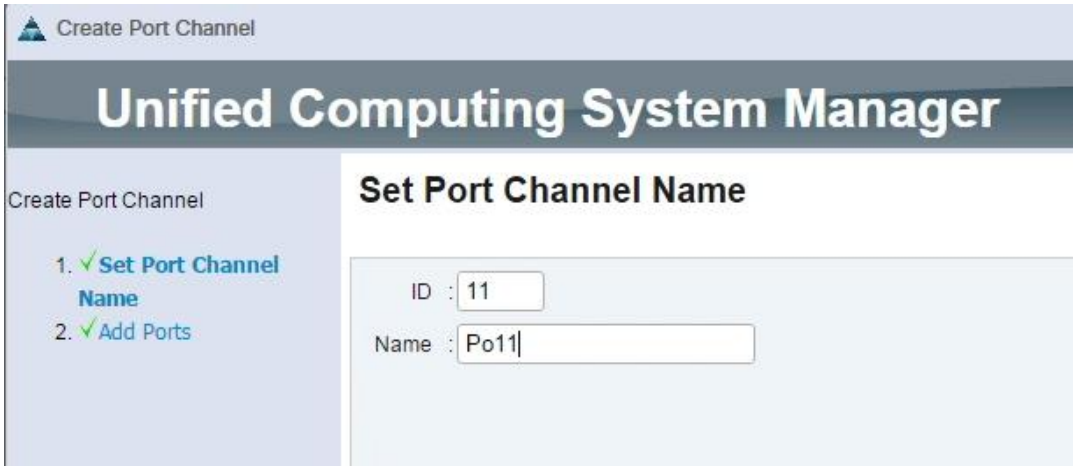
To initialize a quick sync of the connections to the MDS switch, right-click the recently created port channels, disable port channel and then re-enable the port channel. Create Uplink Port Channels to Cisco Nexus Switches.

Create Port Channels for Ethernet Uplinks

To configure the necessary Ethernet port channels out of the Cisco UCS environment, complete the following steps:

In this procedure, two port channels are created one from each Fabric Interconnect (A and B) to both the Cisco Nexus 9372 leaf switches.

1. In Cisco UCS Manager, click the **LAN** tab in the navigation pane.
2. Under **LAN** > **LAN Cloud**, expand the Fabric A tree.
3. Right-click Port Channels and choose Create Port Channel.
4. Enter 11 as the unique ID of the port channel.
5. Enter Po11 as the name of the port channel and click **Next**.



6. Select the network uplink ports to be added to the port channel.
7. Click **>>** to add the ports to the port channel (27 and 28).
8. Click **Finish** to create the port channel and then click OK.
9. In the navigation pane, under **LAN** > **LAN Cloud**, expand the Fabric B tree.
10. Right-click Port Channels and choose **Create Port Channel**.
11. Enter 12 as the unique ID of the port channel.
12. Enter P012 as the name of the port channel and click **Next**.
13. Select the network uplink ports (27 and 28) to be added to the port channel.
14. Click **>>** to add the ports to the port channel.
15. Click **Finish** to create the port channel and click **OK**.

Since the ACI fabric is not configured as yet, the port channels will remain in down state.

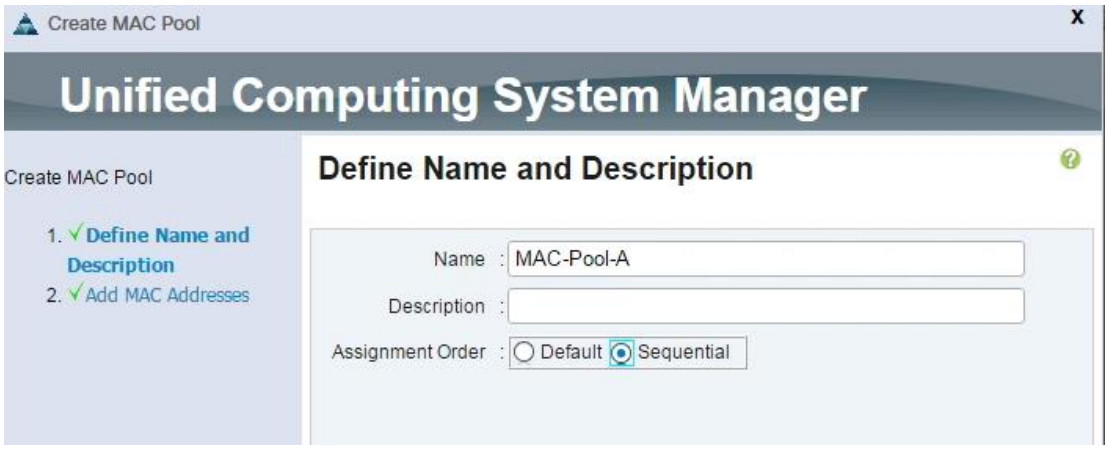
Create MAC Address Pools

To configure the necessary MAC address pools for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the **LAN** tab in the navigation pane.
2. Select **Pools** > **root**.

In this procedure, two MAC address pools are created, one for each switching fabric.

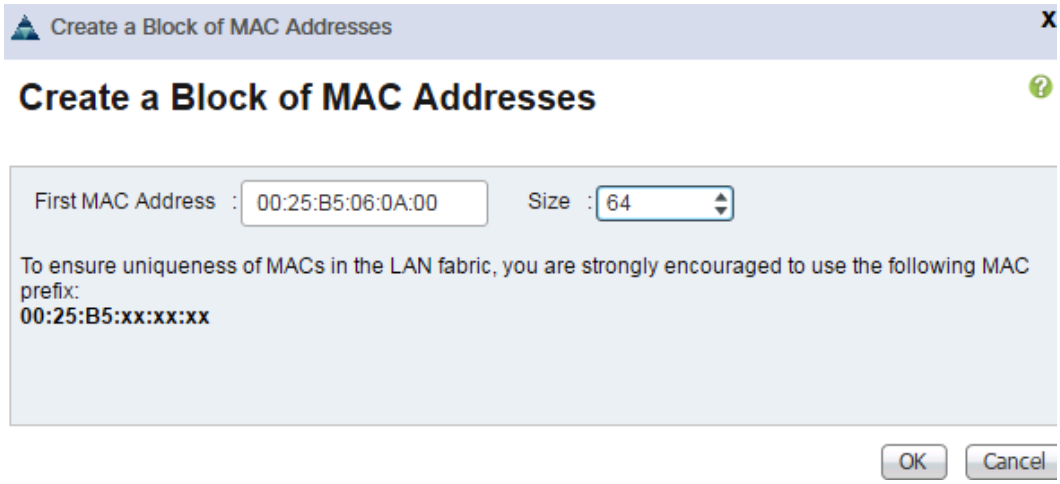
3. Right-click MAC Pools under the root organization.
4. Select **Create MAC Pool** to create the MAC address pool.
5. Enter MAC-Pool-A as the name of the MAC pool.
6. **Optional**: Enter a description for the MAC pool.
7. Select the option Sequential for the Assignment Order field and click **Next**.



8. Click **Add**.
9. Specify a starting MAC address.

It is recommended to place 0A in the second last octet of the starting MAC address to identify all of the MAC addresses as Fabric A addresses. It is also recommended to not change the first three octets of the MAC address.

10. Specify a size for the MAC address pool that is sufficient to support the available blade or rack server resources. Remember that multiple Cisco VIC vNICs will be created on each server and each vNIC will be assigned a MAC address.

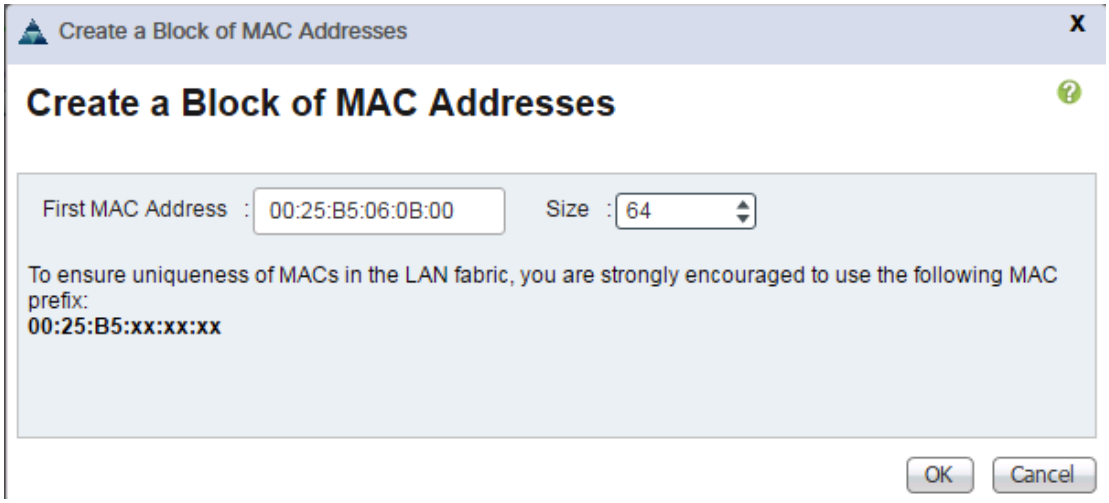


11. Click **OK** and then click **Finish**.
12. In the confirmation message, click **OK**.
13. Right-click MAC Pools under the root organization.
14. Select **Create MAC Pool** to create the MAC address pool.
15. Enter MAC-Pool-B as the name of the MAC pool.
16. **Optional**: Enter a description for the MAC pool.
17. Select the Sequential Assignment Order and click **Next**.

18. Click **Add**.
19. Specify a starting MAC address.

It is recommended to place oB in the second last octet of the starting MAC address to identify all the MAC addresses in this pool as fabric B addresses. It is also recommended to not change the first three octets of the MAC address.

20. Specify a size for the MAC address pool that is sufficient to support the available blade or rack server resources.

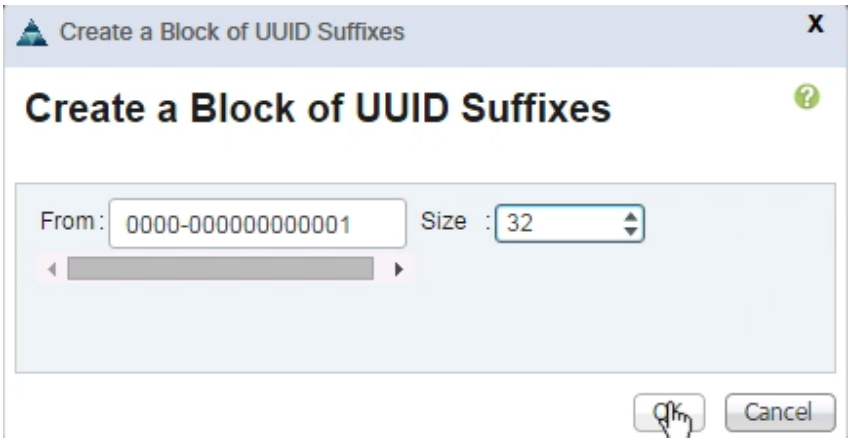


21. Click **OK** and then click **Finish**.
22. In the confirmation message, click **OK**.

Create UUID Suffix Pool

To configure the necessary universally unique identifier (UUID) suffix pool for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the **Servers** tab in the navigation pane.
2. Select **Pools** > **root**.
3. Right-click UUID Suffix Pools and choose Create UUID Suffix Pool.
4. Enter UUID-Pool as the name of the UUID suffix pool.
5. **Optional**: Enter a description for the UUID suffix pool.
6. Keep the prefix at the derived option.
7. Click **Next**.
8. Click **Add** to add a block of UUIDs.
9. Keep the From field at the default setting.
10. Specify a size for the UUID block that is sufficient to support the available blade or rack server resources.



11. Click **OK**. Click **Finish** and then click **OK**.

Create Server Pool

To configure the necessary server pool for the Cisco UCS environment, complete the following steps:

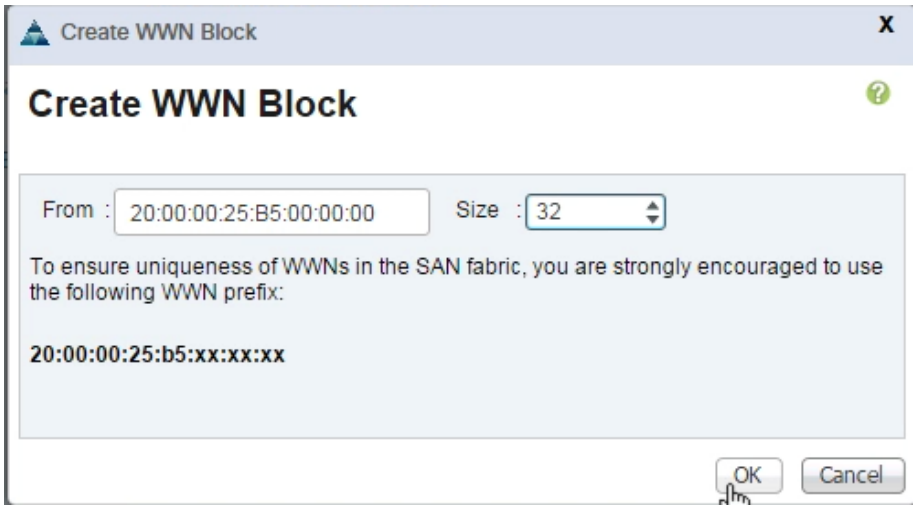
1. In Cisco UCS Manager, click the **Servers** tab in the navigation pane.
2. Select **Pools** > **root**.
3. Right-click Server Pools and choose **Create Server Pool**.
4. Enter Infra-Server-Pool as the name of the server pool.
5. **Optional**: Enter a description for the server pool.
6. Click **Next**.
7. Select at least two (or more) servers to be used for the setting up the VMware environment and click **>>** to add them to the Infra-Pool server pool.
8. Click **Finish** and click **OK**.

Create a WWNN Address Pool for FC based Storage Access (IBM v7000 Only)

For FC boot as well as access to FC LUNs, create a World Wide Node Name (WWNN) pool by completing the following steps:

1. In Cisco UCS Manager, click the **SAN** tab in the navigation pane.
2. Select **Pools** > **root**.
3. Right-click WWNN Pools under the root organization and choose **Create WWNN Pool** to create the WWNN address pool.
4. Enter WWNN-Pool as the name of the WWNN pool.
5. **Optional**: Enter a description for the WWNN pool.

6. Select the Sequential Assignment Order and click **Next**.
7. Click **Add**.
8. Specify a starting WWNN address.
9. Specify a size for the WWNN address pool that is sufficient to support the available blade or rack server resources. Each server will receive one WWNN.



10. Click **OK** and click **Finish**.
11. In the confirmation message, click **OK**.

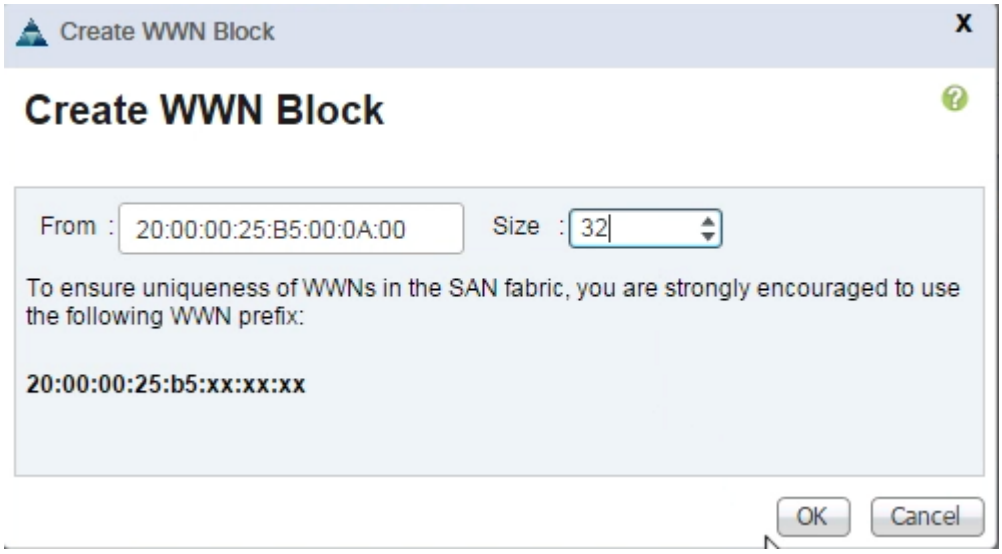
Create a WWPN Address Pools for FC Based Storage Access (IBM v7000 Only)

If you are providing FCoE boot or access to FCoE LUNs, create a World Wide Port Name (WWPN) pool for each SAN switching fabric by completing the following steps:

1. In Cisco UCS Manager, click the **SAN** tab in the navigation pane.
2. Select **Pools** > **root**.
3. Right-click WWPN Pools under the root organization and choose **Create WWPN Pool** to create the first WWPN address pool.
4. Enter WWPN-Pool-A as the name of the WWPN pool.
5. **Optional**: Enter a description for the WWPN pool.
6. Select the Sequential Assignment Order and click **Next**.
7. Click **Add**.
8. Specify a starting WWPN address.

It is recommended to place 0A in the second last octet of the starting WWPN address to identify all of the WWPN addresses as Fabric A addresses.

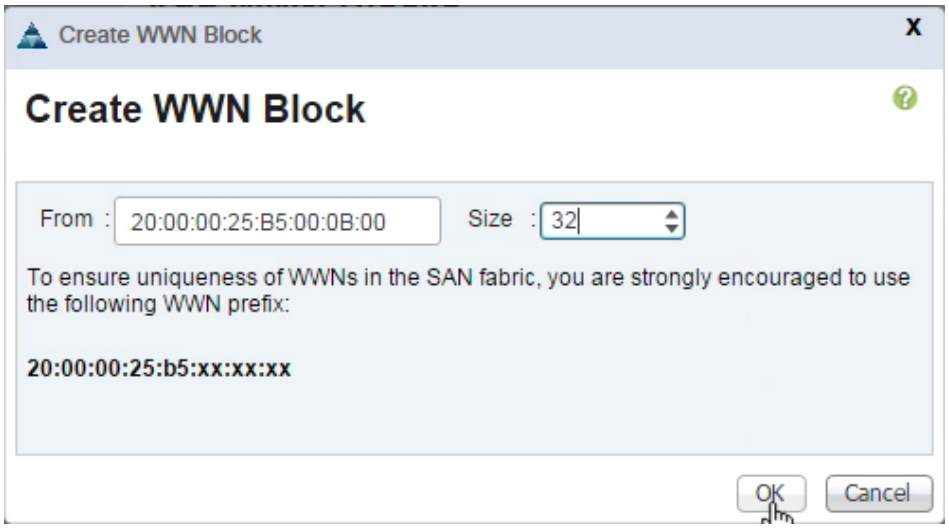
9. Specify a size for the WWPN address pool that is sufficient to support the available blade or rack server resources. Each server's Fabric A vHBA will receive one WWPN from this pool.



10. Click **OK** and click **Finish**.
11. In the confirmation message, click **OK**.
12. Right-click WWPN Pools under the root organization and choose **Create WWPN Pool** to create the second WWPN address pool.
13. Enter WWPN-Pool-B as the name of the WWPN pool.
14. **Optional**: Enter a description for the WWPN pool.
15. Select the Sequential Assignment Order and click **Next**.
16. Click **Add**.
17. Specify a starting WWPN address.

It is recommended to place 0B in the second last octet of the starting WWPN address to identify all of the WWPN addresses as Fabric B addresses.

18. Specify a size for the WWPN address pool that is sufficient to support the available blade or rack server resources. Each server's Fabric B vHBA will receive one WWPN from this pool.

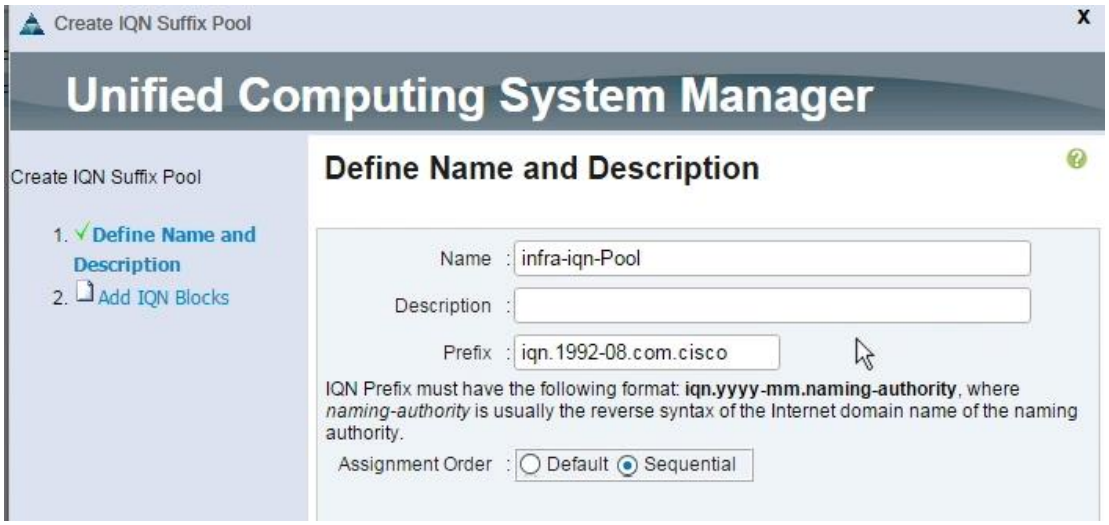


19. Click **OK** and click **Finish**.
20. In the confirmation message, click **OK**.

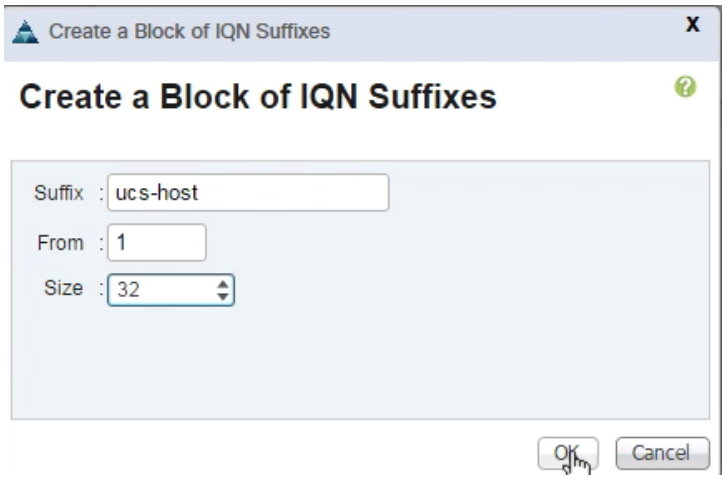
Create IQN Pools for iSCSI Boot and LUN Access (IBM v9000 Only)

To enable iSCSI boot and provide access to iSCSI LUNs, configure the necessary IQN pools in the Cisco UCS Manager by completing the following steps:

1. In the UCS Manager, select the **SAN** tab.
2. Select **Pools** > **root**.
3. Right-click IQN Pools under the root organization and choose **Create IQN Suffix Pool** to create the IQN pool.
4. Enter infra-iqn-Pool for the name of the IQN pool.
5. **Optional**: Enter a description for the IQN pool.
6. Enter iqn.1992-08.com.cisco as the prefix
7. Select the option Sequential for Assignment Order field. Click **Next**.



8. Click **Add**.
9. Enter an identifier with ucs-host as the suffix.
10. Enter 1 in the From field.
11. Specify a size of the IQN block sufficient to support the available server resources. Each server will receive one IQN.
12. Click **OK**.



13. Click **Finish**. In the message box that displays, click **OK**.

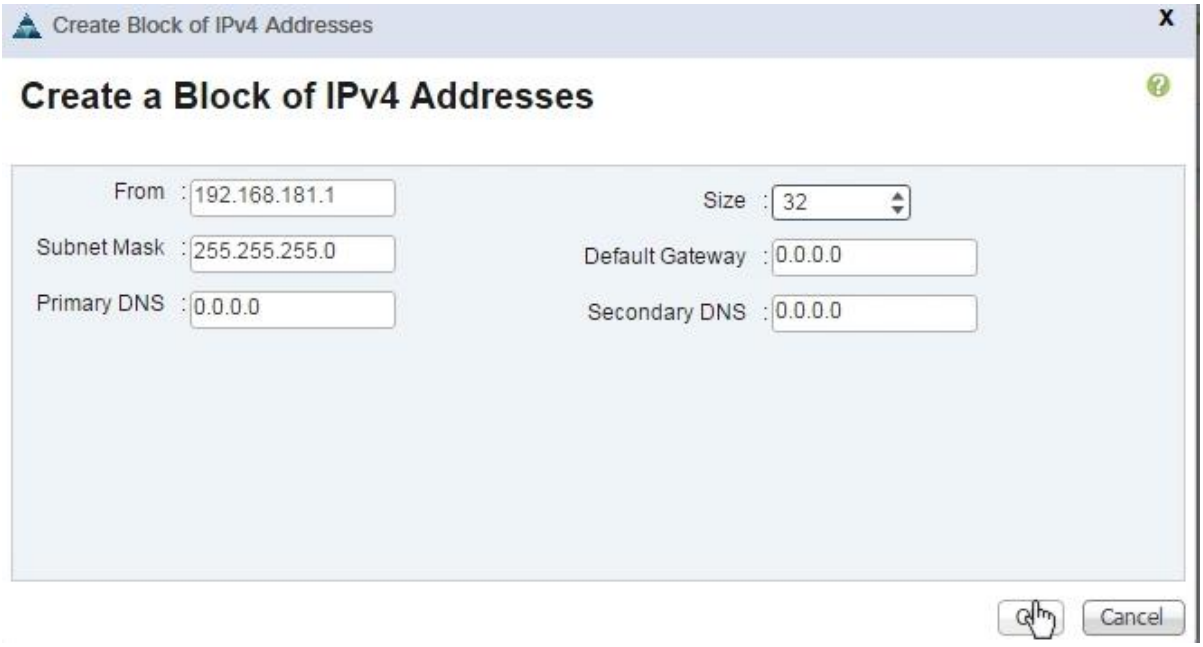
Create IP Pools for iSCSI Boot and LUN Access (IBM v9000 Only)

For enabling iSCSI storage access, these steps provide details for configuring the necessary IP pools in the Cisco UCS Manager:

Two IP pools are created, one for each switching fabric.

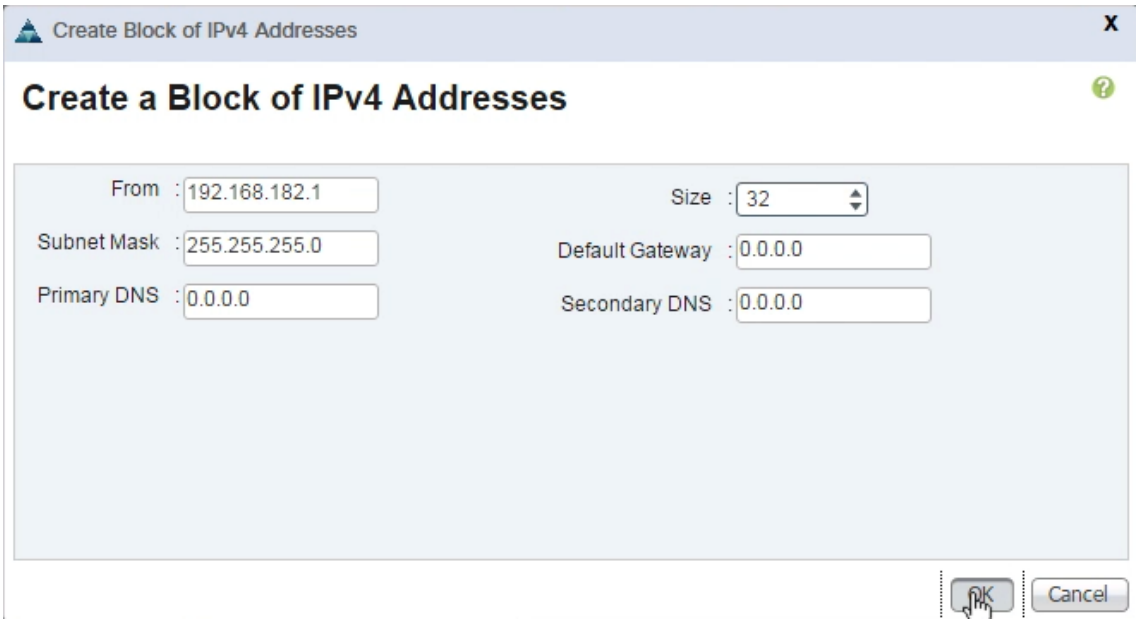
1. In Cisco UCS Manager, select the **LAN** tab.

2. Select **Pools** > **root**.
3. Right-click IP Pools under the root organization and choose **Create IP Pool** to create the IP pool.
4. Enter iSCSI-initiator-A for the name of the IP pool.
5. **Optional**: Enter a description of the IP pool.
6. Select the option Sequential for the Assignment Order field. Click **Next**.
7. Click **Add**.
8. In the From field, enter the beginning of the range to assign an iSCSI IP addresses. These addresses are covered in Table 11.
9. Enter the Subnet Mask.
10. Set the size with sufficient address range to accommodate the servers. Click **OK**.



11. Click **Next** and then click **Finish**.
12. Click **OK** in the confirmation message.
13. Right-click IP Pools under the root organization and choose **Create IP Pool** to create the IP pool.
14. Enter iSCSI-initiator-B for the name of the IP pool.
15. **Optional**: Enter a description of the IP pool.
16. Select the Sequential option for the Assignment Order field. Click **Next**.
17. Click **Add**.

18. In the From field, enter the beginning of the range to assign an iSCSI IP addresses. These addresses are covered in Table 11.
19. Enter the Subnet Mask.
20. Set the size with sufficient address range to accommodate the servers. Click **OK**.



21. Click **Next** and then click **Finish**.
22. Click **OK** in the confirmation message.

Create VLANs

To configure the necessary VLANs in the Cisco UCS Manager, complete the following steps for all the VLANs listed in Table 12:

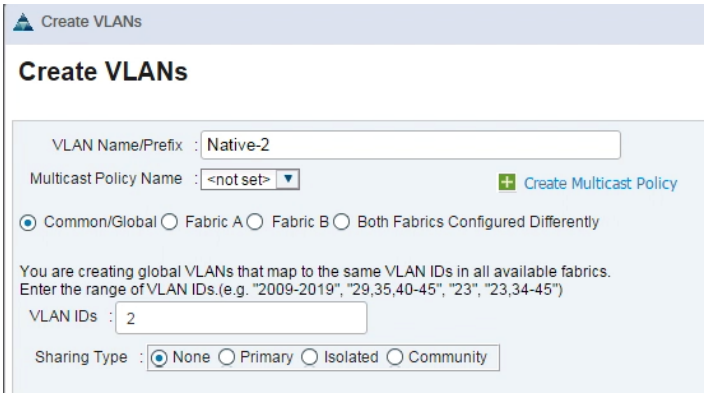
Table 12 VLANs on the UCS System

VLAN Name	VLAN
IB-MGMT	111
Infra-iSCSI-A*	3030
infra-iSCSI-B*	3040
Infra-NFS**	3050
vMotion	3000
Native-2	2
APIC-Pool-	1101-1120
AVS-Infra	4093

* Infra-iSCSI-A/B VLANs are only needed for IBM V9000 iSCSI deployments

** Infra-NFS VLAN only needed for IBM v7000 Unified File Modules deployments

1. In Cisco UCS Manager, click the **LAN** tab in the navigation pane.
2. Select LAN > LAN Cloud.
3. Right-click VLANs and **choose** Create VLANs.
4. Enter name from the VLAN Name column.
5. Keep the Common/Global option selected for the scope of the VLAN.
6. Enter the VLAN ID associated with the name.
7. Keep the Sharing Type as None.
8. Click **OK,** and then click **OK** again.



9. Click **Yes,** and then click **OK** twice.

For defining a range of VLANs from a single screen, refer to figure below. In the figure, APIC-Pool- prefix will be appended to all the VLAN names (for example, APIC-Pool-1101, APIC-Pool-1102 and so on).

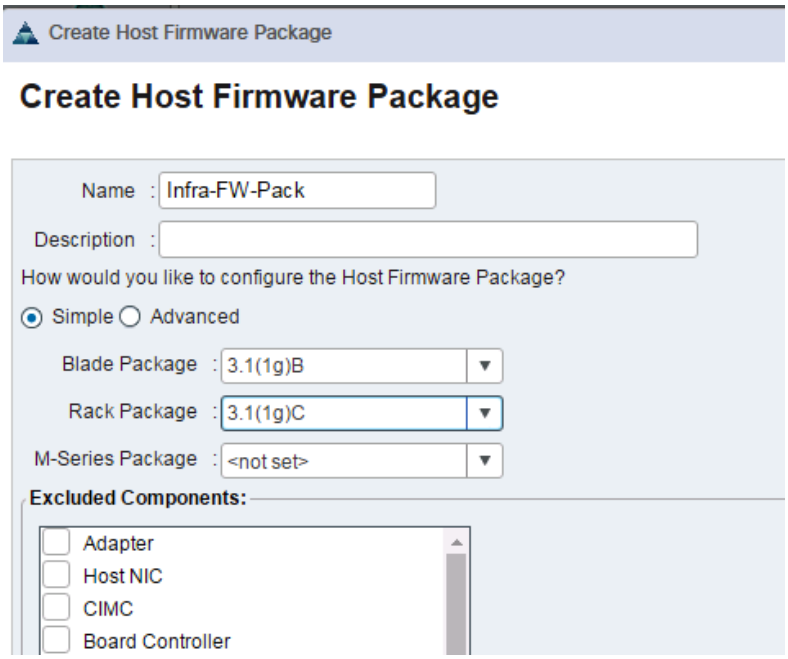
10. Repeat these steps for all the VLAN in Table 12.

Create Host Firmware Package

Firmware management policies allow the administrator to select the corresponding packages for a given server configuration. These policies often include packages for adapter, BIOS, board controller, FC adapters, host bus adapter (HBA) option ROM, and storage controller.

To create a firmware management policy for a given server configuration in the Cisco UCS environment, complete the following steps:

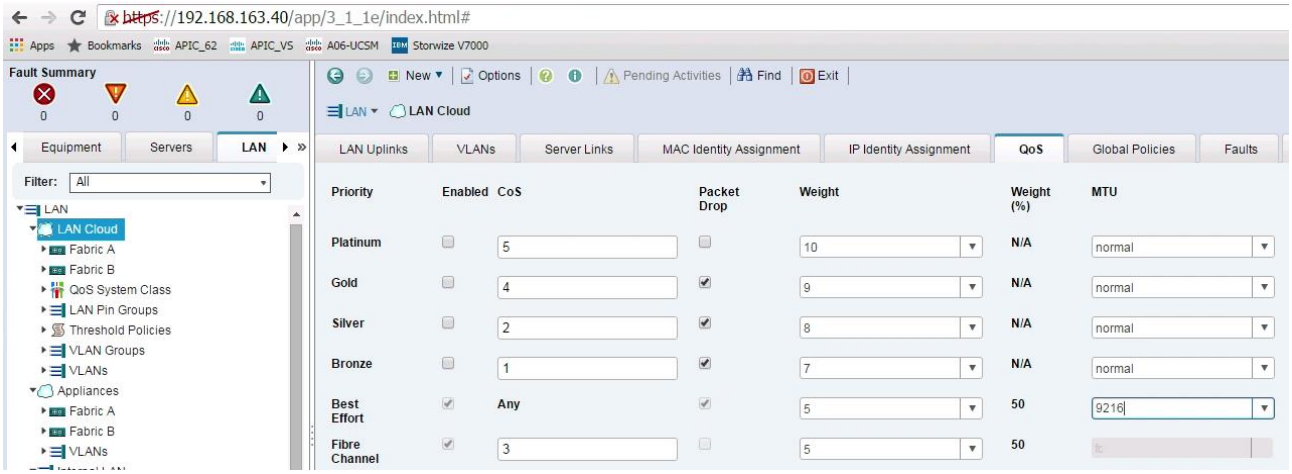
1. In Cisco UCS Manager, click the **Servers** tab in the navigation pane.
2. Select Policies > root.
3. Right-click Host Firmware Packages and choose **Create Host Firmware Package**.
4. Enter Infra-FW-Pack as the name of the host firmware package.
5. Keep the Host Firmware Package as Simple.
6. Select the version 3.1(1g) for both the Blade and Rack Packages.
7. Click **OK** to create the host firmware package.
8. Click **OK**.



Set Jumbo Frames in Cisco UCS Fabric

To configure jumbo frames in the Cisco UCS fabric, complete the following steps:

1. In Cisco UCS Manager, click the **LAN** tab in the navigation pane.
2. Select LAN > LAN Cloud > QoS System Class.
3. In the right pane, click the **General** tab.
4. On the Best Effort row, enter 9216 in the box under the MTU column.
5. Click **Save Changes** in the bottom of the window.
6. Click **Yes**, and then **OK**.



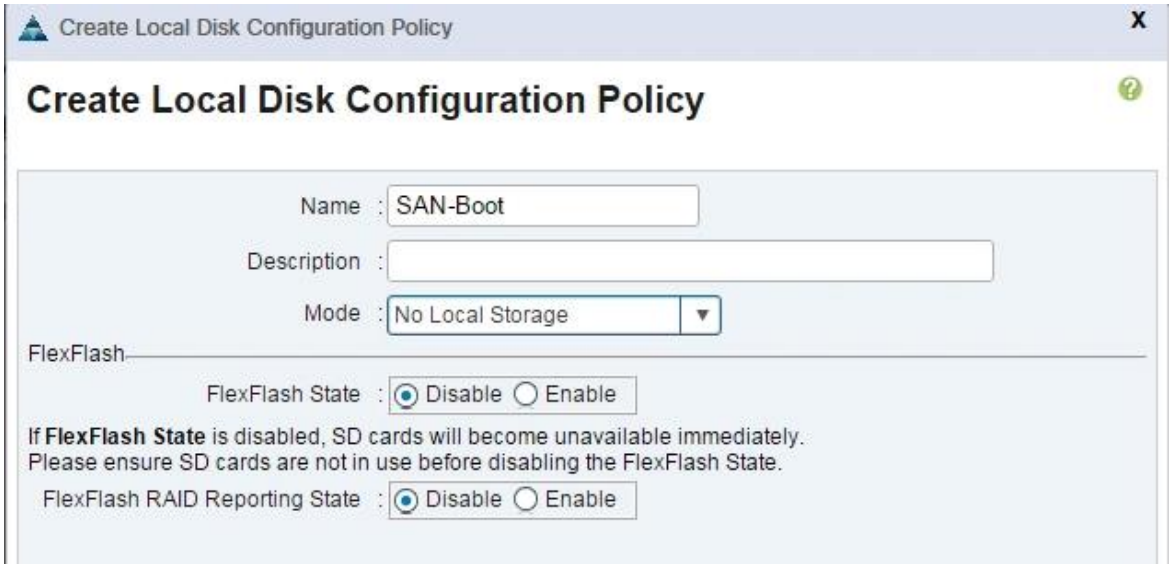
Create Local Disk Configuration Policy

When using an external storage system, a local disk configuration for the Cisco UCS environment is necessary because the servers in the environment will not contain a local disk.

This policy should not be applied to the servers that contain local disks.

To create a local disk configuration policy for no local disks, complete the following steps:

1. In Cisco UCS Manager, click the **Servers** tab in the navigation pane.
2. Select Policies > root.
3. Right-click Local Disk Config Policies and choose **Create Local Disk Configuration Policy**.
4. Enter SAN-Boot as the local disk configuration policy name.
5. Change the mode to **No Local Storage**.
6. Click **OK** to create the local disk configuration policy.



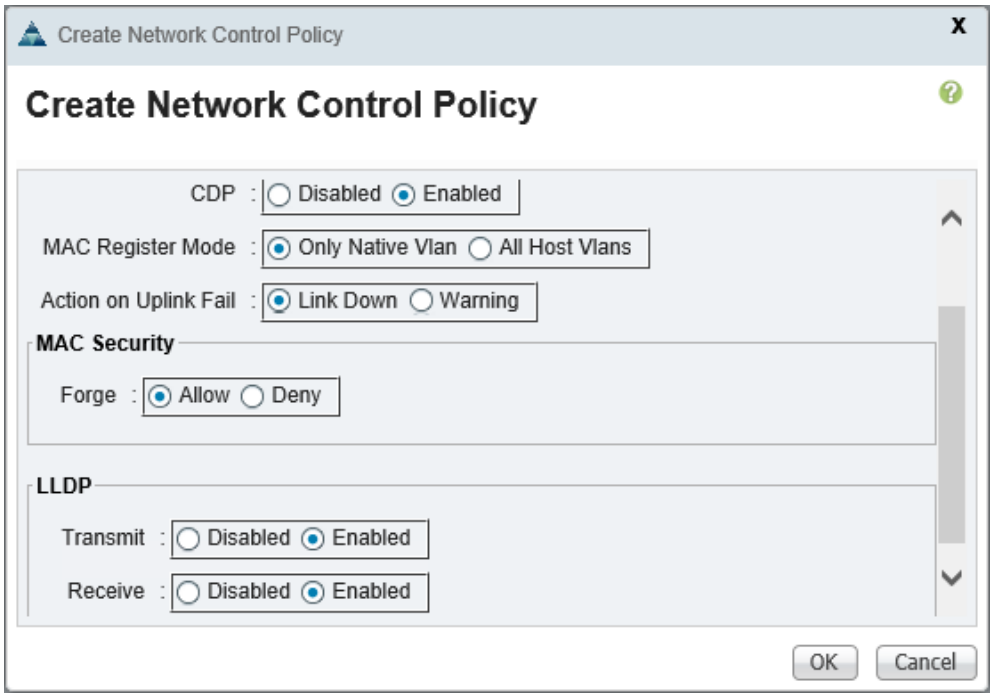
7. Click **OK** again.

Create Network Control Policy for Cisco Discovery Protocol and Link Layer Discovery Protocol

To create a network control policy that enables Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) on virtual network ports, complete the following steps:

1. In Cisco UCS Manager, click the **LAN** tab in the navigation pane.
2. Select Policies > root.
3. Right-click Network Control Policies and choose Create Network Control Policy.

4. Enter Enable-LLDP-CDP as the policy name.
5. For CDP, select the Enabled option.
6. For LLDP, select Enabled for both Transmit and Receive.
7. Click **OK** to create the network control policy.

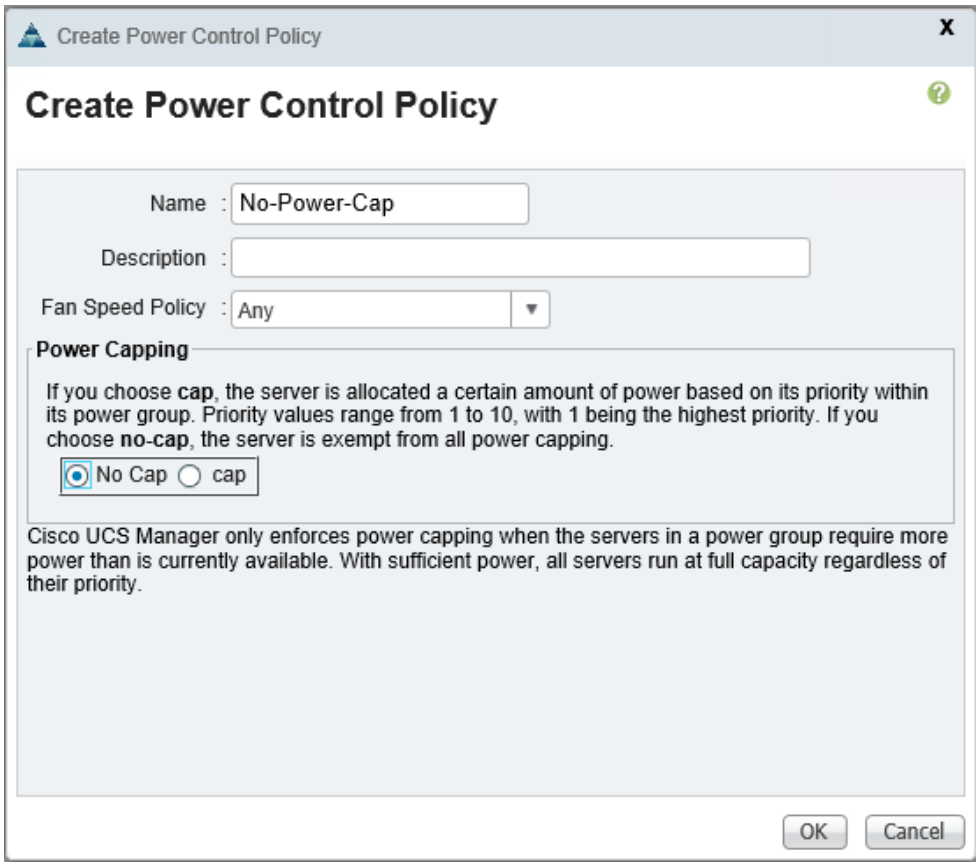


8. Click **OK**.

Create Power Control Policy

To create a power control policy for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the **Servers** tab in the navigation pane.
2. Select Policies > root.
3. Right-click Power Control Policies and choose Create Power Control Policy.
4. Enter No-Power-Cap as the power control policy name.
5. Change the power capping setting to No Cap.
6. Click **OK** to create the power control policy.
7. Click **OK**.



Create Server Pool Qualification Policy (Optional)

To create an optional server pool qualification policy for the Cisco UCS environment, complete the following steps:

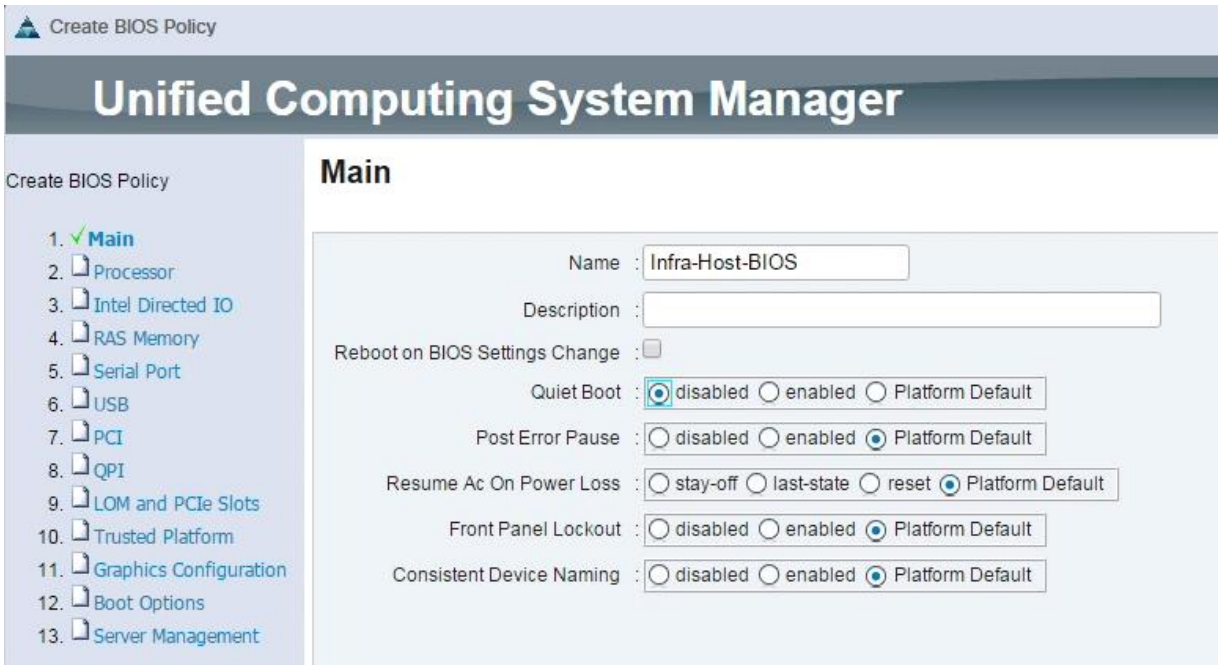
This example creates a policy for selecting a Cisco UCS B200-M4 server.

1. In Cisco UCS Manager, click the **Servers** tab in the navigation pane.
2. Select Policies > root.
3. Right-click Server Pool Policy Qualifications and choose Create Server Pool Policy Qualification.
4. Enter UCSB-B200-M4 as the name for the policy.
5. Choose Create Server PID Qualifications.
6. Select UCSB-B200-M4 as the PID.
7. Click **OK**.
8. Click **OK** to create the server pool policy qualification.

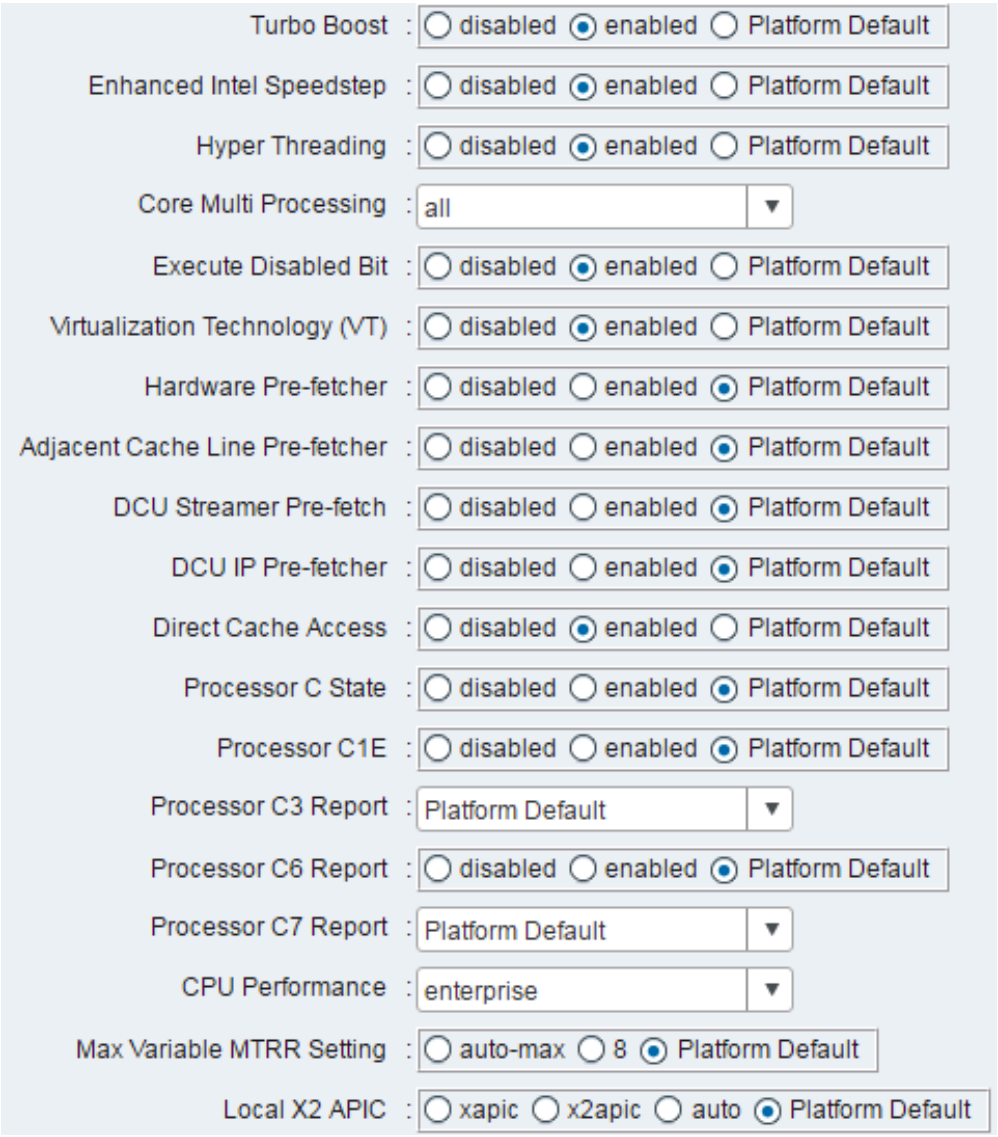
Create Server BIOS Policy

To create a server BIOS policy for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the **Servers** tab in the navigation pane.
2. Select Policies > root.
3. Right-click BIOS Policies and choose Create BIOS Policy.
4. Enter Infra-Host-BIOS as the BIOS policy name.
5. Change the Quiet Boot setting to disabled.

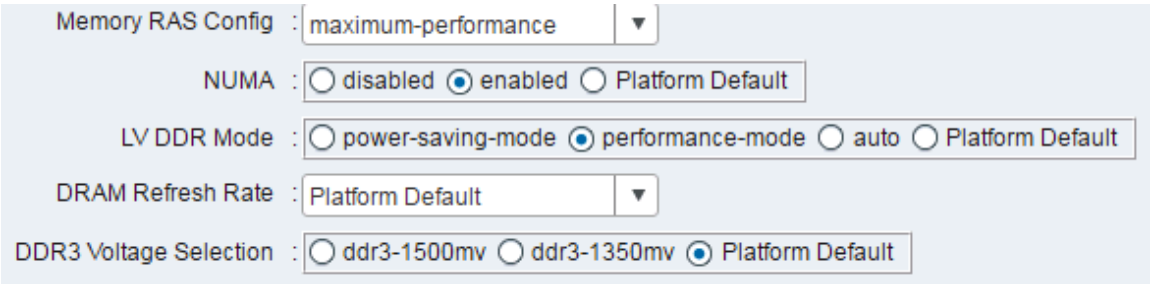


6. Click **Next**.
7. On the next screen labeled as Processor, make changes as captured in the following figure for high compute performance.



8. Click **Next** and under the screen labeled Intel Direct IO, make changes as captured in the following figure.

9. Click **Next** and under the screen labeled RAS Memory, make changes as captured in the following figure.

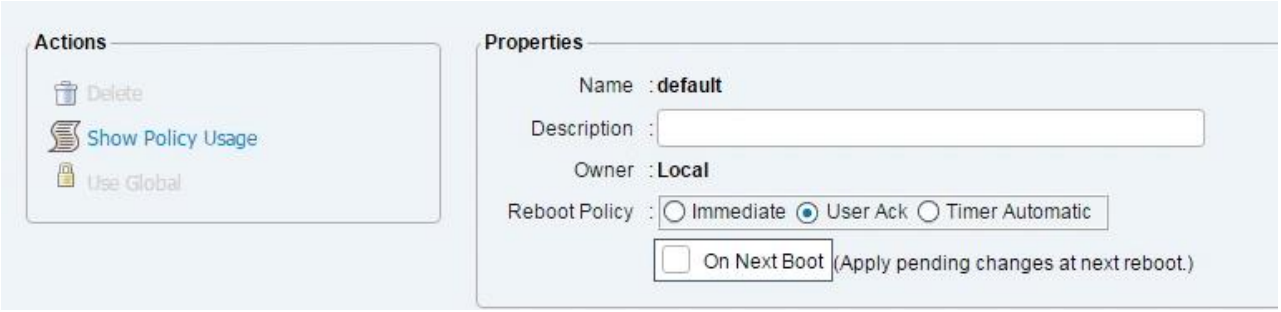


10. Click **Finish** to create the BIOS policy.
11. Click **OK**.

Update Default Maintenance Policy

To update the default Maintenance Policy, complete the following steps:

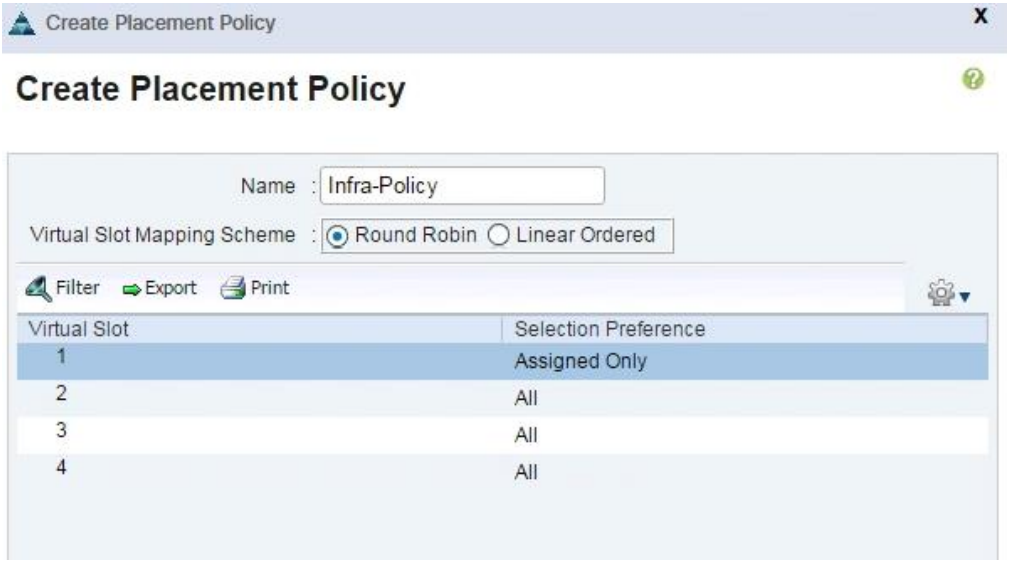
1. In Cisco UCS Manager, click the **Servers** tab in the navigation pane.
2. Select Policies > root and then select Maintenance Policies > default.
3. Change the Reboot Policy to User Ack.
4. Click Save Changes and OK.
5. Click **OK** to accept the change.



Create vNIC/vHBA Placement Policy

To create a vNIC/vHBA placement policy for the infrastructure hosts, complete the following steps:

1. In Cisco UCS Manager, click the **Servers** tab in the navigation pane.
2. Select Policies > root.
3. Right-click vNIC/vHBA Placement Policies and choose **Create Placement Policy**.
4. Enter Infra-Policy as the name of the placement policy.
5. Click 1 and select Assigned Only.
6. Click **OK** and then click **OK** again.



Create vNIC Templates

Eight different vNIC Templates are covered in Table 13 below. Not all the VNICs need to be created in all deployments. The vNICs templates covered below are for iSCSI vNICs, infrastructure (storage, management etc.) vNICs, and data vNICs (VM traffic) for VMware VDS or Cisco AVS. Refer to Usage column in Table 13 below to see if a vNIC is needed for a particular ESXi host.

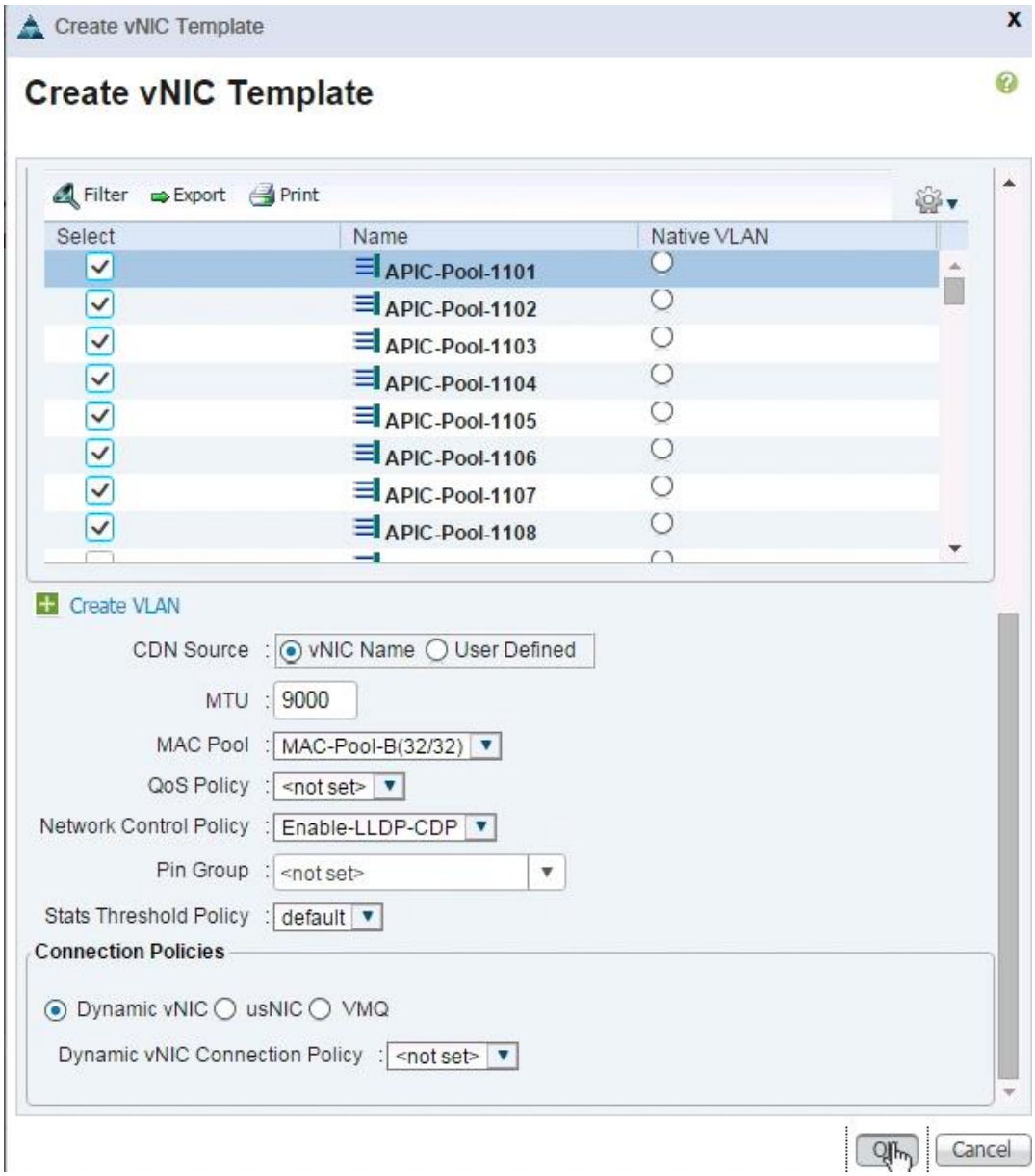
Table 13 vNIC Templates and associated VLANs

Name	Fabric ID	VLANs	Native VLAN	MAC Pool	Usage
Infra-vNIC-A	A	IB-Mgmt, Infra-NFS*, Native-2, vMotion	Native-2	MAC-Pool-A	All ESXi Hosts; * Infra-NFS VLAN only needed when using IBM v7000 Unified File Modules
Infra-vNIC-B	B	IB-Mgmt, Infra-NFS*, Native-2, vMotion	Native-2	MAC-Pool-B	All ESXi Hosts; * Infra-NFS VLAN only needed when using IBM v7000 Unified File Modules
Infra-iSCSI-A	A	Infra-iSCSI-A	Infra-iSCSI-A	MAC-Pool-A	iSCSI hosts only (IBM v9000)
Infra-iSCSI-B	B	Infra-iSCSI-B	Infra-iSCSI-B	MAC-Pool-B	iSCSI hosts only (IBM v9000)
Infra-vNIC-VDS-A	A	APIC-Pool-1101 through APIC-Pool-1200		MAC-Pool-A	All hosts using APIC controlled VDS as distributed switch
Infra-vNIC-VDS-B	B	APIC-Pool-1101 through APIC-Pool-1200		MAC-Pool-B	All hosts using APIC controlled VDS as distributed switch
Infra-vNIC-AVS-A	A	AVS-Infra		MAC-Pool-A	All hosts using APIC controlled AVS as distributed switch

Infra-vNIC-AVS-B	B	AVS-Infra		MAC-Pool-B	All hosts using APIC controlled AVS as distributed switch

Repeat the following steps for all the required vNICs in a customer deployment scenario (Table 13):

1. In Cisco UCS Manager, select the **LAN** tab.
2. Select Policies > root.
3. Right-click vNIC Templates and choose Create vNIC Template.
4. Enter Name (listed in Table 13) of the vNIC template name.
5. Select Fabric A or B as listed in Table 13. Do not select the Enable Failover check box.
6. Under Target, make sure that the VM check box is not selected.
7. Select Updating Template for Template Type.
8. Under VLANs, select all the VLANs as listed in Table 13.
9. Set appropriate VLAN as Native VLAN; if a Native VLAN is not listed in the Table 13; do not change the Native VLAN parameters.
10. Under MTU, enter 9000.
11. From the MAC Pool list, select appropriate MAC pool as listed in Table 13.
12. From the Network Control Policy list, select Enable-CDP-LLDP.
13. Click **OK** to complete creating the vNIC template.
14. A sample screenshot for a vNIC is shown below.



15. Click **OK**.

16. Repeat the process to define all the necessary vNIC templates.

Create LAN Connectivity Policies

A LAN connectivity policy defines the vNICs that will be created as part of a service profile deployment. Depending on the storage protocol in use and distributed switch selected, LAN connectivity policy will differ. Refer to Table 14 for a list of vNICs that need to be created as part of LAN connectivity policy definition.

Table 14 vNIC list for LAN connectivity policy

vNIC Name	vNIC Template	Usage
vNIC-A	Infra-vNIC-A	All ESXi Hosts
vNIC-B	Infra-vNIC-B	All ESXi Hosts

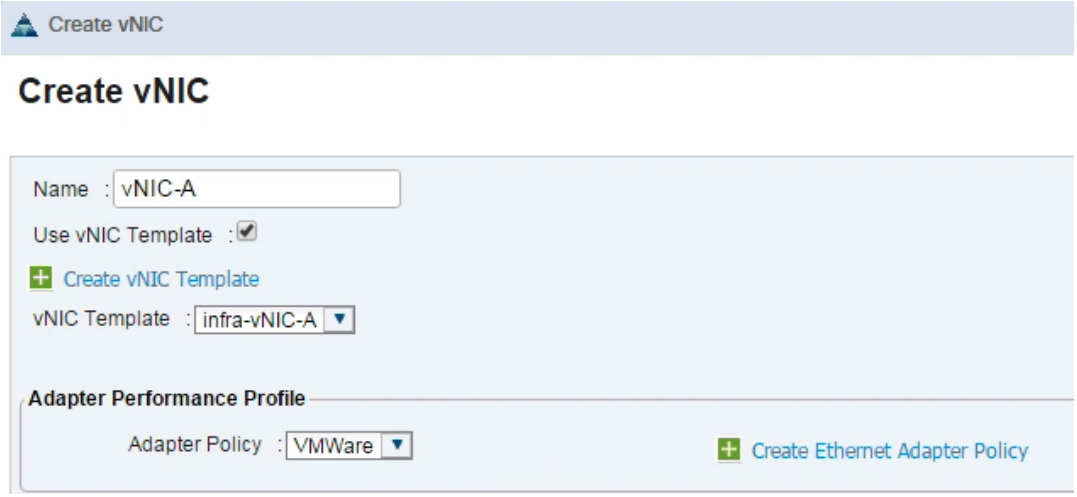
vNIC-VDS-A	Infra-vNIC-VDS-A	Hosts using APIC controlled VDS as distributed switch
vNIC-VDS-B	Infra-vNIC-VDS-B	Hosts using APIC controlled VDS as distributed switch
vNIC-AVS-A	Infra-vNIC-AVS-A	All hosts using APIC controlled AVS as distributed switch
vNIC-AVS-B	Infra-vNIC-AVS-B	All hosts using APIC controlled AVS as distributed switch
vNIC-iSCSI-A	Infra-iSCSI-A	iSCSI hosts only - IBM v9000
vNIC-iSCSI-B	Infra-iSCSI-B	iSCSI hosts only - IBM v9000

To configure the necessary Infrastructure LAN Connectivity Policies, complete the following steps:

Adding vNICs in LAN policy

The steps in this procedure would be repeated to create all the necessary vNICs covered in Table 14.

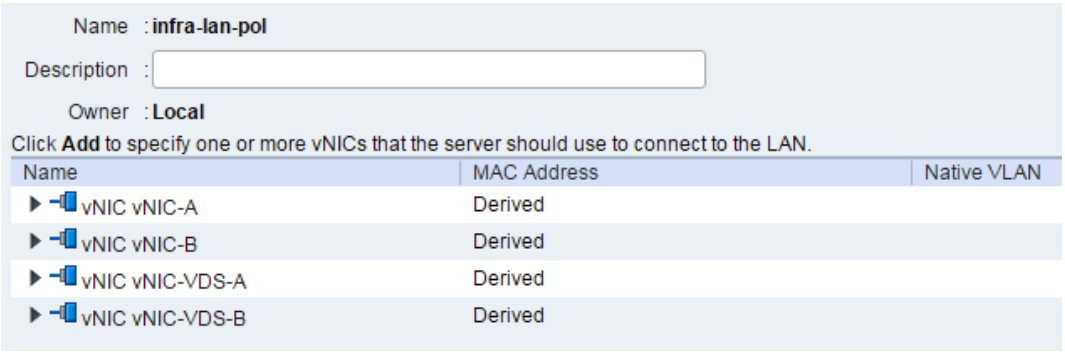
1. In Cisco UCS Manager, click the **LAN** tab in the navigation pane.
2. Select LAN > Policies > root.
3. Right-click LAN Connectivity Policies and choose Create LAN Connectivity Policy.
4. Enter Infra-lan-policy as the name of the policy.
5. Click **Add** to add a vNIC.
6. In the Create vNIC dialog box, the name of the vNIC from Table 14.
7. Select the Use vNIC Template checkbox.
8. In the vNIC Template list, select the corresponding vNIC template from Table 14.
9. For the Adapter Policy field, select VMWare.
10. Click **OK** to add this vNIC to the policy.



11. Click **Add** to add another vNIC to the policy.

12. Repeat the above steps to add all the vNICs as defined in Table 14.

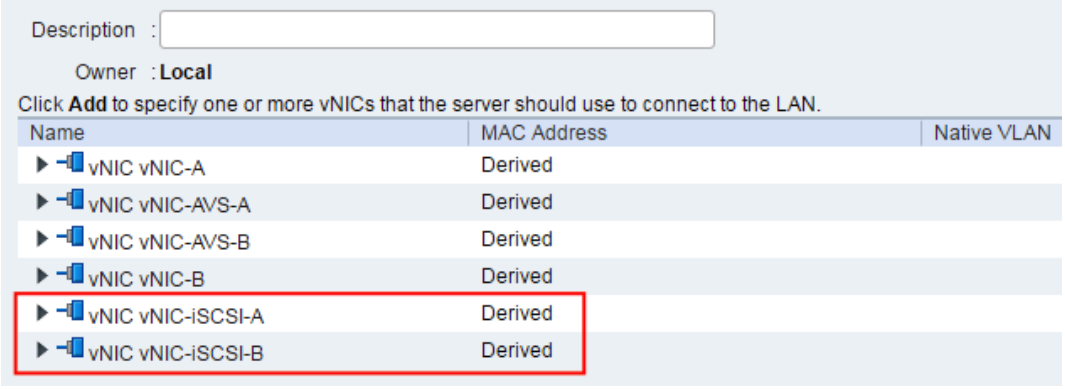
13. Verify that the proper vNICs have been created for your VersaStack Implementation. A sample output for FC only hosts is shown below.



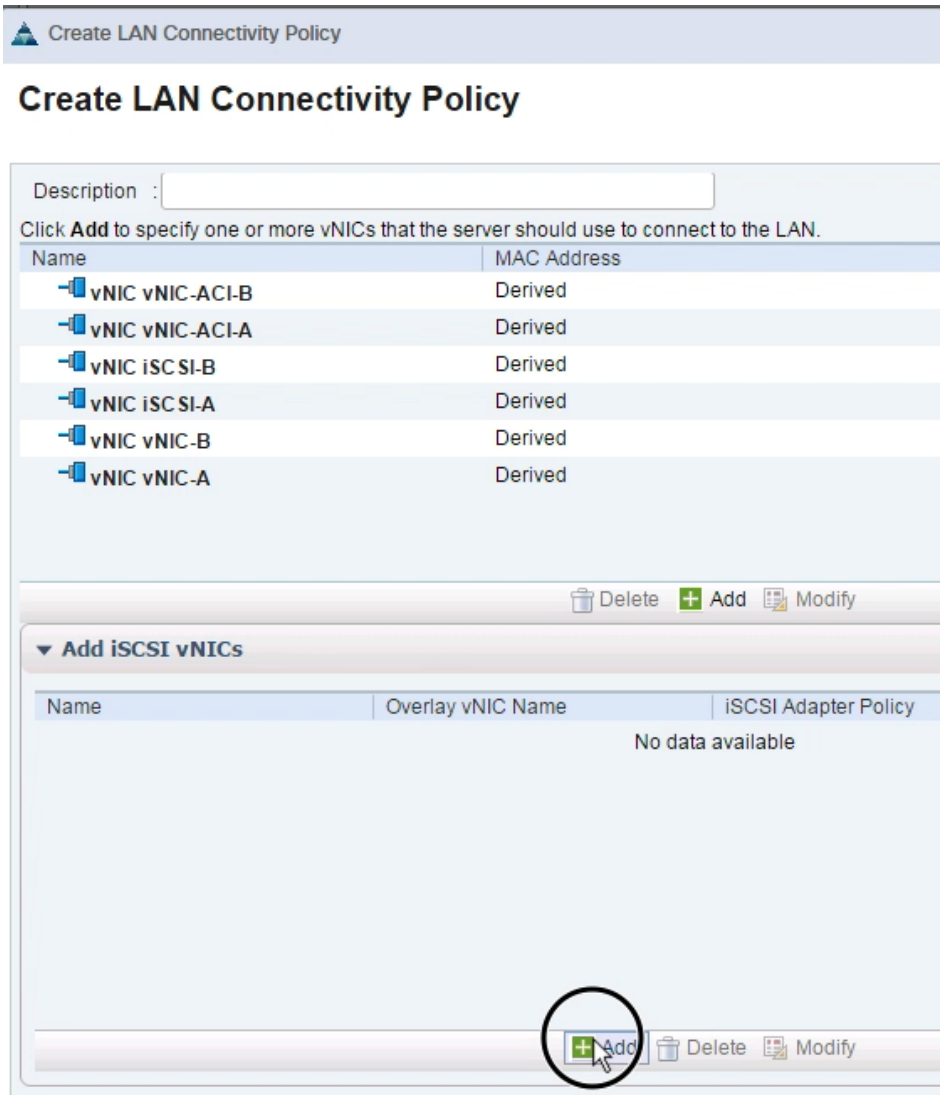
Adding iSCSI vNICs in LAN policy

Complete the following Steps only if you are using iSCSI SAN access:

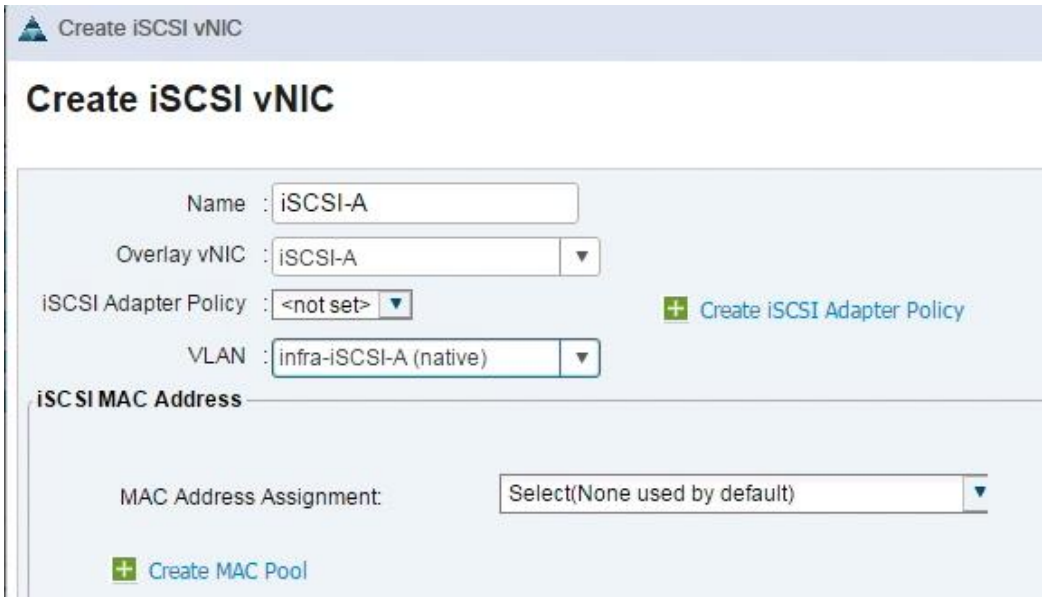
1. Verify the iSCSI base vNICs are already added as part of vNIC implementation (steps 1-14).



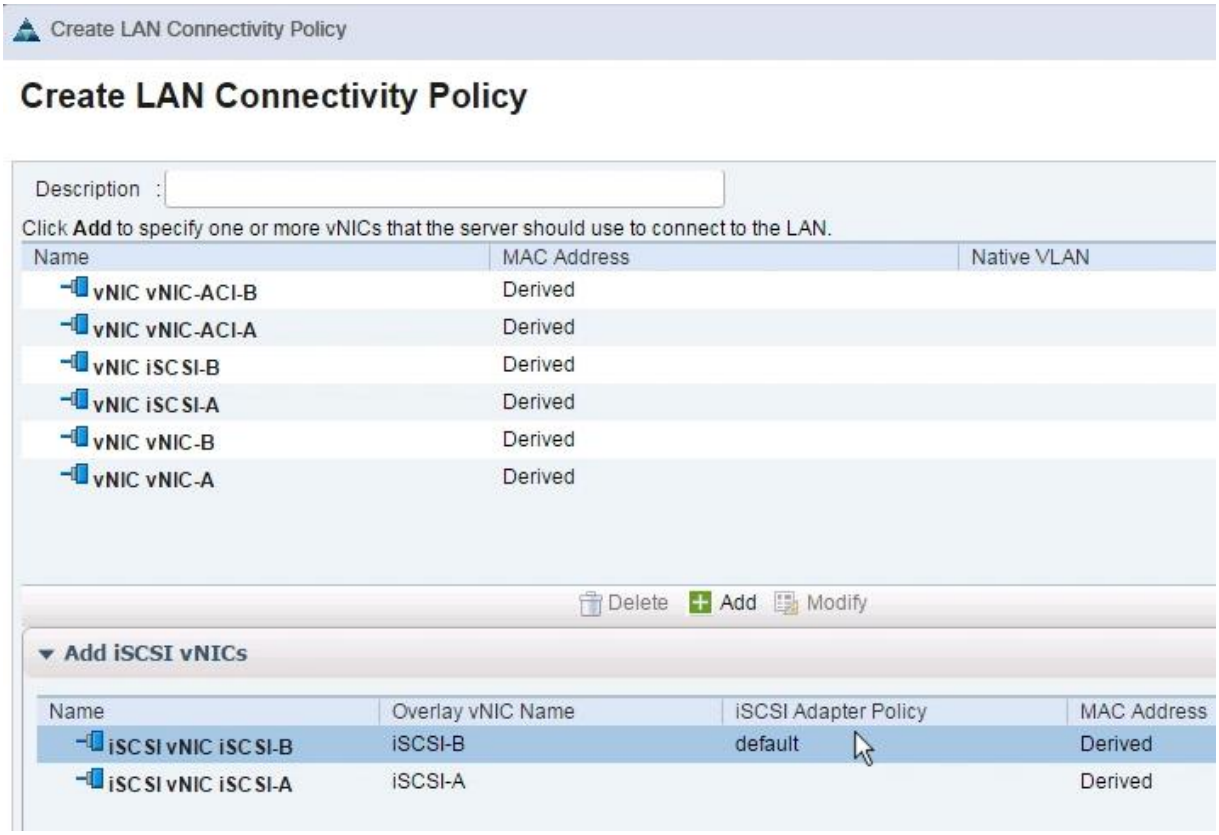
2. Expand the Add iSCSI vNICs section to add the iSCSI boot vNICs.
3. Click **Add** in the iSCSI vNIC section to define an iSCSI boot vNIC.



4. Enter iSCSI-A as the name of the vNIC.
5. Select Infra-iSCSI-A for Overlay vNIC.
6. Set the iSCSI Adapter Policy to default.
7. Set the VLAN to Infra-iSCSI-A (native).
8. Leave the MAC Address set to None.
9. Click **OK**.



10. Click **Add** in the iSCSI vNIC section again.
11. Enter iSCSI-B as the name of the vNIC.
12. Set the Overlay vNIC to Infra-iSCSI-B.
13. Set the iSCSI Adapter Policy to default.
14. Set the VLAN to Infra-iSCSI-B (native).
15. Leave the MAC Address set to None.
16. Click **OK**.
17. Verify that the iSCSI vNICs are created correctly.

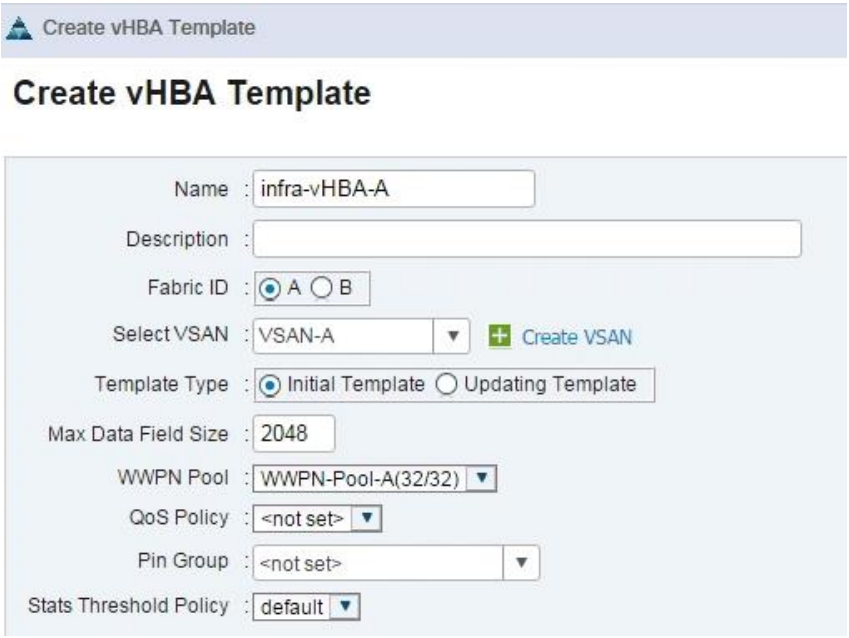


18. Click **OK** then **OK** again to create the LAN Connectivity Policy.

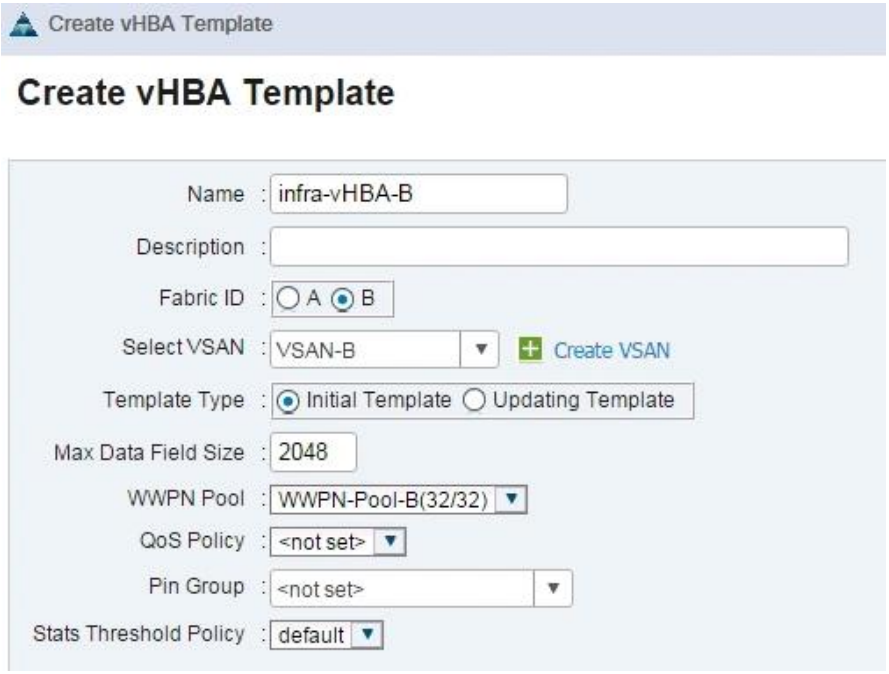
Create vHBA Templates for FC Connectivity (IBM V7000 only)

To create virtual host bus adapter (vHBA) templates for the Cisco UCS environment, follow these steps:

1. In Cisco UCS Manager, click the **SAN** tab in the navigation pane.
2. Select Policies > root.
3. Right-click vHBA Templates and choose Create vHBA Template.
4. Enter Infra-vHBA-A as the vHBA template name.
5. Click the radio button to select Fabric A.
6. In the Select VSAN list, Choose VSAN-A.
7. In the WWPN Pool list, Choose WWPN-Pool-A.



8. Click **OK** to create the vHBA template.
9. Click **OK**.
10. Right-click vHBA Templates again and choose Create vHBA Template.
11. Enter Infra-vHBA-B as the vHBA template name.
12. Click the radio button to select Fabric B.
13. In the Select VSAN list, Choose VSAN-B.
14. In the WWPN Pool, Choose WWPN-Pool-B.



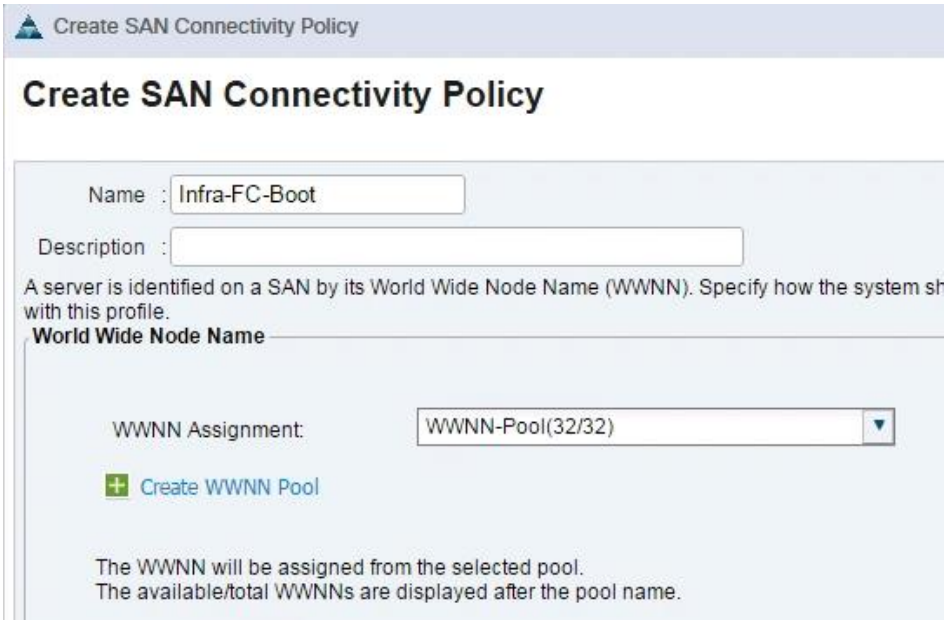
15. Click **OK** to create the vHBA template.
16. Click **OK**.

Create FC SAN Connectivity Policies (IBM V7000 only)

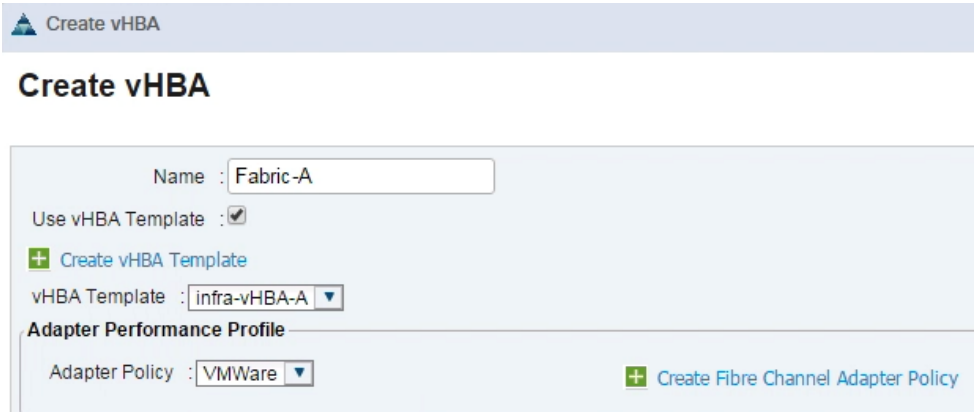
A SAN connectivity policy defines the vHBAs that will be created as part of a service profile deployment.

To configure the necessary Infrastructure LAN Connectivity Policies, complete the following steps:

1. In Cisco UCS Manager, click the **SAN** tab in the navigation pane.
2. Select SAN > Policies > root.
3. Right-click SAN Connectivity Policies and choose Create SAN Connectivity Policy.
4. Enter Infra-FC-Boot as the name of the policy.
5. Select WWNN-Pool from the drop-down list under World Wide Node Name.

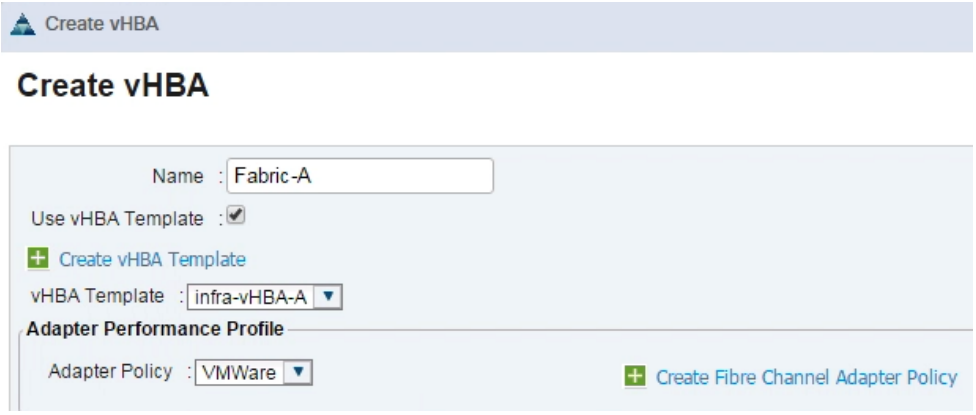


6. Click **Add**.
7. Under Create vHBA, enter Fabric-A in the Name field.
8. Check the check box Use vHBA Template.
9. From the vHBA Template drop-down list, select infra-vHBA-A.
10. From the Adapter Policy drop-down list, select VMWare.



11. Click **OK**.
12. Click **Add**.
13. Under Create vHBA, enter Fabric-B in the Name field.
14. Check the check box next to Use vHBA Template.
15. From the vHBA Template drop-down list, select infra-vHBA-B.

16. From the Adapter Policy drop-down list, select VMWare.



17. Click **OK**.
18. Click **OK** again to accept creating the SAN connectivity policy.

Create iSCSI Boot Policy (IBM V9000 Only)

This procedure applies to a Cisco UCS environment in which iSCSI interface on Controller A is chosen as the primary target.

To create boot the policy for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the **Servers** tab in the navigation pane.
2. Select Policies > root.
3. Right-click Boot Policies and choose Create Boot Policy.
4. Enter Boot-iSCSI-A as the name of the boot policy.
5. **Optional**: Enter a description for the boot policy.
6. Keep the Reboot on Boot Order Change option cleared.
7. Expand the Local Devices drop-down menu and select Add CD/DVD.
8. Expand the iSCSI vNICs section and select Add iSCSI Boot.
9. In the Add iSCSI Boot dialog box, enter iSCSI-vNIC-A.
10. Click **OK**.
11. Select Add iSCSI Boot.
12. In the Add iSCSI Boot dialog box, enter iSCSI-vNIC-B.
13. Click **OK**.

14. Click **OK** then **OK** again to save the boot policy.

Create FC Boot Policies (IBM v7000 Only)

This procedure applies to a Cisco UCS environment in which two FC interfaces are used on the IBM Storwize V7000 Node 1 and two FC interfaces are used on Node 2. This procedure captures a single boot policy which defines Fabric-A as the primary fabric. Customer can choose to create a second boot policy which can use Fabric-B as primary fabric to spread the boot-from-san traffic load on both the nodes in case of disaster recovery.

WWPN information from the IBM v7000 is required to complete this section. This information can be found by logging into the IBM Storwize GUI and hovering the mouse over the FC ports as shown in the figure below. The information can be recorded in Table 15.

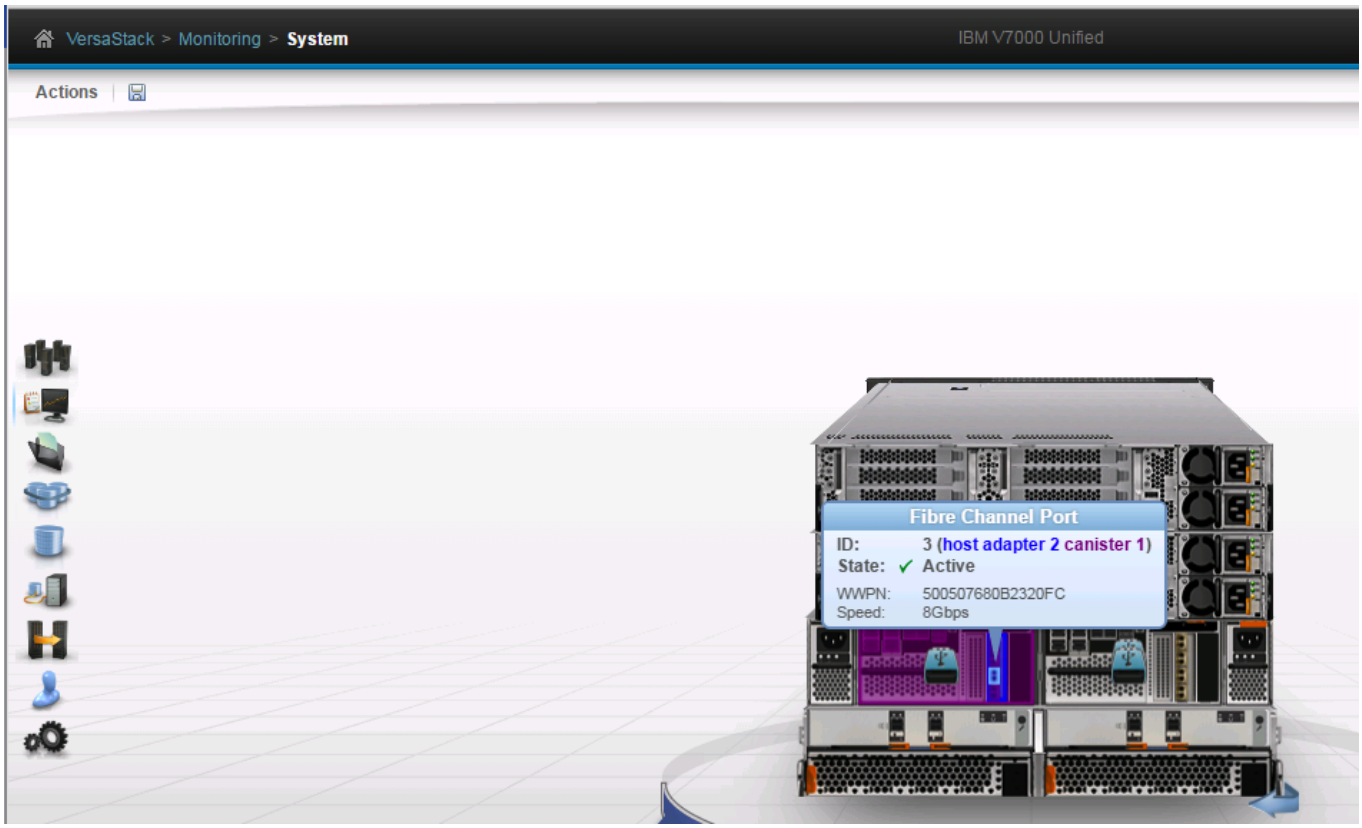
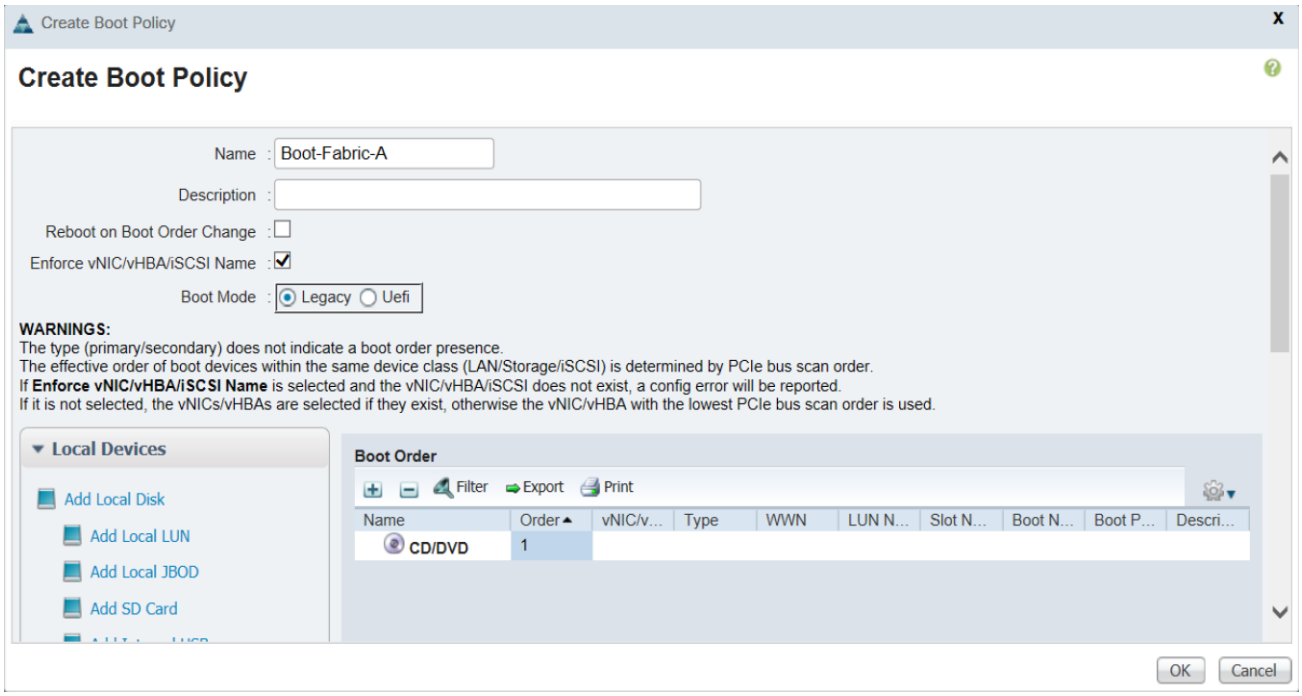


Table 15 IBM V7000 Unified – WWPN Information

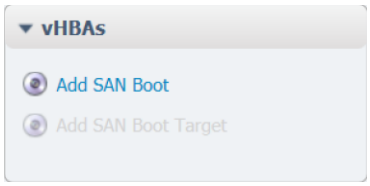
Node	Port ID	WWPN	Variable
Node 1	3		WWPN-Node-1-Fabric-A
Node 1	4		WWPN-Node-1-Fabric-B
Node 2	3		WWPN-Node-2-Fabric-A
Node 2	4		WWPN-Node-2-Fabric-B

To create boot policies for the Cisco UCS environment, complete the following steps:

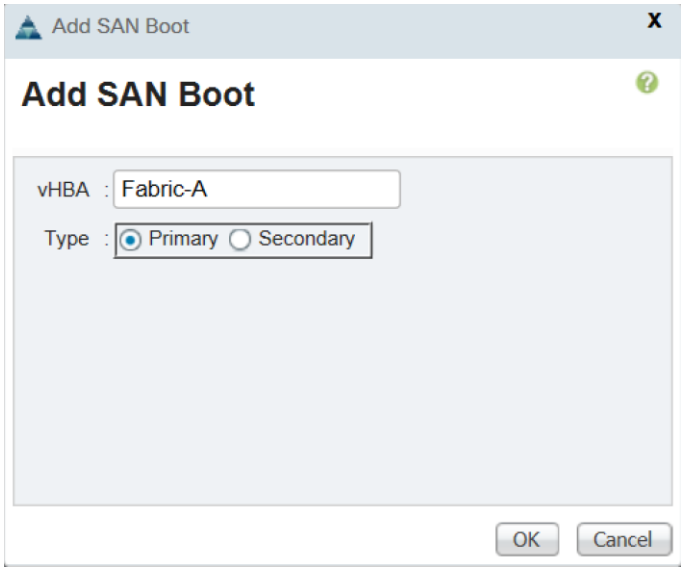
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Choose Policies > root.
3. Right-click Boot Policies and choose Create Boot Policy.
4. Enter Boot-Fabric-A as the name of the boot policy.
5. **Optional**: Enter a description for the boot policy.
6. Keep the Reboot on the Boot Order Change check box unchecked.
7. Expand the Local Devices drop-down list and Choose Add CD/DVD.



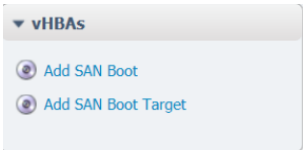
8. Expand the vHBAs drop-down list and Choose Add SAN Boot.



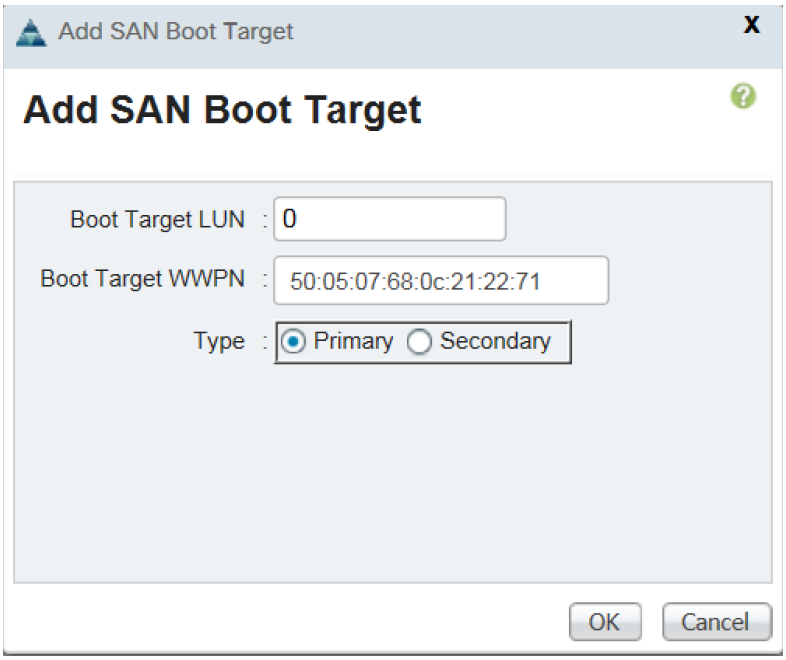
9. In the Add SAN Boot dialog box, enter Fabric-A in the vHBA field.
10. Make sure that the Primary radio button is selected as the SAN boot type.
11. Click **OK** to add the SAN boot initiator.



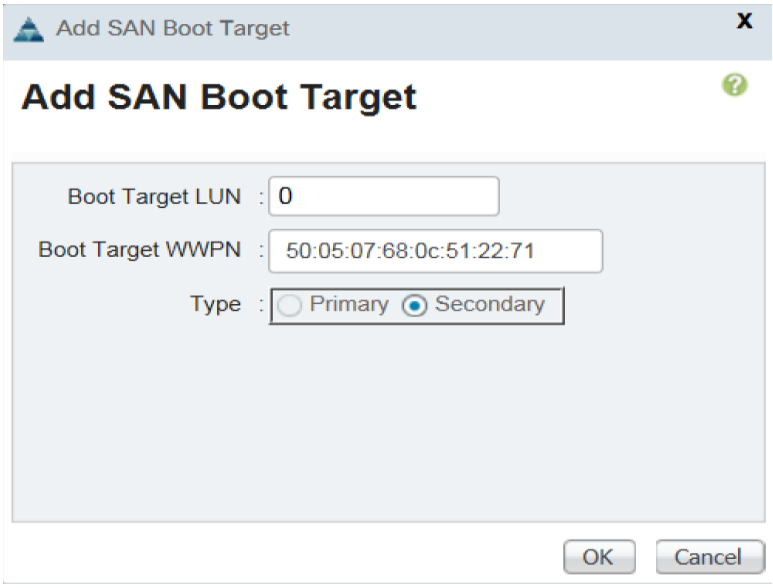
12. From the vHBA drop-down menu, choose Add SAN Boot Target.



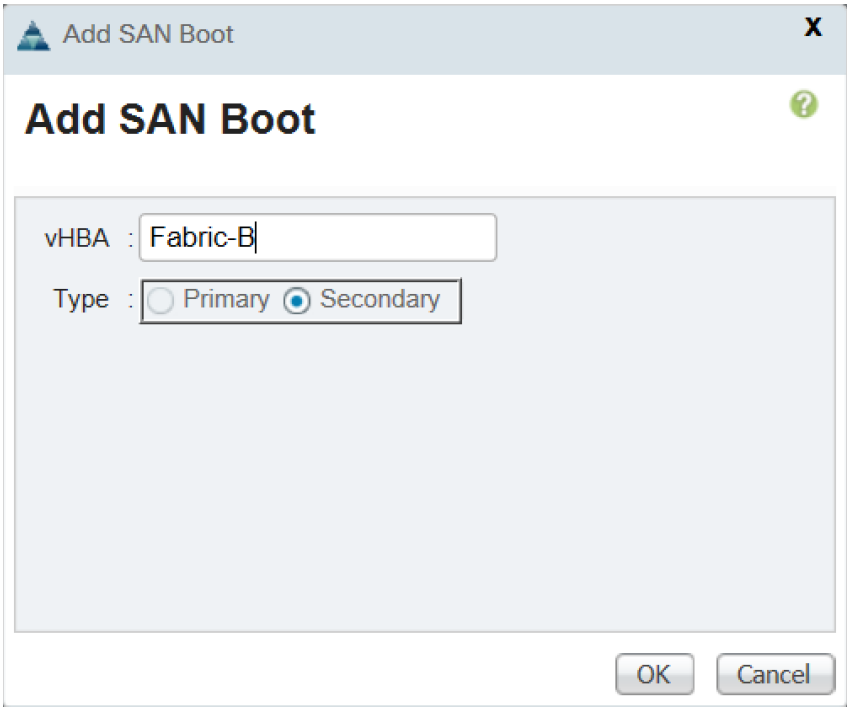
13. Keep 0 as the value for Boot Target LUN.
14. Enter the WWPN <WWPN-Node-1-Fabric-A> from Table 15.
15. Keep the Primary radio button selected as the SAN boot target type.
16. Click **OK** to add the SAN boot target.



17. From the vHBA drop-down menu, choose Add SAN Boot Target.
18. Keep 0 as the value for Boot Target LUN.
19. Enter the WWPN <WWPN-Node-2-Fabric-A> from Table 15.
20. Click **OK** to add the SAN boot target.

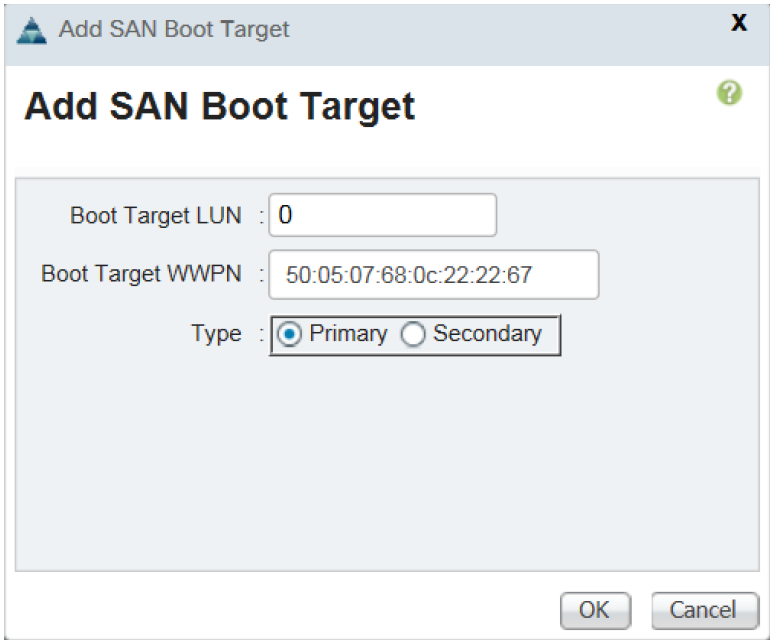


21. From the vHBA drop-down list, choose Add SAN Boot.
22. In the Add SAN Boot dialog box, enter Fabric-B in the vHBA box.
23. The SAN boot type should automatically be set to Secondary.
24. Click **OK** to add the SAN boot initiator.

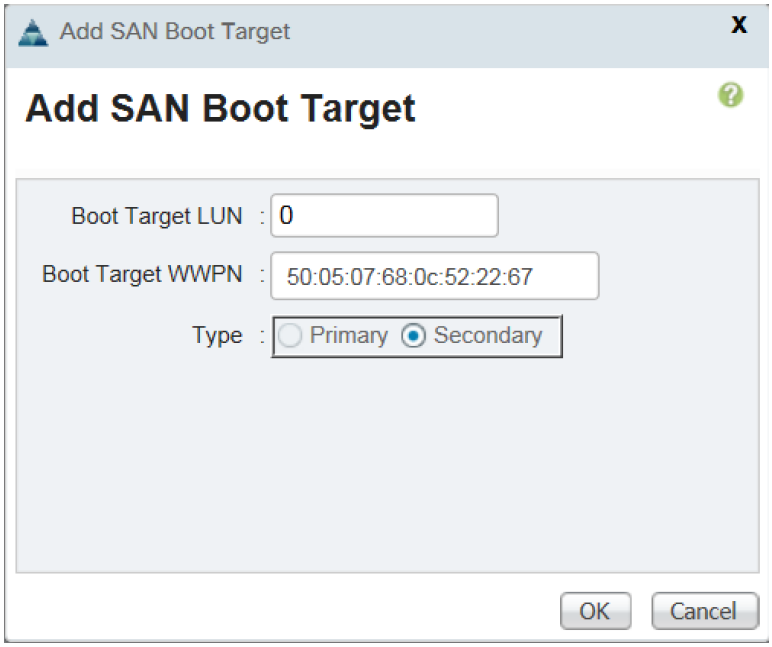


25. From the vHBA drop-down list, choose Add SAN Boot Target.
26. Keep 0 as the value for Boot Target LUN.
27. Enter the WWPN <WWPN-Node-1-Fabric-B> from Table 15.

28. Keep Primary as the SAN boot target type.
29. Click **OK** to add the SAN boot target.

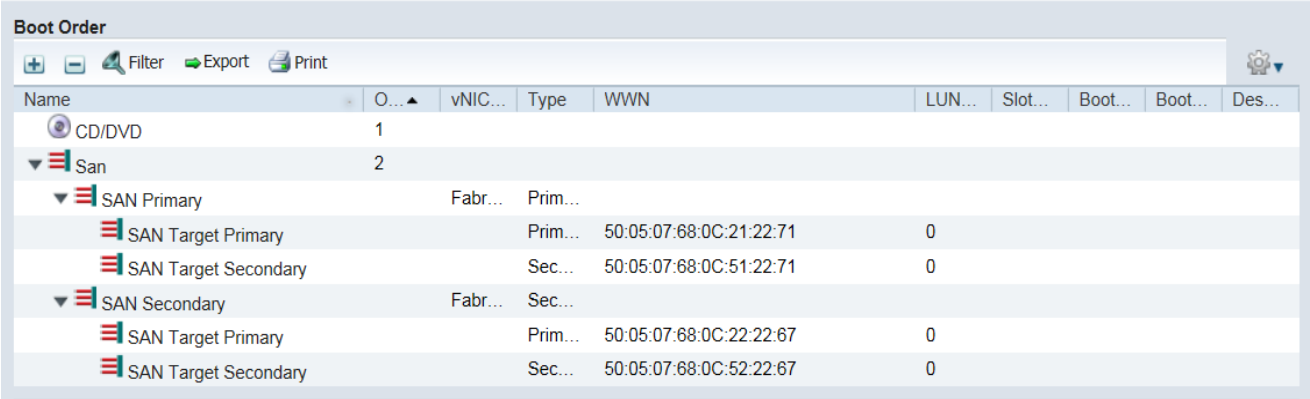


30. From the vHBA drop-down list, choose Add SAN Boot Target.
31. Keep 0 as the value for Boot Target LUN.
32. Enter the WWPN <WWPN-Node-2-Fabric-B> from Table 15
33. Click **OK** to add the SAN boot target.



34. Click **OK**, and then click **OK** again to create the boot policy.

35. Verify that your configuration looks similar to the screenshot below.

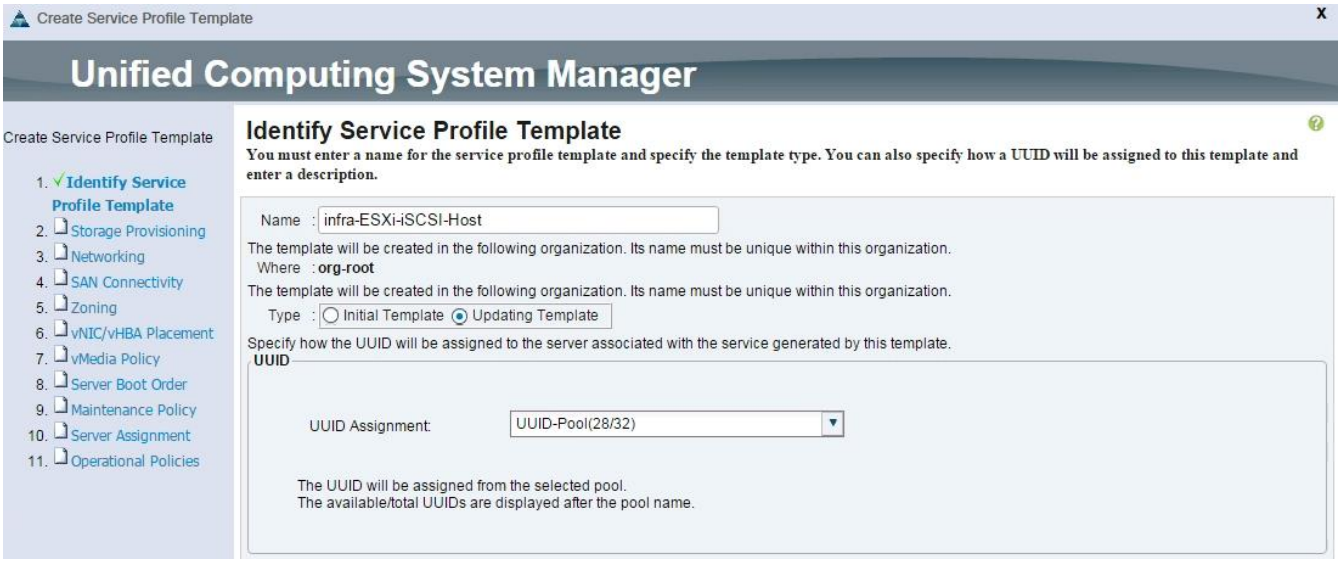


Create iSCSI Boot Service Profile Template (IBM V9000 only)

Service profile template configuration for the IBM V9000 iSCSI based SAN access is covered in this section.

To create the service profile template, complete the following steps:

1. In Cisco UCS Manager, click the **Servers** tab in the navigation pane.
2. Select Service Profile Templates > root.
3. Right-click root and choose **Create Service Profile Template**. This opens the Create Service Profile Template wizard.
4. Enter infra-ESXi-iSCSI-Host as the name of the service profile template. This service profile template is configured to boot from storage node 1 on fabric A.
5. Select the Updating Template option.
6. Under UUID, select UUID-Pool as the UUID pool.
7. Click **Next**.

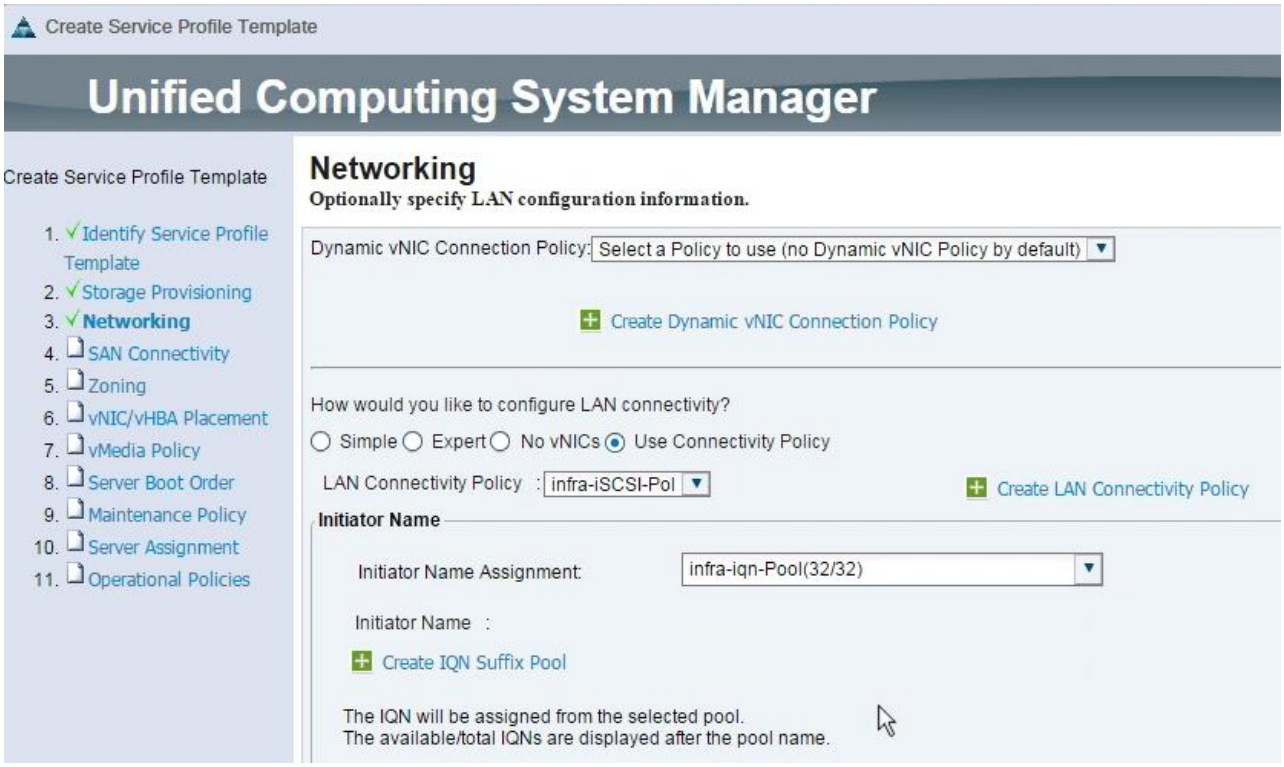


Configure Storage Provisioning:

1. In Storage Provisioning window, select the **Local Disk Configuration Policy** tab.
2. Select the option SAN-Boot for Local Storage Policy. This policy usage requires servers with no local HDDs.
3. Click **Next**.

Configure Networking Options:

1. In the Networking window, keep the default setting for Dynamic vNIC Connection Policy.
2. Select the Use Connectivity Policy option to configure the LAN connectivity.
3. Select the infra-iSCSI-Pol as the LAN Connectivity Policy.
4. Select infra-iqn-Pool for Initiator Name Assignment.
5. Click **Next**.



Configure SAN Connectivity:

6. Select the No vHBAs option for the How would you like to configure SAN connectivity? field and continue on to the next section.

7. Click **Next**.

Configure Zoning

1. For iSCSI boot option, it is not necessary to configure any Zoning options. Click **Next**.

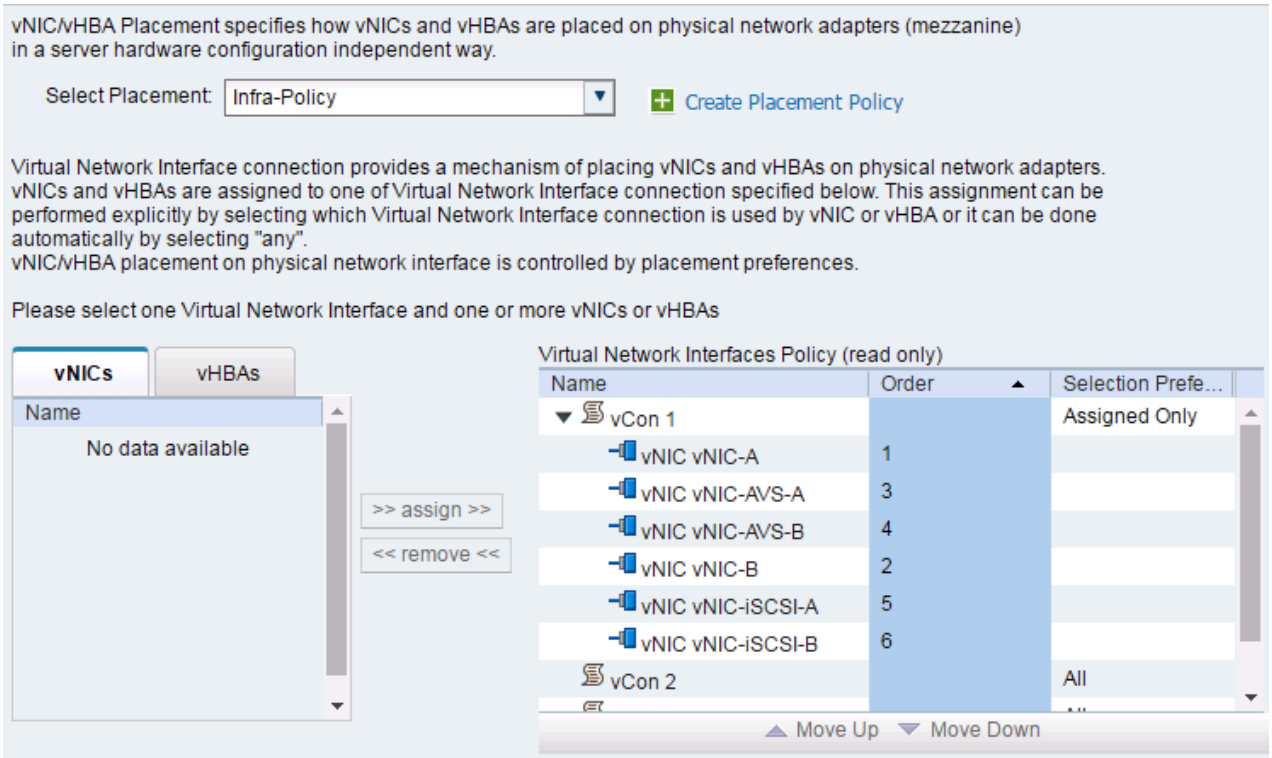
Configure vNIC/vHBA Placement

1. In the vNIC/vHBA Placement window, for the field Select Placement, select Infra-Policy.

2. Choose vCon 1 and assign the vHBAs/vNICs to the virtual network interfaces policy in the following order:

   - vNIC-A
   - vNIC-B
   - vNIC-VDS-A OR vNIC-AVS-A (depending on distributed switch in use)
   - vNIC-VDS-B OR vNIC-AVS-B (depending on distributed switch in use)
   - vNIC-iSCSI-A
   - vNIC-iSCSI-B

3. Click **Next**.

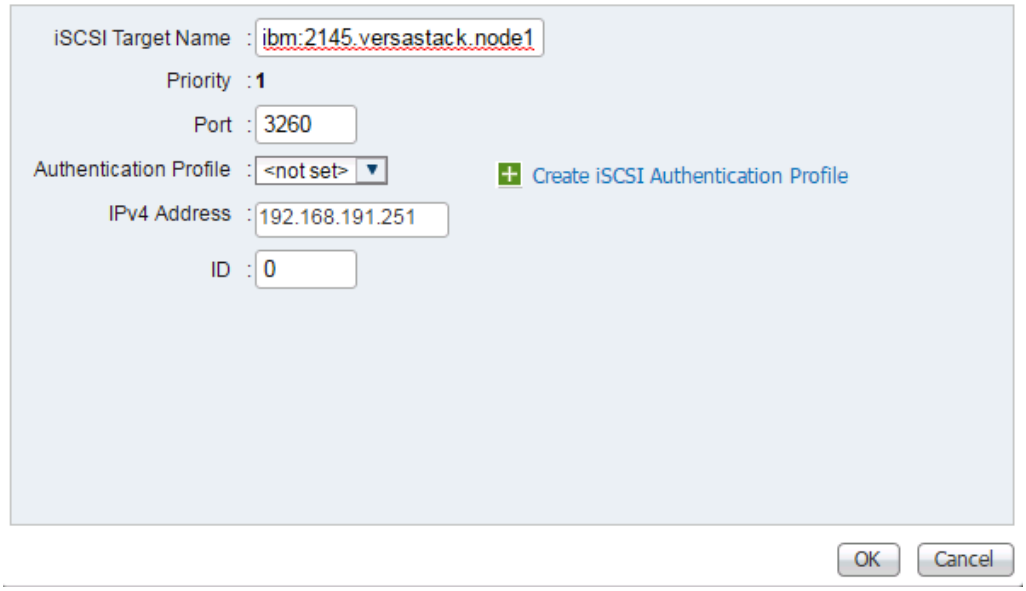


Configure vMedia Policy

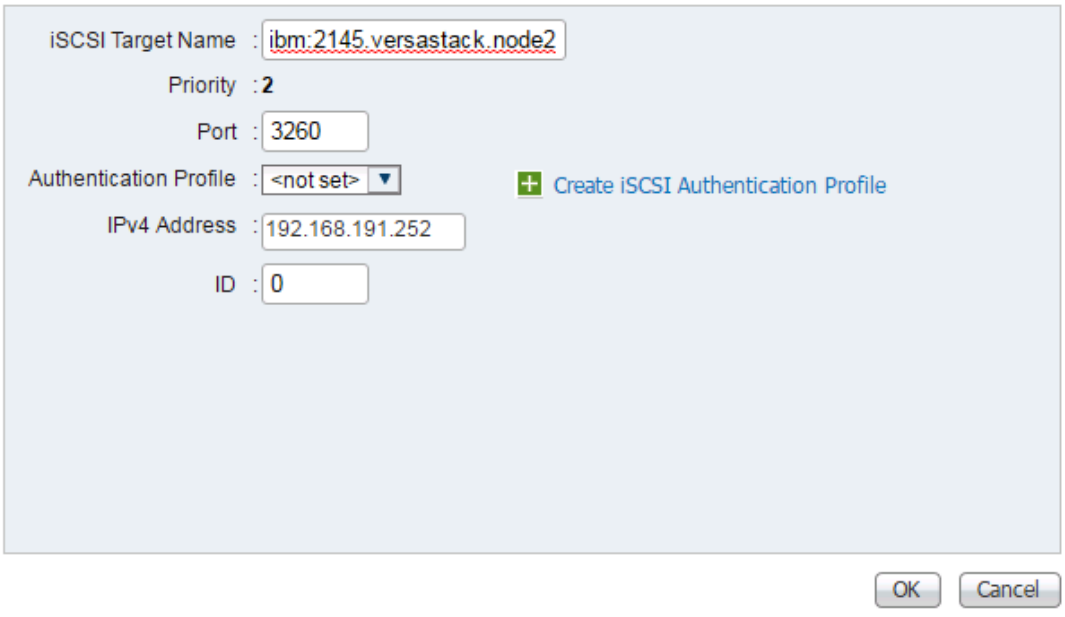
1. Do not configure a vMedia Policy.
2. Click **Next**.

Configure Server Boot Order

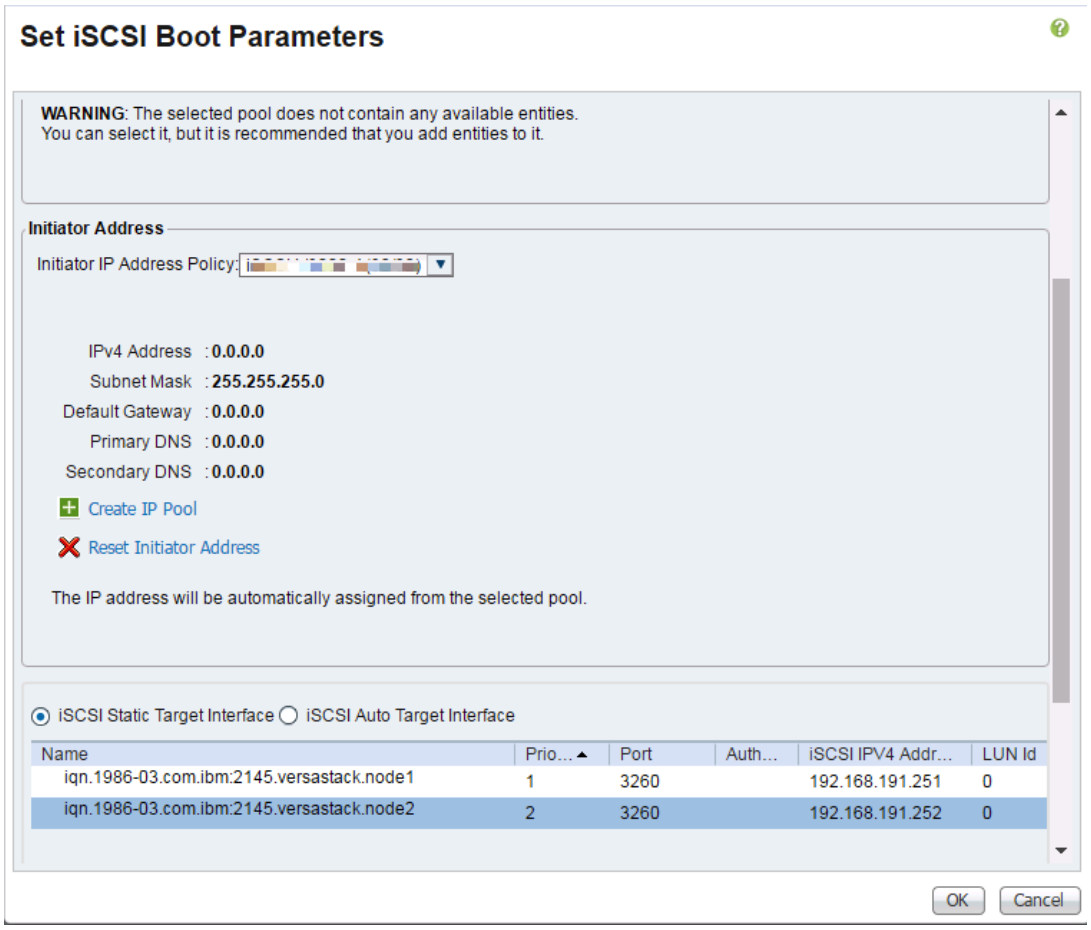
1. Select Boot-iSCSI-A for Boot Policy.
2. In the Boot Order pane, expand iSCSI and select iSCSI-A .
3. Click Set iSCSI Boot Parameters.
4. Leave the Initiator Name Assignment dialog box <not set> to use the single Service Profile Initiator Name defined in the previous steps.
5. Set iSCSI-initiator-A as the Initiator IP address Policy.
6. Keep the iSCSI Static Target Interface selected and click to Add.
7. In the Create iSCSI Static Target field, add the iSCSI target node name for Node 1 (IQN) from Table 10 .
8. Enter the IP address of Node 1 Port 4.



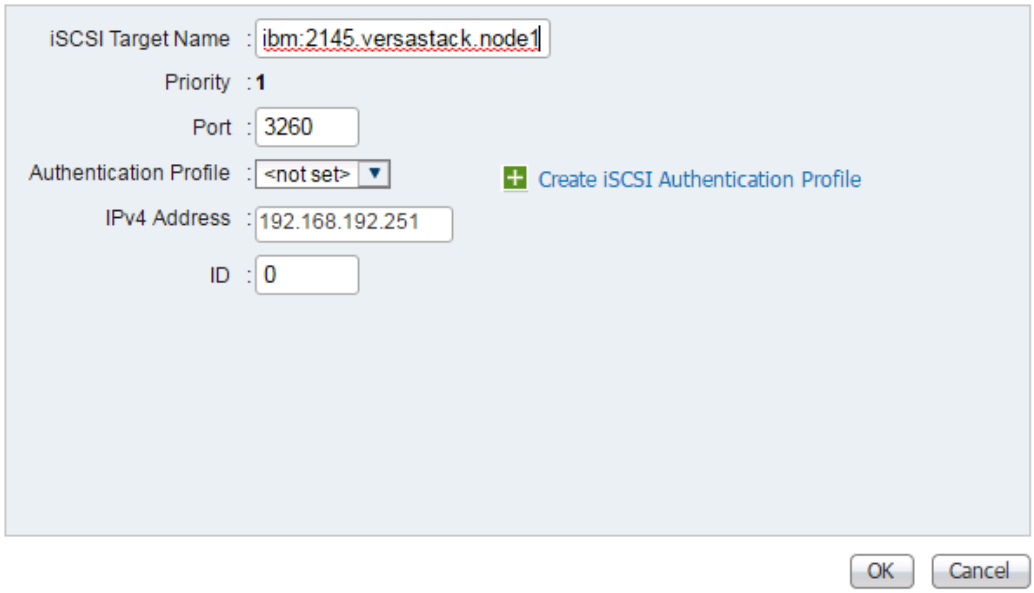
9. Click **OK** to add the iSCSI static target.
10. Keep the iSCSI Static Target Interface option selected and click to Add.
11. In the Create iSCSI Static Target dialog box, add the iSCSI target node name for Node 2 (IQN) from Table 10 .
12. Enter the IP address of Node 2 Port 4.



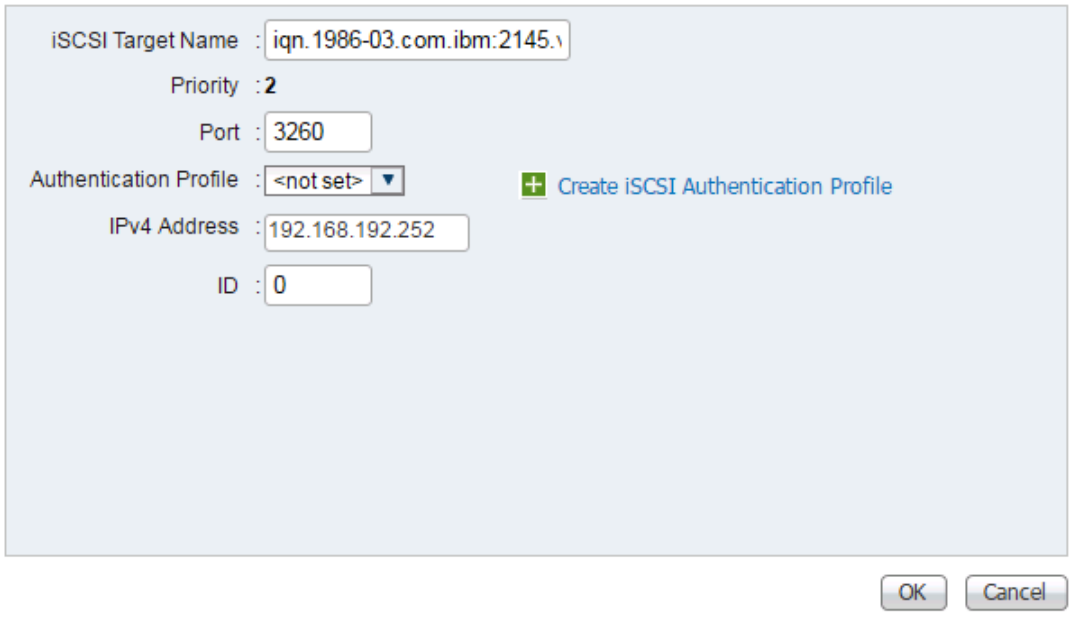
13. Click **OK**.
14. Verify both the targets on iSCSI Path A as shown below:



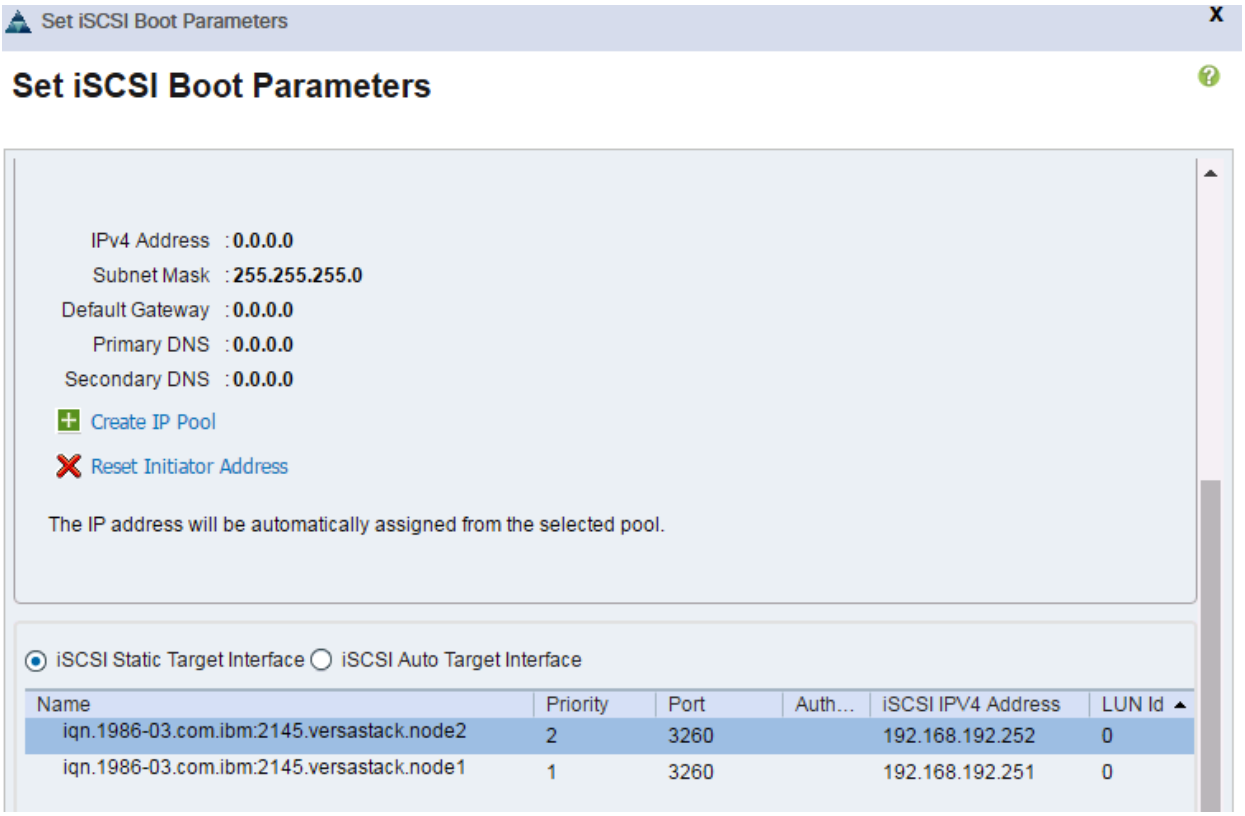
15. Click **OK**.
16. In the Boot Order pane, select iSCIS-B.
17. Click Set iSCSI Boot Parameters.
18. In the Set iSCSI Boot Parameters dialog box, set the leave the "Initiator Name Assignment" to <not set>.
19. In the Set iSCSI Boot Parameters dialog box, set the initiator IP address policy to iSCSI-initiator-B.
20. Keep the iSCSI Static Target Interface option selected and click the button for Add.
21. In the Create iSCSI Static Target dialog box, add the iSCSI target node name for Node 1 (IQN) from Table 10 .
22. Enter the IP address of Node 1 Port 5



23. Click **OK** to add the iSCSI static target.
24. Keep the iSCSI Static Target Interface option selected and click the button for Add.
25. In the Create iSCSI Static Target dialog box, add the iSCSI target node name for Node 2 (IQN) from Table 10 .
26. Enter the IP address of Node 2 Port 5.



27. Click **OK**.
28. Verify both the targets on iSCSI Path A as shown below:



29. Click **OK**.

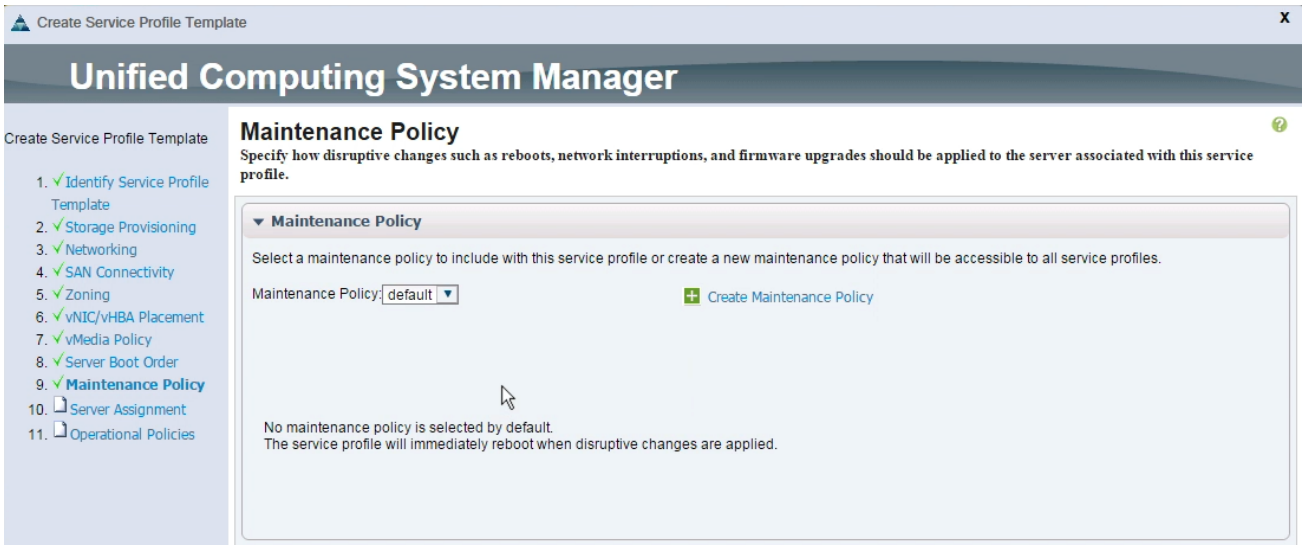
30. Review the table to make sure that all boot devices were created and identified. Verify that the boot devices are in the correct boot sequence.

31. Click **Next** to continue to the next section.

Configure Maintenance Policy

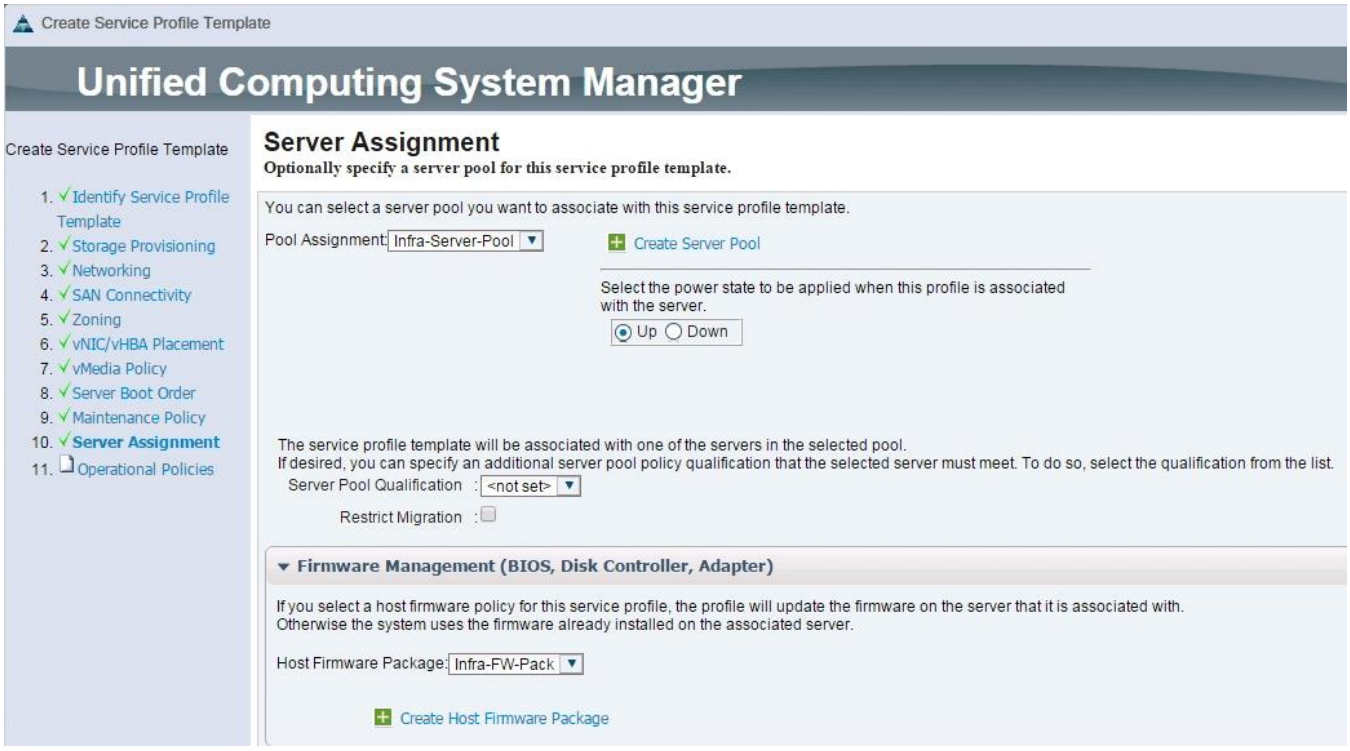
1. Select the default Maintenance Policy from the drop-down list.

2. Click **Next**.



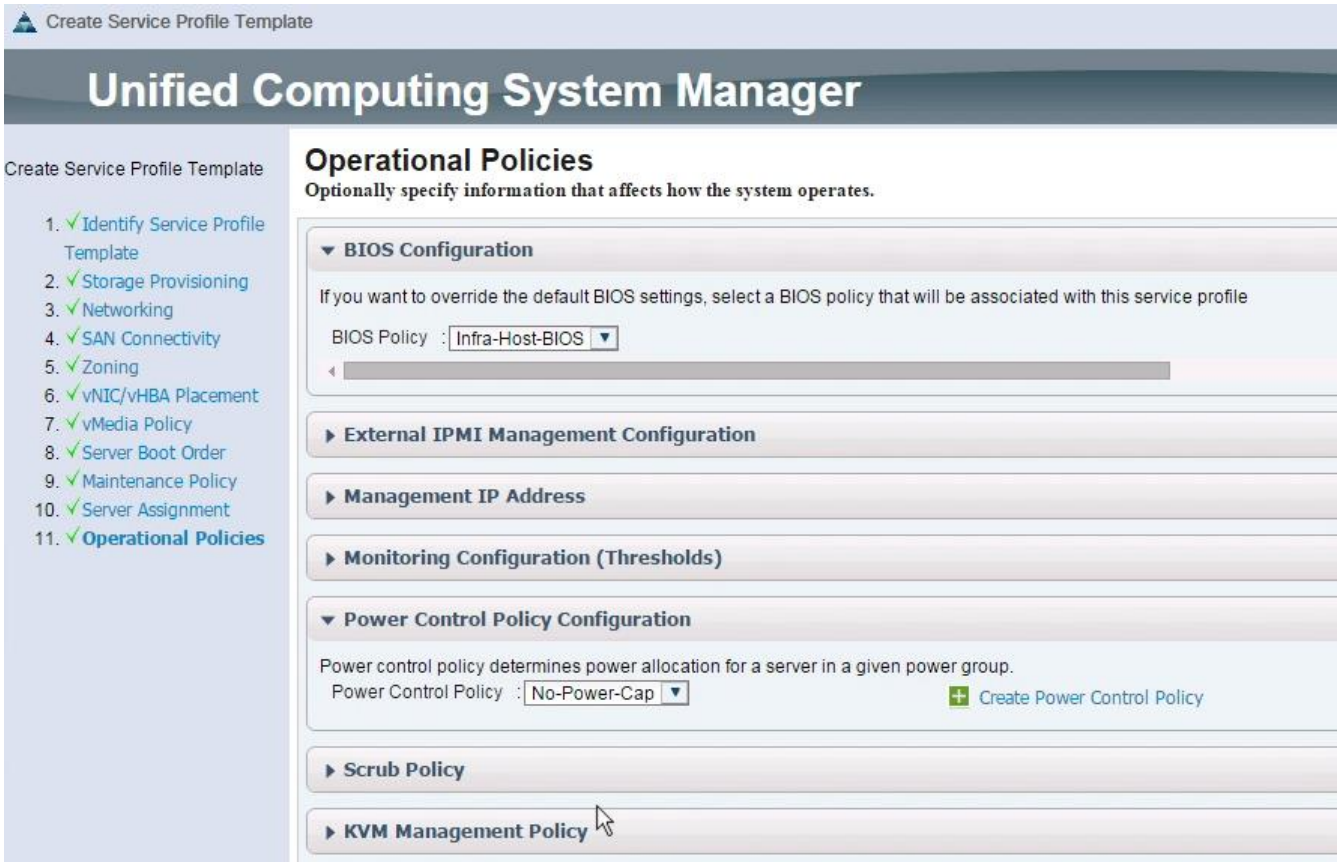
Configure Server Assignment

1. In the Pool Assignment list, select Infra-Server-Pool
2. **Optional**: Select a Server Pool Qualification policy.
3. Select Up as the power state to be applied when the profile is associated with the server.
4. Expand Firmware Management at the bottom of the page and select Infra-FW-Pack from the Host Firmware list.
5. Click **Next**.



Configure Operational Policies

1. In the BIOS Policy list, select Infra-Host-BIOS.
2. Expand Power Control Policy Configuration and select No-Power-Cap in the Power Control Policy list.



3. Click **Finish** to create the service profile template.
4. Click **OK** in the confirmation message.

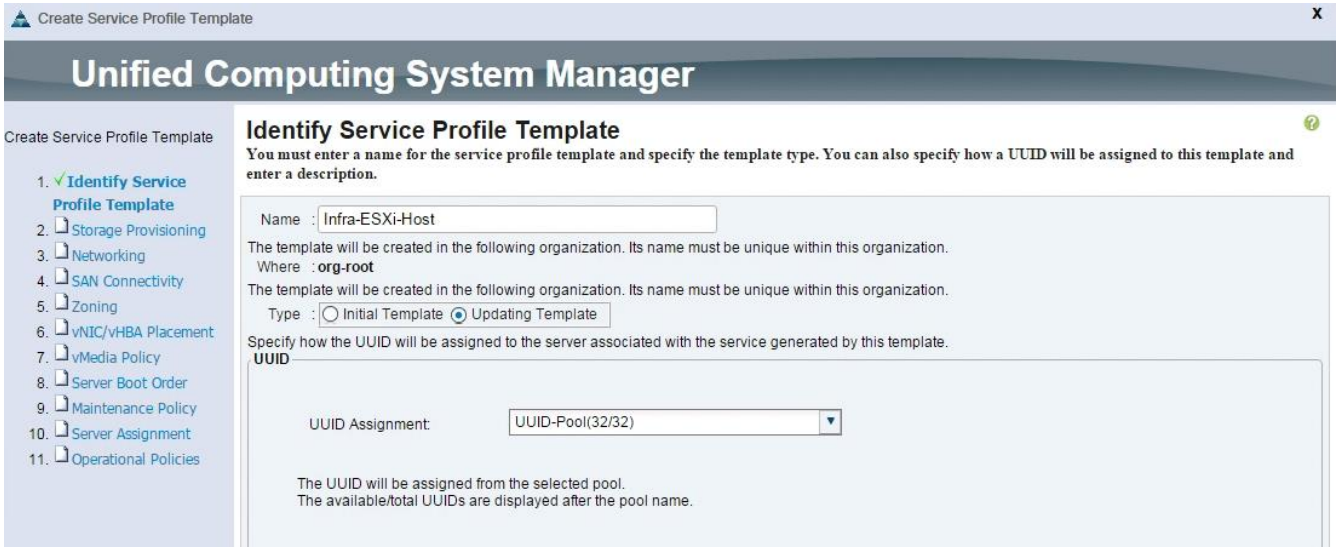
Create FC Boot Service Profile Template (IBM v7000 Only)

In this procedure, a service profile template is created to use FC Fabric A as primary boot path.

To create service profile templates, complete the following steps:

1. In Cisco UCS Manager, click the **Servers** tab in the navigation pane.
2. Choose Service Profile Templates > root.
3. Right-click root and choose **Create Service Profile Template**. This opens the Create Service Profile Template wizard.
4. Enter infra-ESXi-Host as the name of the service profile template.
5. Select the Updating Template option.

6. Under UUID, select UUID-Pool as the UUID pool.
7. Click **Next**.



Configure Storage Provisioning:

1. Select the Local Disk Configuration Policy tab.
2. Select the SAN-Boot Local Storage Policy. This policy usage requires servers with no local HDDs.
3. Click **Next**.

Configure Networking Options:

1. Keep the default setting for Dynamic vNIC Connection Policy.
2. Select the Use Connectivity Policy option to configure the LAN connectivity.
3. Select the infra-LAN-Policy as the LAN Connectivity Policy.
4. Click **Next**.

Configure SAN Connectivity:

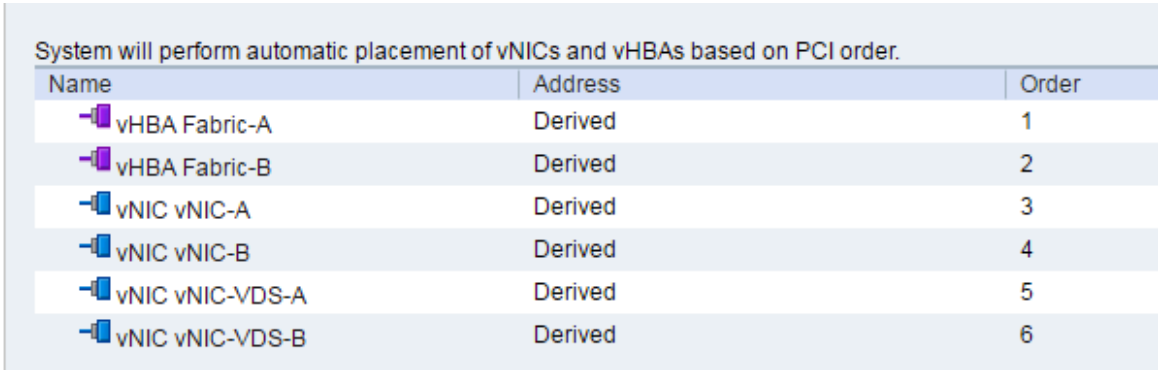
1. Select the Use Connectivity Policy option to configure the SAN connectivity.
2. Select the infra-FC-Boot as the SAN Connectivity Policy.
3. Click **Next**.

Configure Zoning

1. It is not necessary to configure any Zoning options.
2. Click **Next**.

Configure vNIC/HBA Placement

1. For the Select Placement field, select the Infra-Policy.
2. Choose vCon1 and assign the vHBAs/vNICs to the virtual network interfaces policy in the following order:
   - vHBA Fabric-A
   - vHBA Fabric-B
   - vNIC vNIC-A
   - vNIC vNIC-B
   - vNIC vNIC-VDS-A OR vNIC-AVS-A (depending on distributed switch in use)
   - vNIC vNIC-VDS-B OR vNIC-AVS-A (depending on distributed switch in use)
3. Review to verify that all vNICs and vHBAs were assigned to the policy in the appropriate order.


System will perform automatic placement of vNICs and vHBAs based on PCI order.

Name	Address	Order
vHBA Fabric-A	Derived	1
vHBA Fabric-B	Derived	2
vNIC vNIC-A	Derived	3
vNIC vNIC-B	Derived	4
vNIC vNIC-VDS-A	Derived	5
vNIC vNIC-VDS-B	Derived	6

4. Click **Next**.

Configure vMedia Policy

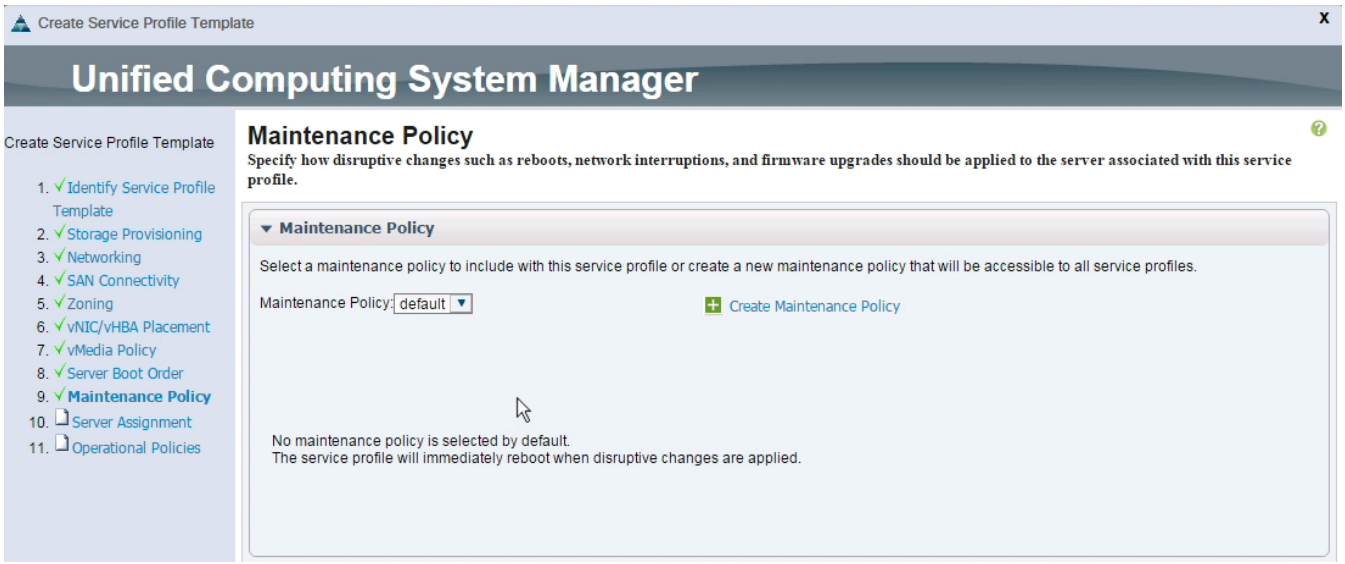
1. There is no need to set a vMedia Policy.
2. Click Next.

Configure Server Boot Order

1. Select Boot-Fabric-A as the Boot Policy.
2. Verify all the boot devices are listed correctly.
3. Click **Next**.

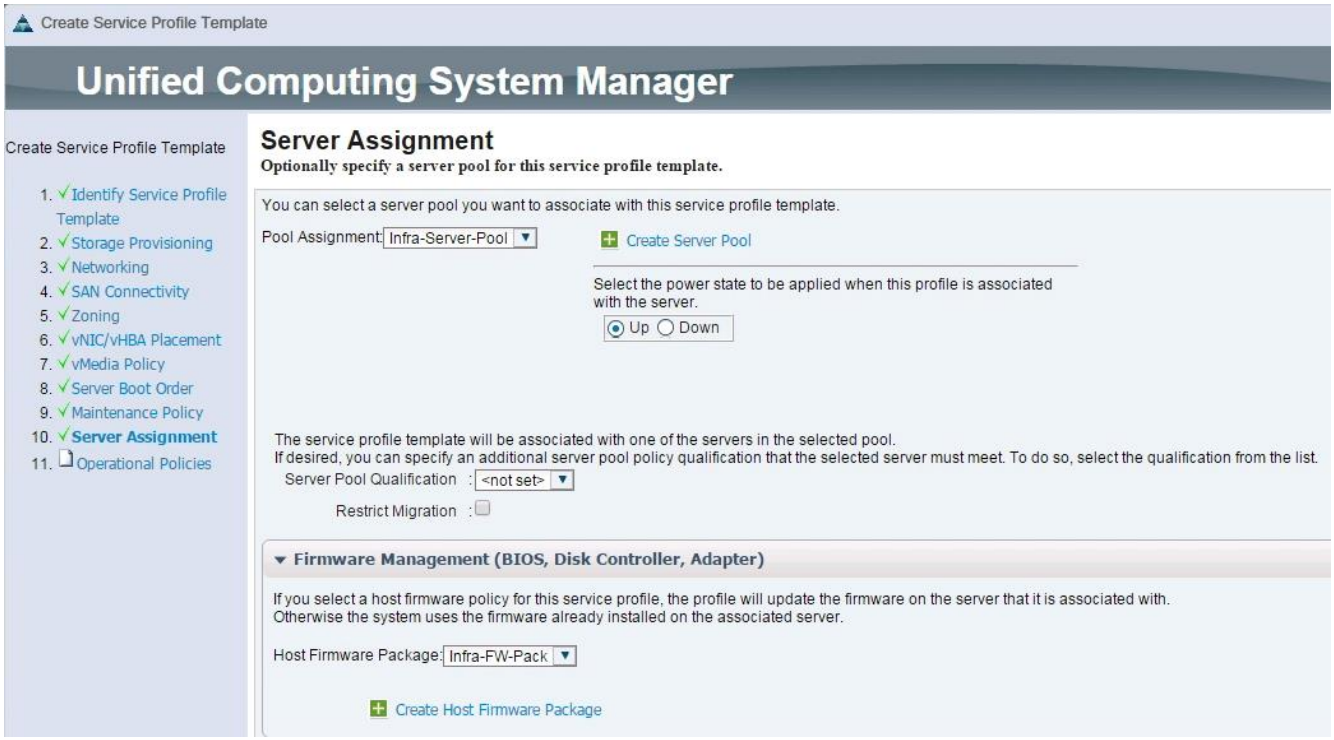
Configure Maintenance Policy

1. Choose the default Maintenance Policy.
2. Click **Next**.



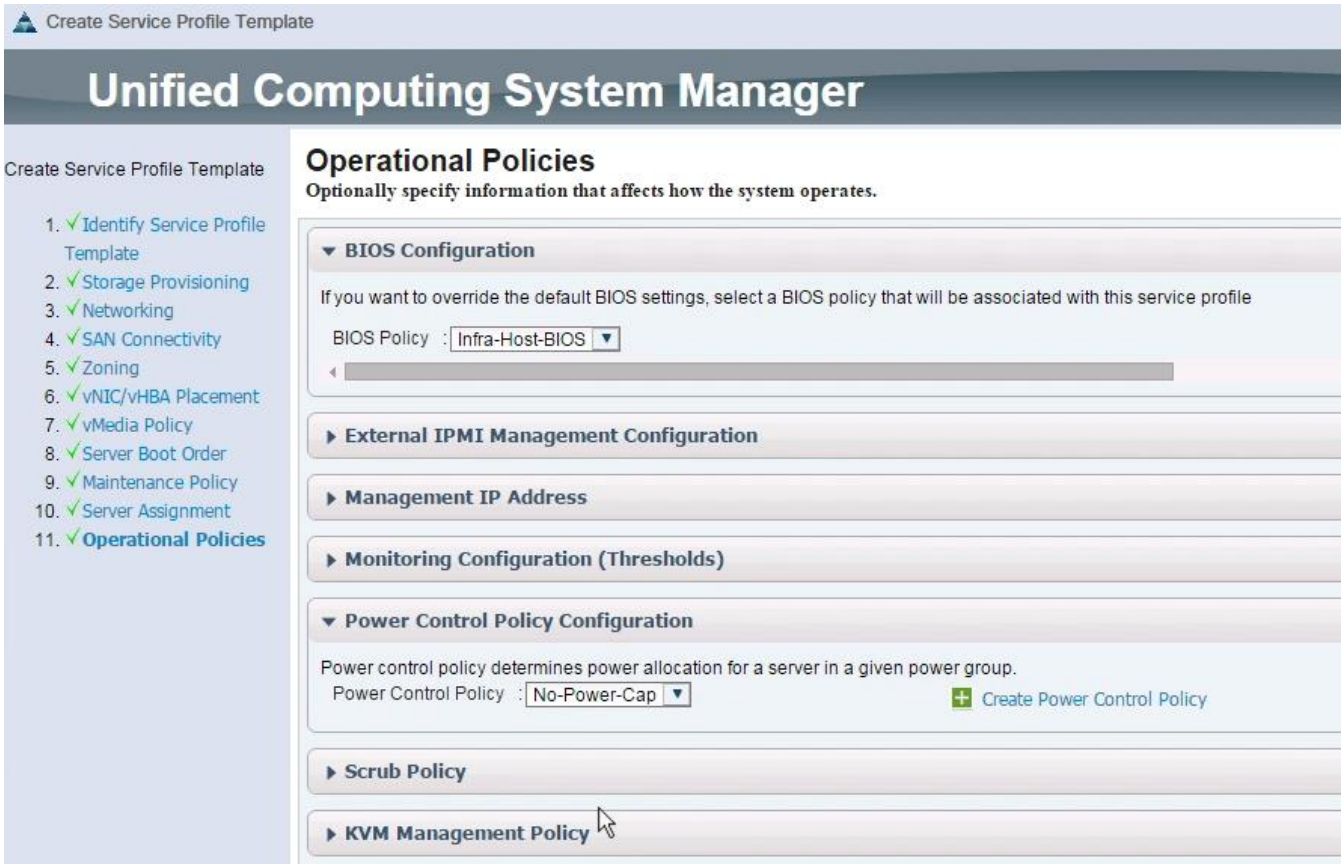
Configure Server Assignment

1. For the Pool Assignment field, select Infra-Server-Pool.
2. **Optional**: Select a Server Pool Qualification policy.
3. Select the option Up for the power state to be applied when the profile is associated with the server.
4. Expand Firmware Management and select Infra-FW-Pack from the Host Firmware list.
5. Click **Next**.



Configure Operational Policies

1. For the BIOS Policy field, select Infra-Host-BIOS.
2. Expand Power Control Policy Configuration and select No-Power-Cap for the Power Control Policy field.

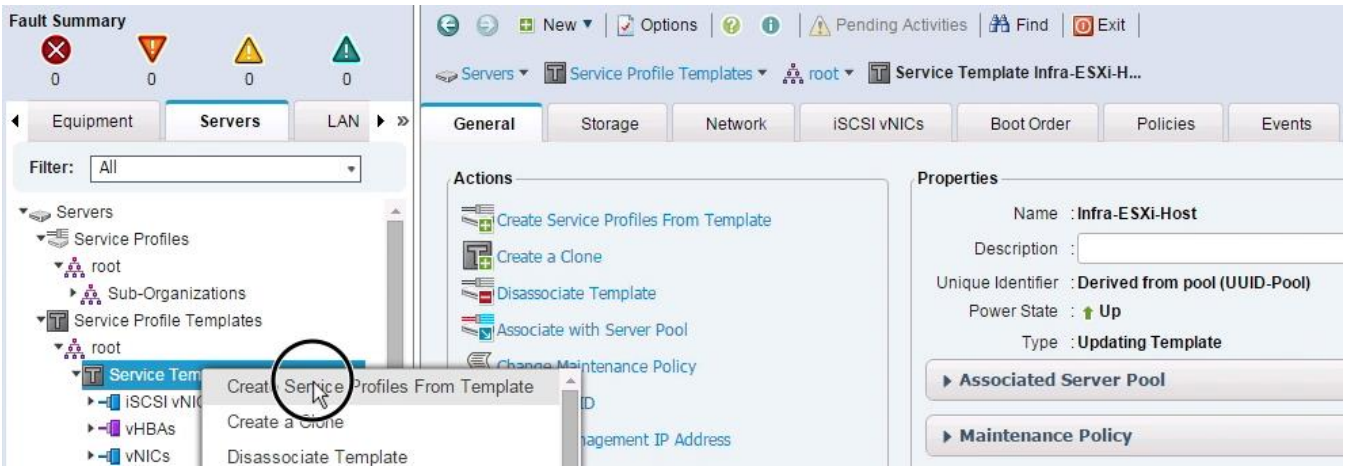


3. Click **Finish** to create the service profile template.
4. Click **OK** in the confirmation message.

Create Service Profiles

To create service profiles from the service profile template, complete the following steps:

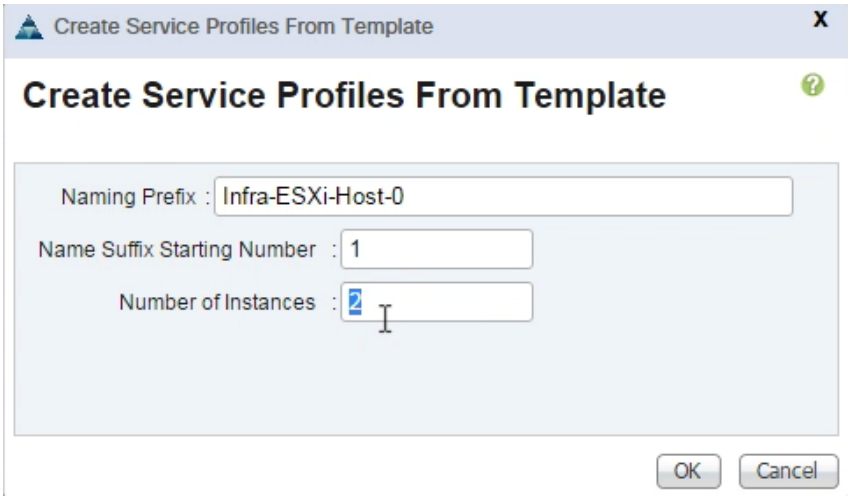
1. In Cisco UCS Manager, click the **Servers** tab in the navigation pane.
2. Choose Service Profile Templates > root > Service Template Infra-ESXi-Host (Infra-ESXi-iSCSI-Host for IBM V9000 iSCSI Deployment).
3. Right-click and choose Create Service Profiles from Template.



4. Enter Infra-ESXi-Host- (Infra-ESXi-iSCSI-Host- for IBM V9000 deployment) as the service profile prefix.
5. Enter 1 as the Name Suffix Staring Number.
6. Enter the Number of servers to be deploy in the Number of Instances field.

Four service profiles were deployed during this validation – two on UCS C-series servers and two on UCS B-series servers.

7. Click **OK** to create the service profile.



8. Click **OK** in the confirmation message.
9. Verify that the service profiles are successfully created and automatically associated with the servers from the pool.

Backup the Cisco UCS Manager Configuration

It is recommended that you backup your Cisco UCS Configuration. Refer to the link below for additional information:

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Admin-Management/3-1/b_Cisco_UCS_Admin_Mgmt_Guide_3_1/b_Cisco_UCS_Admin_Mgmt_Guide_3_1_chapter_01001.html

Adding Servers

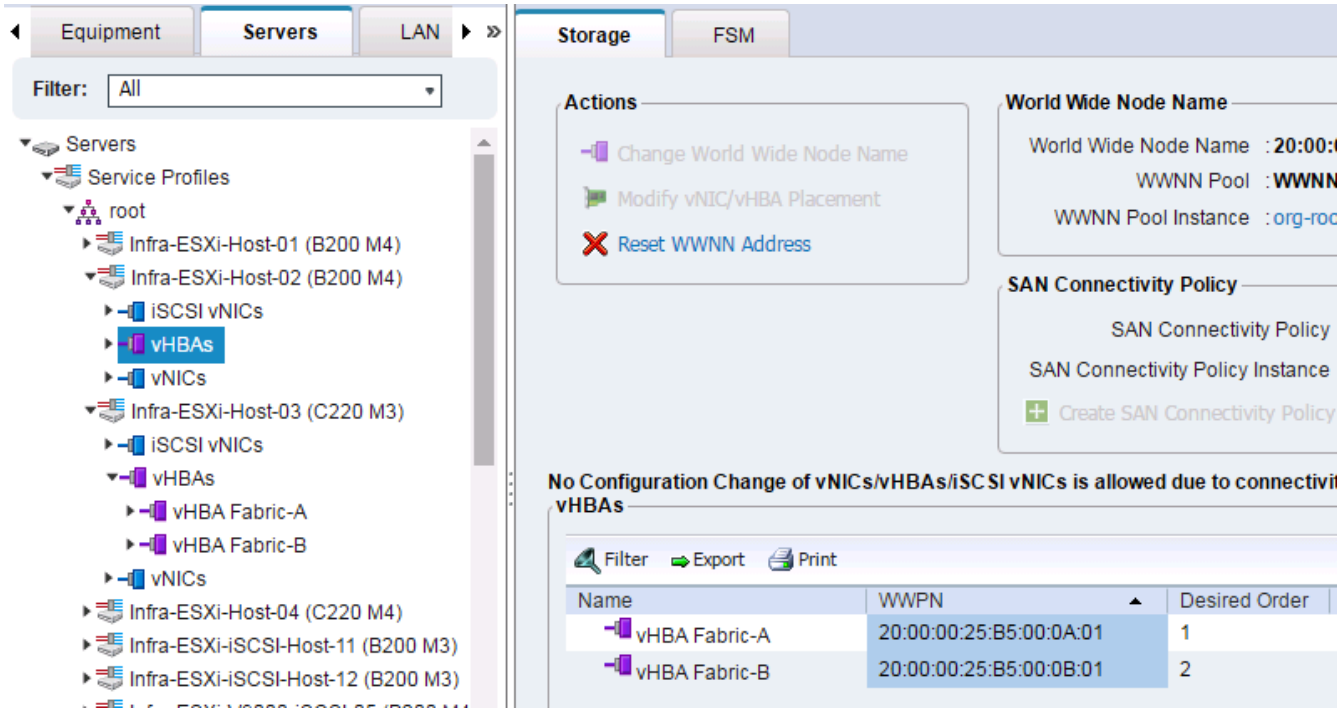
Additional server pools, service profile templates, and service profiles can be created under root or in organizations under the root. All the policies at the root level can be shared among the organizations. Any new physical blades can be added to the existing or new server pools and associated with the existing or new service profile templates.

Gather Necessary WWPN Information (FC Deployment – IBM V7000)

After the Cisco UCS service profiles have been created, each infrastructure blade in the environment will be assigned certain unique configuration parameters. To proceed with the SAN configuration, this deployment specific information must be gathered from each Cisco UCS blade. Complete the following steps:

1. To gather the vHBA WWPN information, launch the Cisco UCS Manager GUI. In the navigation pane, click the Servers tab. Expand **Servers** > **Service Profiles** > **root**. Select each service profile and expand to see the vHBAs.

2. Click **vHBAs** in the **general** tab to see the WWPNs for both HBAs.



3. Record the WWPN information that is displayed for both the Fabric A vHBA and the Fabric B vHBA for each service profile into the WWPN variable in Table 16.

Table 16 UCS WWPN Information

Host	vHBA		Value
Infra-ESXi-Host-1	Fabric-A	WWPN-Infra-ESXi-Host-1-A	20:00:00:25:b5:
	Fabric-B	WWPN-Infra-ESXi-Host-1-B	20:00:00:25:b5:
Infra-ESXi-Host-2	Fabric-A	WWPN-Infra-ESXi-Host-2-A	20:00:00:25:b5:
	Fabric-B	WWPN-Infra-ESXi-Host-2-B	20:00:00:25:b5:

Infra-ESXi-Host-3	Fabric-A	WWPN-Infra-ESXi-Host-3-A	20:00:00:25:b5:
	Fabric-B	WWPN-Infra-ESXi-Host-3-B	20:00:00:25:b5:
Infra-ESXi-Host-4	Fabric-A	WWPN-Infra-ESXi-Host-4-A	20:00:00:25:b5:
	Fabric-B	WWPN-Infra-ESXi-Host-4-B	20:00:00:25:b5:

Gather Necessary IQN Information (iSCSI Deployment – IBM V9000)

After the Cisco UCS service profiles have been created, each infrastructure blade in the environment will be assigned certain unique configuration parameters. To proceed with the SAN configuration, this deployment specific information must be gathered from each Cisco UCS blade. Complete the following steps:

1. To gather the vNIC IQN information, launch the Cisco UCS Manager GUI. In the navigation pane, click the Servers tab. Expand Servers > Service Profiles > root.

2. Click each service profile and then click the "iSCSI vNICs" tab on the right. Note "Initiator Name" displayed at the top of the page under "Service Profile Initiator Name

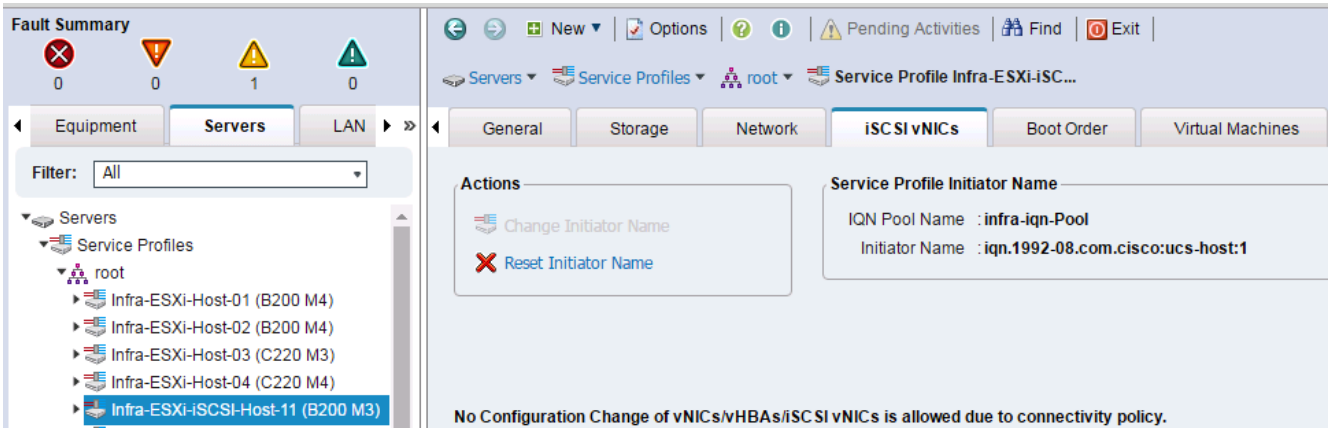


Table 17 Cisco UCS iSCSI IQNs

Cisco UCS Service Profile Name	iSCSI IQN
Infra-ESXi-Host-1	iqn.1992-08.com.cisco:ucs-host:
Infra-ESXi-Host-2	iqn.1992-08.com.cisco:ucs-host:
Infra-ESXi-Host-3	iqn.1992-08.com.cisco:ucs-host:
Infra-ESXi-Host-4	iqn.1992-08.com.cisco:ucs-host:

IBM v9000 iSCSI Storage Configuration

IBM FlashSystem V9000 iSCSI Configuration

As part of IBM V9000 iSCSI configuration, complete the following steps:

- Setup Volumes
- Map Volumes to Hosts

Table 18 List of Volumes on IBM v9000

Volume Name	Capacity (GB)	Purpose	Mapping
Infra-ESXi-Host-01	10	Boot LUN for the Host	Infra-ESXi-Host-01
Infra-ESXi-Host-02	10	Boot LUN for the Host	Infra-ESXi-Host-02
Infra-ESXi-Host-03	10	Boot LUN for the Host	Infra-ESXi-Host-03
Infra-ESXi-Host-04	10	Boot LUN for the Host	Infra-ESXi-Host-03
Infra-datastore-1	1000*	Shared volume to host VMs	All ESXi hosts: Infra-ESXi-Host-01 to Infra-ESXi-Host-04
Infra-swap	300*	Shared volume to host VMware VM swap directory	All ESXi hosts: Infra-ESXi-Host-01 to Infra-ESXi-Host-04

* Customers can adjust these values based on the size of their environment.

Create Volumes on the Storage System

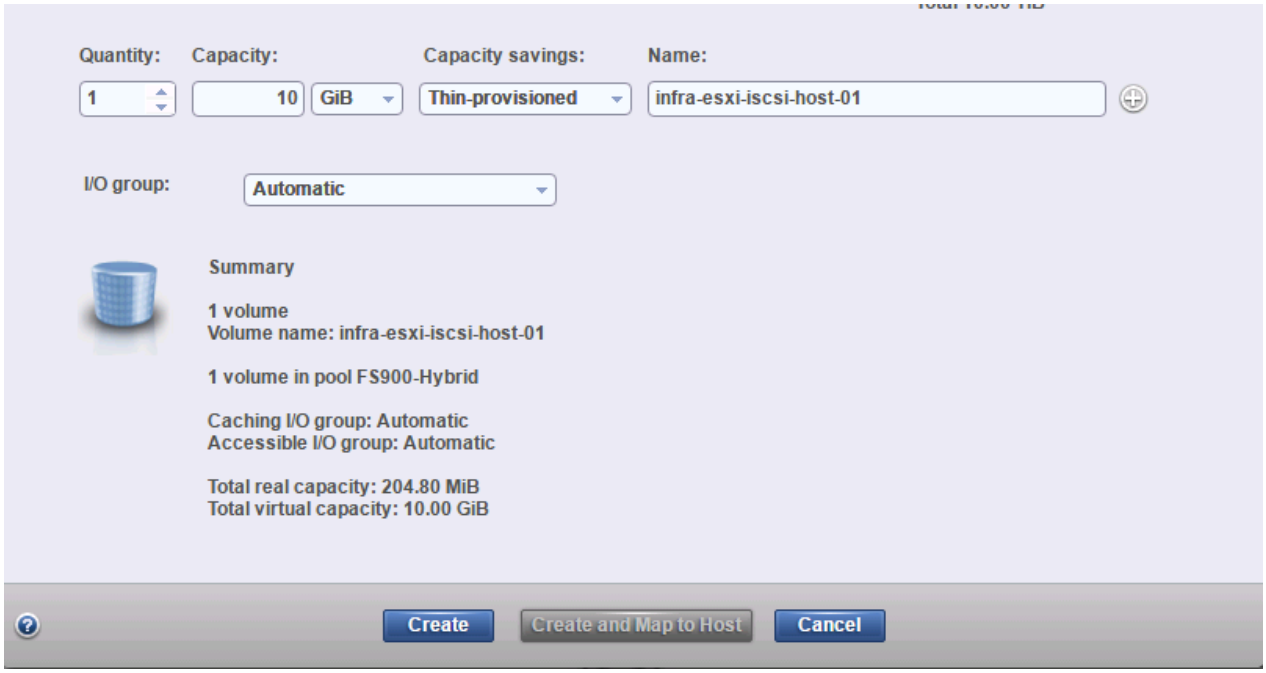
Log into the IBM v9000 GUI and select the Pools icon one the left screen and select Volumes

Following steps will be repeated to create and map all the volumes shown in Table 18.

3. Click **Create Volumes** as shown in the figure.

4. Click **Basic** and the select the pool from the drop-down menu.

5. Input quantity 1 and the capacity and name from Table 18. Select Thin-provisioned for Capacity savings and enter the Name of the volume.



6. Click **Create**.

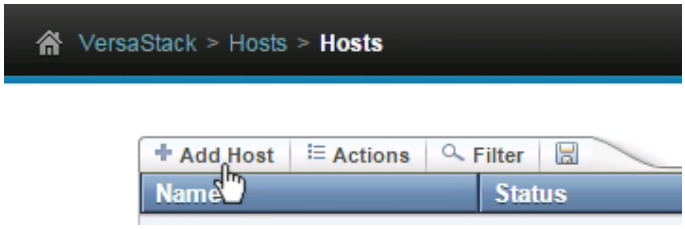
7. Repeat the steps above to create all the required volumes and verify all the volumes have successfully been created as shown in the sample output below.

Map Volumes to Hosts

1. Click **Hosts**.

2. Follow the procedure below to add all ESXi hosts (Table 17) to the IBM 9000 system.

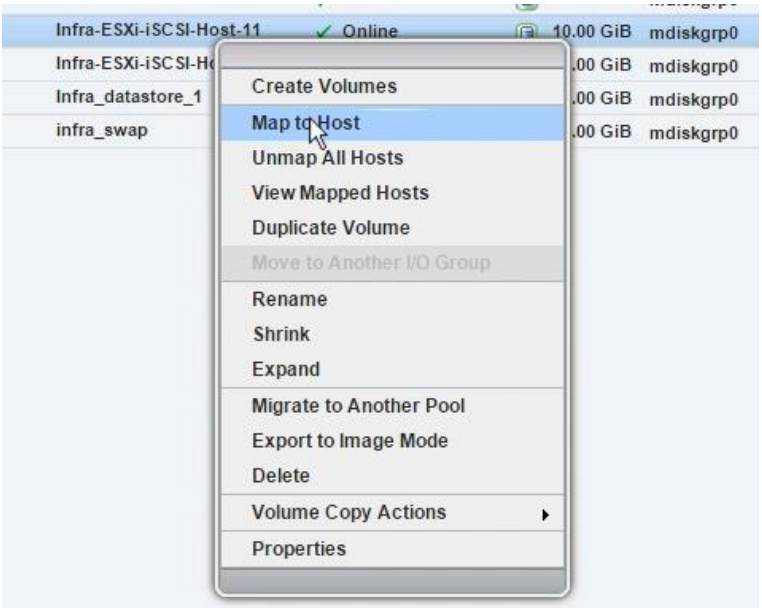
3. Click Add Host.



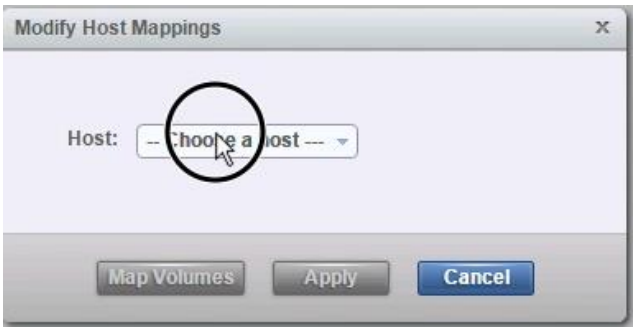
4. Select iSCSI Host.
5. Add the name of the host to match the ESXi service profile name from Table 17.
6. Type the IQN corresponding to the ESXi host from Table 17 and click **Add Port to List**.

7. Click Add Host.
8. Click **Volumes**.

9. Right-click the Boot LUN for the ESXi host and choose **Map to Host**.



10. From the drop-down menu, select the newly created iSCIS host.



11. Click **Map Volumes** and when the process is complete, click **Close**.

12. Repeat the steps 9-11 to map shared volumes from Table 18 to the host as well.

13. Repeat the steps outlined in this procedure to add all the ESXi hosts to the storage system and modify their volume mappings to add both the boot LUN as well as the shared volumes to the host.

IBM v7000 Fibre Channel Storage Configuration

As part of IBM Storwize V7000 Fibre Channel configuration, complete the following steps:

- Setup Zoning on Cisco MDS switches
- Setup Volumes on IBM V7000
- Map Volumes to Hosts

Cisco MDS 9148S SAN Zoning

The following steps will configure zoning for the WWPNs from the server and the IBM Storwize V7000. WWPN information collected from the previous steps will be used in this section. Multiple zones will be created for servers in VSAN 101 on Switch A and VSAN 102 on Switch B.

Host to storage connectivity zones are separate from IBM cluster configuration zone. This section only covers host to storage connectivity. IBM cluster configuration is part of base storage configuration.

The configuration below assumes 4 UCS services profiles have been deployed in this example. Customers can adjust the configuration according to their deployment size.

Cisco MDS - A Switch

The configuration below assumes 4 UCS services profiles have been deployed. Customers can adjust the configuration according to their deployment.

Log in to the MDS switch and complete the following steps.

1. Configure the ports and the port-channel for UCS.

```
interface port-channel1 (For UCS)
  channel mode active
  switchport rate-mode dedicated
!
interface fc1/1 (IBM Node 1)
  port-license acquire
  no shutdown
!
interface fc1/2 (IBM Node 2)
  port-license acquire
  no shutdown
!
interface fc1/31 (UCS Fabric A)
  port-license acquire
  channel-group 1 force
  no shutdown
!
interface fc1/32 (UCS Fabric A)
  port-license acquire
  channel-group 1 force
  no shutdown
```

2. Create the VSAN.

```
vsan database
  vsan 101 interface port-channel1
  vsan 101 interface fc1/1
  vsan 101 interface fc1/2
```

3. The WWPNs recorded in Table 15 and Table 16 will be used in the next step. Replace the variables with actual WWPN values.

```
device-alias database
device-alias name Infra-ESXi-Host-01 pwwn <WWPN-Infra-ESXi-Host-1-A>
device-alias name Infra-ESXi-Host-02 pwwn <WWPN-Infra-ESXi-Host-2-A>
device-alias name Infra-ESXi-Host-03 pwwn <WWPN-Infra-ESXi-Host-3-A>
device-alias name Infra-ESXi-Host-04 pwwn <WWPN-Infra-ESXi-Host-4-A>
device-alias name V7000-Node1-Fabric-A pwwn <WWPN-Node-1-Fabric-A>
device-alias name V7000-Node2-Fabric-A pwwn <WWPN-Node-2-Fabric-A>
device-alias commit
```

4. Create the zones and add device-alias members for the 4 blades.

```
zone name Infra-ESXi-Host-01 vsan 101
member device-alias  Infra-ESXi-Host-01
member device-alias V7000-Node1-Fabric-A
member device-alias V7000-Node2-Fabric-A
!

zone name Infra-ESXi-Host-02 vsan 101
member device-alias  Infra-ESXi-Host-02
member device-alias V7000-Node1-Fabric-A
member device-alias V7000-Node2-Fabric-A
!

zone name Infra-ESXi-Host-03 vsan 101
member device-alias  Infra-ESXi-Host-03
member device-alias V7000-Node1-Fabric-A
member device-alias V7000-Node2-Fabric-A
!

zone name Infra-ESXi-Host-04 vsan 101
member device-alias  Infra-ESXi-Host-04
member device-alias V7000-Node1-Fabric-A
member device-alias V7000-Node2-Fabric-A
!
```

5. Add zones to zoneset.

```
zoneset name V7000-zoneset vsan 101
    member Infra-ESXi-Host-01
    member Infra-ESXi-Host-02
    member Infra-ESXi-Host-03
    member Infra-ESXi-Host-04
```

6. Activate the zoneset.

```
zoneset activate  name V7000-zoneset vsan 101
```

Validate all the HBA's are logged into the MDS switch. The V9000 and the Cisco servers should be powered on. To start the Cisco server's from Cisco UCS Manager, select the server tab, then click Servers→Service→Profiles→root, and right-click service profile, for ex VM-Host-Infra-01 then select boot server.

7. Validate that all the powered on system's HBAs are logged into the switch through the show zoneset command.

```
show zoneset active

MDS-9148S-A# show zoneset active

zoneset name V7000-zoneset vsan 101


  zone name Infra-ESXi-Host-01 vsan 101

  * fcid 0x440201 [pwwn 20:00:00:25:b5:00:0a:00] [Infra-ESXi-Host-01]

  * fcid 0x440000 [pwwn 50:05:07:68:0b:23:20:fc] [V7000-Node1-Fabric-A]

  * fcid 0x440100 [pwwn 50:05:07:68:0b:23:20:fd] [V7000-Node2-Fabric-A]


  zone name Infra-ESXi-Host-02 vsan 101

  * fcid 0x440202 [pwwn 20:00:00:25:b5:00:0a:01] [Infra-ESXi-Host-02]

  * fcid 0x440000 [pwwn 50:05:07:68:0b:23:20:fc] [V7000-Node1-Fabric-A]

  * fcid 0x440100 [pwwn 50:05:07:68:0b:23:20:fd] [V7000-Node2-Fabric-A]


  zone name Infra-ESXi-Host-03 vsan 101

  * fcid 0x440203 [pwwn 20:00:00:25:b5:00:0a:02] [Infra-ESXi-Host-03]

  * fcid 0x440000 [pwwn 50:05:07:68:0b:23:20:fc] [V7000-Node1-Fabric-A]

  * fcid 0x440100 [pwwn 50:05:07:68:0b:23:20:fd] [V7000-Node2-Fabric-A]


  zone name Infra-ESXi-Host-04 vsan 101

  * fcid 0x440204 [pwwn 20:00:00:25:b5:00:0a:03] [Infra-ESXi-Host-04]

  * fcid 0x440000 [pwwn 50:05:07:68:0b:23:20:fc] [V7000-Node1-Fabric-A]

  * fcid 0x440100 [pwwn 50:05:07:68:0b:23:20:fd] [V7000-Node2-Fabric-A]
```

8. Save the configuration.

```
copy run start
```

Cisco MDS - B Switch

The configuration below assumes that 4 UCS service profiles have been deployed. Customers can adjust the configuration according to their deployment.

Log into the MDS switch and complete the following steps:

1. Configure the ports and the port-channel for UCS.

```
interface port-channel2 (For UCS)
  channel mode active
  switchport rate-mode dedicated
!
interface fc1/1 (IBM Node 1)
  port-license acquire
  no shutdown
!
interface fc1/2 (IBM Node 2)
  port-license acquire
  no shutdown
!
interface fc1/31 (UCS Fabric B)
  port-license acquire
  channel-group 2 force
  no shutdown
!
interface fc1/32 (UCS Fabric B)
  port-license acquire
  channel-group 2 force
  no shutdown
```

2. Create the VSAN.

```
vsan database
  vsan 102 interface port-channel2
  vsan 102 interface fc1/1
  vsan 102 interface fc1/2
```

3. The WWPNs recorded in Table 15 and Table 16 will be used here. Replace the variables with actual WWPN values.

```
device-alias database
device-alias name Infra-ESXi-Host-01 pwwn <WWPN-Infra-ESXi-Host-1-B>
device-alias name Infra-ESXi-Host-02 pwwn <WWPN-Infra-ESXi-Host-2-B>
device-alias name Infra-ESXi-Host-03 pwwn <WWPN-Infra-ESXi-Host-3-B>
device-alias name Infra-ESXi-Host-04 pwwn <WWPN-Infra-ESXi-Host-4-B>
device-alias name V7000-Node1-Fabric-B pwwn <WWPN-Node-1-Fabric-B>
device-alias name V7000-Node2-Fabric-B pwwn <WWPN-Node-2-Fabric-B>
device-alias commit
```

4. Create the zones and add device-alias members for the 4 servers.

```
zone name Infra-ESXi-Host-01 vsan 102
member device-alias  Infra-ESXi-Host-01
member device-alias V7000-Node1-Fabric-B
member device-alias V7000-Node2-Fabric-B
!

zone name Infra-ESXi-Host-02 vsan 102
member device-alias  Infra-ESXi-Host-02
member device-alias V7000-Node1-Fabric-B
member device-alias V7000-Node2-Fabric-B
!
```

```
zone name Infra-ESXi-Host-03 vsan 102
member device-alias  Infra-ESXi-Host-03
member device-alias V7000-Node1-Fabric-B
member device-alias V7000-Node2-Fabric-B
!

zone name Infra-ESXi-Host-04 vsan 102
member device-alias  Infra-ESXi-Host-04
member device-alias V7000-Node1-Fabric-B
member device-alias V7000-Node2-Fabric-B
!
```

5. Add zones to zoneset.

```
zoneset name V7000-zoneset vsan 102
    member Infra-ESXi-Host-01
    member Infra-ESXi-Host-02
    member Infra-ESXi-Host-03
    member Infra-ESXi-Host-04
```

6. Activate the zoneset.

```
zoneset activate name V7000-zoneset vsan 102
```

Validate all the HBA's are logged into the MDS switch. The V9000 and the Cisco servers should be powered on. To start the Cisco server's from Cisco UCS Manager, select the server tab, then click Servers→Service→Profiles→root, and right-click service profile, for ex VM-Host-Infra-01 then select boot server.

7. Validate the all powered on systems HBA's are logged into the switch using the following command:

```
show zoneset active

   zone name Infra-ESXi-Host-01 vsan 102
  * fcid 0x940201 [pwwn 20:00:00:25:b5:00:0b:00] [Infra-ESXi-Host-01]
  * fcid 0x940000 [pwwn 50:05:07:68:0b:24:20:fc] [V7000-Node1-Fabric-B]
  * fcid 0x940100 [pwwn 50:05:07:68:0b:24:20:fd] [V7000-Node2-Fabric-B]

  zone name Infra-ESXi-Host-02 vsan 102
  * fcid 0x940202 [pwwn 20:00:00:25:b5:00:0b:01] [Infra-ESXi-Host-02]
  * fcid 0x940000 [pwwn 50:05:07:68:0b:24:20:fc] [V7000-Node1-Fabric-B]
  * fcid 0x940100 [pwwn 50:05:07:68:0b:24:20:fd] [V7000-Node2-Fabric-B]

  zone name Infra-ESXi-Host-03 vsan 102
  * fcid 0x940203 [pwwn 20:00:00:25:b5:00:0b:02] [Infra-ESXi-Host-03]
  * fcid 0x940000 [pwwn 50:05:07:68:0b:24:20:fc] [V7000-Node1-Fabric-B]
  * fcid 0x940100 [pwwn 50:05:07:68:0b:24:20:fd] [V7000-Node2-Fabric-B]

  zone name Infra-ESXi-Host-04 vsan 102
  * fcid 0x940204 [pwwn 20:00:00:25:b5:00:0b:03] [Infra-ESXi-Host-04]
  * fcid 0x940000 [pwwn 50:05:07:68:0b:24:20:fc] [V7000-Node1-Fabric-B]
  * fcid 0x940100 [pwwn 50:05:07:68:0b:24:20:fd] [V7000-Node2-Fabric-B]
```

8. Save the configuration.

```
copy run start
```

IBM Storwize V7000 Configuration

As part of V7000 configuration, complete the following steps:

- Create ESXi boot Volumes (Boot LUNs for all the ESXi hosts)
- Create Share Storage Volumes (for hosting VMs)
- Map Volumes to Hosts

In this deployment example, there are four ESXi hosts – following volumes will be created in this process:

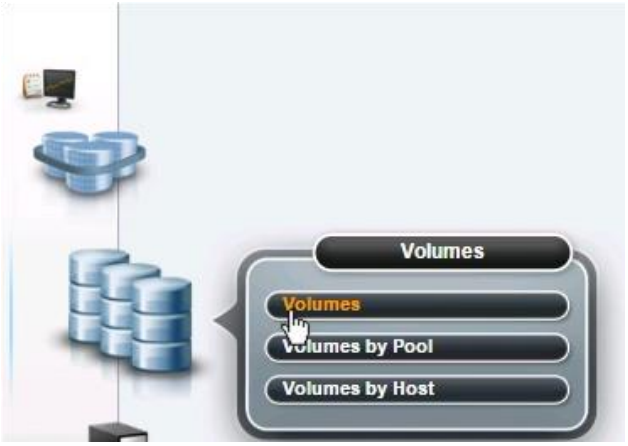
Table 19 List of volumes on IBM V7000

Volume Name	Capacity (GB)	Purpose	Mapping
Infra-ESXi-Host-01	10	Boot LUN for the Host	Infra-ESXi-Host-01
Infra-ESXi-Host-02	10	Boot LUN for the Host	Infra-ESXi-Host-02
Infra-ESXi-Host-03	10	Boot LUN for the Host	Infra-ESXi-Host-03
Infra-ESXi-Host-04	10	Boot LUN for the Host	Infra-ESXi-Host-03
Infra-datastore-1	1000*	Shared volume to host VMs	All ESXi hosts: Infra-ESXi-Host-01 to Infra-ESXi-Host-04
Infra-swap	300*	Shared volume to host VMware VM swap directory	All ESXi hosts: Infra-ESXi-Host-01 to Infra-ESXi-Host-04

* Customers can adjust these values based on the size of their environment.

Create Volumes on the Storage System

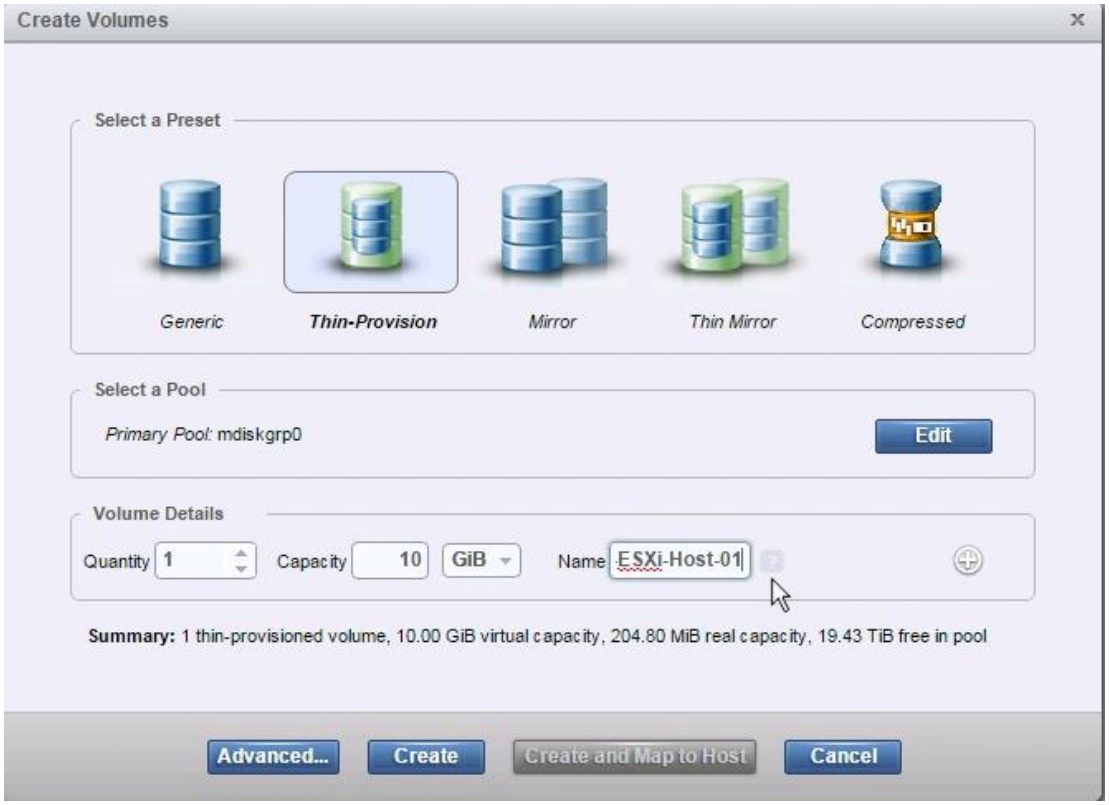
1. Log into the IBM v7000 GUI and select the Pools icon in the left pane and select **Volumes**.



2. Repeat the following steps to create and map the volumes shown in Table 19.
3. Click Create Volumes.

4. Click **Thin-Provision** and select the pool as shown in the figure.

5. Input quantity as 1, the capacity as required (atleast 10GB) and the name from Table 19.



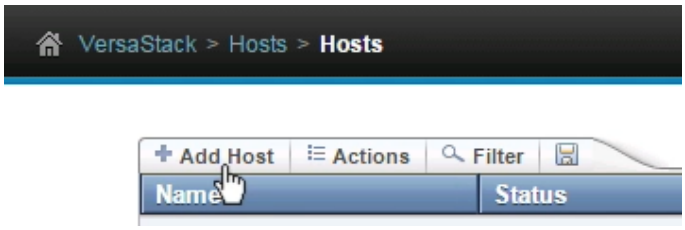
6. Click **Create**.
7. Repeat the steps above to create all the required volumes.
8. Verify all the volumes have been successfully created.

Name	State	Capacity	Pool	Host Mappings	UID
Infra-ESXi-Host-01	Online	10.00 GiB	mdiskgrp0	No	600507640090800588000000000000004
Infra-ESXi-Host-02	Online	10.00 GiB	mdiskgrp0	No	600507640090800588000000000000005
Infra-ESXi-Host-03	Online	10.00 GiB	mdiskgrp0	No	600507640090800588000000000000006
Infra-ESXi-Host-04	Online	10.00 GiB	mdiskgrp0	No	600507640090800588000000000000007
Infra_datastore_1	Online	500.00 GiB	mdiskgrp0	No	600507640090800588000000000000002
infra_swap	Online	100.00 GiB	mdiskgrp0	No	600507640090800588000000000000003

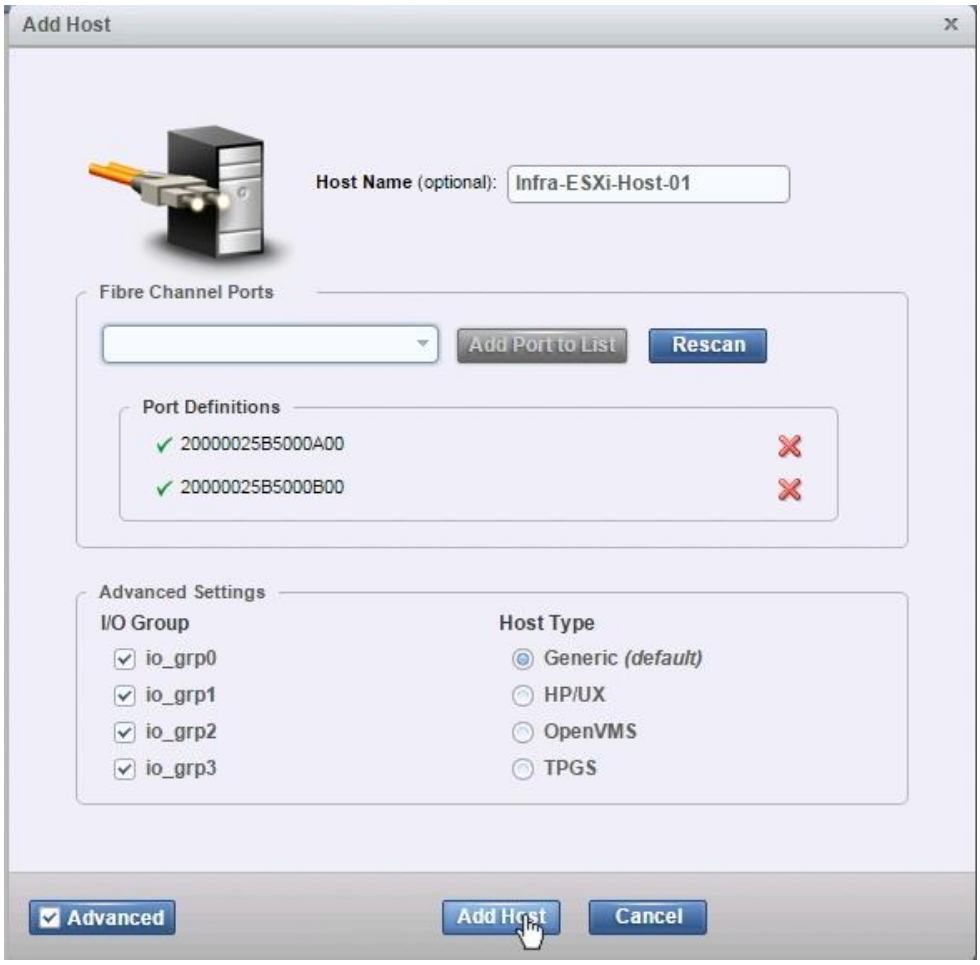
Map Volumes to Hosts

1. Select Host Icon in the left pane and click **Hosts**.

2. Follow the procedure below to add all ESXi hosts (Table 16) to the IBM V7000 system.
3. Click Add Host.

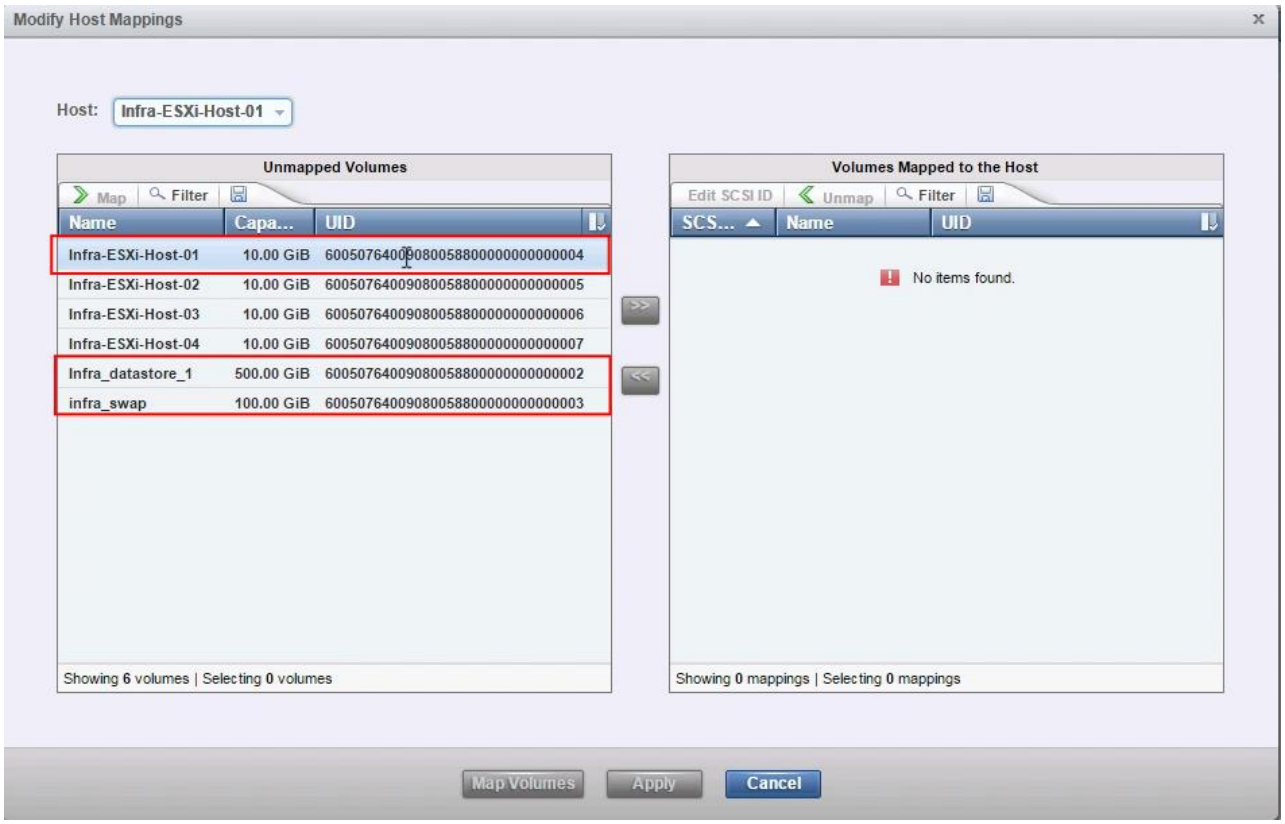


4. Select the Fibre Channel Host.
5. Add the name of the host to match the ESXi service profile name from Table 16.
6. From the drop-down menu, select both (Fabric A and B) WWPNs corresponding to the host in Table 16.



7. Click Add Host.
8. Right-click on the newly created host and select **Modify Mappings**.

9. Select the Boot LUN corresponding to the host and the shared volumes to the column on the right labelled as Volume Mapped to the Host.



10. Click **Map Volumes**. Once the process is complete, the Host Mappings column should show Yes as shown in the below screenshot.

11. Repeat the steps above to add all the ESXi hosts in the environment and modify their mappings.

IBM v7000 Unified File Module Configuration

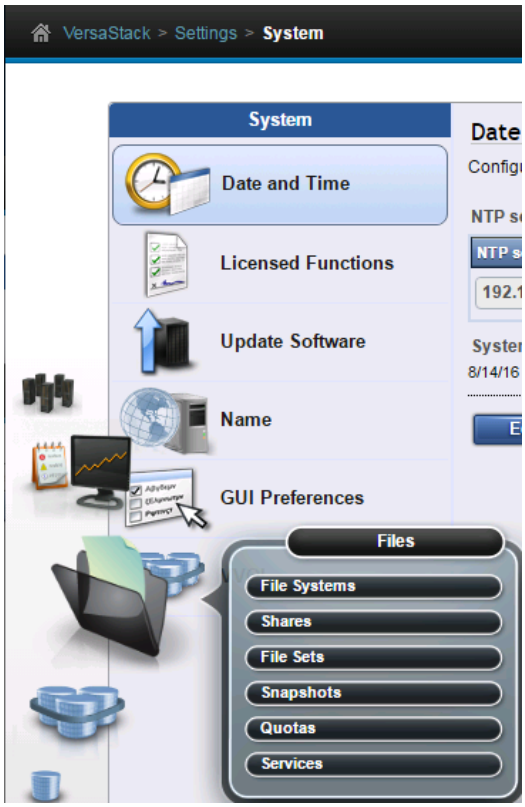
As part of IBM Storwize V7000 File Module configuration, following steps will be completed:

- Setup File System
- Setup NFS Shares

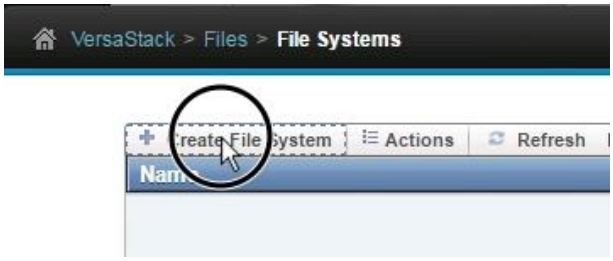
The shares created in this step will be mounted on to ESXi hosts after ACI based fabric is configured to enable NFS communication between File Modules and the ESXi hosts. The network configuration is covered in the upcoming section.

Create File System

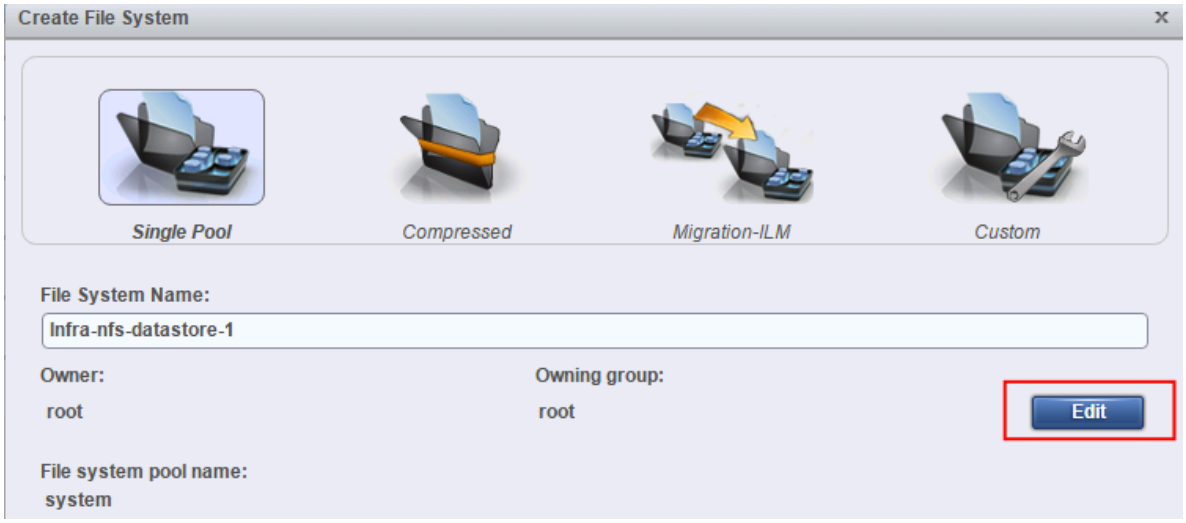
1. Log into the IBM v7000 File Module GUI and select the File System icon one the left pane and click File Systems.



2. Click Create File System.



3. Enter infra-nfs-datastore-1 as the name of the file system.
4. Click **Edit**.



5. Check the check boxes to allow Read, Write and Execute privileges.

6. Click **OK**.
7. Set the Size of the File System to 500GB (or choose a size depending on the environment).
8. Click **OK**.
9. Click **Next** to Review the Access Control information and click Yes.
10. Wait for the file system to be created; it might take a few minutes. On completion, click **Close**.

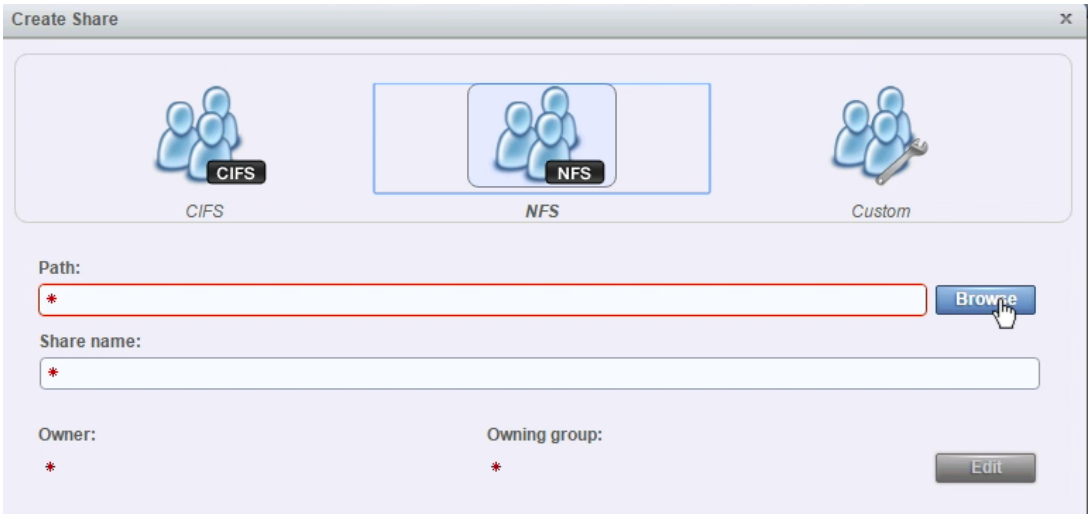
Create a Share

1. Click the File Icon in the left pane and click **Share**.

2. Click **Create Share** to add a share.

3. On the Create Share screen, select NFS and the share type.

4. Click **Browse** next to Path.



5. Select the File System created in the last step.

6. Click **OK**.

7. Add infra-nfs-datastore-1 as the share name.

8. Click Create NFS Client.

9. Add the NFS IP subnet information from Table 11 (192.168.180.0/24).

10. Change the Access type to Read/Write.

11. Click **Add**.

12. Click **OK** to create the share.
13. Review the Share information and note the path in Table 20 to be used late in the document.
14. Create other NFS shares using the procedure listed above (if needed).

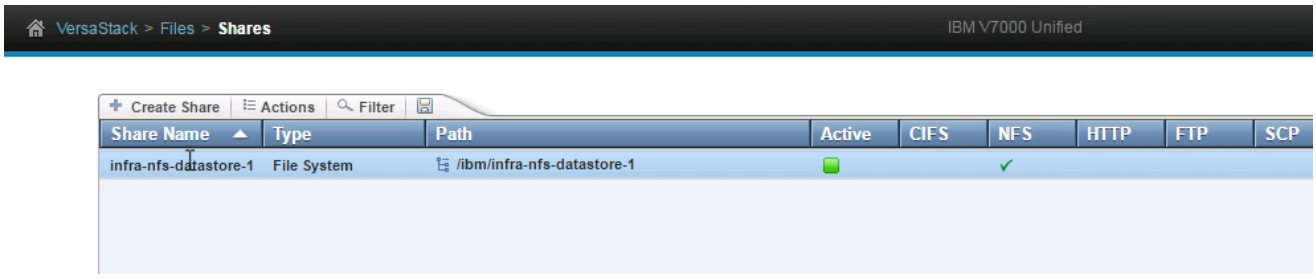


Table 20 IBM V7000 Unified File Module – NFS Shares

Share Name	Share Path	Purpose
infra-nfs-datastore	/ibm/infra-nfs-datastore-1	NFS datastore for Hosting VMs

Network (Cisco ACI) Configuration

This section provides a detailed configuration procedure of the Cisco ACI Fabric and Infrastructure (Foundation) Tenant for the use in a VersaStack environment.

Physical Connectivity

Follow the physical connectivity guidelines for VersaStack as covered in Figure 3.

In ACI, both spine and leaf switches are configured using APIC, individual configuration of the switches is not required. Cisco APIC discovers the ACI infrastructure switches using LLDP and acts as the central control and management point for the entire configuration.

Cisco Application Policy Infrastructure Controller (APIC) Setup

This sub-section guides you through setting up the Cisco APIC. Cisco recommends a cluster of at least 3 APICs controlling an ACI Fabric.

1. On the back of the first APIC, connect the M port, the Eth1-1 and Eth1-2 ports to the out of band management switches. The M port will be used for connectivity to the server's Cisco Integrated Management Controller (CIMC) and the Eth1-1/2 ports will provide HTTPS and SSH access to the APIC.

Cisco recommends connecting E1-1 and Eth1-2 to two different management switches for redundancy.

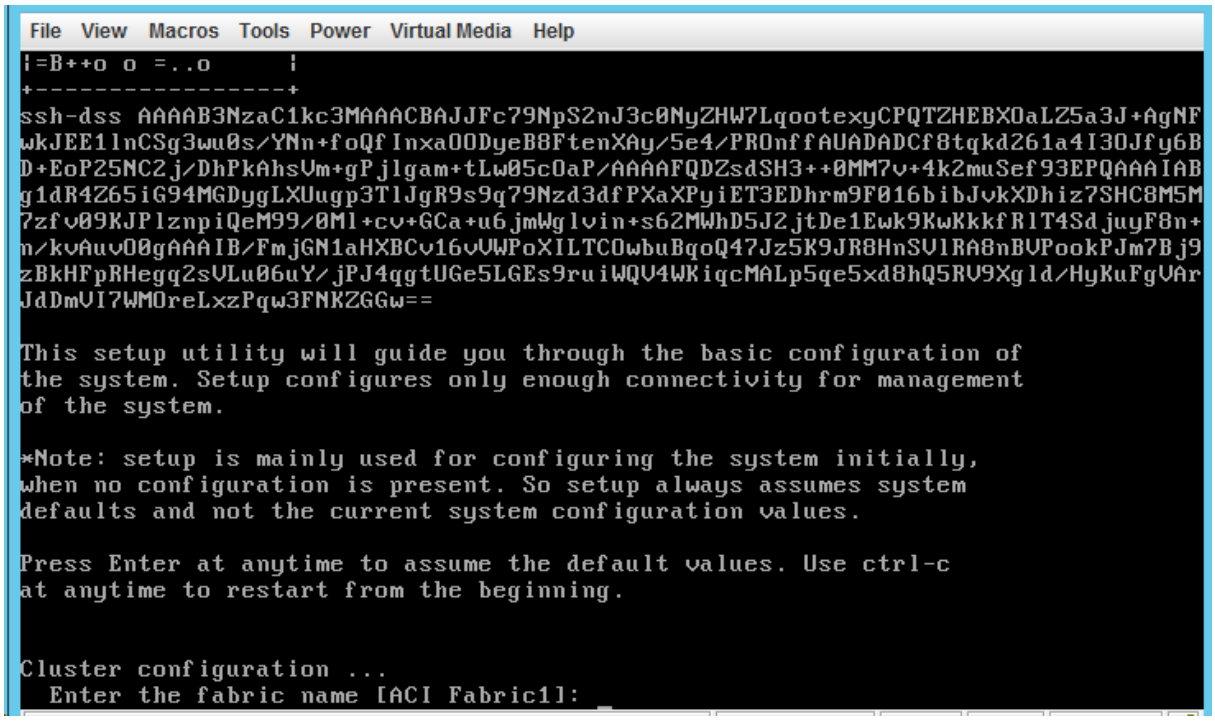
2. Using the supplied KVM dongle cable, connect a keyboard and monitor to the first APIC. Power on the machine, and using **<F8>** key enter the CIMC Configuration Utility. Configure the CIMC with an OOB management IP address. Make sure Dedicated NIC Mode and No NIC Redundancy are selected to put the CIMC interface on the M port. Also set the CIMC password.

3. Save the CIMC configuration using **<F10>** and use **<ESC>** to exit the configuration tool.

The following configuration can be completed using the same KVM console or CIMC connection

4. Press **Enter** to start APIC initial Setup.

Make sure the CIMC Version is 2.0(3i). If it is not, go to Cisco UCS C220M3 downloads and download the version 2.0(3i) Cisco UCS Host Upgrade Utility and upgrade all server firmware following the Cisco Host Upgrade Utility 2.0(3) User Guide.



5. Press <**Enter**> to accept the default fabric name. This value can be changed if desired.

6. Press <**Enter**> to select the default value for the field Enter the number of controllers in the fabric. While the fabric can operate with a single APIC, a minimum 3 APICs are recommended for redundancy and to overcome the split brain condition.

7. Enter the controller number currently being set up under Enter the controller ID (1-3). Remember only controller number 1 will allow you to setup the admin password. Remaining controllers and switches sync their passwords to the admin password set on the controller 1.

8. Enter the controller name or press <**Enter**> to accept the default.

9. Press <**Enter**> to select the default pool under Enter the address pool for TEP addresses. If this subnet is already in use, select a different range.

10. Enter the VLAN ID for the fabric's infra network or the fabric's system VLAN. A recommended ID for this VLAN is 4093 specially when using Cisco AVS.

11. Press <**Enter**> to select the default address pool for Bridge Domain (BD) multicast addresses.

12. Press <**Enter**> to disable IPv6 for the Out-of-Band Mgmt Interface.

13. Enter an IP and subnet length in the out of band management subnet for the Out-of-band management interface.

14. Enter the gateway IP address of the out of band management subnet.

15. Press <**Enter**> to select auto speed/duplex mode.

16. Press <**Enter**> to enable strong passwords.

17. Enter the password for the admin user.

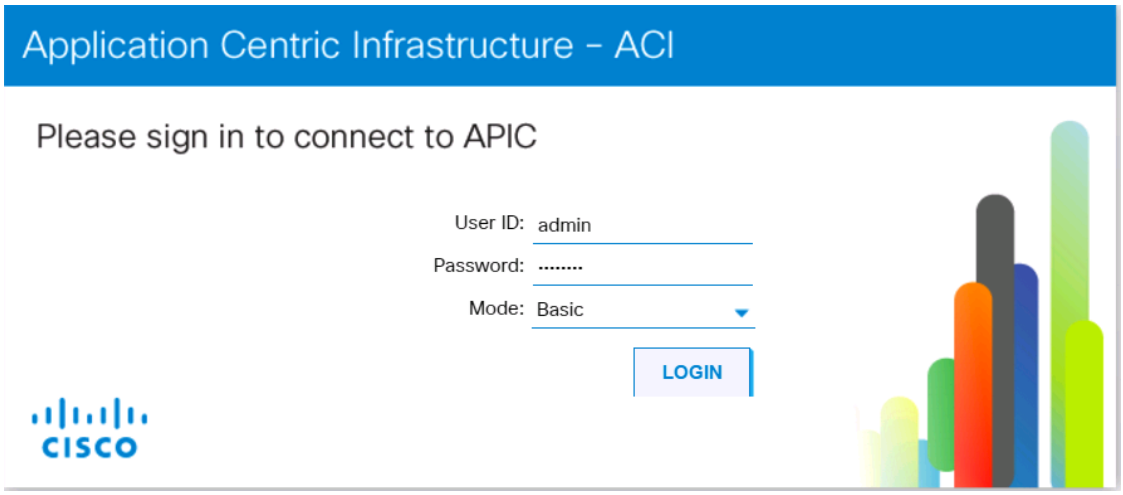
18. Re-enter this password.
19. The Complete configuration is displayed. If all values are correct, press <**Enter**> to exit the configuration without any changes.
20. The APIC will continue configuration and continue boot up until the login: prompt appears.
21. Repeat the above steps for all APIC controllers adjusting the controller ID as necessary.

Cisco ACI Fabric Discovery

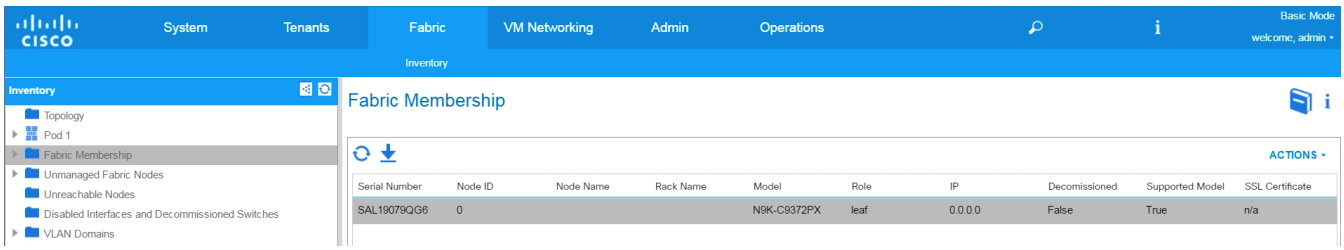
This section details the steps for Cisco ACI Fabric Discovery, where leaf switches, spine switches and APICs are automatically discovered in the ACI Fabric and shows assigned node ids. Cisco recommends a cluster of at least 3 APICs controlling an ACI Fabric.

1. Log into the APIC Advanced GUI using a web browser, by browsing out of band IP address configured for APIC in the last step. Select the **Basic Mode** from the Mode drop-down list and login with the admin user id and password.

In this validation, Google Chrome was used as the web browser. It might take a few minutes before APIC GUI is available after the initial setup



2. Take appropriate action to close any warning screens.
3. At the top in the APIC home page, select the **Fabric** tab.
4. In the left pane, select and expand Fabric Membership.
5. A single Leaf will be listed on the Fabric Membership page as shown:

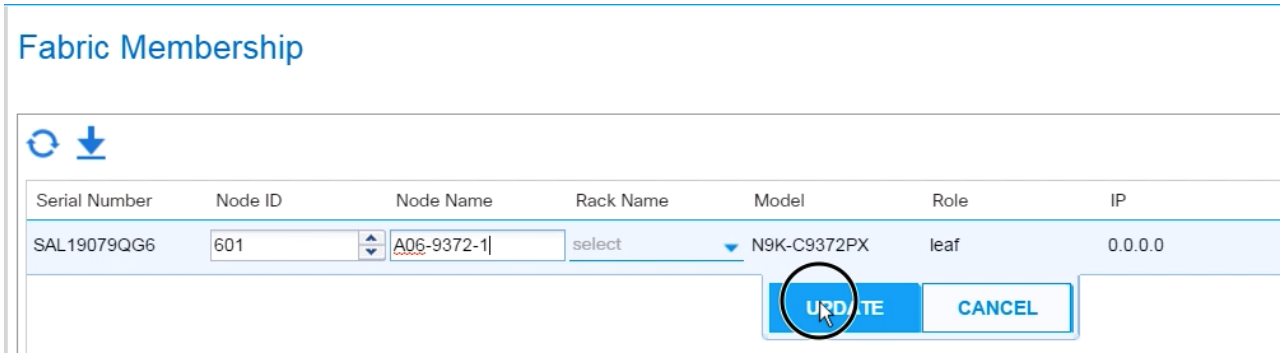


6. Connect to the two leaf and two spine switches using serial consoles and login in as admin with no password (press enter). Use **show inventory** to get the leaf's serial number.

```
show inventory
NAME: "Chassis",  DESCR: "Nexus C9372PX Chassis"
PID: N9K-C9372PX          ,  VID: V02  ,  SN: SAL19079QG6
```

7. Match the serial numbers from the leaf listing to determine whether Leaf 1 or Leaf 2 has appeared under Fabric Membership.

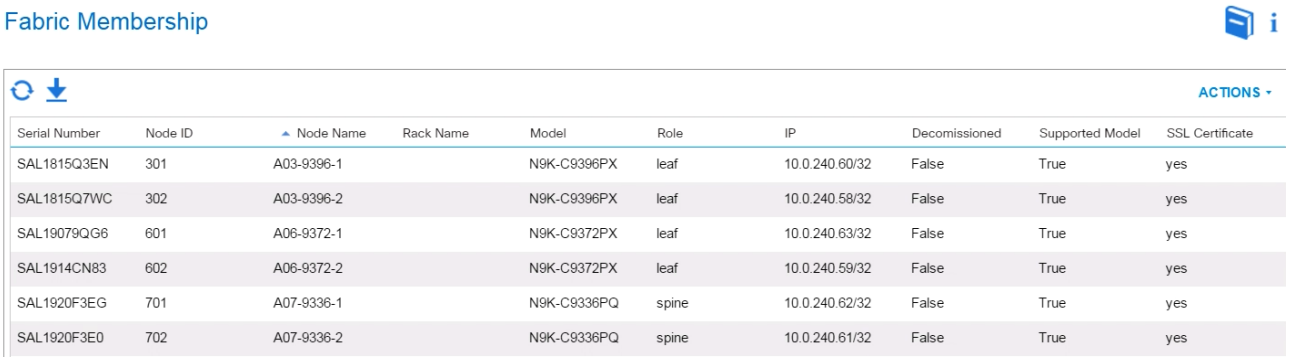
8. In the APIC GUI, under Fabric Membership, double click the leaf in the list. Enter a Node ID and a Node Name for the Leaf switch and click **Update**.



9. The fabric discovery will continue and all the spines and leaves will start appearing under Fabric Membership one after another.

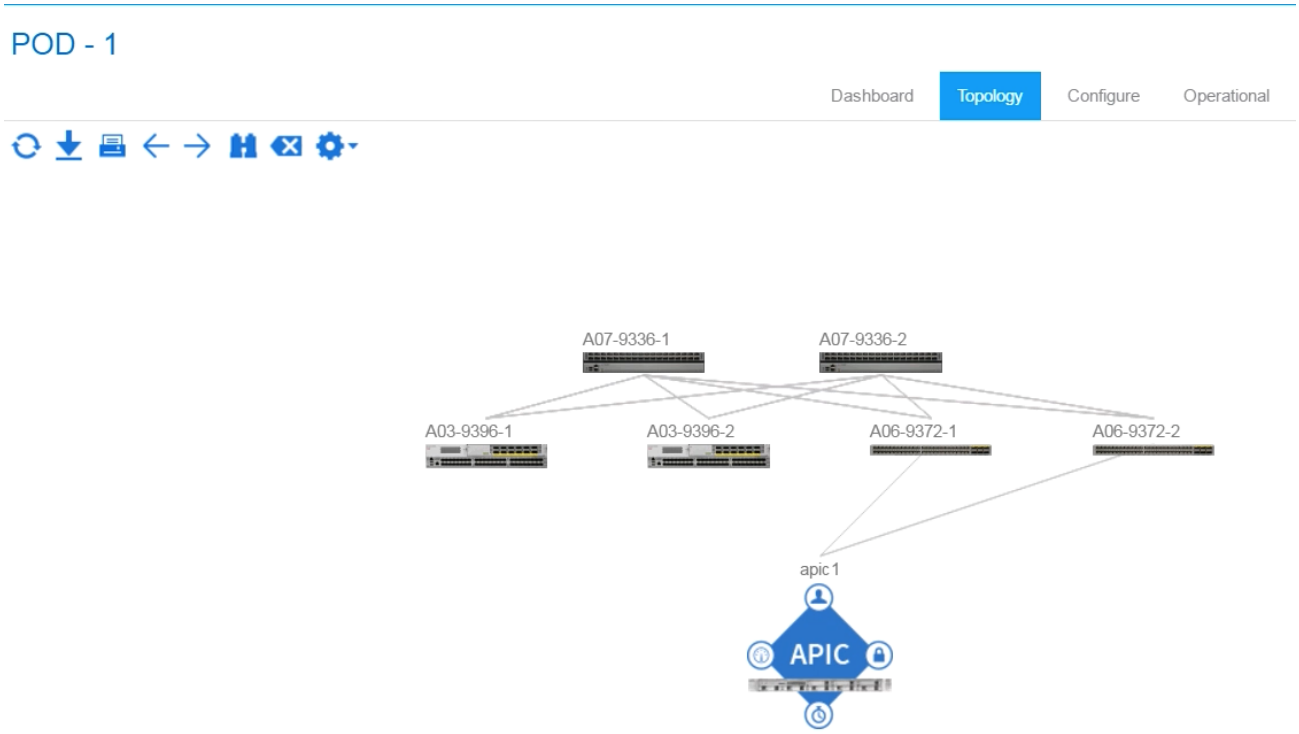
It may be necessary to click the refresh button to see new items in the Fabric Membership list.

10. Repeat steps 7-9 to assign Node IDs and Node Names to these switches. Continue this process until all switches have been assigned Node IDs and Node Names. All switches will also receive IPs in the TEP address space assigned during the initial setup of the APIC.



Serial Number	Node ID	Node Name	Rack Name	Model	Role	IP	Decomissioned	Supported Model	SSL Certificate
SAL1815Q3EN	301	A03-9396-1		N9K-C9396PX	leaf	10.0.240.60/32	False	True	yes
SAL1815Q7WC	302	A03-9396-2		N9K-C9396PX	leaf	10.0.240.58/32	False	True	yes
SAL19079QG6	601	A06-9372-1		N9K-C9372PX	leaf	10.0.240.63/32	False	True	yes
SAL1914CN83	602	A06-9372-2		N9K-C9372PX	leaf	10.0.240.59/32	False	True	yes
SAL1920F3EG	701	A07-9336-1		N9K-C9336PQ	spine	10.0.240.62/32	False	True	yes
SAL1920F3E0	702	A07-9336-2		N9K-C9336PQ	spine	10.0.240.61/32	False	True	yes

11. Click **Topology** in the left pane. The discovered ACI Fabric topology will appear. It may take a few minutes and you will need to click the refresh button for the complete topology to appear.



The topology shown in the capture above is a sample topology containing 4 leaf switches, 2 spine switches, and a single APIC. Customer topology will vary depending on number and type of devices. While a single APIC is captured in this topology, Cisco recommends a cluster of at least 3 APICs in a production environment.

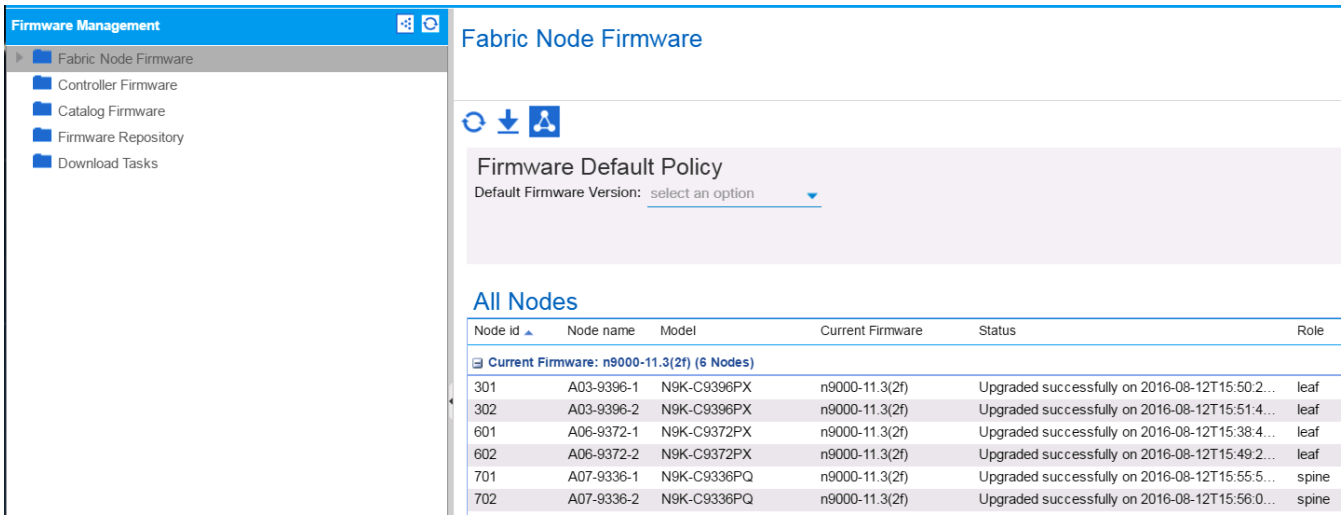
Initial ACI Fabric Setup

This section details the steps for initial setup of the Cisco ACI Fabric, where the software release is validated, out of band management IPs are assigned to the leaves and spines, NTP is setup, and the fabric BGP route reflectors are set up.

Software Upgrade

1. In the APIC Basic GUI, at the top select **Admin** > **Firmware**.

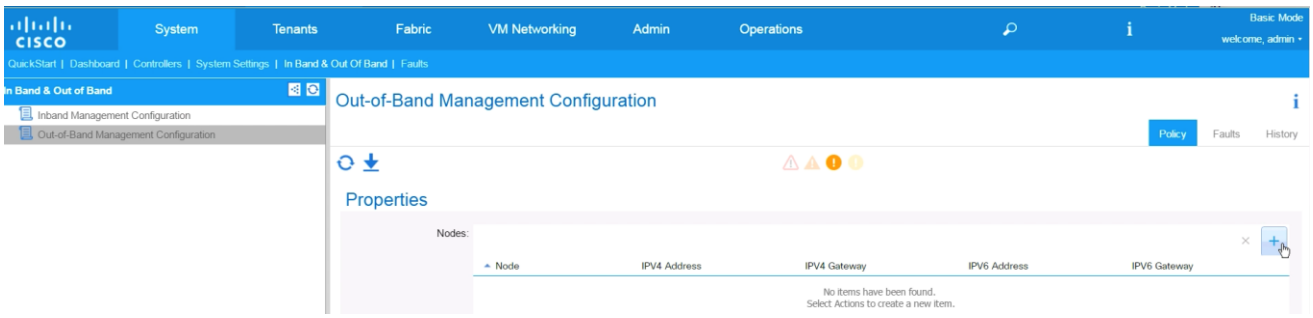
2. This document was validated with ACI software release 1.3(2f). Select Fabric Node Firmware in the left pane under Firmware Management. All switches should show the same firmware release and the release version should be at minimum n9000-11.3(2f). The switch software version should also match the APIC version.



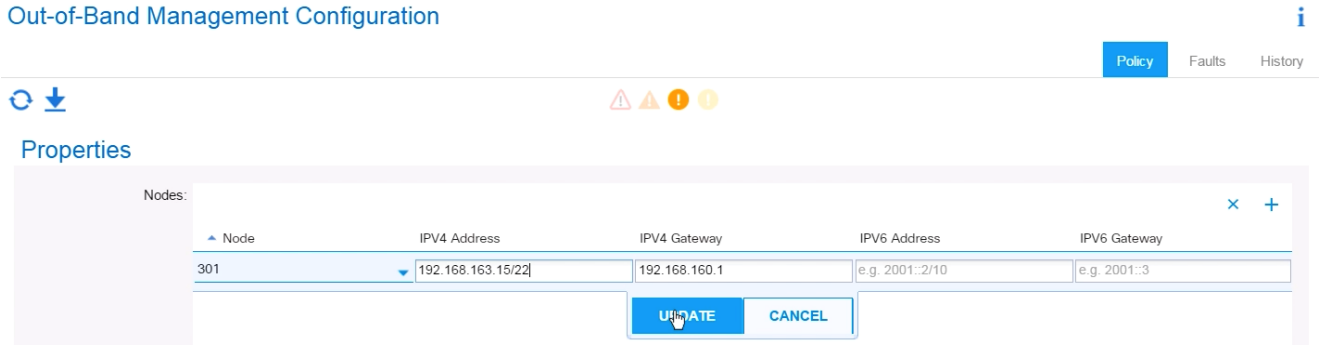
3. If the APICs have not already been upgraded, click Admin > Firmware > Controller Firmware. If all APICs are not at the same release at a minimum of 1.3(2f), follow the Cisco APIC Controller and Switch Software Upgrade and Downgrade Guide to upgrade both the APICs and switches to a minimum release of 1.3(2f) on APIC and 11.2(2f) on the switches.

Setting up Out of Band Management IP Addresses for Leaf and Spine Switches

1. To add out of band management interfaces for all the switches in the ACI Fabric, select System > In Band & Out of Band
2. Click Out-of-Band Management Configuration in the left pane.
3. Click **+** under Properties in the right pane as shown in the screenshot below.



4. Select the Node/Switch from the drop-down list.
5. Enter IP address with mask and Gateway address.
6. Click **Update**.

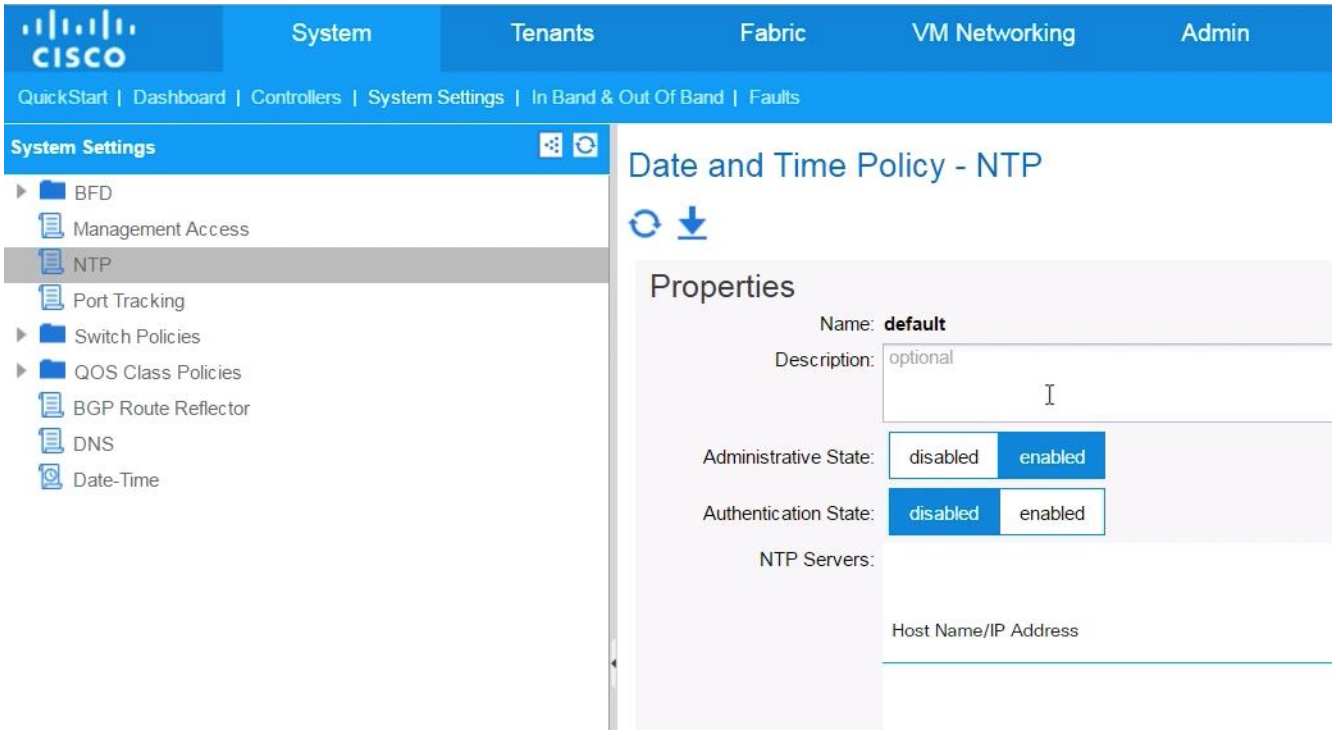


7. Repeat the process to provide an out of band management IP address for all the switches.
8. Direct SSH access to the switches should now be available.

Setting NTP Server

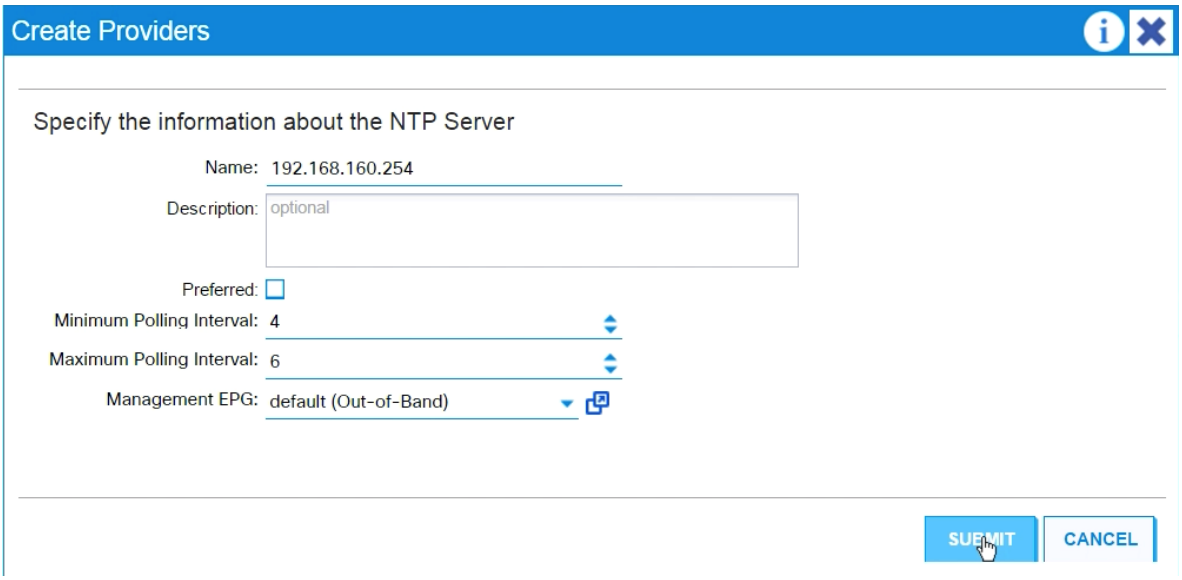
This procedure will allow customers to setup an NTP server for synchronizing the fabric time.

1. To set up NTP in the fabric, select System > System Settings.
2. In the left pane under System Settings, click **NTP**.



3. Make sure Administrative State is set to enabled.
4. Click **+** under the NTP servers.
5. Enter the IP address of the NTP server.
6. From the Management EPG, select default (Out-of-Band).

7. Click **SUBMIT**.



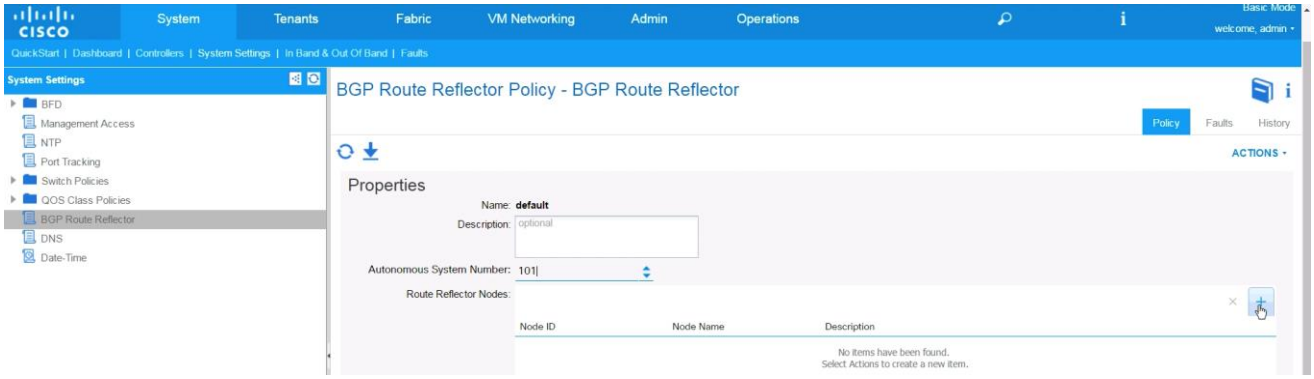
Setting BGP Route Reflectors

In this ACI deployment, both the spine switches are set up as BGP route-reflectors to distribute the leaf routes throughout the fabric.

1. To configure BGP Route Reflector settings, select System > System Settings.

2. In the left pane under System Settings, select **BGP Route Reflector**.

3. Enter 101 as the Autonomous System Number. The AS number can be modified based on the customer environment.



4. Click **+** in the right pane and select the Spine-1 switch ID.

5. **Optional**: Add description.

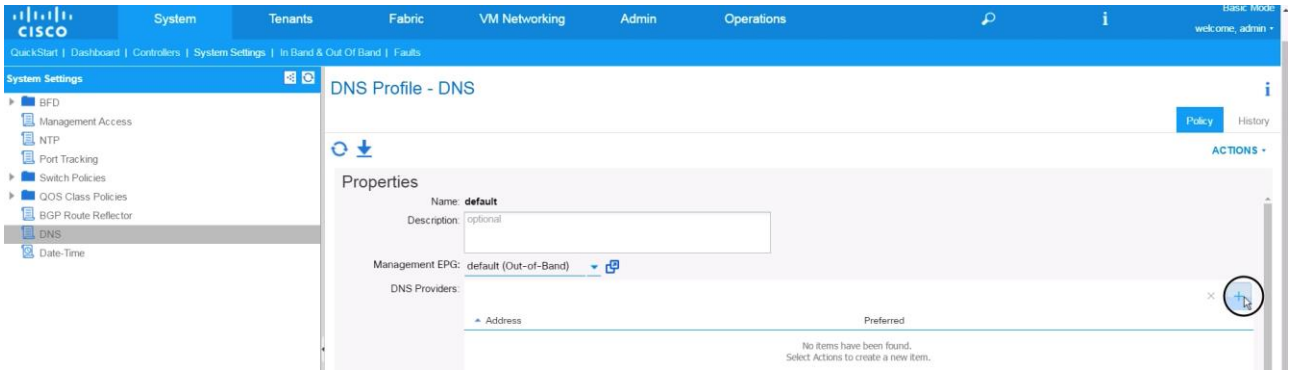
6. Click **SUBMIT**.
7. Click **+** again and set the second Spine Node as a Route Reflector.

8. Click **SUBMIT**.
9. Click **SUBMIT CHANGES** if the system generates a warning.

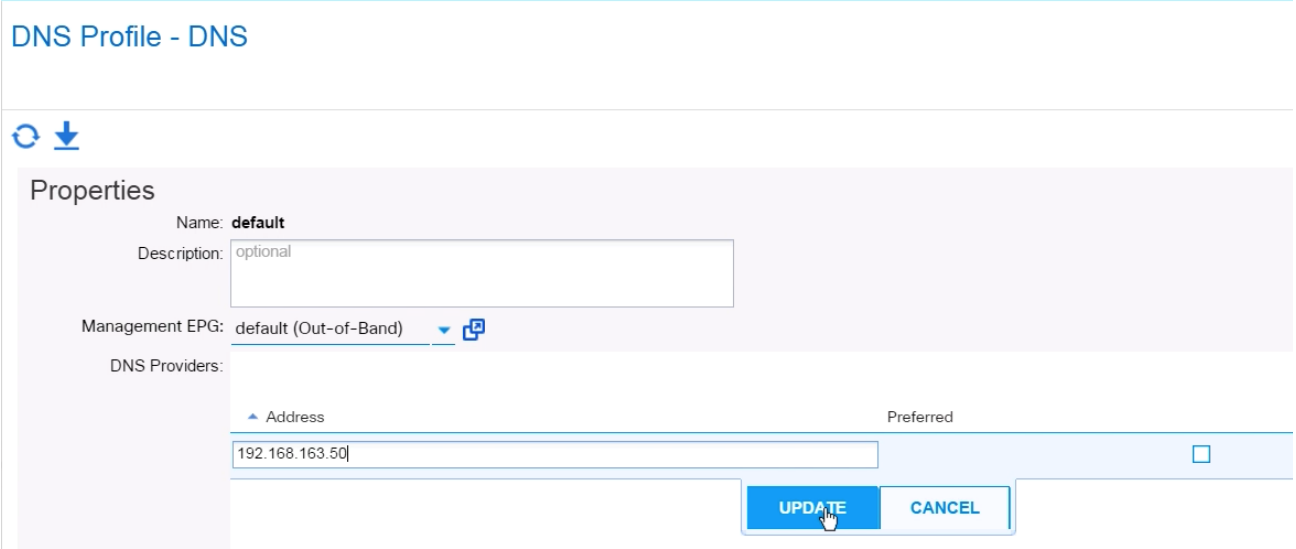
Setting DNS

To set the DNS server and the domain, complete the following configuration steps:

1. For setting up DNS, select System > System Settings.
2. In the left pane under System Settings, select **DNS**.
3. In the right pane under Properties, select default (Out-of-Band) from the drop-down list for the Management EPG.
4. Click **+** to add DNS Providers.



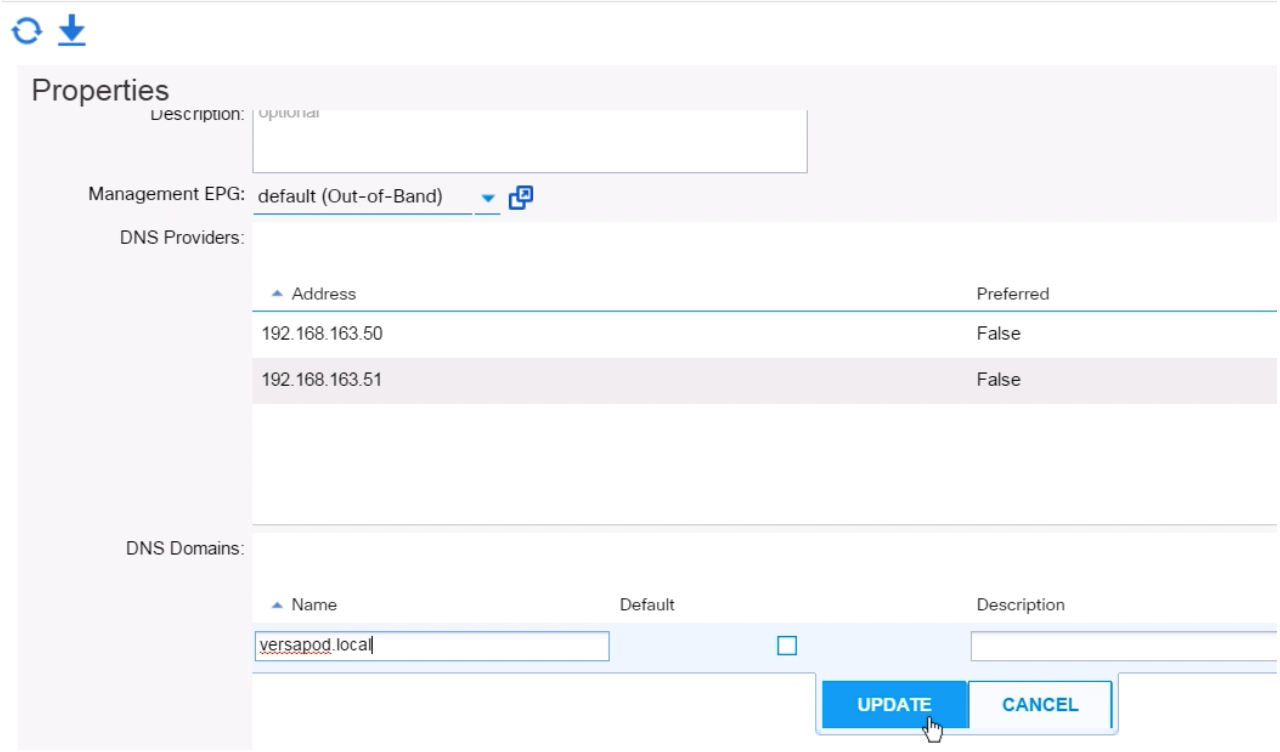
5. Enter the IP address of the DNS server and check the Preferred check box if applicable.



6. Click **UPDATE**.

7. Add additional DNS servers if applicable.

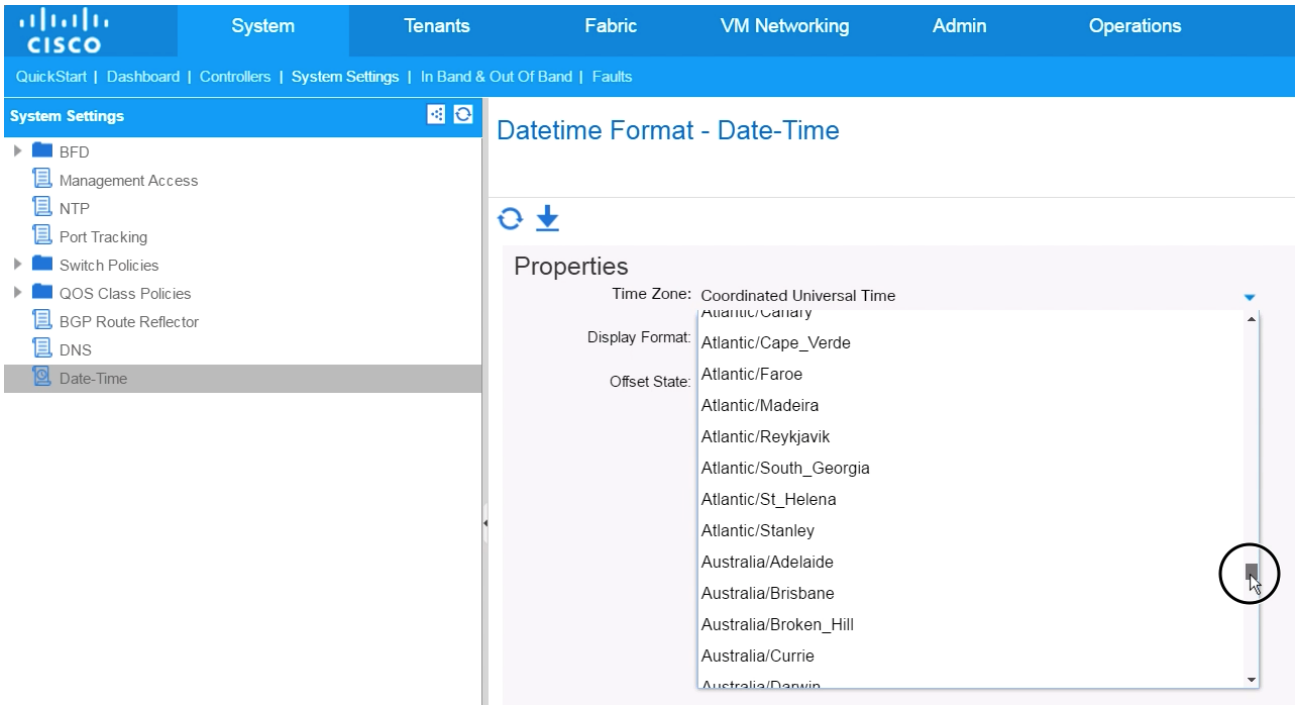
8. Add DNS Domains by clicking the **+** and typing the DNS Domain Name and click **UPDATE**.



9. Click **SUBMIT**.

Set the TimeZone

1. To setup the correct timezone for the ACI fabric, select System > System Settings.
2. In the left pane under System Settings, select **Date-Time**.
3. In the right pane under Properties, select the correct Time Zone from the drop-down list.

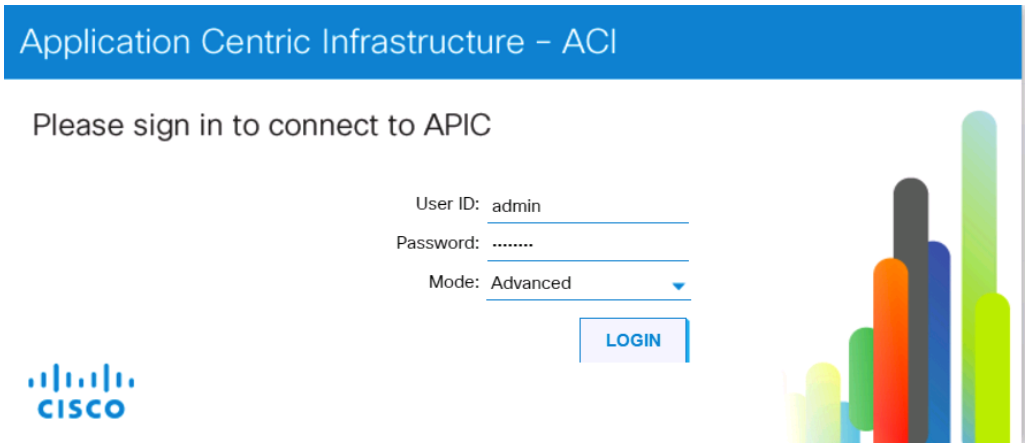


4. Click **SUBMIT**.

Set up Fabric Access Policy Setup

This section details the steps to create various access policies creating parameters for CDP, LLDP, LACP, etc. These policies will be used during vPC and VM domain creation. To define fabric access policies, complete the following steps:

1. Log into APIC Advanced GUI as shown in the screenshot.



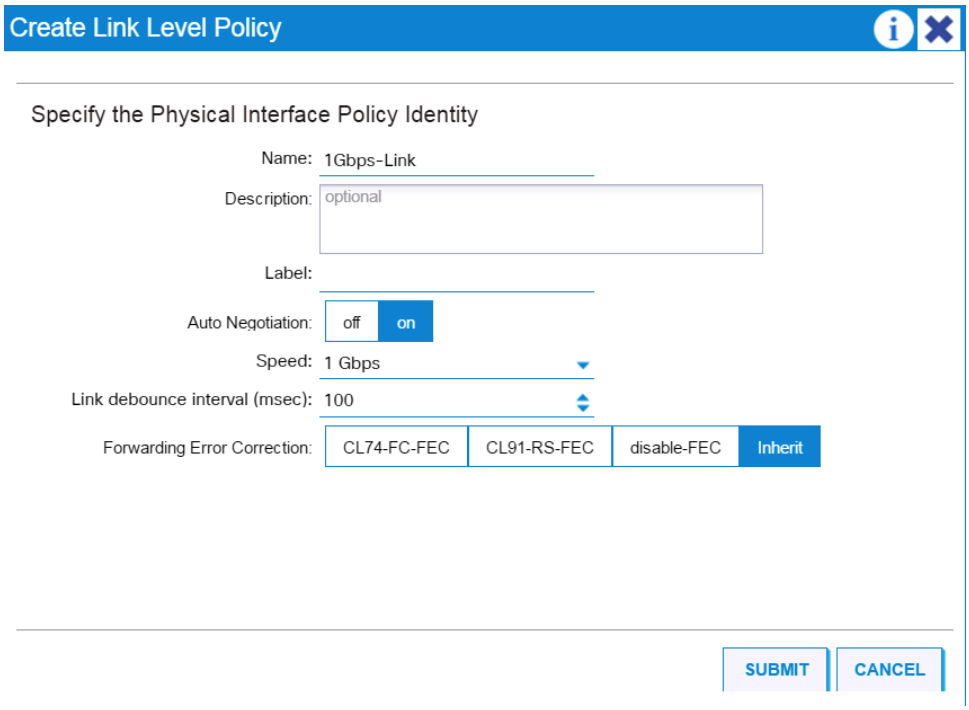
2. In the APIC Advanced GUI, select and expand Fabric > Access Policies > Interface Policies > Policies.

Create Link Level Policy

This procedure will create link level policies for setting up the 1Gbps and 10Gbps link speeds.

1. In the left pane, right-click Link Level and select **Create Link Level Policy**.

2. Name the policy as 1Gbps-Link and select the 1Gbps Speed.

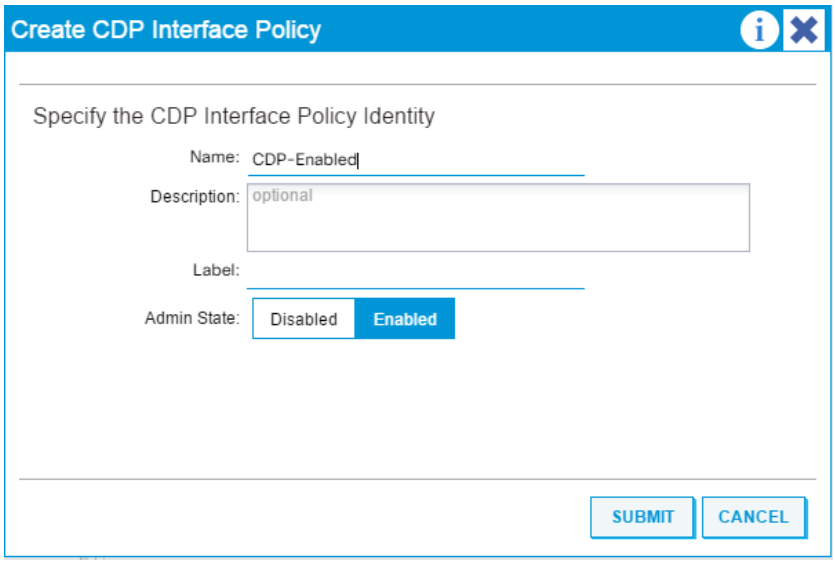


3. Click **SUBMIT** to complete creating the policy.
4. In the left pane, right-click on Link Level and select **Create Link Level Policy**.
5. Name the policy 10Gbps-Link and select the 10Gbps Speed.
6. Click **SUBMIT** to complete creating the policy.

Create CDP Policy

This procedure will create policies to enable or disable CDP on a link.

1. In the left pane, right-click CDP interface and select **Create CDP Interface Policy**.
2. Name the policy as CDP-Enabled and enable the Admin State.

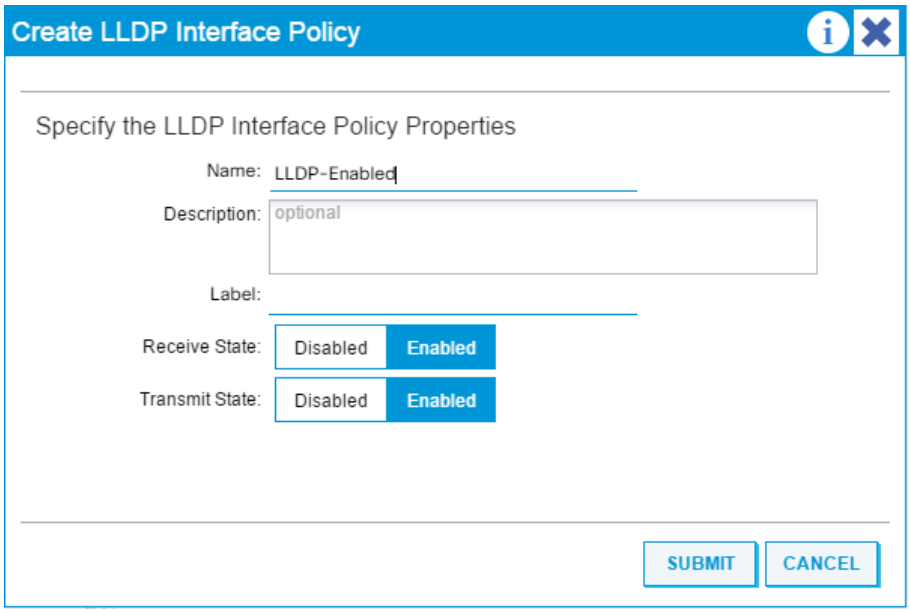


3. Click **SUBMIT** to complete creating the policy.
4. In the left pane, right-click on the CDP Interface and select **Create CDP Interface Policy**.
5. Name the policy CDP-Disabled and disable the Admin State.
6. Click **SUBMIT** to complete creating the policy.

Create LLDP Interface Policies

This procedure will create policies to enable or disable LLDP on a link.

1. In the left pane, right-click LLDP Interface and select **Create LLDP Interface Policy**.
2. Name the policy as LLDP-Enabled and enable both Transmit State and Receive State.

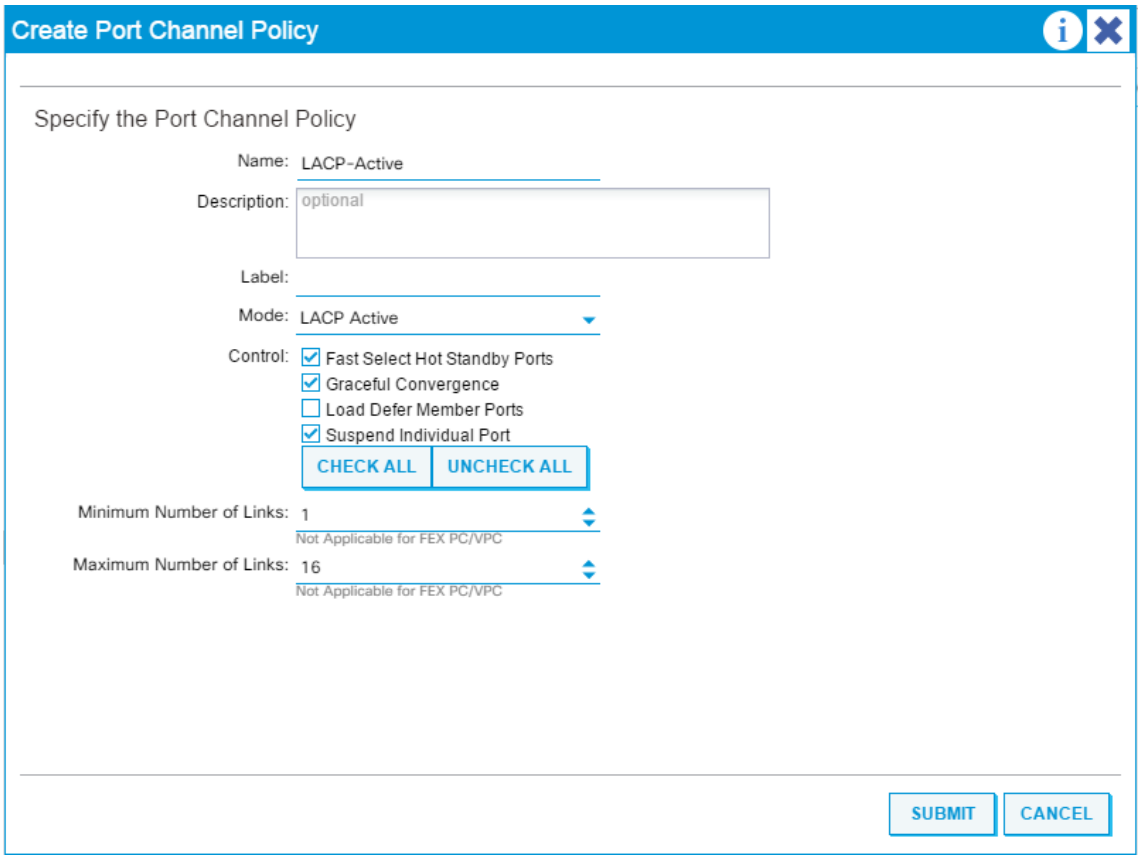


3. Click **SUBMIT** to complete creating the policy.
4. In the left, right-click the LLDP Interface and select **Create LLDP Interface Policy**.
5. Name the policy as LLDP-Disabled and disable both the Transmit State and Receive State.
6. Click **SUBMIT** to complete creating the policy.

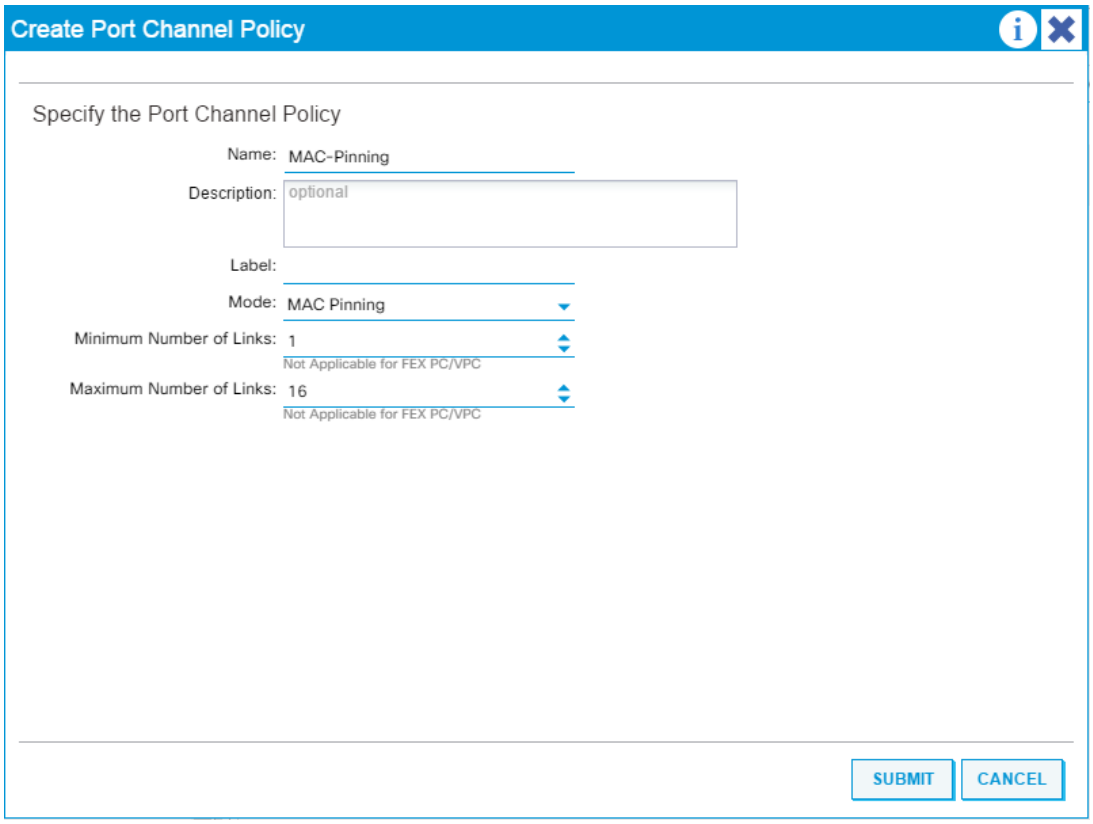
Create Port-Channel Policy

This procedure will create policies to set LACP active mode configuration and the MAC-Pinning mode configuration.

1. In the left pane, right-click the Port Channel and select **Create Port Channel Policy**.
2. Name the policy as LACP-Active and select LACP Active for the Mode. Do not change any of the other values.



3. Click **SUBMIT** to complete creating the policy.
4. In the left pane, right-click Port Channel and select **Create Port Channel Policy**.
5. Name the policy as MAC-Pinning and select MAC Pinning for the Mode. Do not change any of the other values.

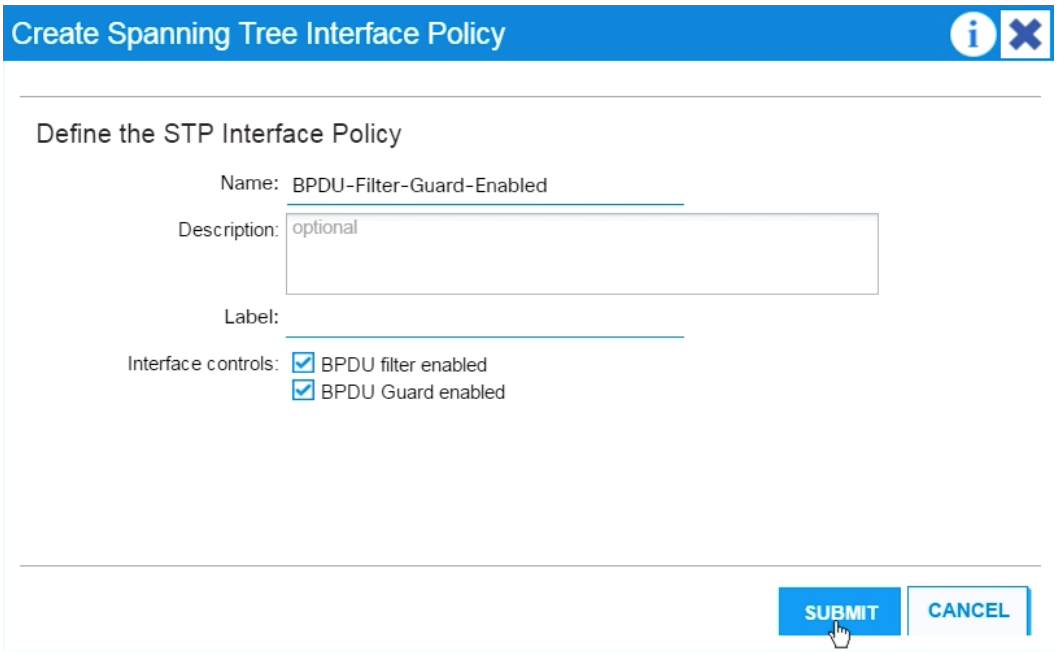


6. Click **SUBMIT** to complete creating the policy.

Create BPDU Filter/Guard Policies

This procedure will create policies to enabled or disabled BPDU filter and guard.

1. In the left pane, right-click Spanning Tree Interface and select **Create Spanning Tree Interface Policy**.
2. Name the policy as BPDU-Filter-Guard-Enabled and select both the BPDU filter and BPDU Guard Interface Controls.

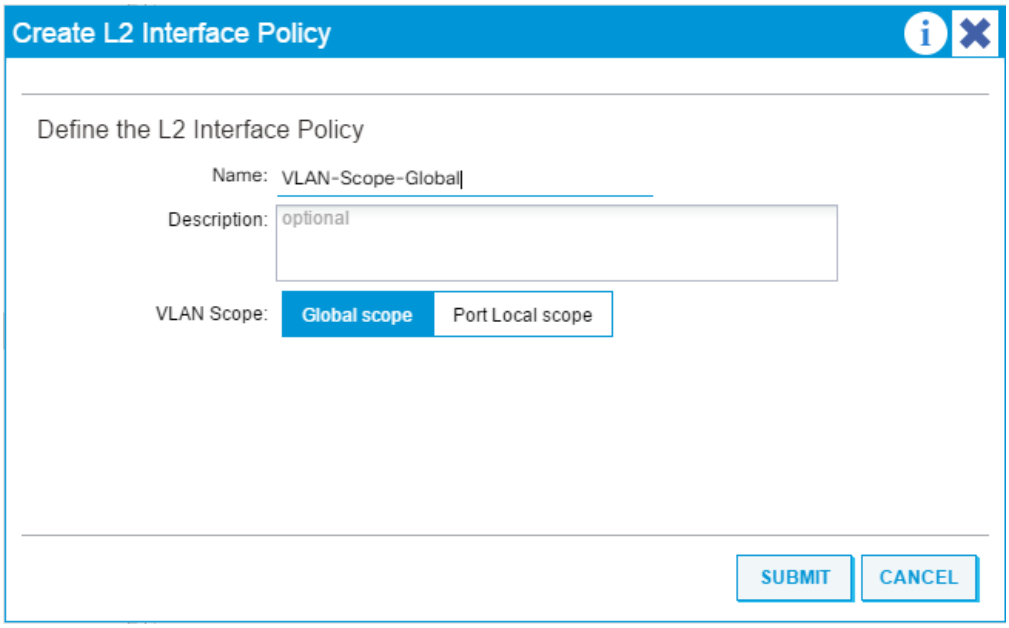


3. Click **SUBMIT** to complete creating the policy.
4. In the left pane, right-click Spanning Tree Interface and select **Create Spanning Tree Interface Policy**.
5. Name the policy as BPDU-Filter-Guard-Disabled and make sure both the BPDU filter and BPDU Guard Interface Controls are cleared.
6. Click **SUBMIT** to complete creating the policy.

Create Global VLAN Policy

This procedure will create policies to enable global scope for all the VLANs.

1. In the left pane, right-click on the L2 Interface and select **Create L2 Interface Policy**.
2. Name the policy as VLAN-Scope-Global and make sure Global scope is selected.

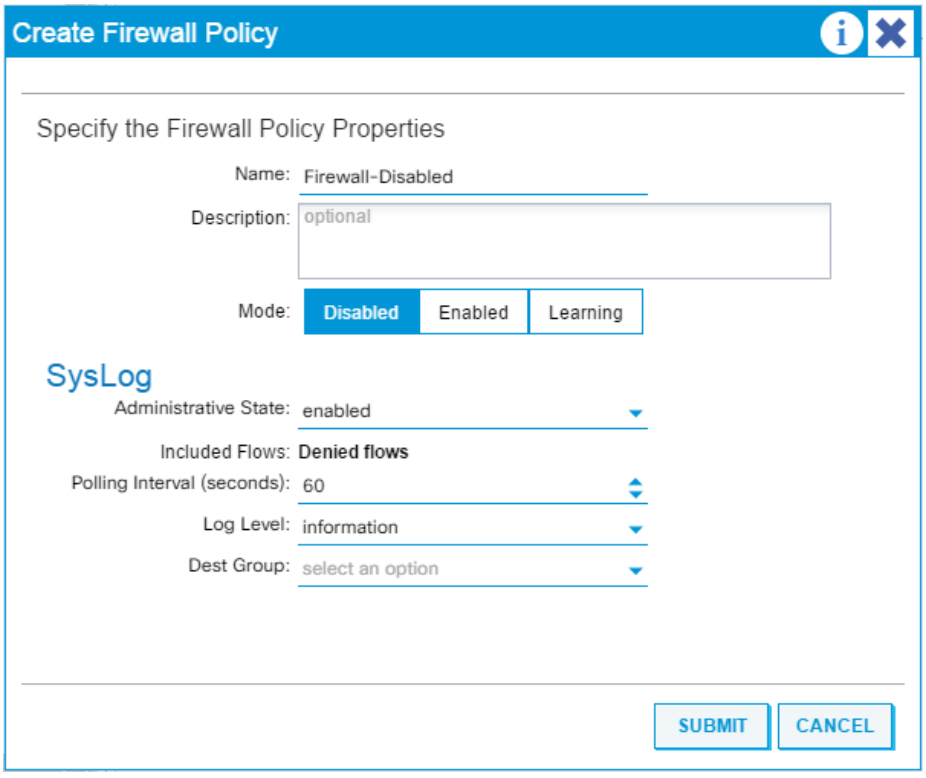


3. Click **SUBMIT** to complete creating the policy.

Create Firewall Policy

This procedure will create policies to disable Firewall.

1. In the left, right-click Firewall and select Create Firewall Policy.
2. Name the policy Firewall-Disabled and select Disabled for Mode. Do not change any of the other values.



3. Click **SUBMIT** to complete creating the policy.

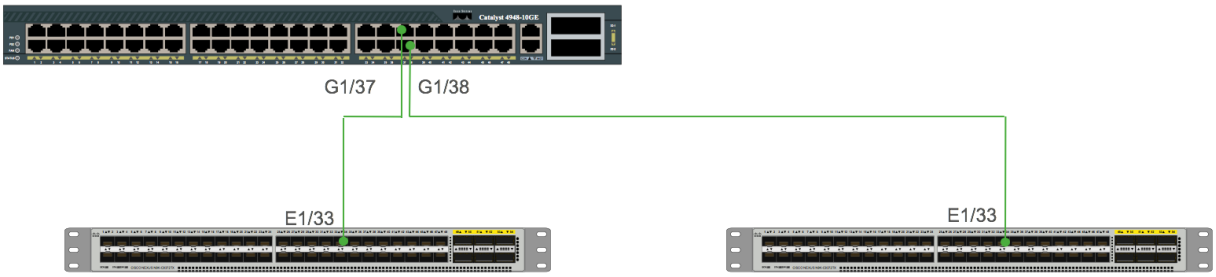
Create Virtual Port Channels (vPCs)

This sub-section details the steps to setup vPCs for connectivity to the Management Network, Cisco UCS and IBM Storage.

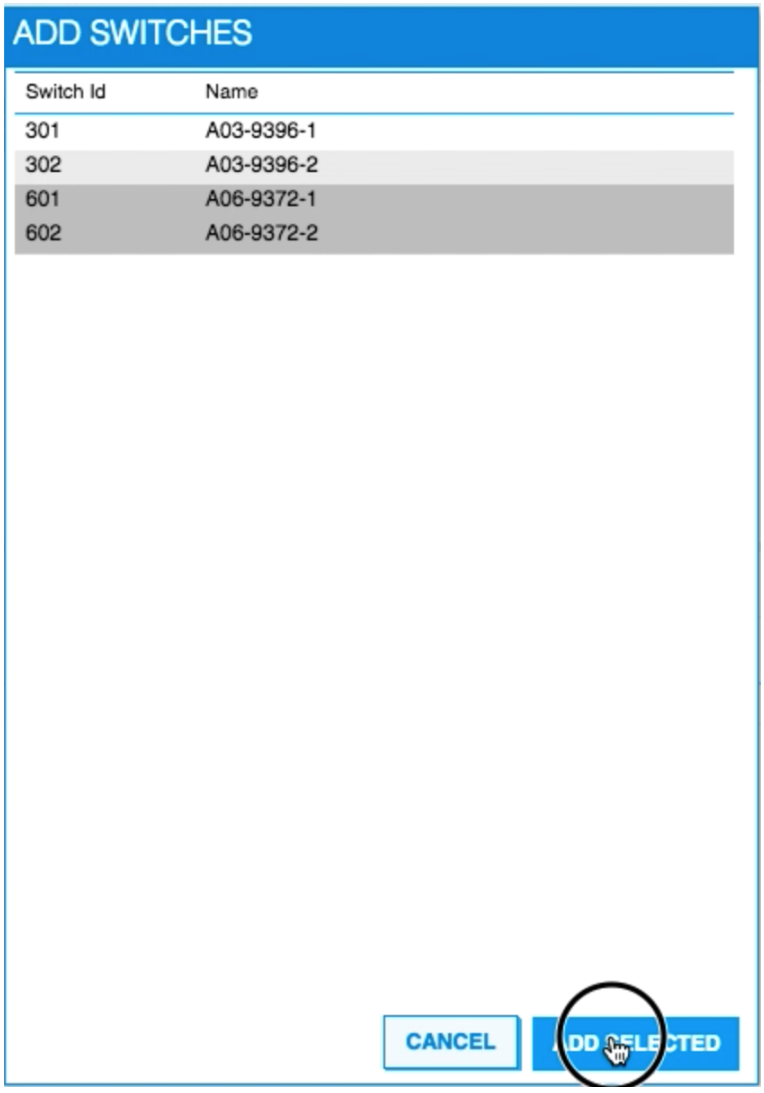
VPC - Management Switch

Complete the following steps to setup vPCs for connectivity to the existing Management Network.

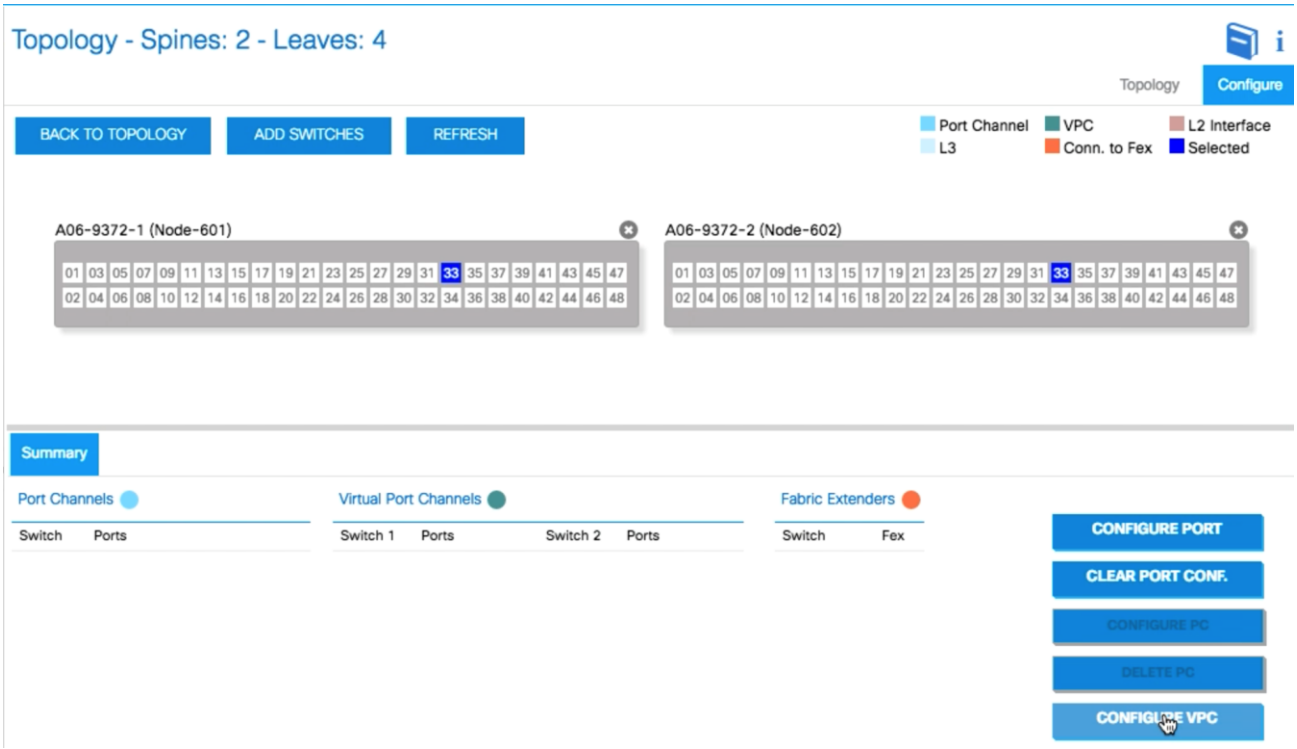
This deployment guide covers configuration for a pre-existing Cisco Catalyst management switch. Customers can adjust the configuration depending on their management connectivity.



1. In the APIC Advanced GUI, at the top select Fabric > Inventory > Topology.
2. In the right pane, select **Configure**.
3. Click **ADD SWITCHES**. Select both the leaf switches and select **ADD SELECTED**.

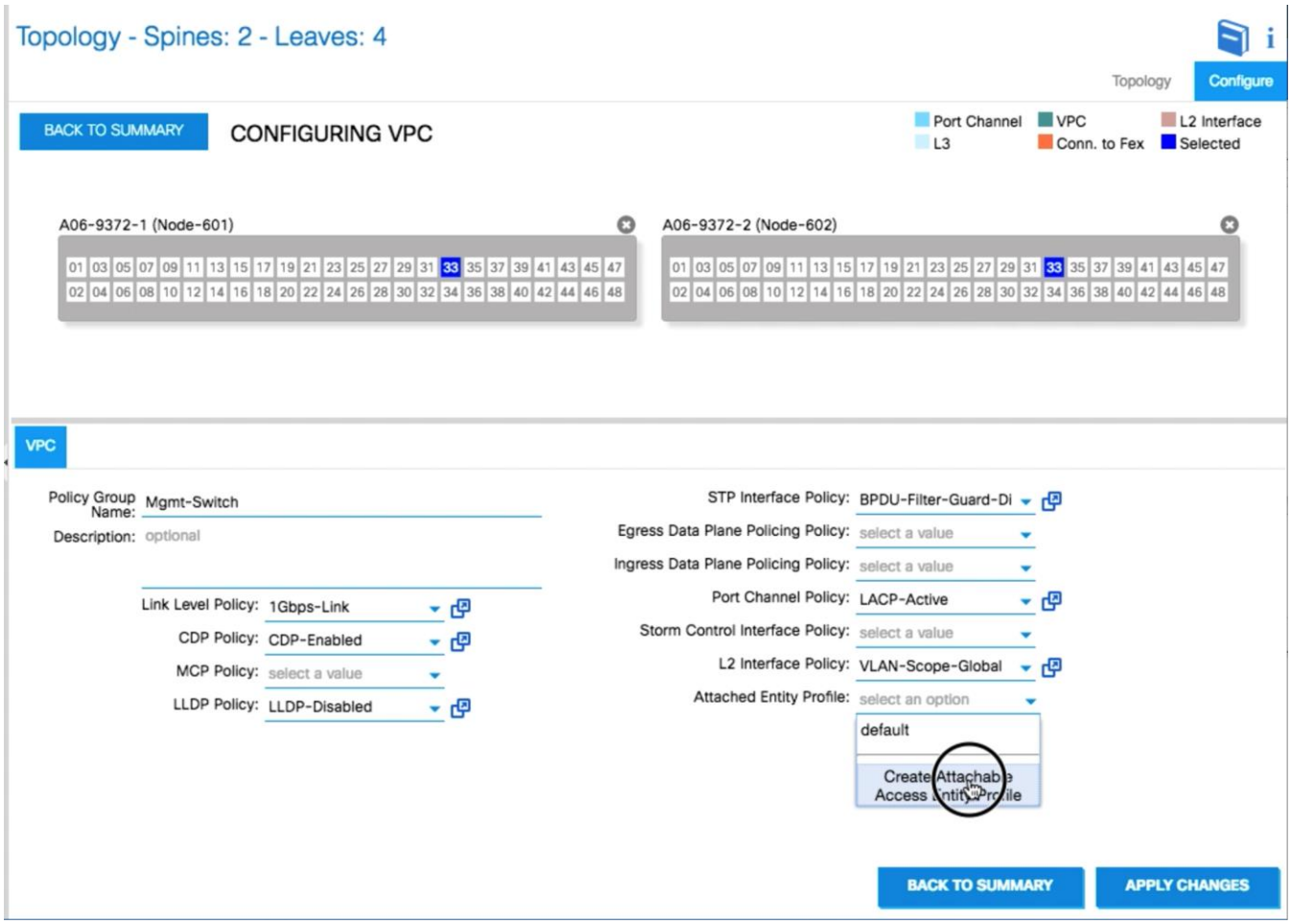


4. On both the switches, select the port connected for your In-Band Management connection.
5. Select CONFIGURE VPC.

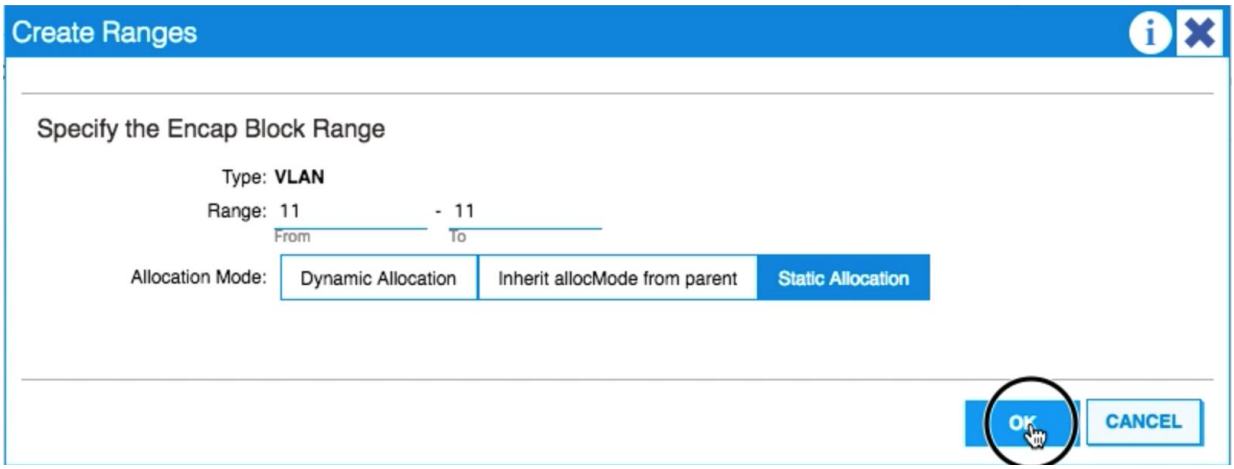


6. For the Policy Group Name, enter Mgmt-Switch. Select the appropriate policies as shown in the screenshot below.

In this validation, Cisco Catalyst switch was configured with a 1Gbps ports based port-channel in trunk mode.



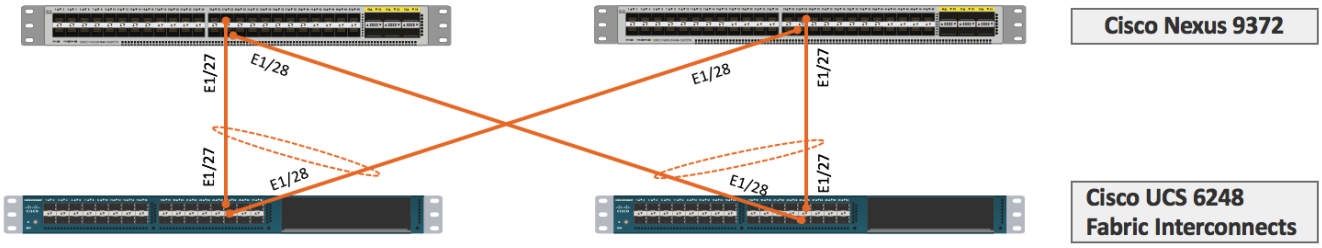
7. For the Attached Entity Policy field, select **Create Attachable Access Entity Profile**.
8. Name the profile as aep-Mgmt-Switch. Click **+** to add a Physical Domain.
9. From the drop-down list, select **Create Physical Domain**.
10. In the Create Physical Domain window, name the Domain as pd-Mgmt-Switch.
11. From the VLAN Pool drop-down list, select **create VLAN Pool**.
12. In the create VLAN Pool window, name the VLAN Pool as vp-Mgmt-Switch. Select **Static Allocation**.
13. Click **+** to add an Encapsulation Block.
14. Enter the in-band management VLAN for both the From and To parts of the Range. Select **Static Allocation**.



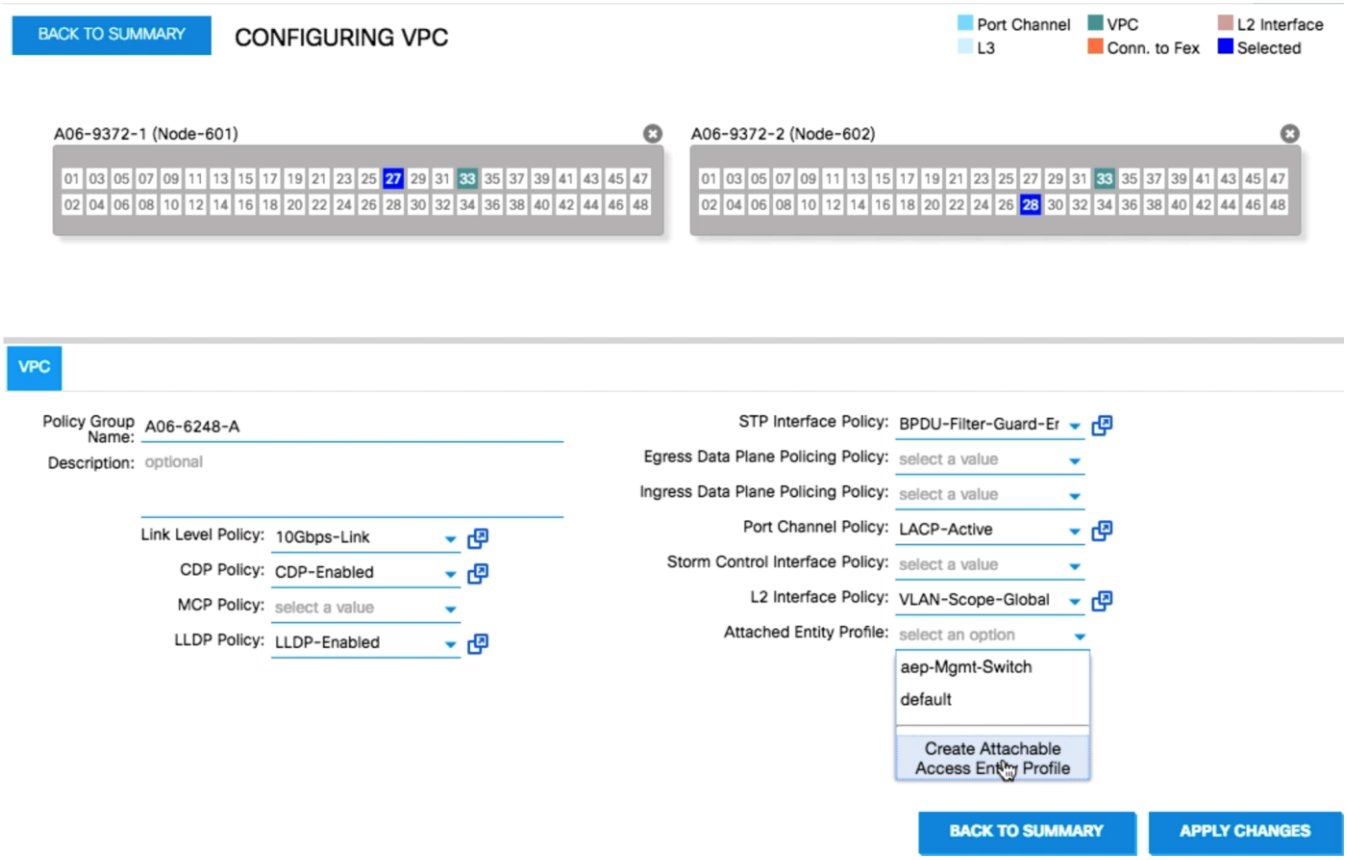
15. Click **OK** to complete creating the range.
16. Click **SUBMIT** to complete creating the VLAN Pool.
17. Click **SUBMIT** to complete creating the Physical Domain.
18. Click **UPDATE** and **SUBMIT** to complete creating the Attachable Access Entity Profile.
19. Click **APPLY CHANGES** to complete creating the vPC. Click **OK** for the confirmation message.

VPC – UCS Fabric Interconnects

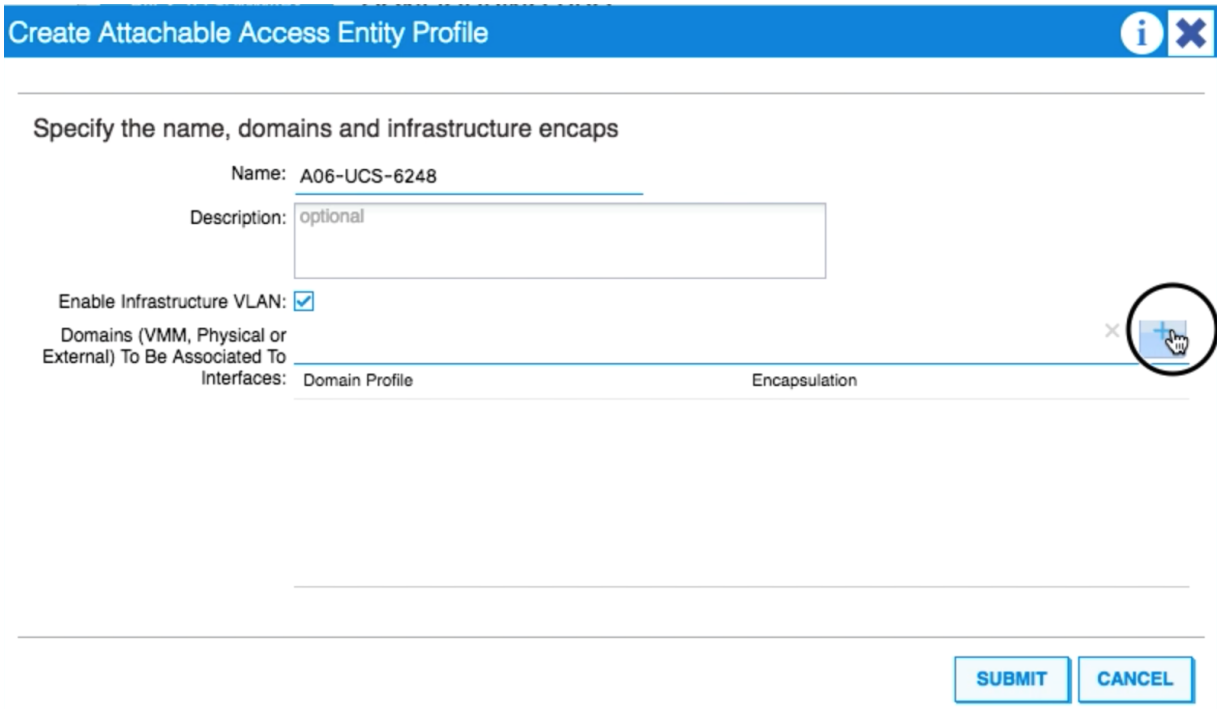
Complete the following steps to setup vPCs for connectivity to the UCS Fabric Interconnects.



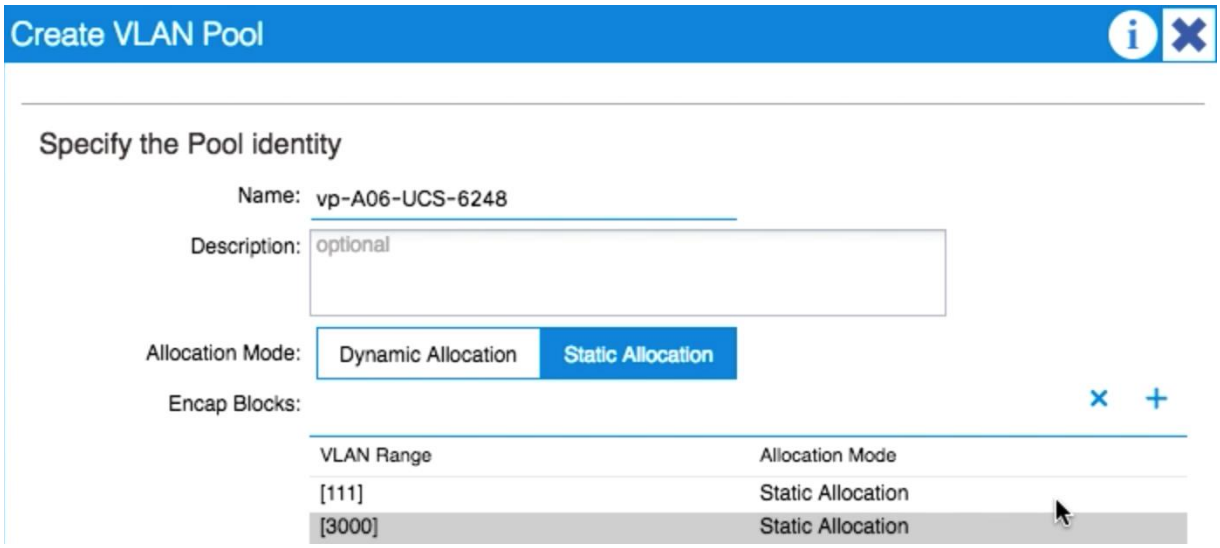
1. In the APIC Advanced GUI, select Fabric > Inventory > Topology.
2. In the right pane, select **Configure**.
3. Click **ADD SWITCHES**. Select both the leaf switches and select **ADD SELECTED** on both the switches. Select the port connected for the UCS Fabric Interconnect A.
4. For the Policy Group Name, enter <FI-A-Name>. Select the appropriate policies as shown in the screenshot.



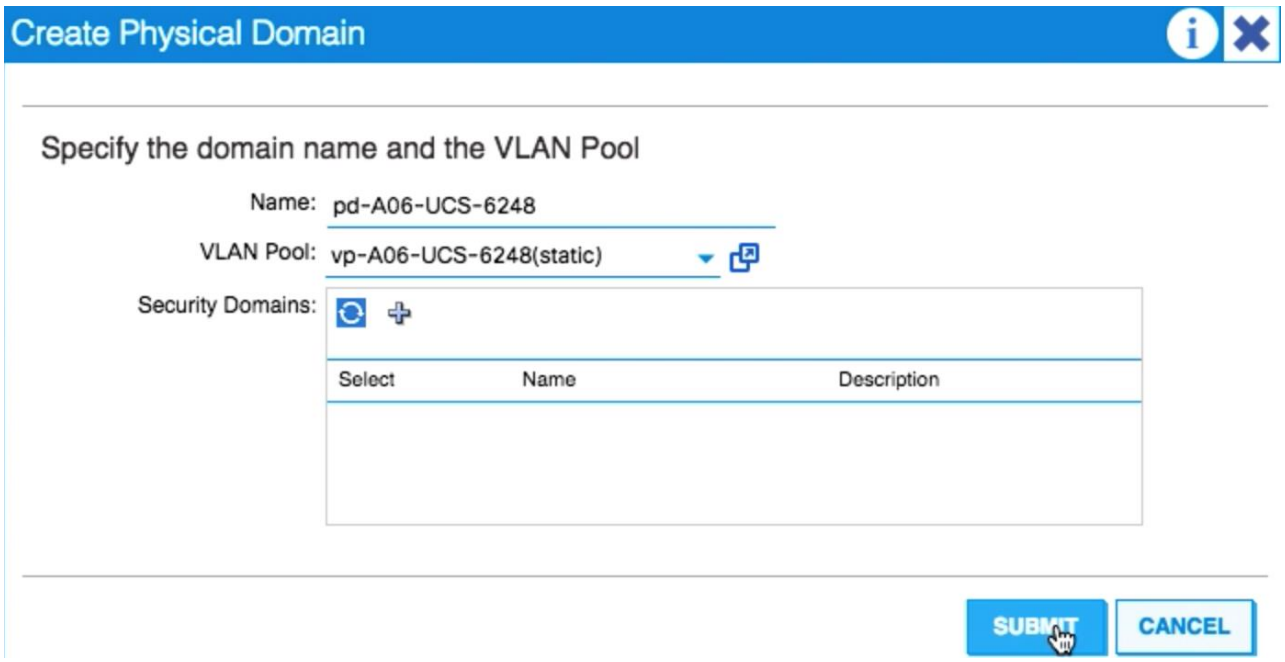
5. From the Attached Entity Policy drop-down list, select **Create Attachable Access Entity Profile**.
6. Name the profile as aep-<UCS-Name>.
7. Check the check box Enable Infrastructure VLAN, if planning on deploying AVS.
8. Click **+** to add a Physical Domain.



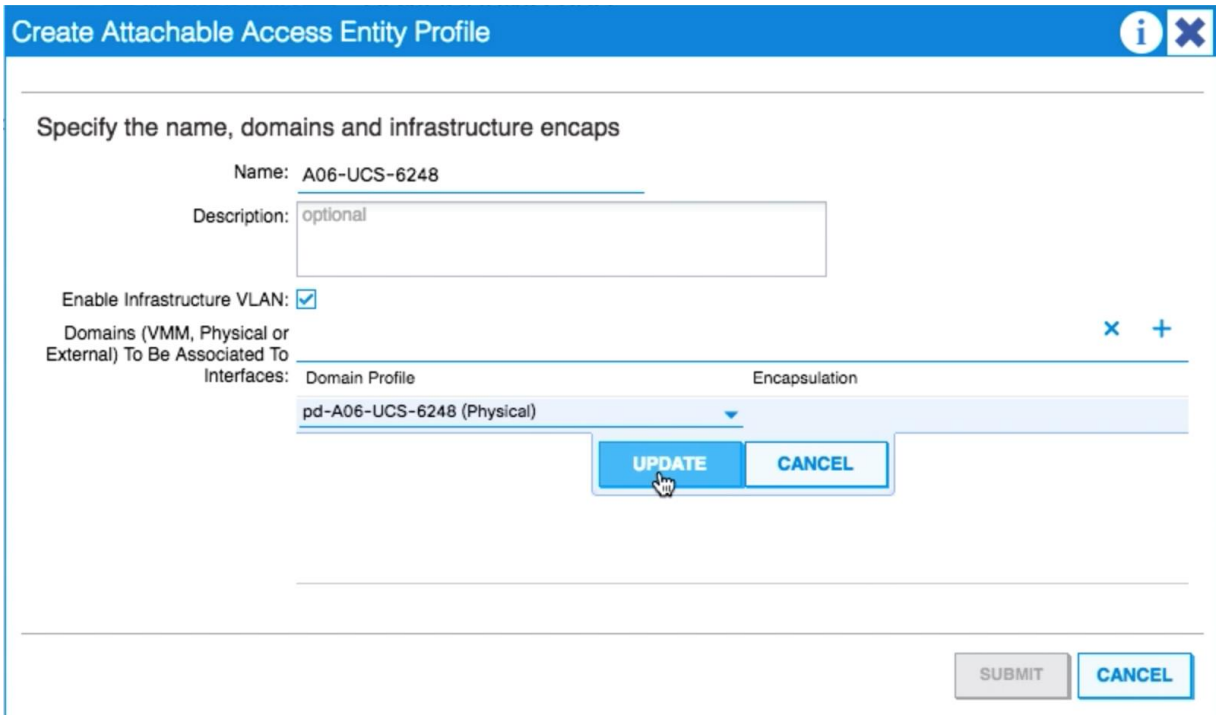
9. From the drop-down list, select **Create Physical Domain**.
10. In the Create Physical Domain window, name the Domain as pd-<UCS-Name>.
11. From the VLAN Pool drop-down list, select **create VLAN Pool**.
12. In the create VLAN Pool window, name the VLAN Pool as vp-<UCS-Name>. Select **Static Allocation**.
13. Click **+** to add an Encapsulation Block.
14. Create multiple ranges to add the following VLANs:
15. Native-2 VLAN (2)
16. In-band Management VLAN (111)
17. vMotion VLAN (3000)
18. iSCSI-A VLAN (3030)
19. iSCSI-B VLAN (3040)
20. NFS VLAN (3050)



21. Verify all the necessary VLANs are added to the UCS VLAN pool
22. Click **SUBMIT** to complete creating the VLAN Pool.

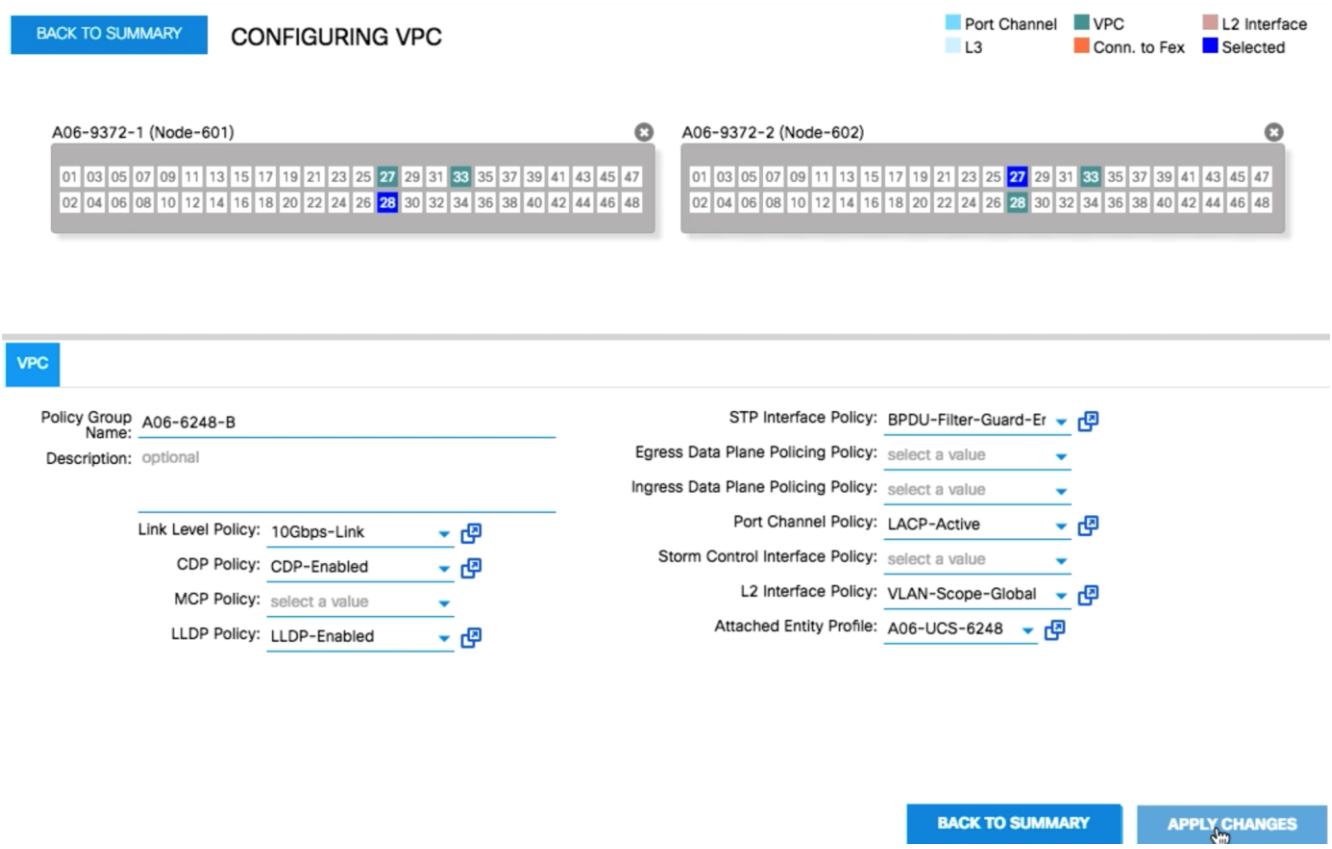


23. Click **SUBMIT** to complete creating the Physical Domain.
24. Click **UPDATE** and **SUBMIT** to complete creating the Attachable Access Entity Profile.



25. Click **APPLY CHANGES** to complete creating the vPC. Click **OK** for the confirmation message.

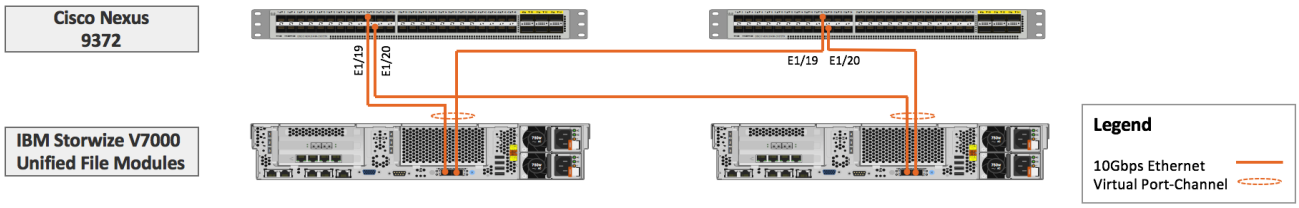
26. Repeat the steps above to add VPC for UCS Fabric Interconnect B. Do not create a new AEP and reuse the AEP created for Fabric Interconnect A.



27. Click **APPLY CHANGES** to complete creating the vPC. Click **OK** for the confirmation message.

VPC – IBM Unified File Module (IBM v7000 Unified NFS Deployment only)

Follow the steps below to setup vPCs for connectivity to the IBM File Modules.

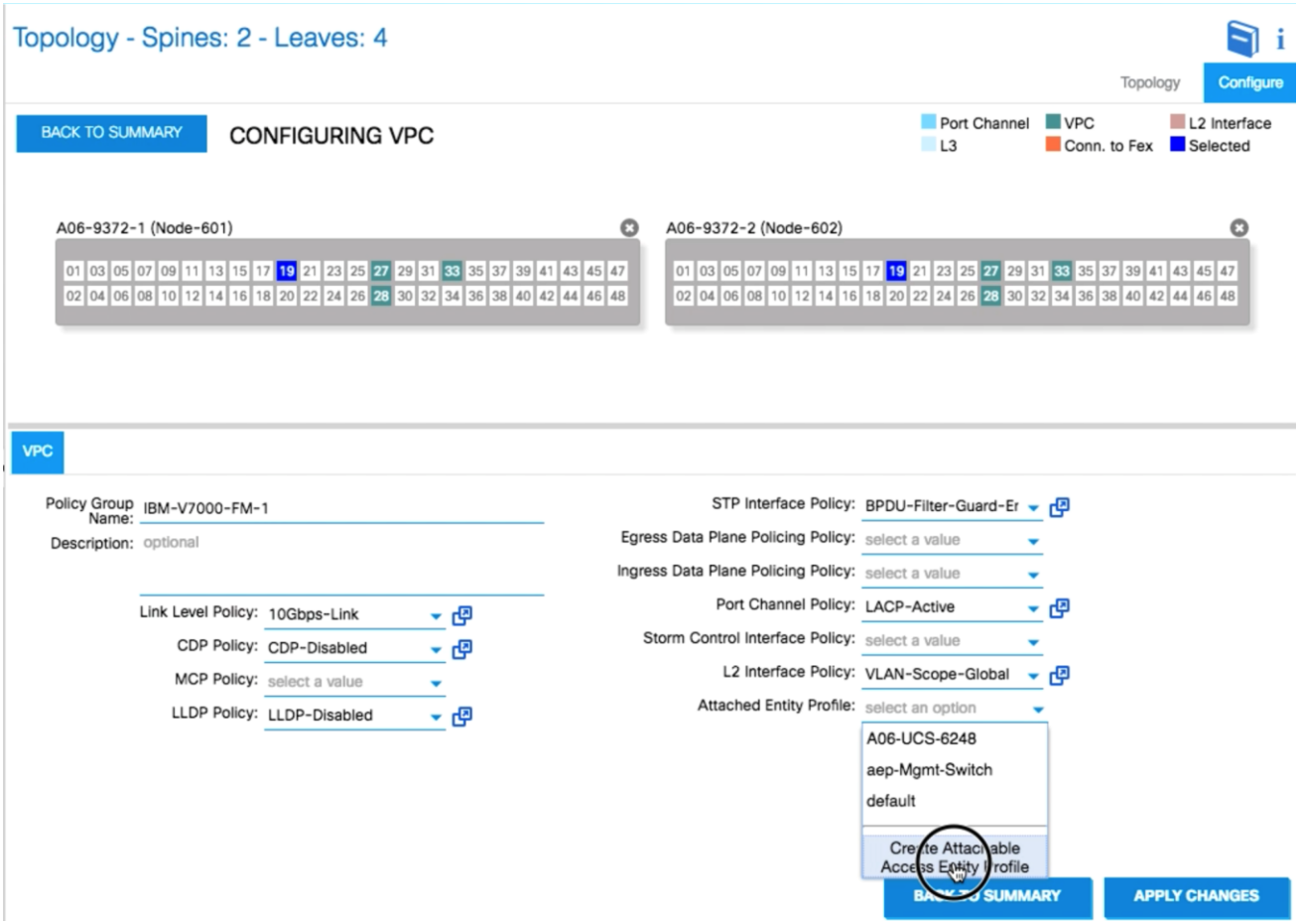


1. In the APIC Advanced GUI, at the top select Fabric > Inventory > Topology.

2. In the right pane, select **Configure**.

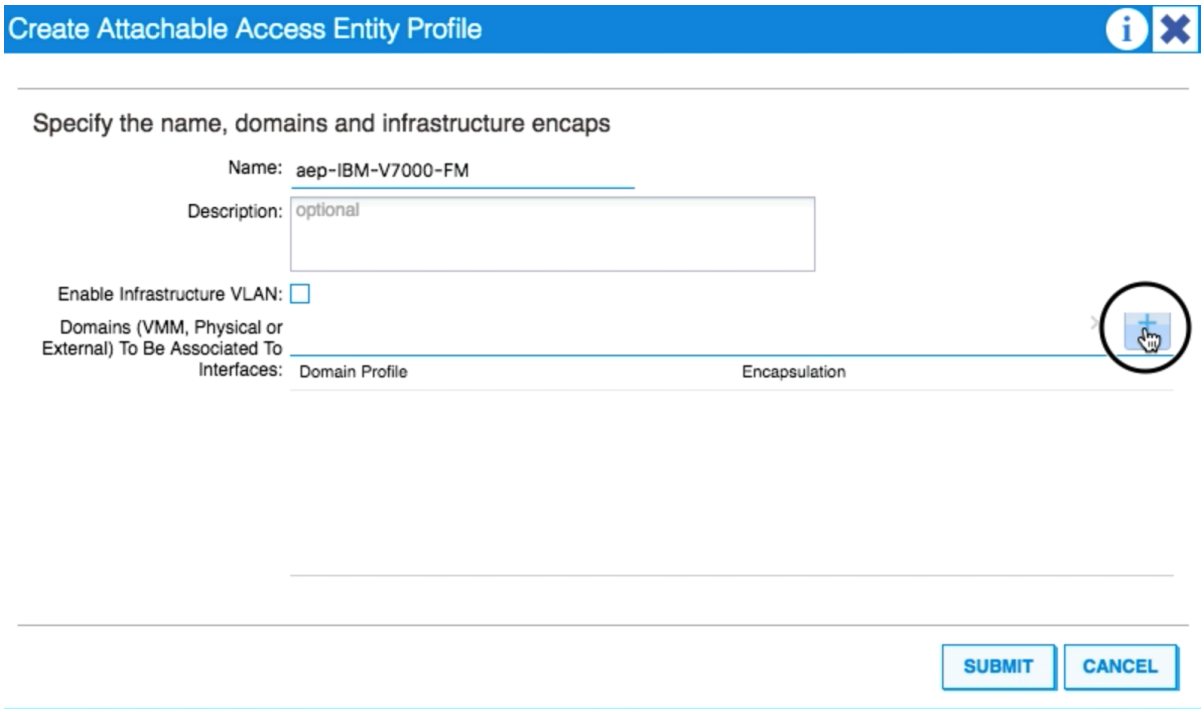
3. Click **ADD SWITCHES**. Select both the leaf switches and select **ADD SELECTED** on both the switches, select the port connected for the IBM File Module 1.

4. For the Policy Group Name, enter <File Module 1>. Select the appropriate policies as shown in the screenshot.

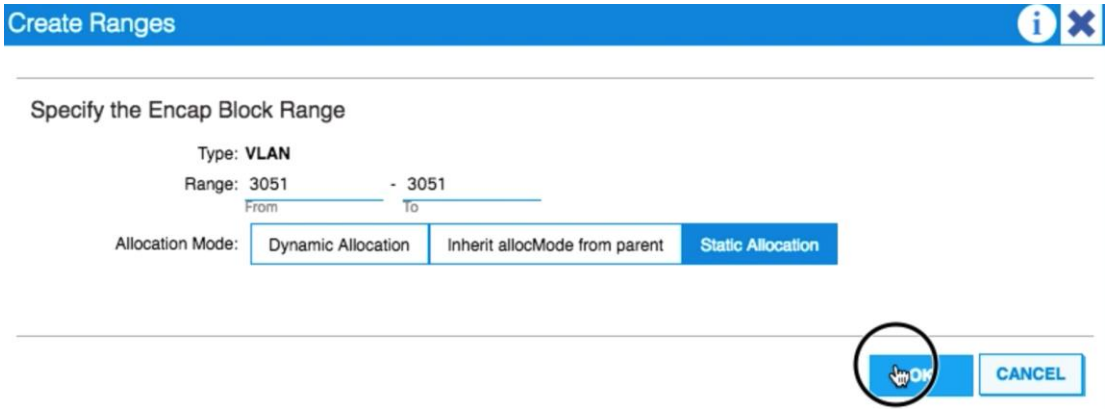


5. From the Attached Entity Policy drop-down list, select **Create Attachable Access Entity Profile**.

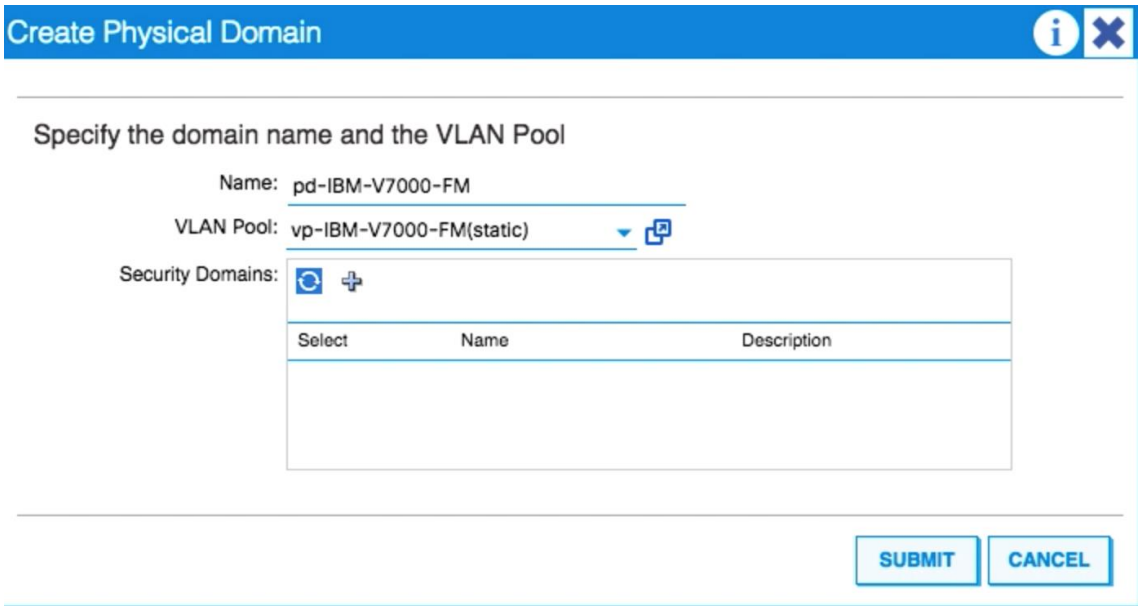
6. Name the profile as aep-<File Module Name>.
7. Click **+** to add a Physical Domain.



8. From the drop-down list, select **Create Physical Domain**.
9. In the Create Physical Domain window, name the Domain as pd-<File Module Name>.
10. From the VLAN Pool drop-down list, select **create VLAN Pool**.
11. In the create VLAN Pool window, name the VLAN Pool as vp-<File Module Name>. Select **Static Allocation**.
12. Click **+** to add an Encapsulation Block.
13. **Add NFS VLAN** (3050) to the range.

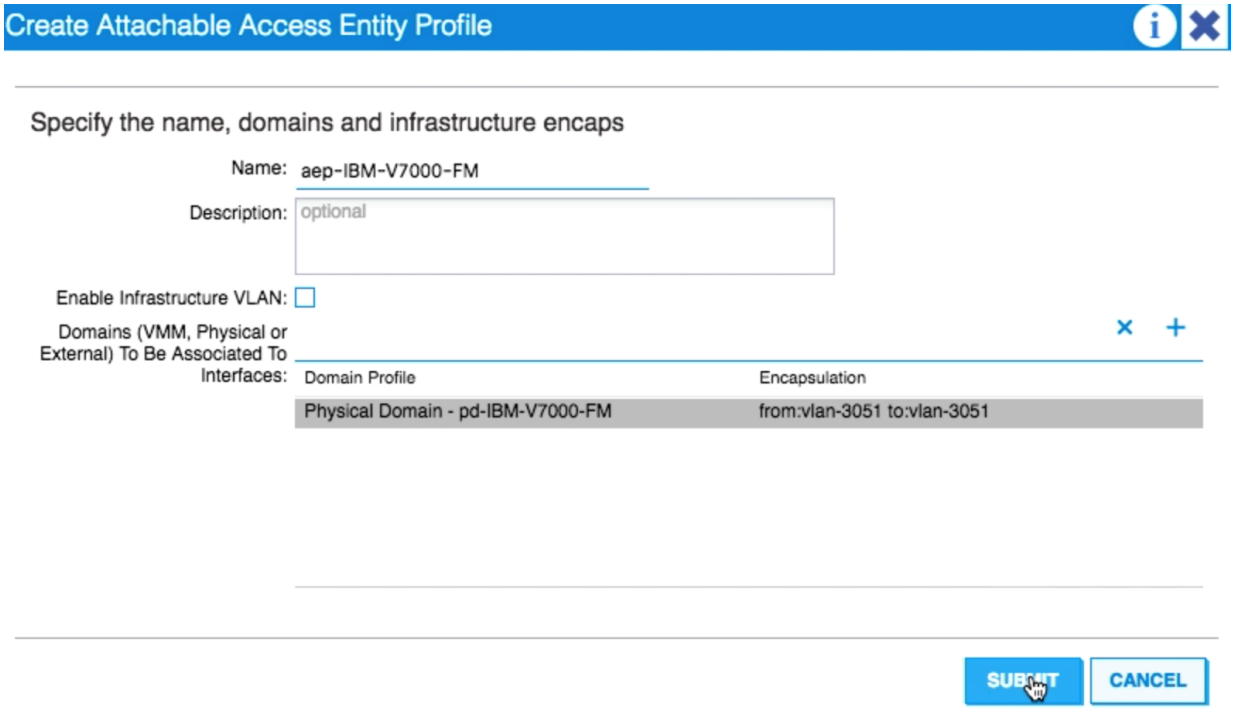


14. Click **OK** and then Click **SUBMIT** to complete creating the VLAN Pool.



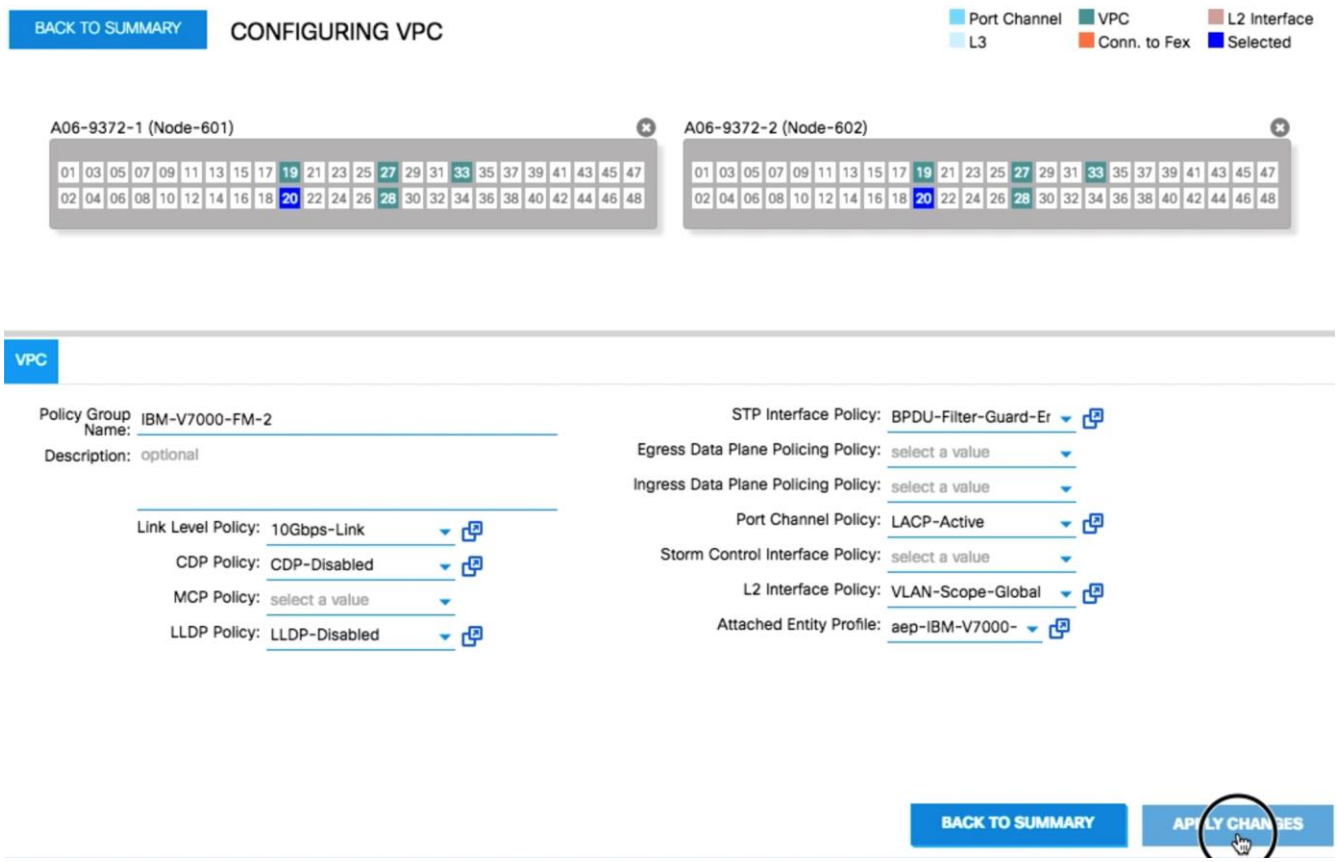
15. Click **SUBMIT** to complete creating the Physical Domain.

16. Click **UPDATE** and **SUBMIT** to complete creating the Attachable Access Entity Profile.



17. Click **APPLY CHANGES** to complete creating the vPC. Click **OK** for the confirmation message.

18. Repeat the steps above to add VPC for IBM File Module 2. Do not create a new AEP and reuse the AEP created for File Module 1.



19. Click **APPLY CHANGES** to complete creating the vPC. Click **OK** for the confirmation message.

Configure individual ports for iSCSI Access (IBM V9000 iSCSI setup only)

This section details the steps to setup four individual ports to provide four separate iSCSI paths between the IBM V9000 and Cisco Nexus 9372 leaf switches.

The physical connectivity between IBM V9000 and Cisco Nexus 9372 switches is shown in the figure below:

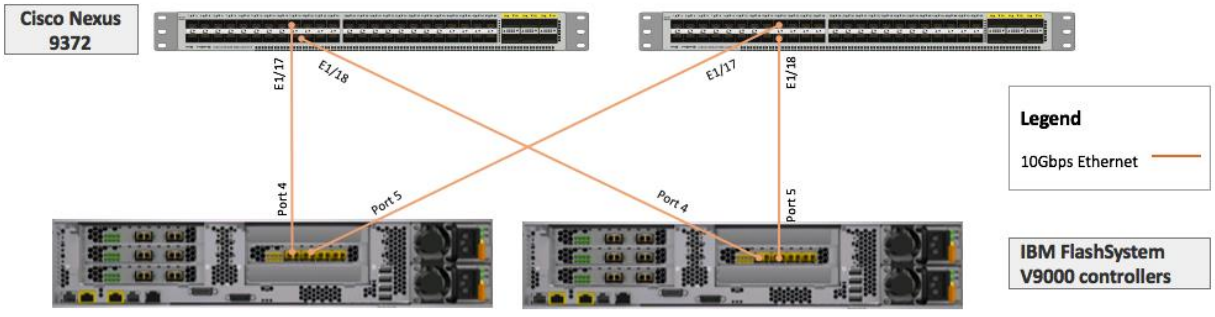


Table 21 shows all the configuration parameters for setting up these four iSCSI links.

Table 21 iSCSI Port Configuration Parameters

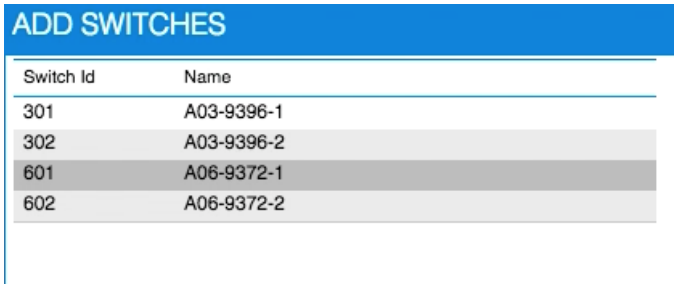
Leaf Switch	Switch Port	IBM Controller	Controller Port	Description	AEP	Physical Domain	VLAN Pool	VLAN

Nexus 9372 1	17	V9000-1	Port 4	V9000-1-iSCSI-A	aep-V9000-iSCSI-A	pd-V9000-iSCSI-A	vp-V9000-iSCSI-A	3031
Nexus 9372 1	18	V9000-2	Port 4	V9000-2-iSCSI-A	aep-V9000-iSCSI-A	pd-V9000-iSCSI-A	vp-V9000-iSCSI-A	3031
Nexus 9372 2	17	V9000-1	Port 5	V9000-1-iSCSI-B	aep-V9000-iSCSI-B	pd-V9000-iSCSI-B	vp-V9000-iSCSI-B	3041
Nexus 9372 2	18	V9000-2	Port 5	V9000-2-iSCSI-B	aep-V9000-iSCSI-B	pd-V9000-iSCSI-B	vp-V9000-iSCSI-B	3041

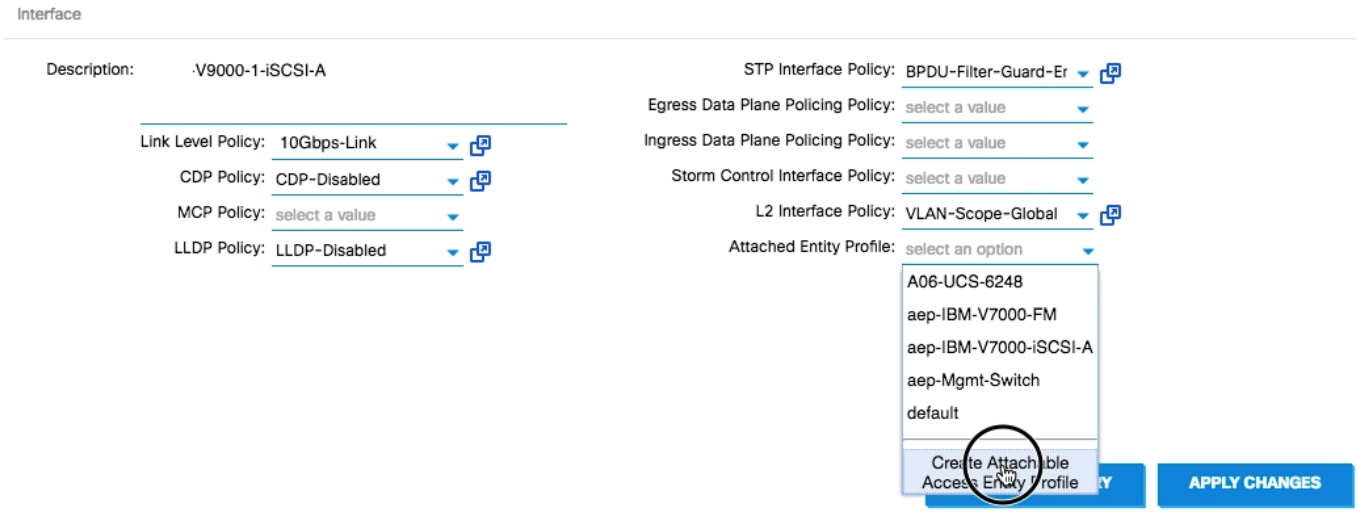
1. In the APIC Advanced GUI, select Fabric > Inventory > Topology.
2. In the right pane, select **Configure**.

Refer to Table 21 for the information required during the following configuration. Items marked by { } will need to be updated according to Table 21.

3. Click **ADD SWITCHES**. Select the first Nexus 9372 switch and click **ADD SELECTED**.



4. On the switch, select the port {17} connected to the IBM V9000 controller.
5. Select CONFIGURE PORT.
6. For Description, enter {V9000-1-iSCSI-A}. Select the policies as shown in the screenshot below.

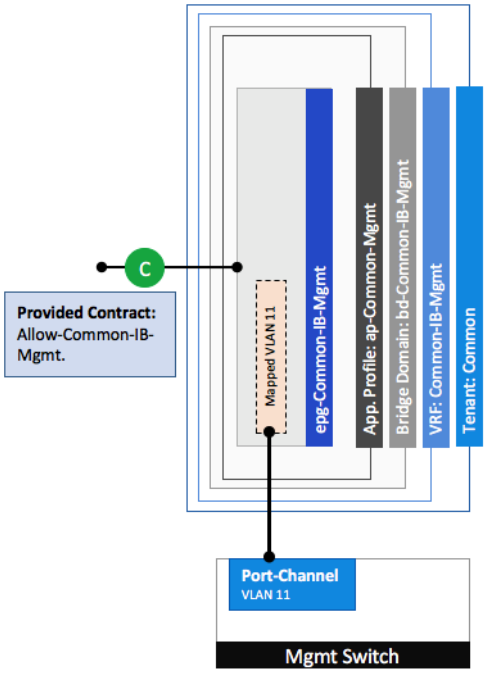


7. From the Attached Entity Profile drop-down list, select **Create Attachable Access Entity Profile**.
8. Name the profile {aep-V9000-iSCSI-A}. Click + to add a Physical Domain.
9. From the drop-down list, select **Create Physical Domain**.
10. In the Create Physical Domain window, name the Domain {pd-V9000-iSCSI-A}.
11. From the VLAN Pool drop-down list, select **create VLAN Pool**.
12. In the create VLAN Pool window, name the VLAN Pool {vp-V9000-iSCSI-A}. Select **Static Allocation**.
13. Click **+** to add an Encapsulation Block.
14. Enter the VLAN {3031} for both the From and To parts of the Range. Select **Static Allocation**.
15. Click **OK** to complete creating the range.
16. Click **SUBMIT** to complete creating the VLAN Pool.
17. Click **SUBMIT** to complete creating the Physical Domain.
18. Click **UPDATE** and **SUBMIT** to complete creating the Attachable Access Entity Profile.
19. Click **APPLY CHANGES** to complete creating the Port. Click **OK** for the confirmation message.
20. Repeat the steps above to configure all four iSCSI ports.

Each AEP policy will be defined only once on the first time use.

Configuring Common Tenant for Management Access

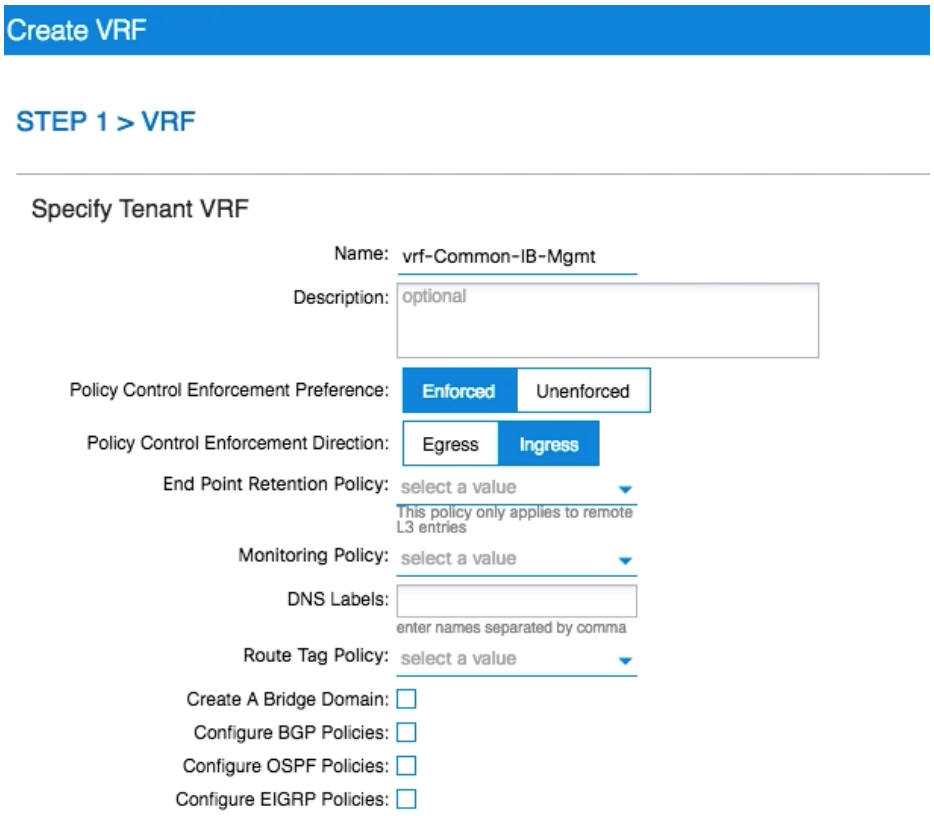
This section details the steps to setup in-band management access in the Tenant common. This design will allow all the other tenant EPGs to access the common management segment. Various constructs of this design are shown in the figure below:



1. In the APIC Advanced GUI, at the top select Tenants > common.
2. In the left pane, expand Tenant common and Networking.

Create VRFs

1. Right-click on VRF and select **Create VRF**.
2. Enter vrf-Common-IB-Mgmt as the name of the VRF.
3. Click **FINISH**.

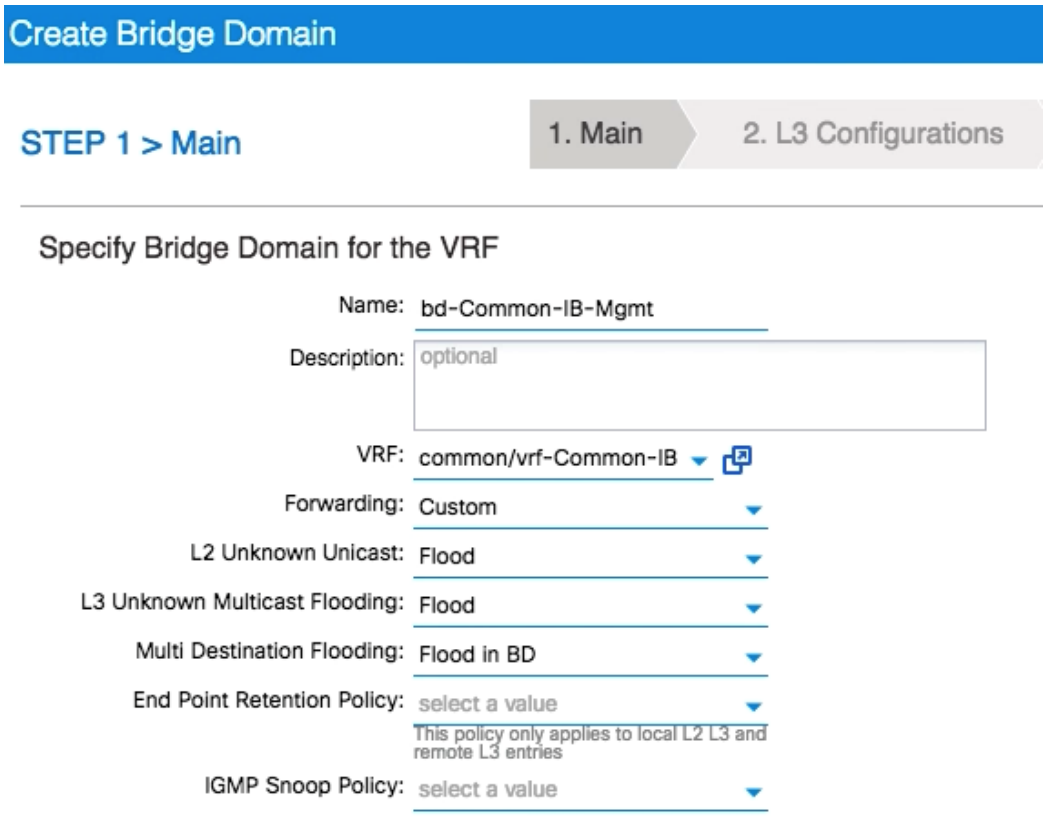


4. Right-click the VRF and select **Create VRF**.
5. Enter vrf-Common-Outside as the name of the VRF.
6. Click **FINISH**.

VRF vrf-Common-Outside is not required for management access but will be utilized later to provide Shared L3 access.

Create Bridge Domains

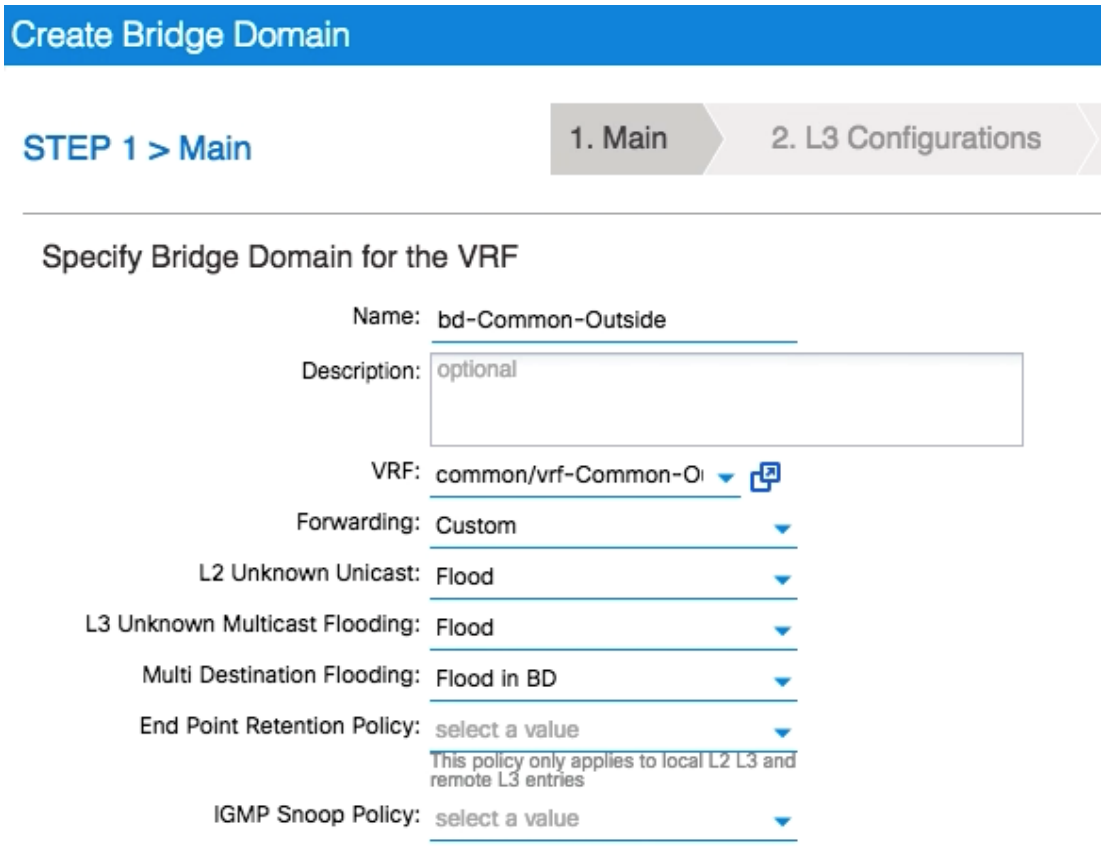
1. In the APIC Advanced GUI, select Tenants > common.
2. In the left pane, expand Tenant common and Networking.
3. Right-click on the Bridge Domain and select **Create Bridge Domain**.
4. Name the Bridge Domain as bd-Common-IB-Mgmt
5. Select common/vrf-Common-IB-Mgmt from the VRF drop-down list.
6. Select Custom under Forwarding and enable the flooding as shown in the figure.



7. Click **NEXT**.
8. Do not change any configuration on next screen (L3 Configurations). Select **NEXT**.
9. No changes are needed Advanced/Troubleshooting. Click **FINISH**.
10. Right-click on the Bridge Domain and select **Create Bridge Domain**.
11. Name the Bridge Domain as bd-Common-Outside.

The bridge domain bd-Common-Outside is not needed for setting up common management segment and will be utilized later in the document when setting up Shared L3 Out

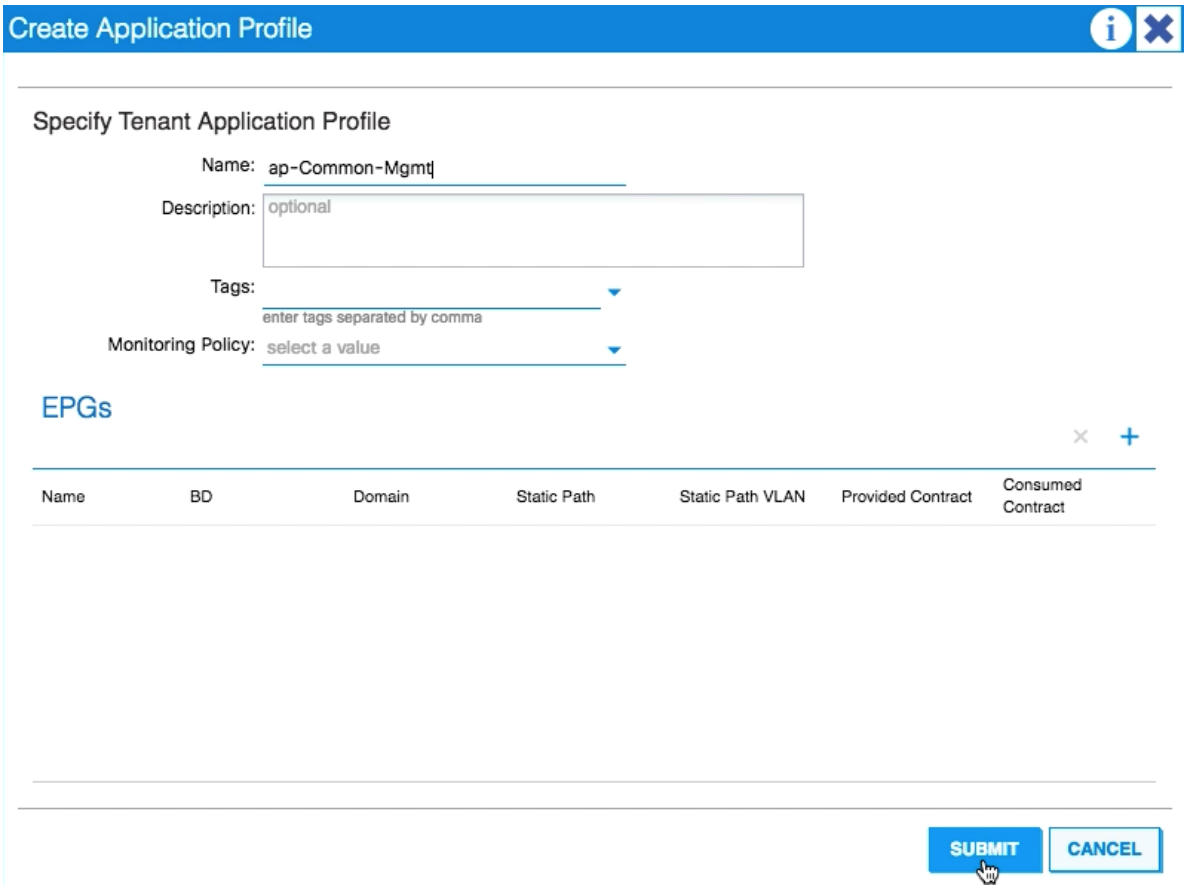
12. Select the common/vrf-Common-Outside.
13. Select Custom under Forwarding and enable the flooding as shown in the figure.



14. Click **NEXT**.
15. Do not change any configuration on next screen (L3 Configurations). Select **NEXT**.
16. No changes are needed Advanced/Troubleshooting. Click **FINISH**.

Create Application Profile

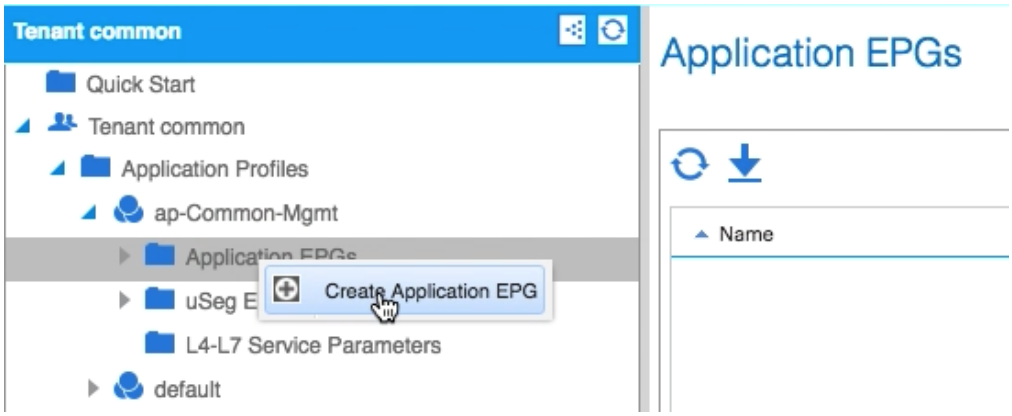
1. In the APIC Advanced GUI, select **Tenants** > **common**.
2. In the left pane, expand Tenant common and Application Profiles.
3. Right-click on the Application Profiles and select **Create Application Profiles**.
4. Enter ap-Common-Mgmt as the name of the application profile.



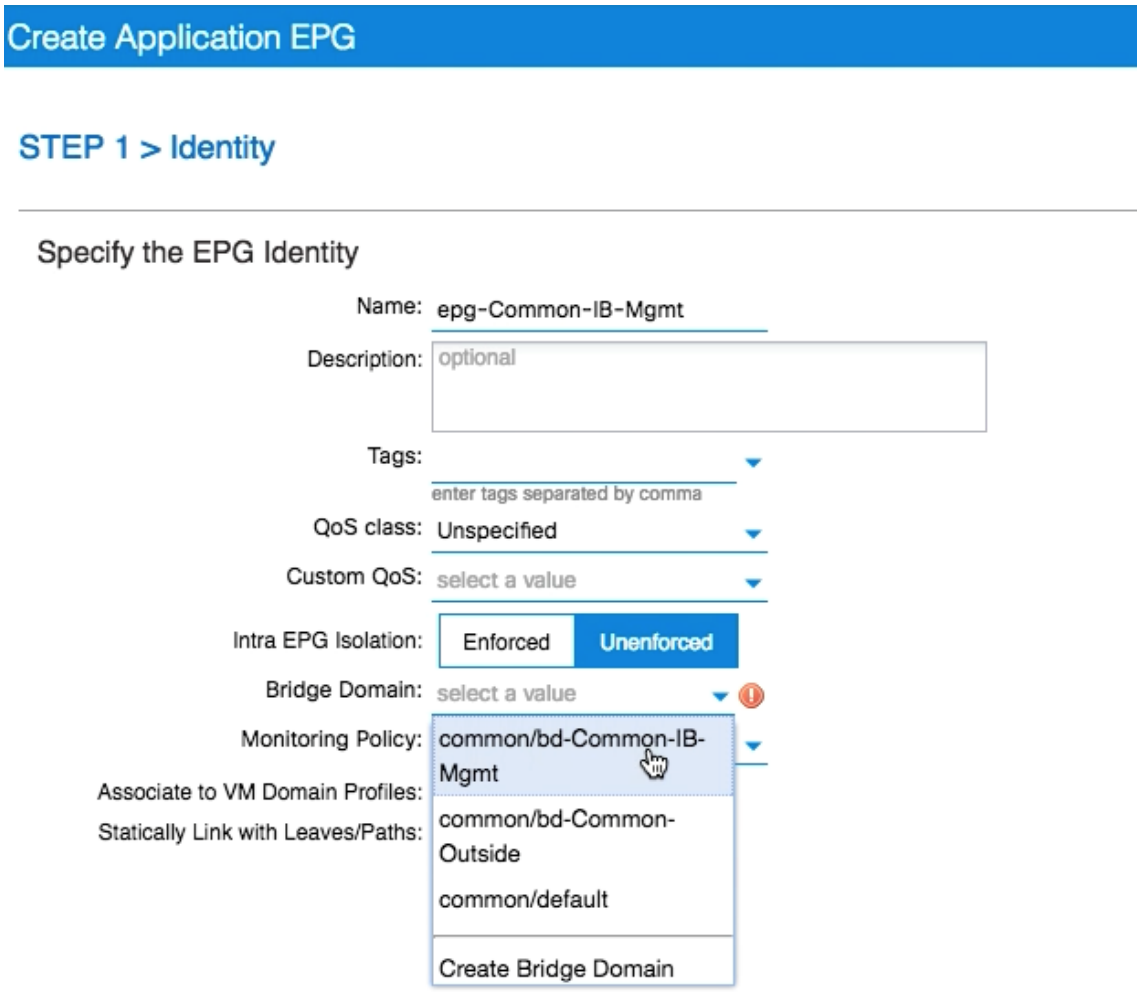
5. Click **SUBMIT**.

Create EPG

1. Expand the ap-Common-Mgmt application profile and right-click on the Application EPGs.
2. Select Create Application EPG.



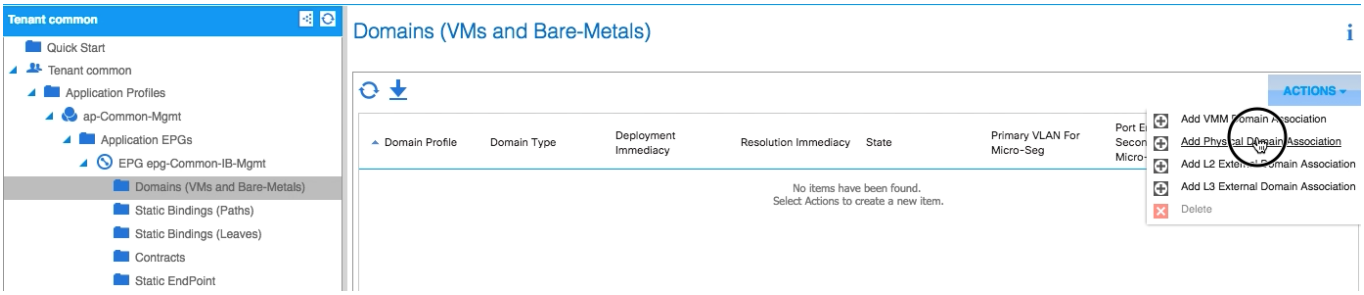
3. Enter epg-Common-IB-Mgmt as the name of the EPG.
4. Select common/bd-Common-IB-Mgmt from the drop-down list for Bridge Domain.



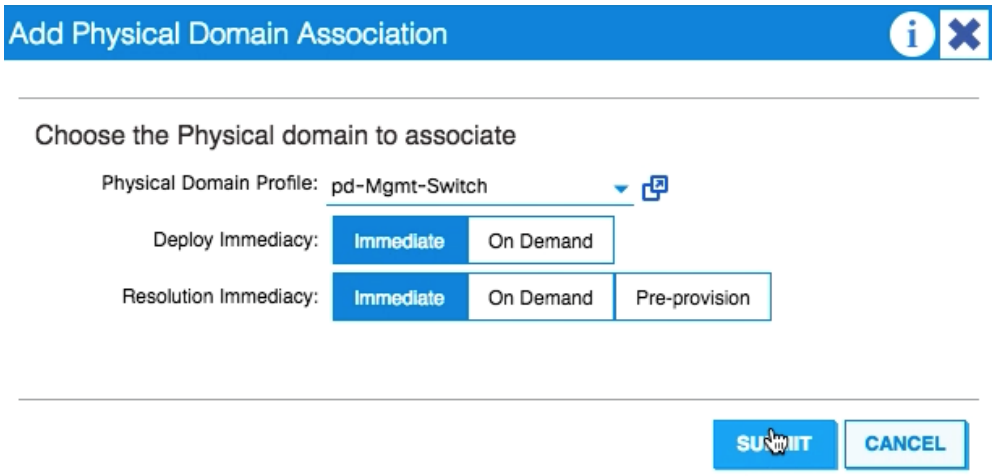
5. Click FINISH.

Set Domains

1. Expand the newly create EPG and click **Domains**.
2. From the ACTIONS drop-down list, select Add Physical Domain Association.



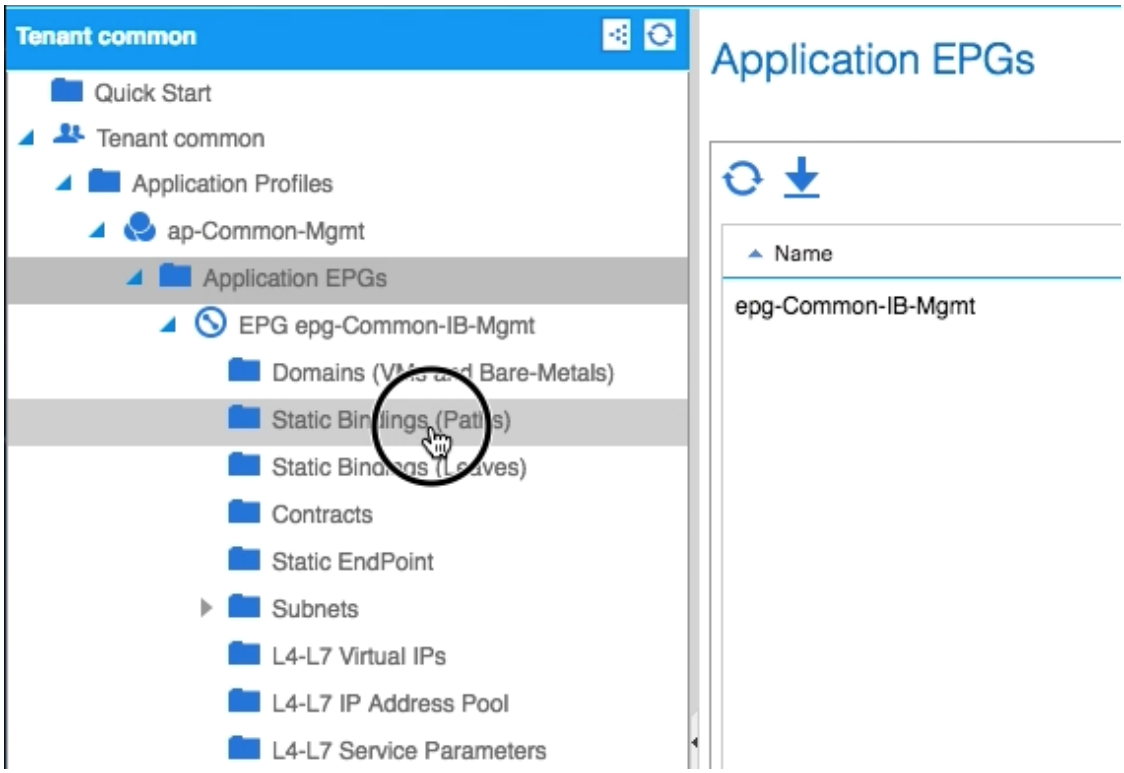
3. Select the pd-Mgmt-Switch as the Physical Domain Profile.
4. Change the Deploy Immediacy and Resolution Immediacy to Immediate.



5. Click **SUBMIT**.

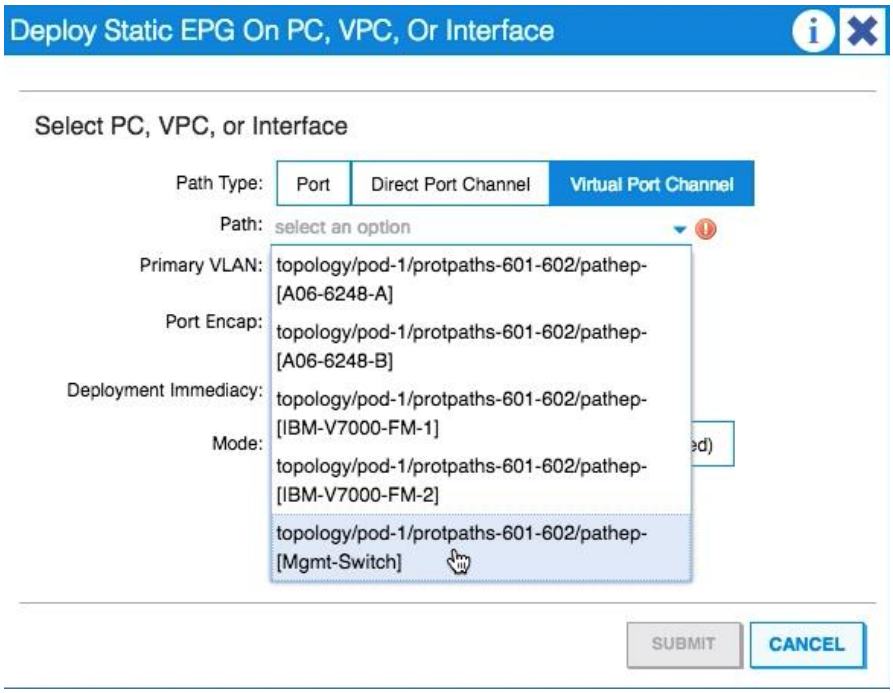
Set Static Bindings (Paths)

1. In the left pane, Right-click on the Static Bindings (Paths).

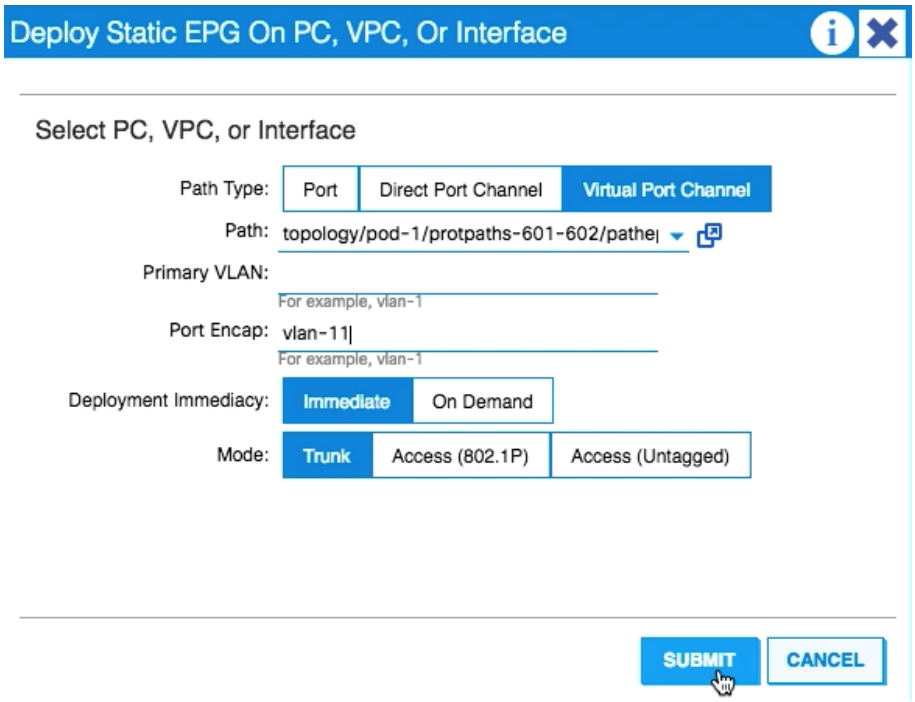


2. Select Deploy Static EPG on PC, VPC, or Interface.

3. In the next screen, for the Path Type, select Virtual Port Channel and from the drop-down list, select the VPC for Mgmt Switch.



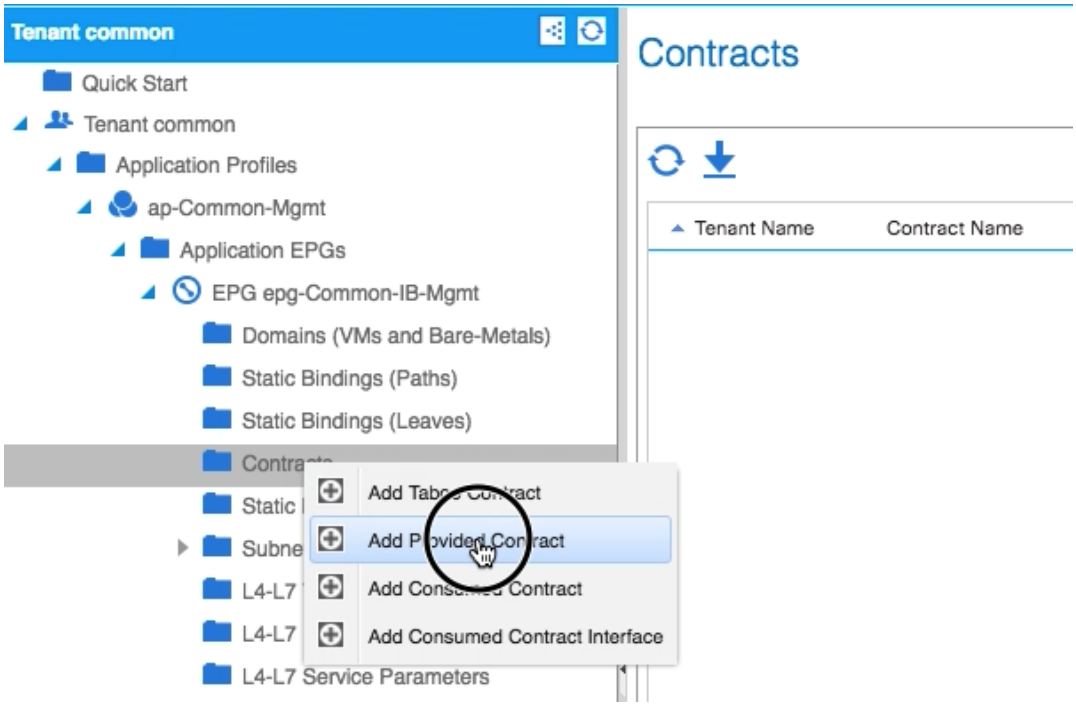
4. Enter the management VLAN under Port Encap.
5. Change Deployment Immediacy to Immediate.
6. Set the Mode to Trunk.



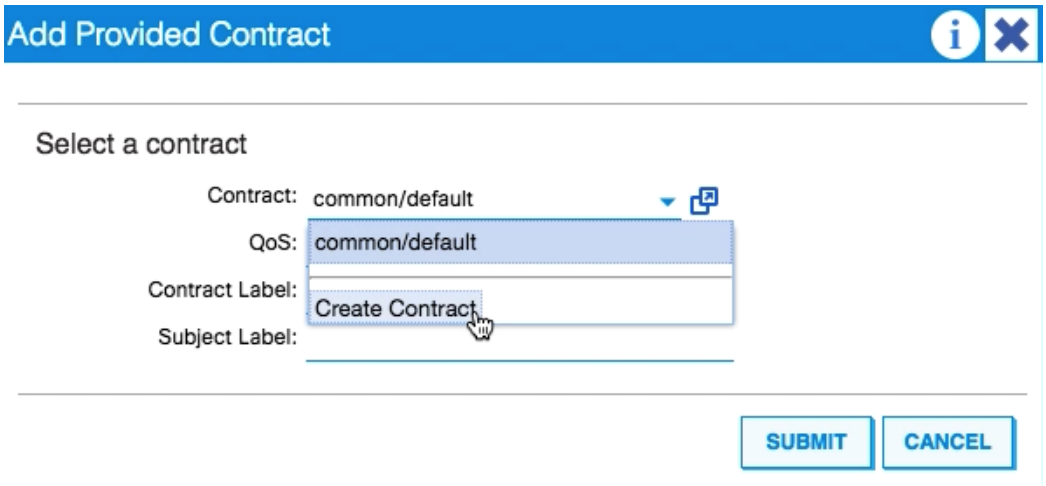
7. Click **SUBMIT**.

Create Provided Contract

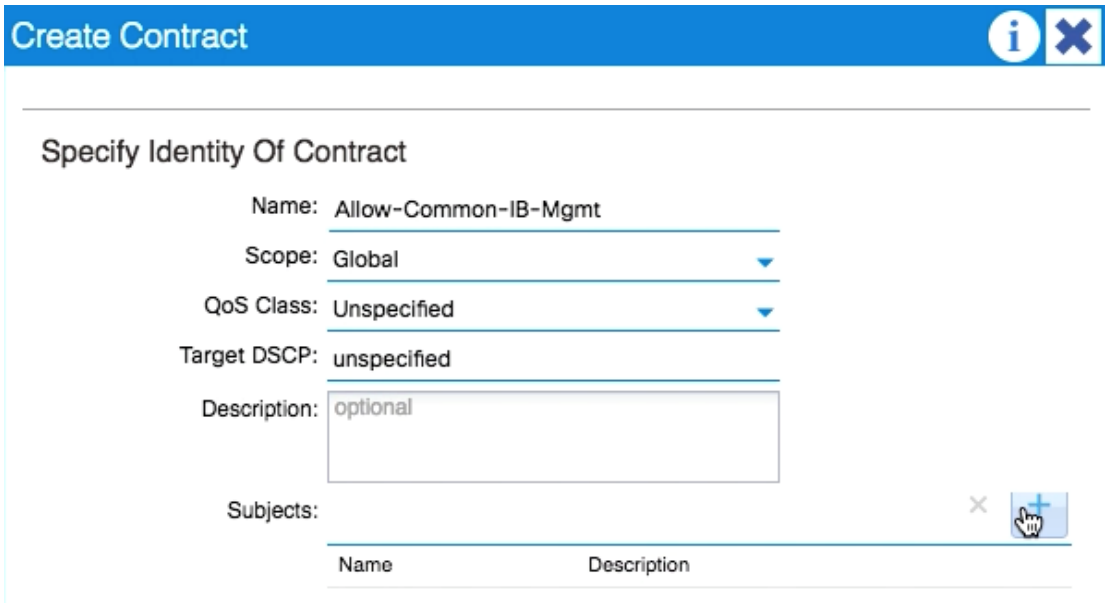
1. In the left pane, right-click on **Contracts** and select **Add Provided Contract**.



2. In the Add Provided Contract window, select **Create Contract** from the drop-down list.

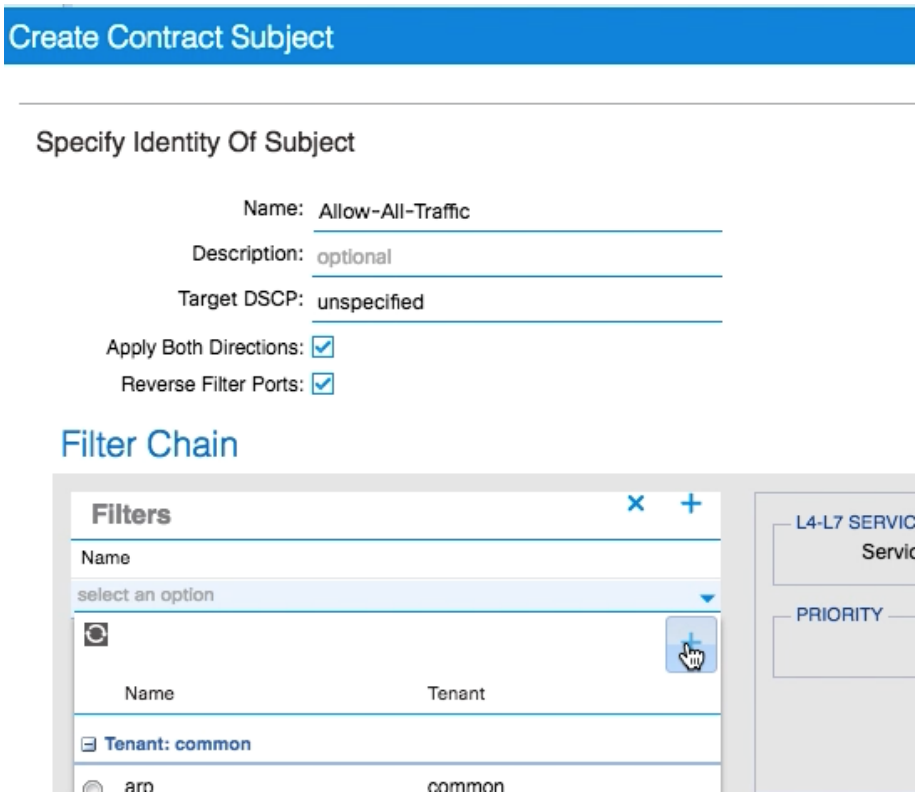


3. Name the Contract as Allow-Common-IB-Mgmt.
4. Set the scope to Global.
5. Click **+** to add a Subject to the Contract.

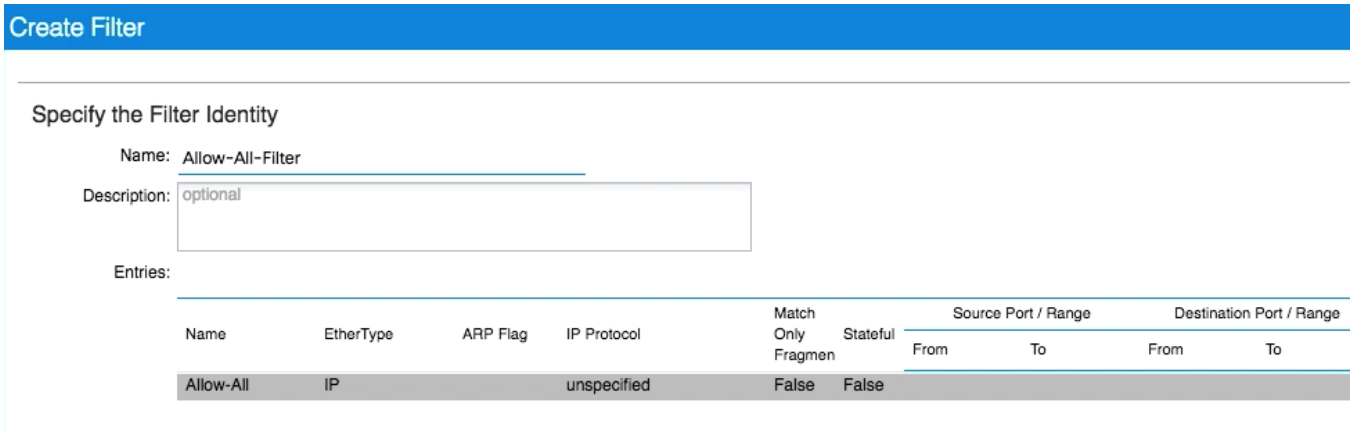


Following steps create a contract to allow all the traffic between various tenants and the common management segment. Customers are encouraged to limit the traffic by setting restrictive filters.

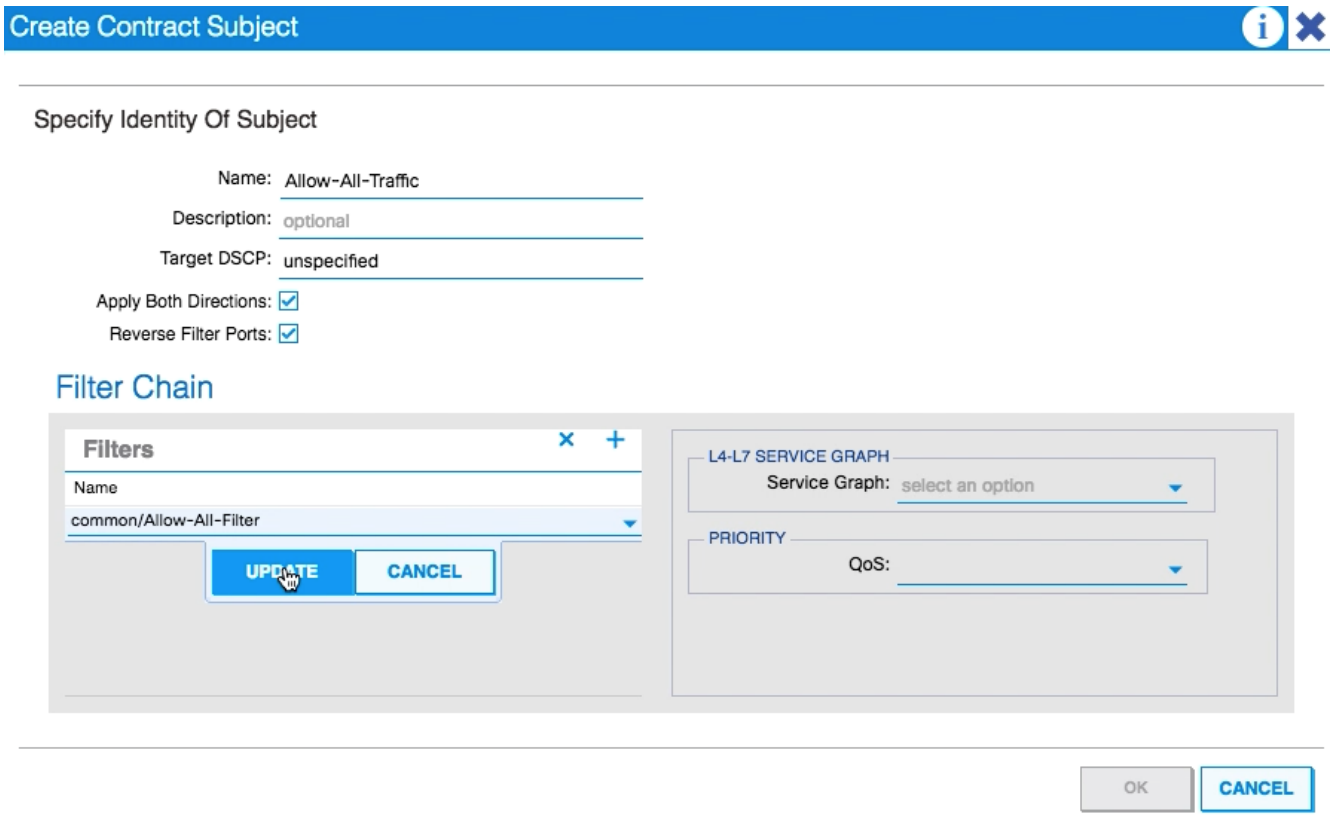
6. Name the subject as Allow-All-Traffic.
7. Click **+** under Filter Chain to add a Filter.
8. Click **+** to add a Filter Identity.



9. Name the Filter as Identity Allow-All.
10. Click **+** to add an Entry to the Filter.
11. Name the Entry Allow-All and select the IP EtherType. Leave the IP Protocol set at Unspecified.
12. Click **UPDATE**.



13. Click **SUBMIT** to add the Filter.
14. In the Create Contract Subject window, click **UPDATE** to add the Filter Chain to the Contract Subject.



15. Click **OK** to add the Contract Subject.

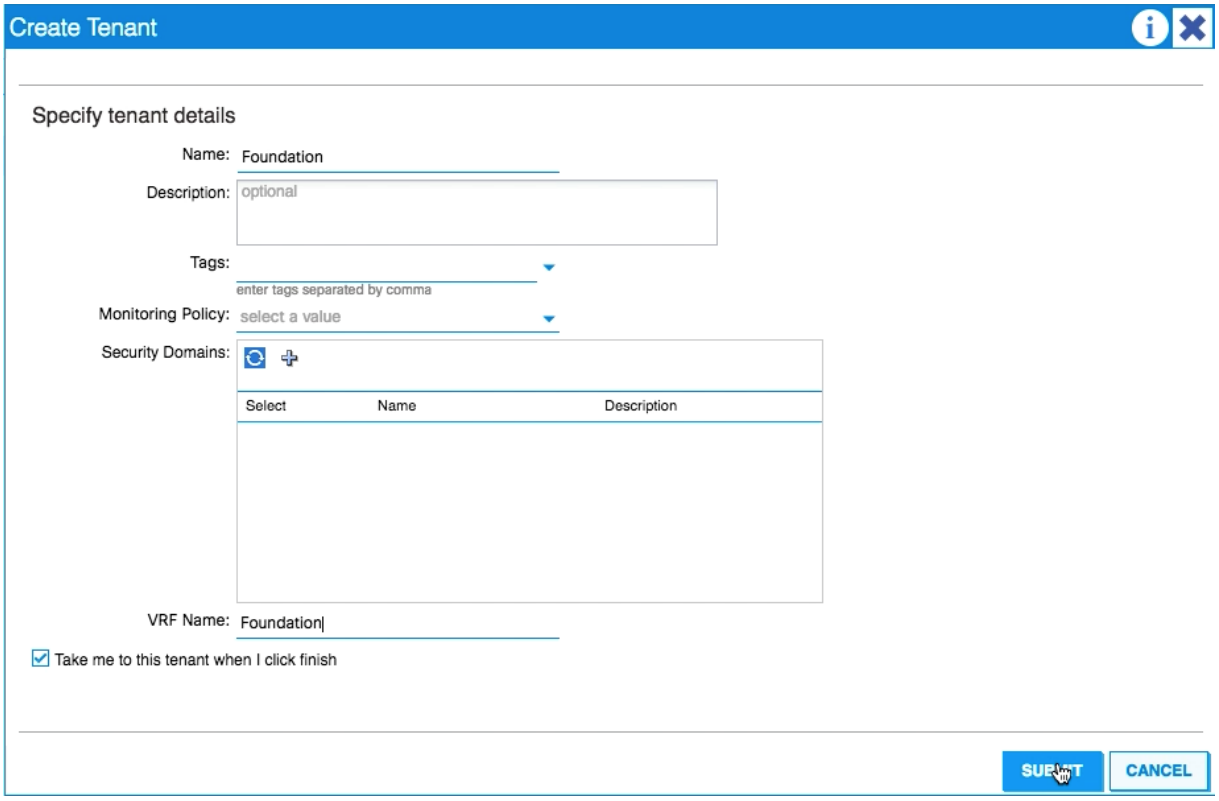
The Contract Subject Filter Chain can be modified later.

16. Click **SUBMIT** to finish creating the Contract.
17. Click **SUBMIT** to finish adding a Provided Contract.

Deploy Foundation Tenant

This section details the steps for creating the Foundation Tenant in the ACI Fabric. This tenant will host infrastructure connectivity between the compute (VMware on UCS) and the storage (IBM) environments. To deploy the Foundation Tenant, complete the following steps.

1. In the APIC Advanced GUI, select Tenants > Add Tenant.
2. Name the Tenant as Foundation.
3. For the VRF Name as well enter Foundation. Keep the check box Take me to this tenant when I click finish, checked.

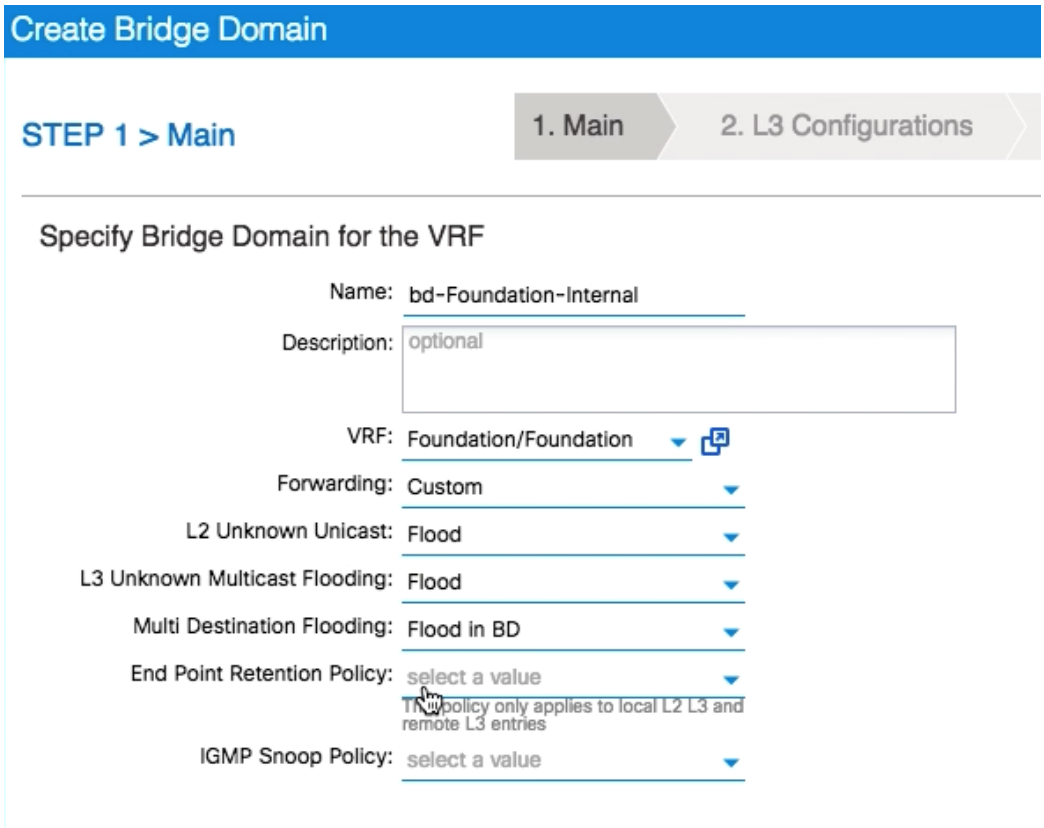


4. Click **SUBMIT** to finish creating the Tenant.

Create Bridge Domain

1. In the left pane, expand Tenant common and Networking.
2. Right-click on the Bridge Domain and select **Create Bridge Domain**.
3. Name the Bridge Domain bd-Foundation-Internal.

4. Select Foundation/Foundation from the VRF drop-down list.
5. Select Custom under Forwarding and enable the flooding as shown in the figure.



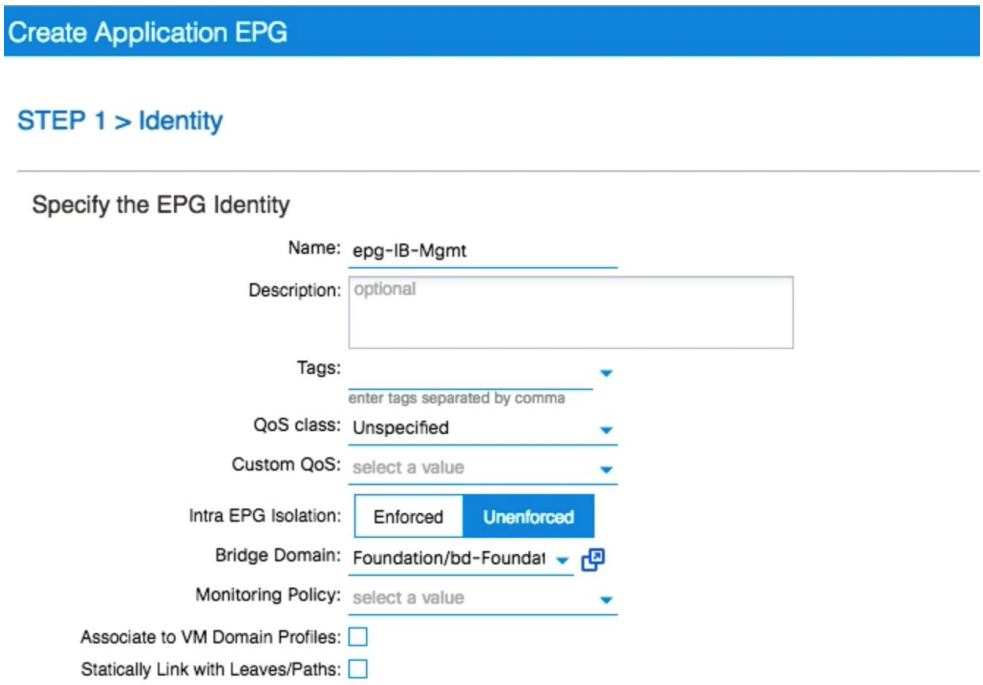
6. Click **NEXT**.
7. Do not change any configuration on next screen (L3 Configurations). Select **NEXT**.
8. No changes are needed for Advanced/Troubleshooting. Click **FINISH** to finish creating Bridge Domain.

Create Application Profile for Management Access

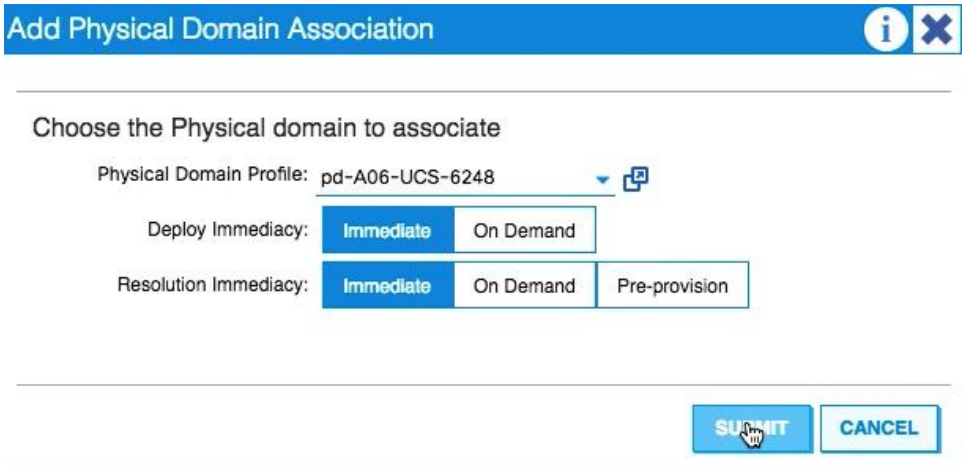
1. In the left pane, expand tenant Foundation, right-click on the Application Profiles and select **Create Application Profile**.
2. Name the Application Profile as ap-Mgmt and click **SUBMIT** to complete adding the Application Profile.

Create EPG for Management Access

1. In the left pane, expand the Application Profiles and right-click the Application EPGs and select **Create Application EPG**.
2. Name the EPG as epg-IB-Mgmt.
3. From the Bridge Domain drop-down list, select Bridge Domain Foundation/bd-Foundation-Internal.

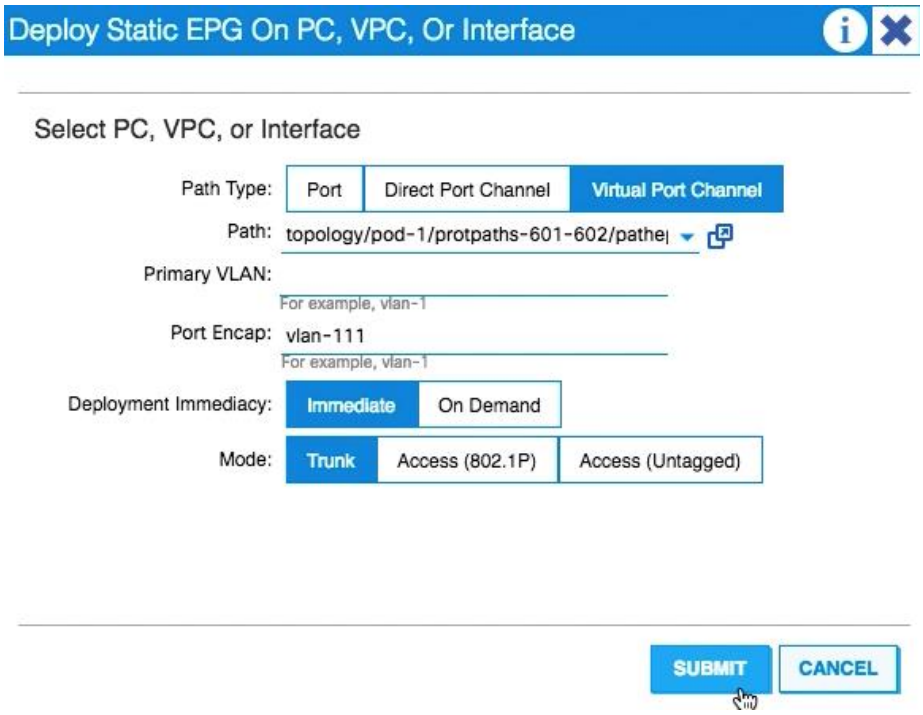


4. Click **FINISH** to complete creating the EPG.
5. In the left pane, expand the Application EPGs and name the EPG as epg-IB-Mgmt.
6. Right-click on the Domains and select **Add Physical Domain Association**.
7. From the drop-down list, select the previously defined pd-<UCS Name> (pd-A06-UCS-6248) Physical Domain Profile.
8. Select Immediate for both the Deploy Immediacy and the Resolution Immediacy.

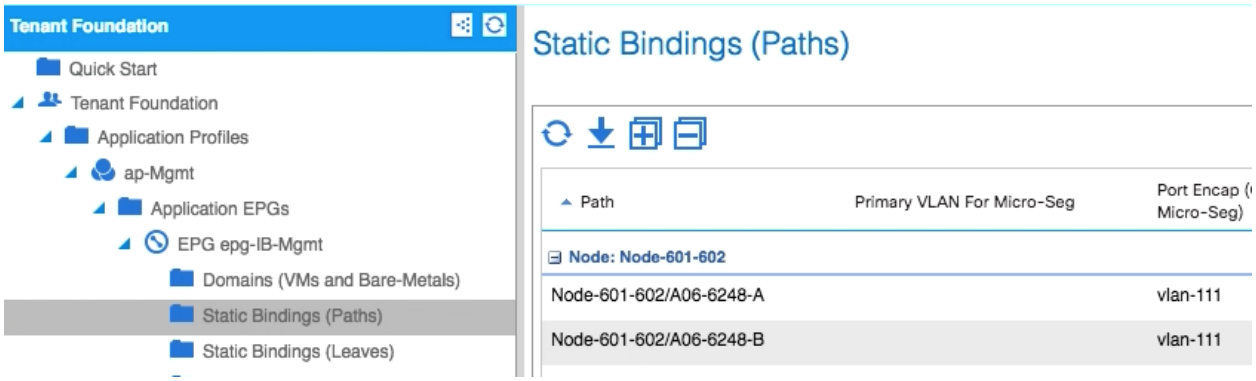


9. Click **SUBMIT** to complete the Physical Domain Association.
10. Right-click Static-Bindings (Paths) and select **Deploy EPG on PC, VPC, or Interface**.
11. In the Deploy Static EPG on PC, VPC, Or Interface Window, select the Virtual Port Channel Path Type.

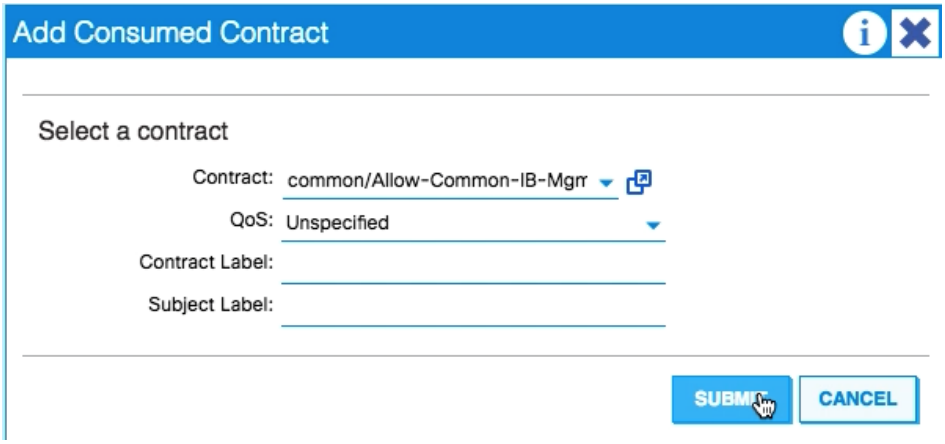
12. From the drop-down list, select the VPC for UCS Fabric Interconnect A.
13. Enter <UCS Management VLAN> (111) for Port Encap.
14. Select the Immediate for Deployment Immediacy and for Mode select Trunk.



15. Click **SUBMIT** to complete adding the Static Path Mapping.
16. Repeat the above steps to add the Static Path Mapping for UCS Fabric Interconnect B.



17. In the left menu, right-click Contracts and select **Add Consumed Contract.**
18. From the drop-down list for the Contract, select common/Allow-Common-IB-Mgmt



19. Click **SUBMIT**.

Connection to the IB-Management segment through tenant common should be enabled now. This EPG will be utilized to provide ESXi hosts as well as the VMs access to the existing management subnet.

Create Application Profile for ESXi Connectivity

1. In the left pane, under the Tenant Foundation, right-click Application Profiles and select **Create Application Profile**.
2. Name the Profile ap-ESXi-Connectivity and click **SUBMIT** to complete adding the Application Profile.

Following EPGs and the corresponding mappings will be created under this application profile. Depending on the customer storage design, not all the EPGs need to be configured.

Refer to Table 22 for the information required during the following configuration. Items marked by { } will need to be updated according to Table 22. The bridge domain used for all the EPGs is Foundation/bd-Foundation-Internal.

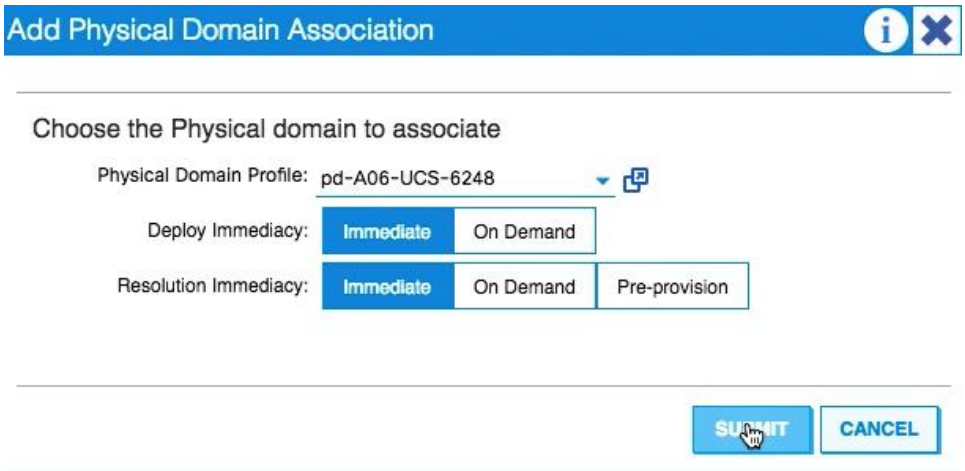
Table 22 EPGs and mappings for ap-ESXi-Connectivity

EPG Name	Default Gateway IP	Domain	Static Path – UCS FI	Static Path - IBM
epg-NFS (IBM V7000 NFS Deployment only)	192.168.180.254/24	pd-IBM-V7000-FM; pd-A06-UCS-6248	VPC for UCS FI-A VLAN 3050 VPC for UCS FI-B VLAN 3050	VPC for V7000 FM 1 VLAN 3051 VPC for V7000 FM 2 VLAN 3051
epg-vMotion	192.168.179.254/24	pd-A06-UCS-6248	VPC for UCS FI-A VLAN 3000 VPC for UCS FI-B VLAN 3000	
epg-iSCSI-A (IBM V9000 iSCSI Deployment only)	192.168.181.254/24	pd-V9000-iSCSI-A; pd-A06-UCS-6248	VPC for UCS FI-A VLAN 3030 VPC for UCS FI-B VLAN 3030	Leaf 9372-1 Port E1/21 for IBM V9000 1 VLAN 3031 Leaf 9372-1 E1/22 for IBM V9000 2 VLAN 3031

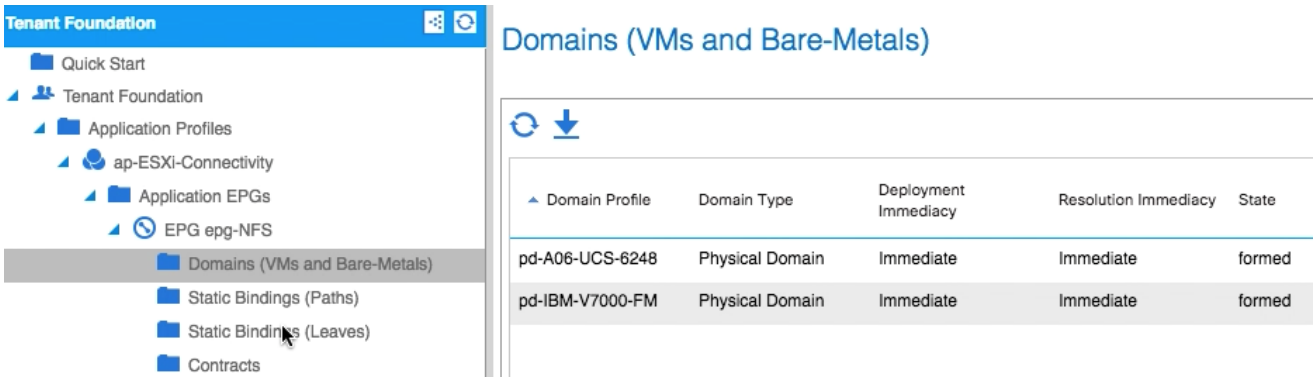
epg-iSCSI-B (IBM V9000 iSCSI Deployment only)	192.168.182.254/24	pd-V9000-iSCSI-B; pd-A06-UCS-6248	VPC for UCS FI-A VLAN 3040 VPC for UCS FI-B VLAN 3040	Leaf 9372-2 Port E1/21 for IBM V9000 1 VLAN 3041 Leaf 9372-2 E1/22 for IBM V9000 2 VLAN 3041

Create EPGs

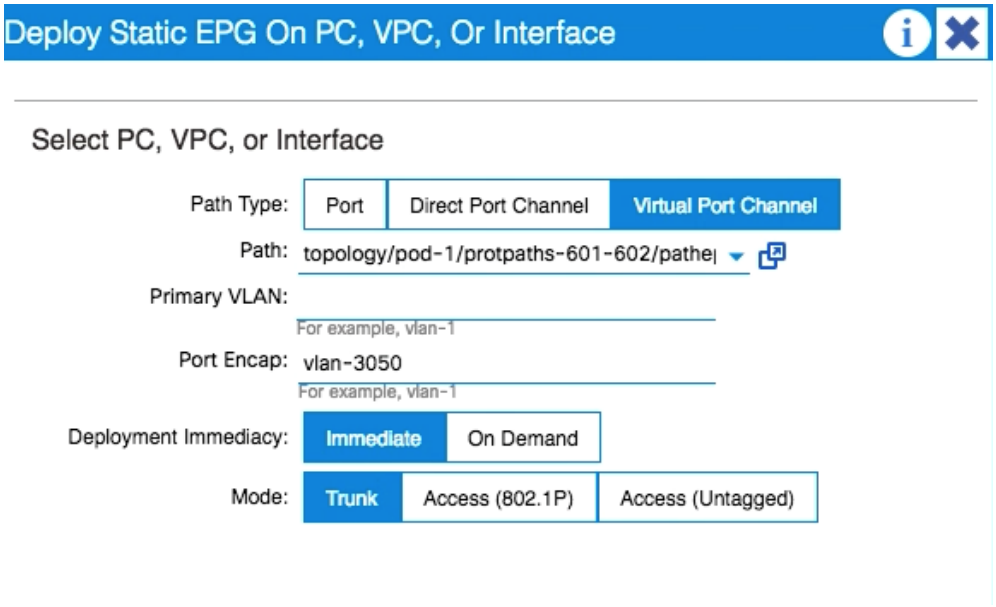
1. In the left pane, expand Application Profiles. Right-click on the Application EPGs and select **Create Application EPG**.
2. Name the EPG {epg-NFS}.
3. From the Bridge Domain drop-down list, select Bridge Domain Foundation/bd-Foundation-Internal
4. Click **FINISH** to complete creating the EPG.
5. In the left pane, expand the Application EPGs and EPG {epg-NFS}.
6. Right-click Domains and select **Add Physical Domain Association**.
7. From the drop-down list, select the previously defined pd-<UCS Name> {pd-A06-UCS-6248} Physical Domain Profile.
8. Select Immediate for both Deploy Immediacy and Resolution Immediacy.



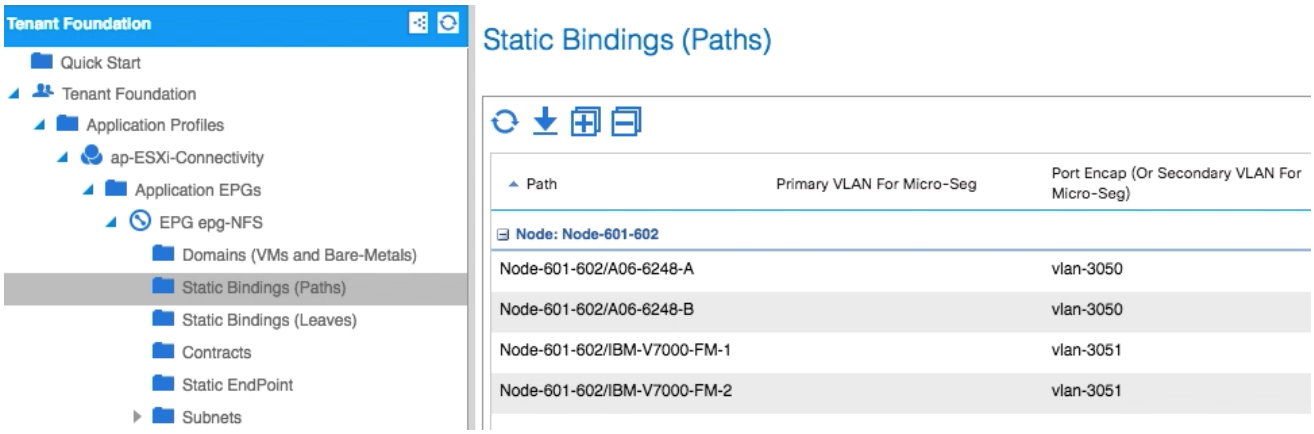
9. Click **SUBMIT** to complete the Physical Domain Association.
10. Repeat the Add Physical Domain Association steps (6-10) to add all the EPG specific domain from Table 22.



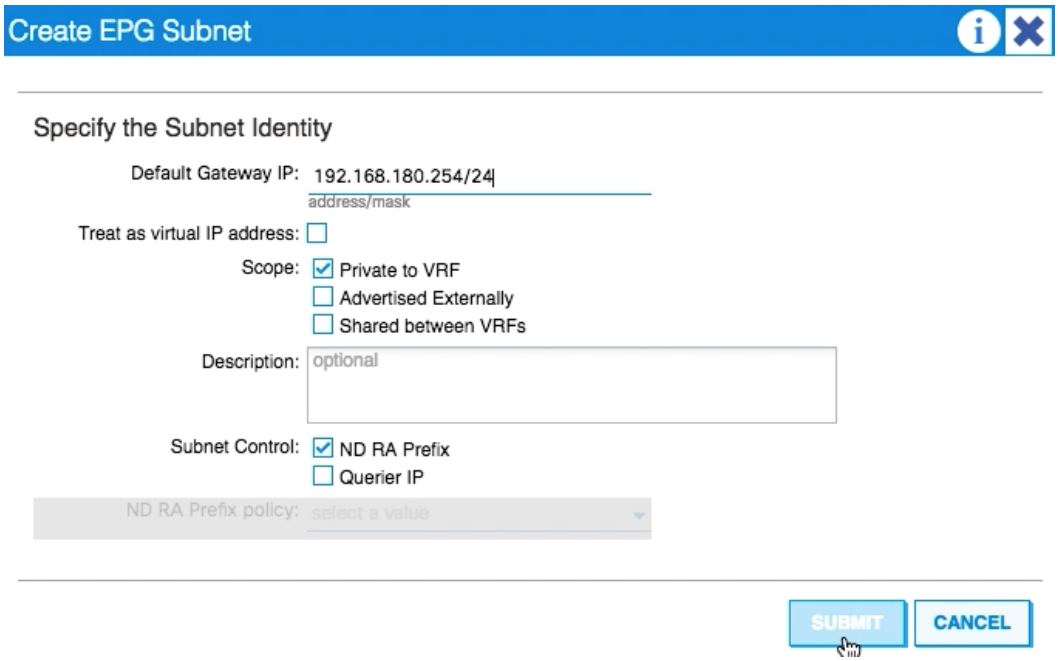
11. Right-click on the Static-Bindings (Paths) and select **Deploy EPG on PC, VPC, or Interface**.
12. In the Deploy Static EPG on PC, VPC, Or Interface Window, select the appropriate Path Type from Table 22. For example, for UCS Fabric Interconnect, select **Virtual Port Channel**.
13. From the drop-down list, select the VPC for UCS Fabric Interconnect A.
14. Enter <UCS NFS VLAN> {3050} for Port Encap.
15. Select Immediate for Deployment Immediacy and for Mode select Trunk.



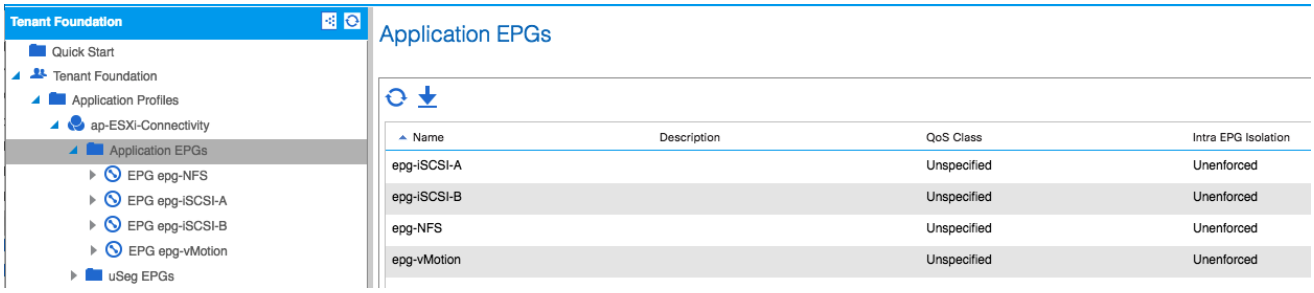
16. Click **SUBMIT** to complete adding the Static Path Mapping.
17. Repeat the above steps to add all the Static Path Mapping for the EPG listed in Table 22.



18. In the left pane, right-click on Subnets and select **Create EPG Subnet**.
19. Enter the Default Gateway IP address and subnet from the Table 22.
20. Leave the field Scope as Private to VRF.



21. Click **SUBMIT**.
22. Repeat these steps to create epg-vMotion, epg-iSCIS-A and epg-iSCSI-B using the values listed in Table 22.



After the EPG configuration is complete, proceed with the VMware configuration as covered in the next section.

VMware vSphere Configuration

VMware ESXi 6.0 U1b

This section provides detailed instructions for installing VMware ESXi 6.0 U1b in the validation environment. After the procedures are completed, multiple booted ESXi hosts will be provisioned.

Several methods exist for installing ESXi in a VMware environment. These procedures focus on how to use the built-in keyboard, video, mouse (KVM) console and virtual media features in Cisco UCS Manager to map remote installation media to individual servers and connect to their boot logical unit numbers (LUNs).

Log in to Cisco UCS Manager

The IP KVM enables the administrator to begin the installation of the operating system (OS) through remote media. It is necessary to log in to the UCS environment to run the IP KVM.

To log in to the Cisco UCS environment, complete the following steps:

1. Open a web browser and enter the IP address for the Cisco UCS cluster address. This step launches the Cisco UCS Manager application.
2. Under HTML, click the **Launch UCS Manager link**.
3. When prompted, enter admin as the user name and enter the administrative password.
4. To log in to Cisco UCS Manager, click **Login**.
5. From the main menu, click the **Servers** tab.
6. Select Servers > Service Profiles > root > Infra-ESXi-Host-01.

For IBM V9000 iSCSI setup, the name of the profile will be Infra-ESXi-iSCSI-Host-01

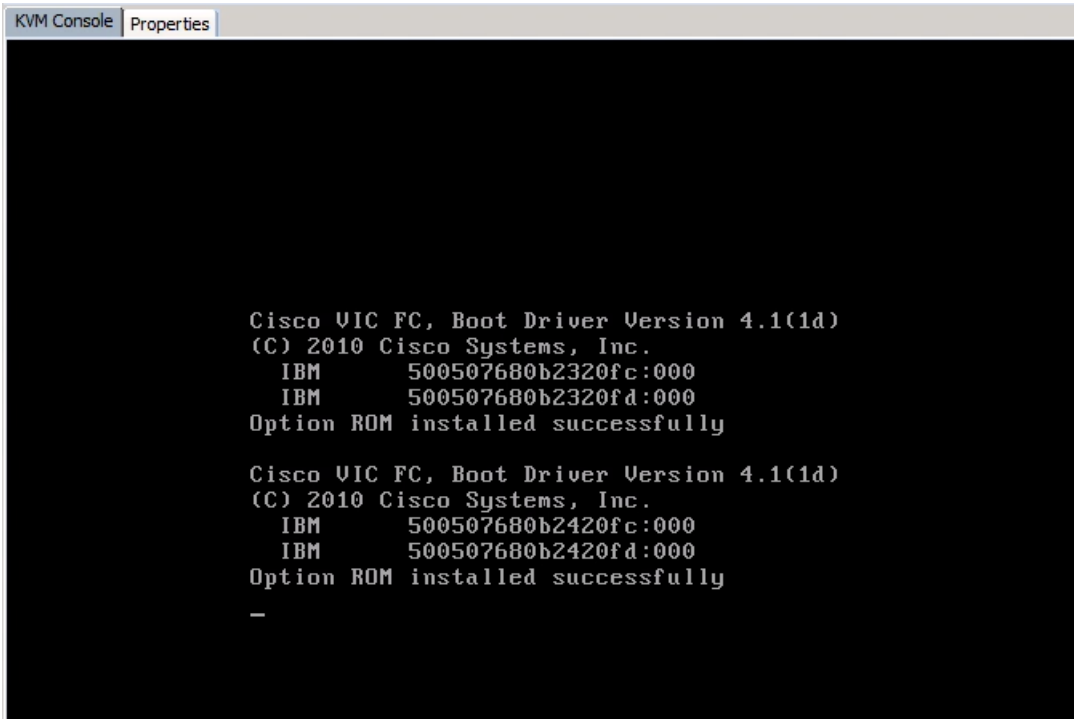
7. Right-click Infra-ESXi-Host-01 and select KVM Console.
8. If prompted to accept an Unencrypted KVM session, accept as necessary.
9. Open KVM connection to all the hosts by right-clicking the Service Profile and launching the KVM console
10. Boot each server by selecting Boot Server and clicking **OK**. Then click **OK** again.

Install ESXi on the Servers

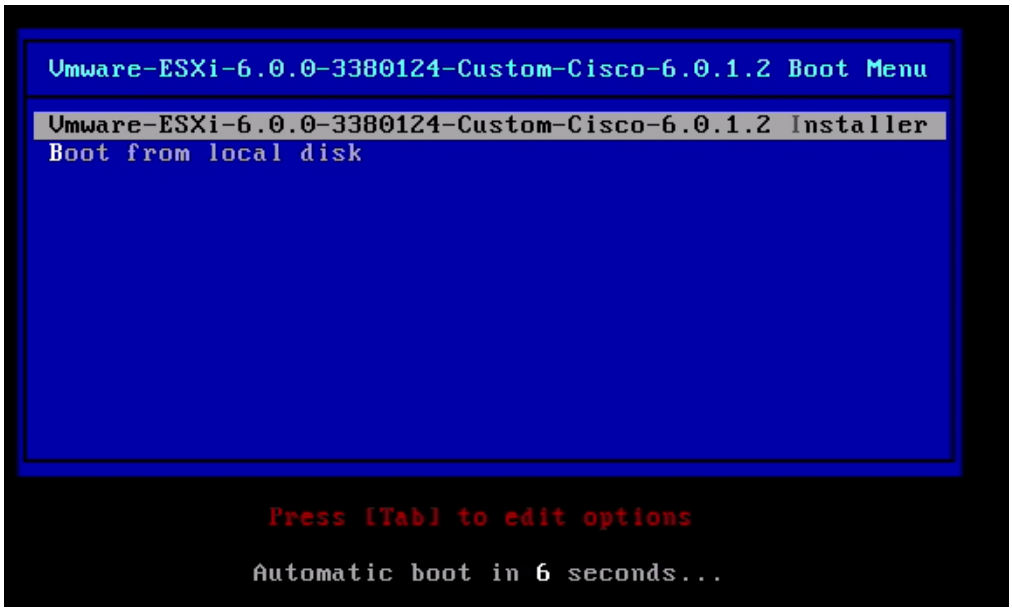
To install VMware ESXi to the boot LUN of the hosts, complete the following steps on each host:

1. In the KVM window, click **Virtual Media**.
2. Click Activate Virtual Devices.
3. If prompted to accept an Unencrypted KVM session, accept as necessary.

4. Click Virtual Media and select Map CD/DVD.
5. Browse to the ESXi installer ISO image file and click **Open**.
6. Click Map Device.
7. Click the **KVM** tab to monitor the server boot.
8. Reset the server by clicking Reset button. Click **OK**.
9. Select Power Cycle on the next window and click **OK** and **OK** again.
10. On reboot, the machine detects the presence of the boot LUNs (sample output below).



11. From the ESXi Boot Menu, select the ESXi installer.



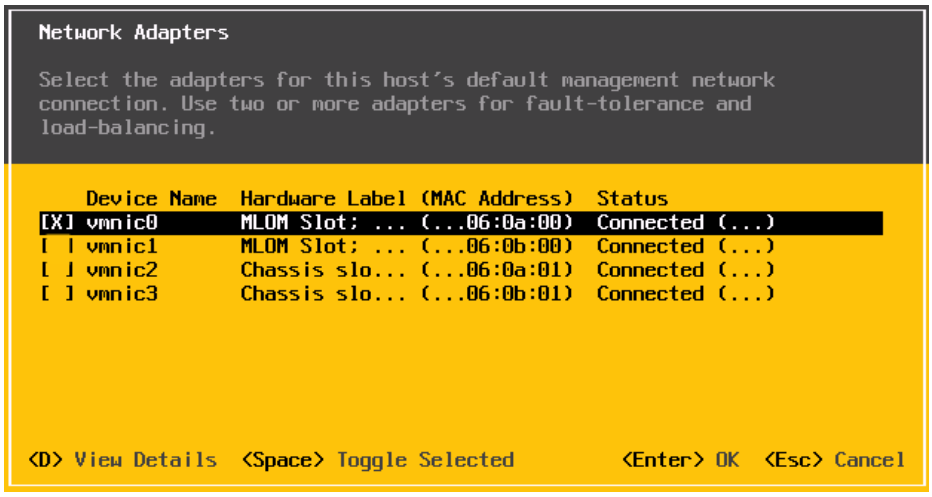
12. After the installer has finished loading, press **Enter** to continue with the installation.
13. Read and accept the end-user license agreement (EULA). Press **F11** to accept and continue.
14. Select the LUN that was previously set up and discovered as the installation disk for ESXi and press **Enter** to continue with the installation.
15. Select the appropriate keyboard layout and press **Enter**.
16. Enter and confirm the root password and press **Enter**.
17. The installer issues a warning that the selected disk will be repartitioned. Press **F11** to continue with the installation.
18. After the installation is complete, press **Enter** to reboot the server.
19. Repeat the ESXi installation process for all the Service Profiles.

Set Up Management Networking for ESXi Hosts

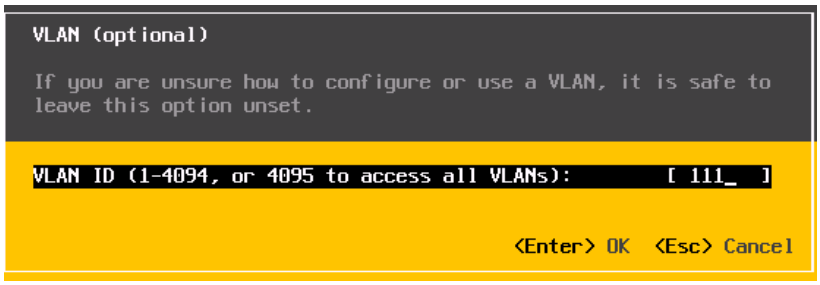
Adding a management network for each VMware host is necessary for managing the host. To add a management network for the VMware hosts, complete the following steps on each ESXi host.

To configure the ESXi hosts with access to the management network, complete the following steps:

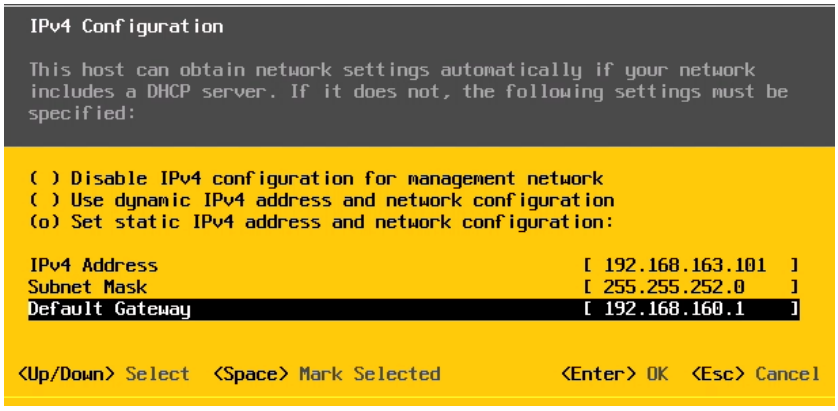
1. After the server has finished post-installation rebooting, press **F2** to customize the system.
2. Log in as root, enter the password chosen during the initial setup, and press **Enter** to log in.
3. Select the Configure Management Network option and press **Enter**.
4. Select vmnico (if it is not already selected) by pressing the Space Bar.



5. Press **Enter** to save and exit the Network Adapters window.
6. Select the VLAN (Optional) and press **Enter**.
7. Enter the <IB Mgmt VLAN> (111) and press **Enter**.



8. Select IPv4 Configuration and press **Enter**.
9. Select the Set Static IP Address and Network Configuration option by using the Space Bar.
10. Enter the IP address for managing the ESXi host.
11. Enter the subnet mask for the management network of the ESXi host.
12. Enter the default gateway for the ESXi host.



13. Press **Enter** to accept the changes to the IP configuration.
14. Select the IPv6 Configuration option and press **Enter**.
15. Using the Space Bar, select Disable IPv6 (restart required) and press **Enter**.
16. Select the DNS Configuration option and press **Enter**.

Because the IP address is assigned manually, the DNS information must also be entered manually.

17. Enter the IP address of the primary DNS server.
18. **Optional**: Enter the IP address of the secondary DNS server.
19. Enter the fully qualified domain name (FQDN) for the ESXi host.
20. Press **Enter** to accept the changes to the DNS configuration.
21. Press **Esc** to exit the Configure Management Network submenu.
22. Press **Y** to confirm the changes and reboot the host.
23. Repeat this procedure for all the ESXi hosts in the setup.

Download VMware vSphere Client

To download the VMware vSphere Client, complete the following steps:

1. Open a web browser on the management workstation and navigate to the management IP address an any ESXi servers.
2. Download and install the vSphere Client for Windows.

Download VMware vSphere CLI

To download the VMware Remote CLI, complete the following steps:

1. Click the following link:
   https://my.vmware.com/web/vmware/details?downloadGroup=VCLI600&productId=491
2. Select the OS and Click **Download** to download the vSphere remote CLI.
3. Save it to destination folder.
4. Install the program on your management workstation.

Log in to VMware ESXi Hosts Using VMware vSphere Client

To log in to the ESXi host using the VMware vSphere Client, complete the following steps:

1. Open the recently downloaded VMware vSphere Client and enter the management IP address of the host.
2. Enter root for the user name.

3. Enter the root password configured during the installation process.
4. Click **Login** to connect.
5. Repeat this process to log into all the ESXi hosts.

Install VMware Drivers for the Cisco Virtual Interface Card (VIC)

Download and extract the following VMware VIC Drivers to the Management workstation:

fnic Driver version 1.6.0.25

enic Driver version 2.3.0.7

Complete the following steps to install VMware VIC Drivers on ALL the ESXi hosts:

1. From each vSphere Client, select the host in the inventory.
2. Click the **Summary** tab to view the environment summary.
3. From Resources > Storage, right-click datastore1 and select **Browse Datastore**.
4. Click the fourth button and select **Upload File**.
5. Navigate to the saved location for the downloaded VIC drivers and select fnic_driver_1.6.0.25-offline_bundle-3642682.zip.
6. Click **Open** and **Yes** to upload the file to datastore1.
7. Click the fourth button and select Upload File.
8. Navigate to the saved location for the downloaded VIC drivers and select ESXi60-enic-2.3.0.7-offline_bundle-3642661.zip.
9. Click **Open** and **Yes** to upload the file to datastore1.
10. Make sure the files have been uploaded to both ESXi hosts.
11. In the ESXi host vSphere Client, select the **Configuration** tab.
12. In the Software pane, select Security Profile.
13. To the right of Services, click **Properties**.
14. Select SSH and click **Options**.
15. Click **Start** and **OK**.

The step above does not enable SSH service and the service will not be restarted when ESXi host reboots.

16. Click **OK** to close the window.
17. Ensure SSH is started on each host.

18. From the management workstation, start an ssh session to each ESXi host. Login as root with the root password.
19. At the command prompt, run the following commands to account for each host:

```
esxcli software vib update -d /vmfs/volumes/datastore1/fnic_driver_1.6.0.25-offline_bundle-3642682.zip

esxcli software vib update -d /vmfs/volumes/datastore1/ESXi60-enic-2.3.0.7-offline_bundle-3642661.zip

reboot
```

20. After each host has rebooted, log back into each host with vSphere Client.

Set Up VMkernel Ports and Configure Virtual Switch

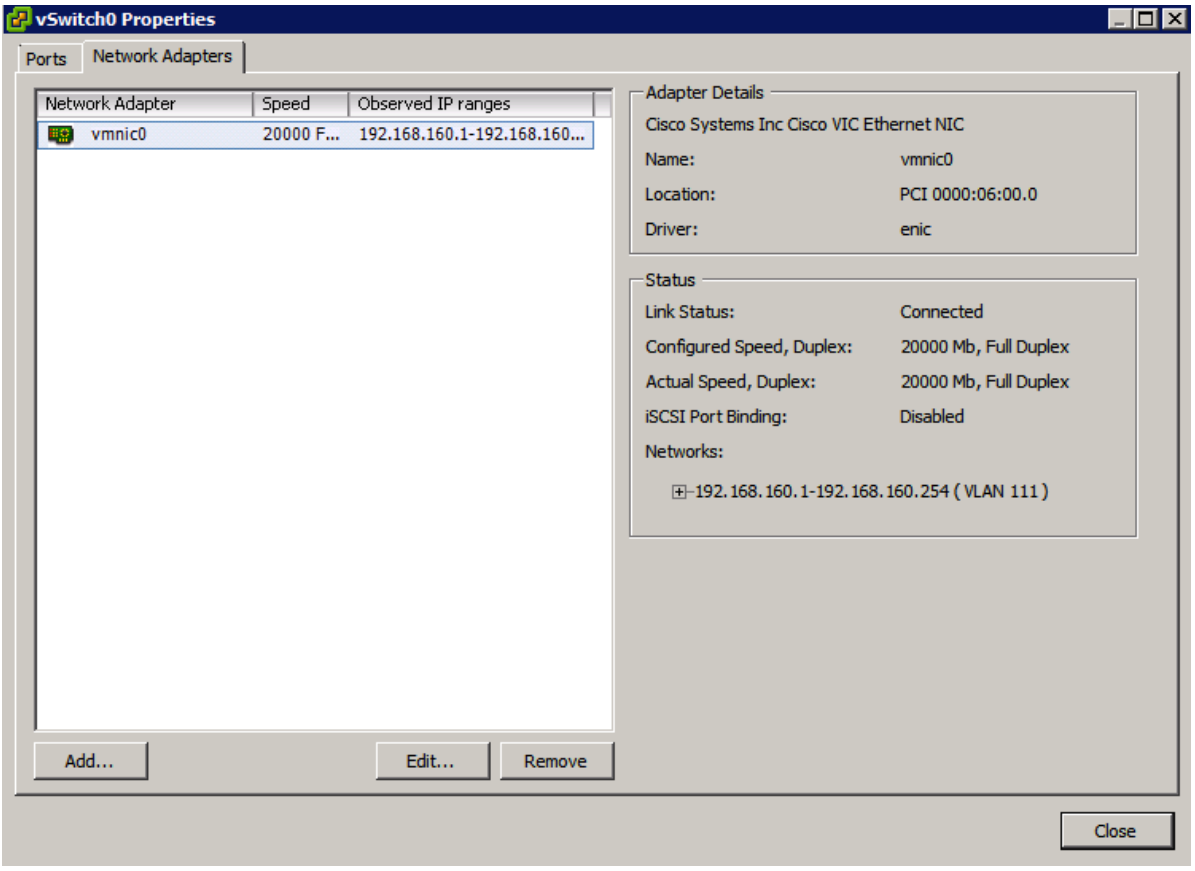
To set up the VMkernel ports and the virtual switches on the ESXi hosts, complete the following steps:

1. From vSphere Client, select the host in the inventory.
2. Click the **Configuration** tab.
3. Click **Networking** in the Hardware pane.
4. Click **Properties** on the right side of vSwitcho.
5. Select the vSwitch configuration and click **Edit**.
6. From the **General** tab, change the MTU to 9000.
7. Click **OK** to close the properties for vSwitcho.
8. Select the Management Network configuration and click **Edit**.
9. Change the network label to VMkernel-MGMT and check the Management Traffic checkbox.
10. Click **OK** to finalize the edits for Management Network.
11. Select the VM Network configuration and click **Edit**.
12. Change the network label to IB-MGMT and enter <<Management VLAN>> (111) in the VLAN ID (Optional) field.
13. Click **OK** to finalize the edits for VM Network.
14. Click **Add** to add a network element.
15. Select VMkernel and click **Next**.
16. Change the network label to VMkernel-vMotion and enter <<vMotion VLAN>> (3000) in the VLAN ID (Optional) field.
17. Select the Use This Port Group for vMotion checkbox.
18. Click **Next** to continue with the vMotion VMkernel creation.

19. Enter the IP address <<vMotion IP address>> and the subnet mask <<vMotionSubnet>> for the vMotion VLAN interface for the ESXi Host.
20. Click **Next** to continue with the vMotion VMkernel creation.
21. Click **Finish** to finalize the creation of the vMotion VMkernel interface.
22. Select the VMkernel-vMotion configuration and click **Edit**.
23. Change the MTU to 9000.
24. Click **OK** to finalize the edits for the VMkernel-vMotion network.

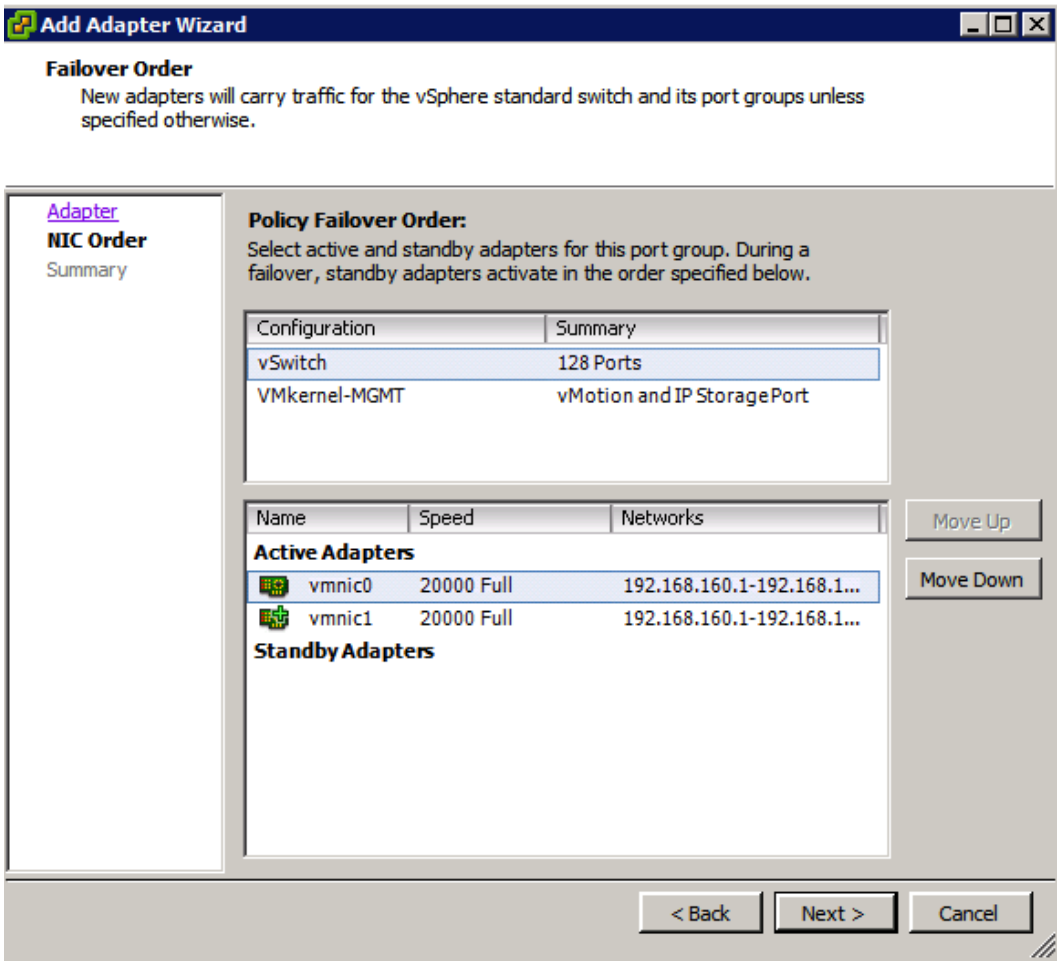
VMkernel port for NFS (steps 25 through 34 below) is only needed when configuring IBM Storwize V7000 Unified for NFS storage connectivity

25. Click **Add** to add a network element.
26. Select VMkernel and click **Next**.
27. Change the network label to VMkernel-NFS and enter <<NFS VLAN>> (3050) in the VLAN ID (Optional) field.
28. Click **Next** to continue with the NFS VMkernel creation.
29. Enter the IP address <<NFS IP>> and the subnet mask <<NFS SUBNET>> for the NFS VLAN interface for the ESXi host.
30. Click **Next** to continue with the NFS VMkernel creation.
31. Click **Finish** to finalize the creation of the NFS VMkernel interface.
32. Select the VMkernel-NFS configuration and click **Edit**.
33. Change the MTU to 9000.
34. Click **OK** to finalize the edits for the VMkernel-NFS network.
35. Click the **Network Adapter** tab at the top of the window and click **Add**.



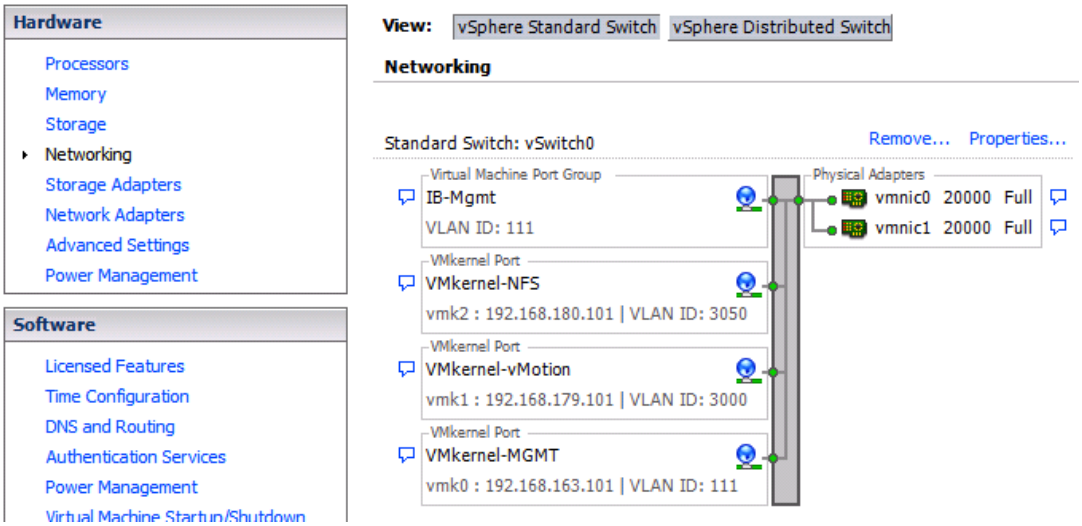
36. Select vmnic1 and click **Next**.

37. Make sure vmnic1 is added to the Active Adapters and click **Next**.



38. Click **Finish**.

39. Close the dialog box to finalize the ESXi host networking setup.



Set Up iSCSI VMkernel Ports and vSwitches (IBM V9000 iSCSI deployment Only)

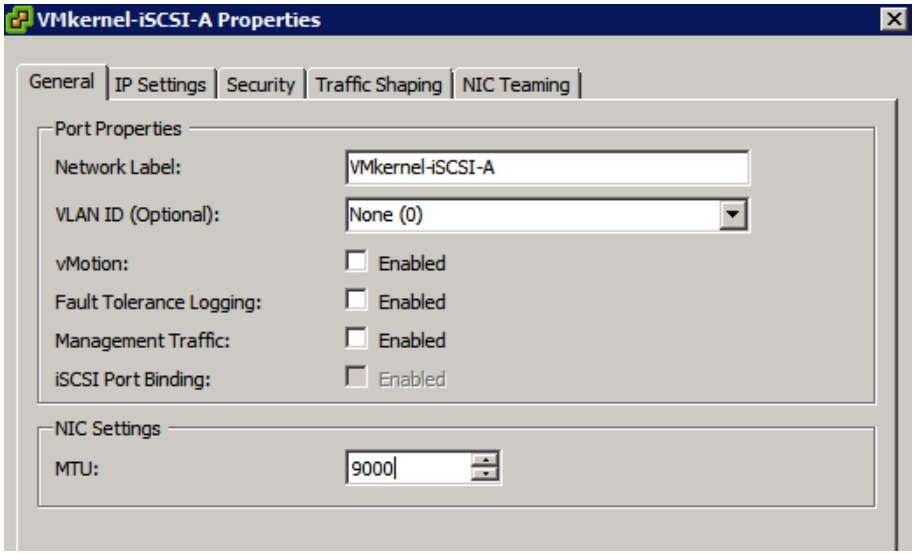
To set up the iSCSI VMkernel ports and the virtual switches on the ESXi hosts, complete the following steps:

1. From vSphere Client, select the host in the inventory.
2. Click the **Configuration** tab.
3. In the Configuration screen select Networking in the left.

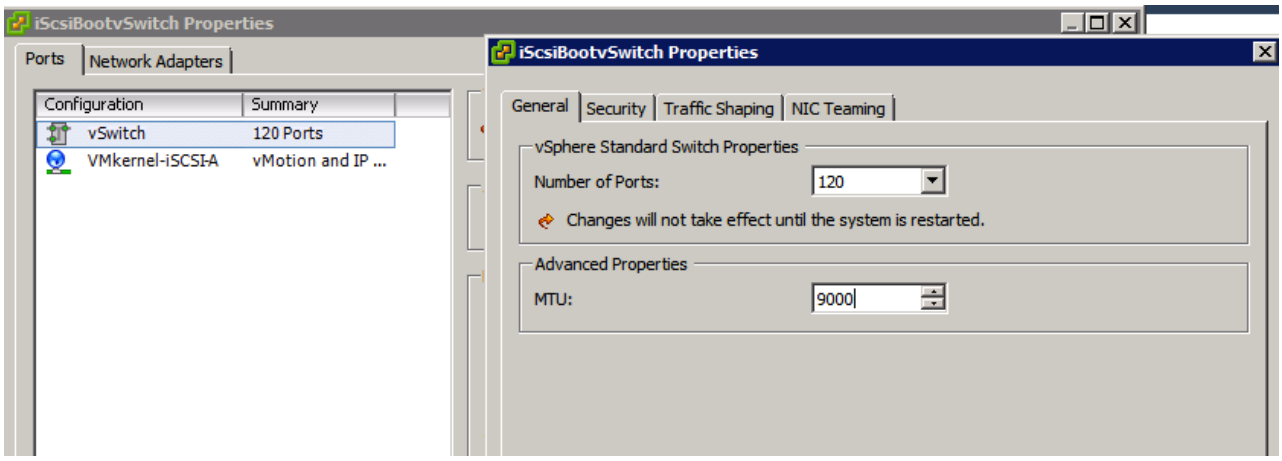
Modify iSCSI Boot vSwitch

1. Click **Properties** next to the iSCSIBootvSwitch.
2. In the popup, select VMkernel and click **Edit**.
3. Rename the VMkernel port to VMkernel-iSCSI-A.
4. Change MTU to 9000.

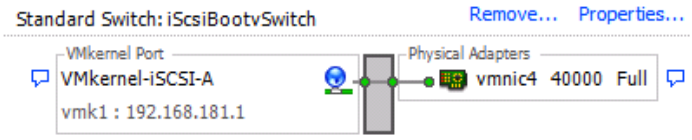
It is important to not set a VLAN ID here because the iSCSI VLAN was set as the Native VLAN of the vNIC and these iSCSI packets should come from the vSwitch without a VLAN tag.



5. Click **OK**.
6. Select the vSwitch configuration and click **Edit**.
7. Change the MTU to 9000.

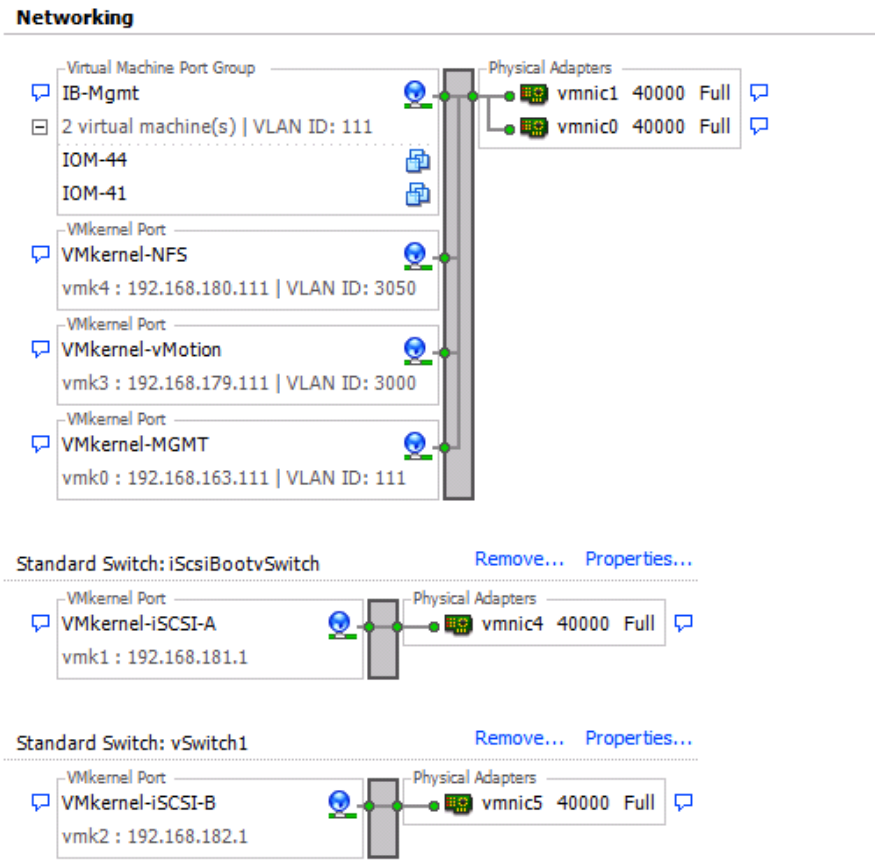


8. Click **OK**.
9. Click **Close**.



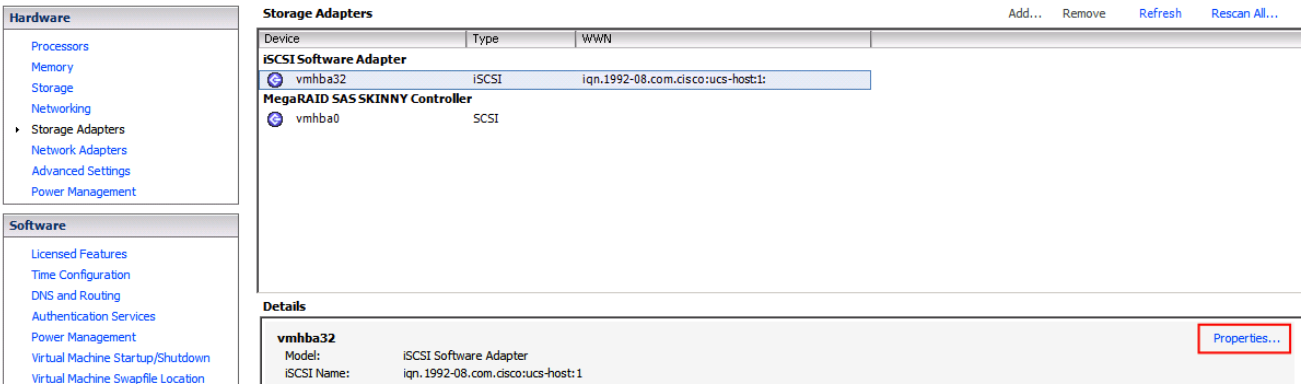
Create iSCSI-B vSwitch

1. In the Networking screen select **Add Networking**.
2. In the popup, select VMkernel to add a VMkernel port in the Infrastructure iSCSI-B subnet. Click **Next**.
3. Select vmnic5 and click **Next**.
4. Label the Network VMkernel-iSCSI-B. Do not add a VLAN ID.
5. Click **Next**.
6. Enter an IP Address for this ESXi host's iSCSI-B interface.
7. Click **Next**.
8. Click **Finish**.
9. Click **Properties** to the right of the newly created vSwitch.
10. Select the vSwitch configuration and click **Edit**.
11. Change the MTU to 9000 and click **OK**.
12. Select the VMkernel-iSCSI-B configuration and click **Edit**.
13. Change the MTU to 9000 and click **OK**.
14. Click **Close**.

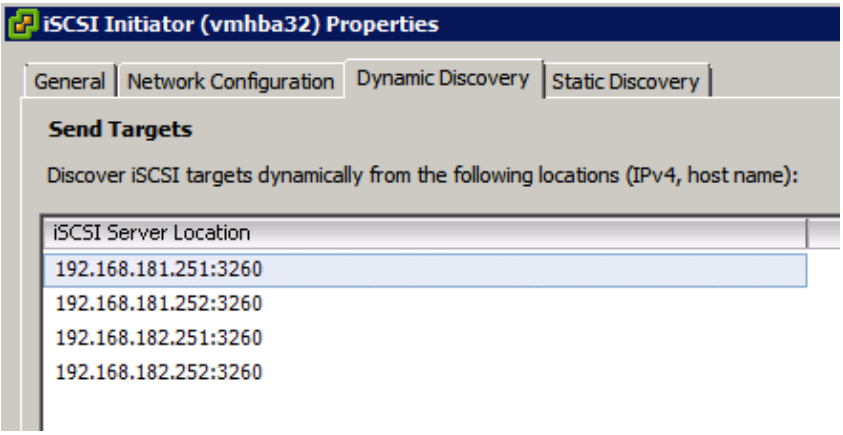


Setup iSCSI Targets

1. In the left pane under the Hardware, select **Storage Adapters**.
2. Select the iSCSI Software Adapter and click **Properties**.



3. In the iSCSI Initiator Properties window, click the **Dynamic Discovery** tab.
4. Click **Add**. Enter the first iSCSI interface IP address for IBM V9000 storage from Table 9 and click **OK**.
5. Repeat the previous step to add all four IP addresses.



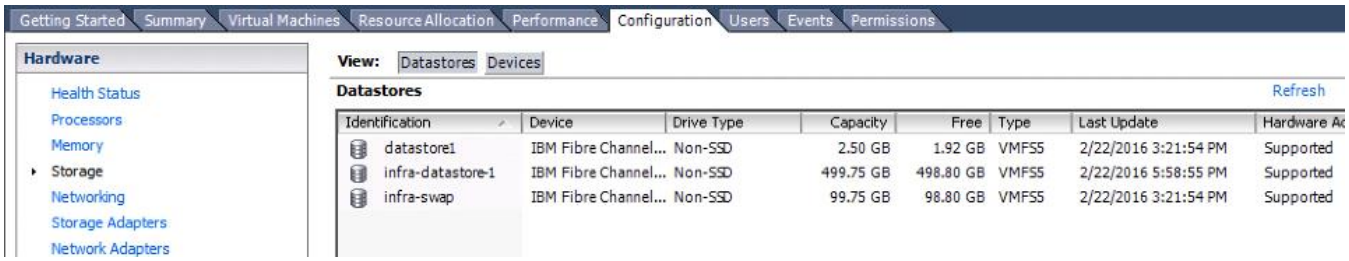
6. Click **Close**.
7. Click **Yes** to Rescan the host bus adapter.
8. Repeat this procedure for all the iSCSI ESXi Hosts.

Mount Required Datastores

To mount the required datastores, complete the following steps on each ESXi host:

1. From the vSphere Client, select the host in the inventory.
2. Click the **Configuration** tab.
3. Click **Storage** in the Hardware window.
4. From the Datastore area, click **Add Storage** to open the Add Storage wizard.
5. Select Disk/LUN and click **Next**.
6. Verifying by using the size of the datastore LUN, select the LUN configured for VM hosting and click **Next**.
7. Accept default VMFS setting and click **Next**.
8. Click **Next** for the disk layout.
9. Enter infra-datastore-1 as the datastore name.
10. Click **Next** to retain maximum available space.
11. Click **Finish**.
12. Select the second LUN configured for swap file location and click **Next**.
13. Accept default VMFS setting and click **Next**.
14. Click **Next** for the disk layout.
15. Enter infra_swap as the datastore name.

16. Click **Next** to retain maximum available space.
17. Click **Finish**.
18. The storage configuration should look similar to figure shown below.
19. Repeat these steps on all the ESXi hosts.



Configure NTP on ESXi Hosts

To configure Network Time Protocol (NTP) on the ESXi hosts, complete the following steps on each host:

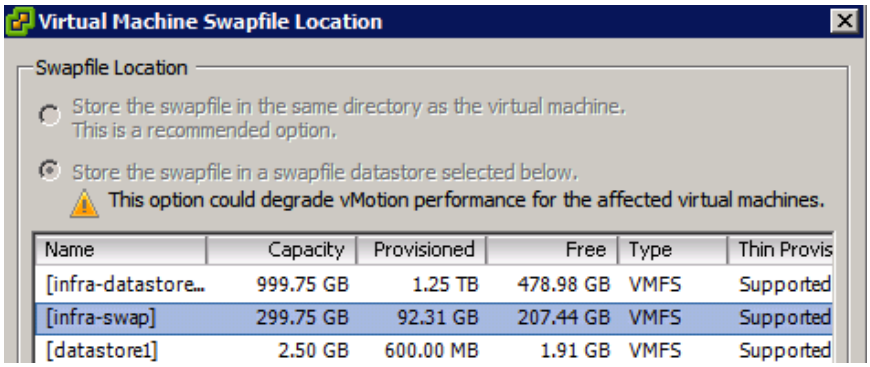
1. From the vSphere Client, select the host in the inventory.
2. Click the **Configuration** tab.
3. Click **Time Configuration** in the Software pane.
4. Click Properties.
5. At the bottom of the Time Configuration dialog box, click **NTP Client Enabled**.
6. At the bottom of the Time Configuration dialog box, click **Options**.
7. In the NTP Daemon (ntpd) Options dialog box, complete the following steps:
   - Click **General** tab in the left pane and select Start and stop with host.
   - Click NTP Settings in the left pane and click **Add**.
   - In the Add NTP Server dialog box, enter <NTP Server IP Address> as the IP address of the NTP server and click **OK**.
   - In the NTP Daemon Options dialog box, select the Restart NTP service to apply changes checkbox and click **OK**.
   - Click **OK**.
8. In the Time Configuration dialog box, verify that the clock is now set to approximately the correct time.

Move VM Swap File Location

To move the VM swap file location, complete the following steps on each ESXi host:

1. From the vSphere Client, select the host in the inventory.
2. Click the **Configuration** tab.

3. Click Virtual Machine Swapfile Location in the Software pane.
4. Click **Edit** at the upper-right side of the window.
5. Select the option Store the swapfile in a swapfile datastore selected below.
6. Select the infra-swap datastore to house the swap files.
7. Click **OK** to finalize the swap file location.

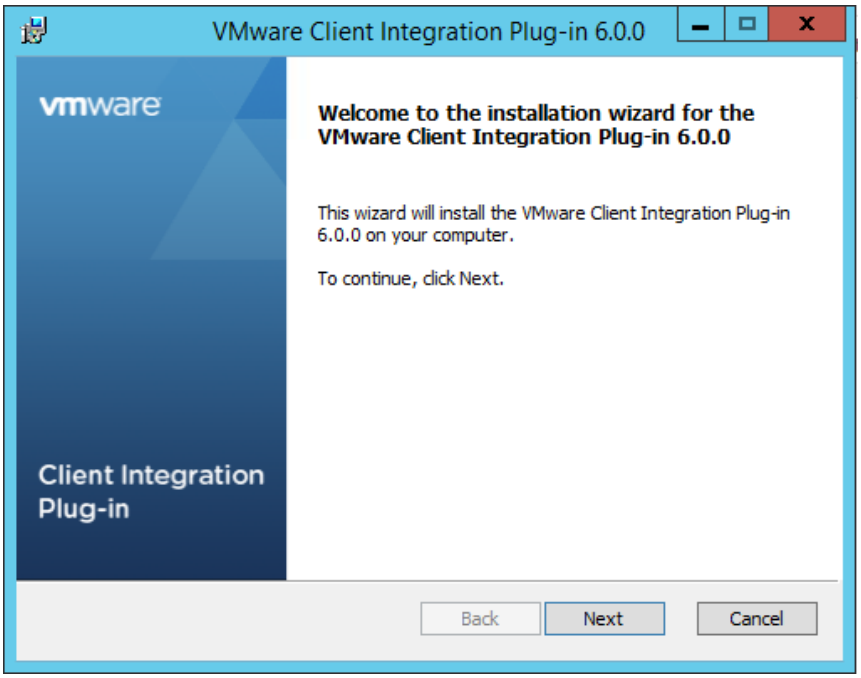


VMware vCenter 6.0U1b

The procedures in the following subsections provide detailed instructions for installing the VMware vCenter 6.0U1b Server Appliance in an environment. After the procedures are completed, a VMware vCenter Server will be configured.

Install the Client Integration Plug-in

1. Download the .iso installer for the version 6.0U1b vCenter Server Appliance and Client Integration Plug-in
2. Mount the ISO image on the management workstation.
3. In the mounted ISO directory, navigate to the vcsa directory and double-click VMware-ClientIntegrationPlugin-6.0.0.exe. The Client Integration Plug-in installation wizard appears.

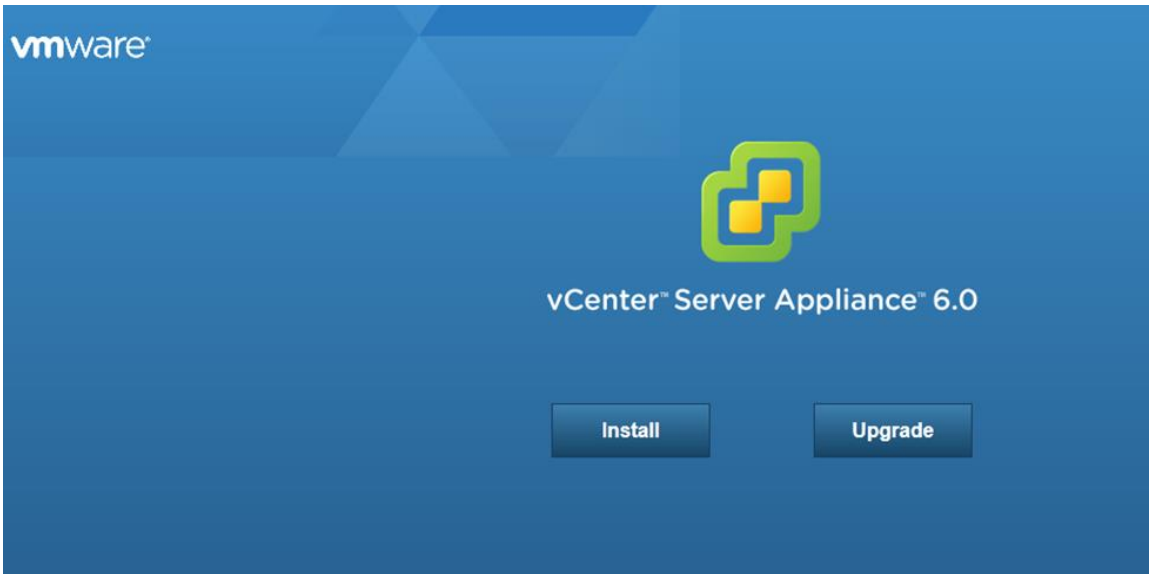


4. On the Welcome page, click **Next**.
5. Read and accept the terms in the End-User License Agreement and click **Next**.
6. Click **Next**.
7. Click **Install**.

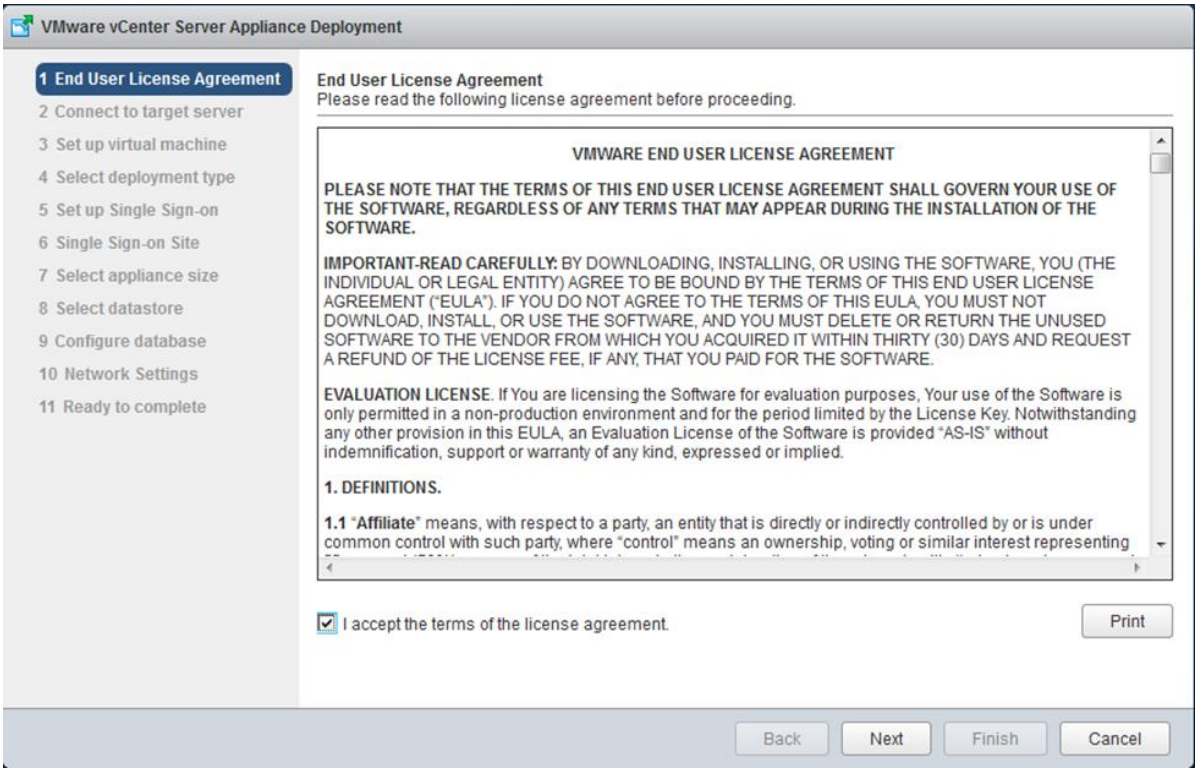
Building the VMware vCenter Server Appliance

To build the VMware vCenter virtual machine, complete the following steps:

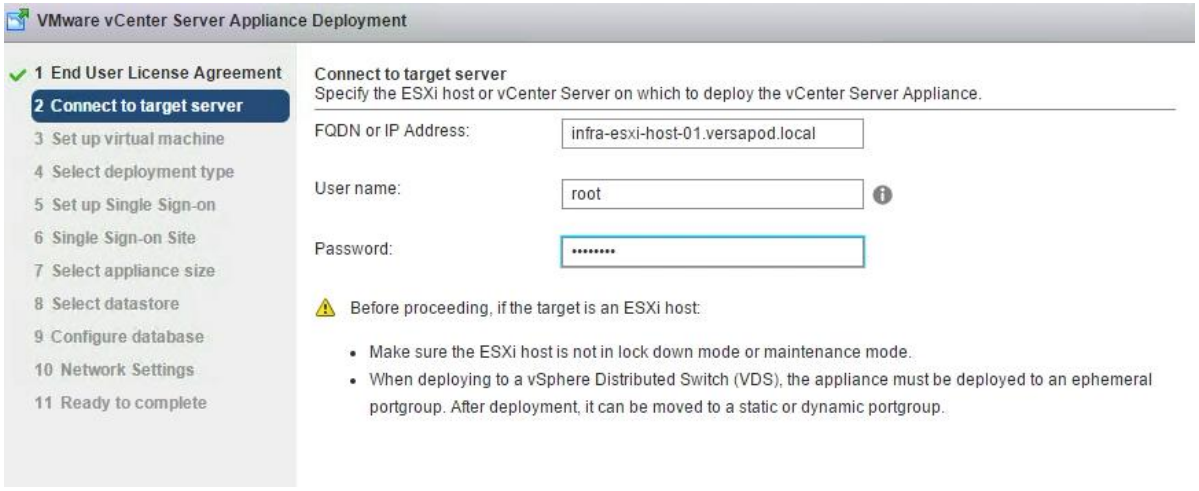
1. In the mounted iso top-level directory, double-click vcsa-setup.html.
2. Allow the plug-in to run on the browser when prompted.
3. In the Home page, click **Install** to start the vCenter Server Appliance deployment wizard.



4. Read and accept the license agreement, and click **Next**.



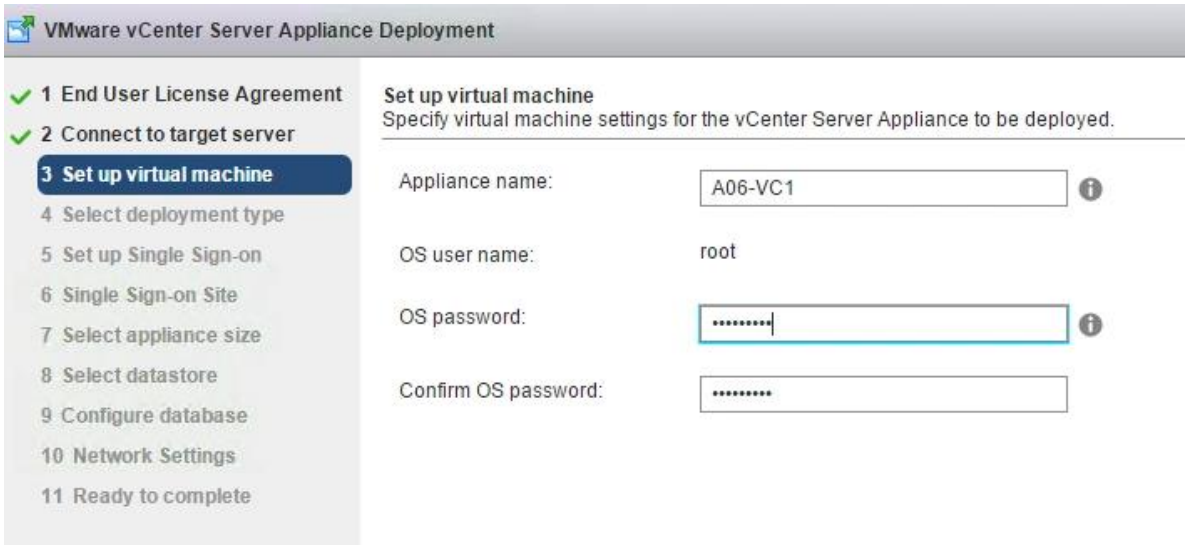
5. In the Connect to target server page, enter the ESXi host name, User name and Password.



6. Click **Next**.

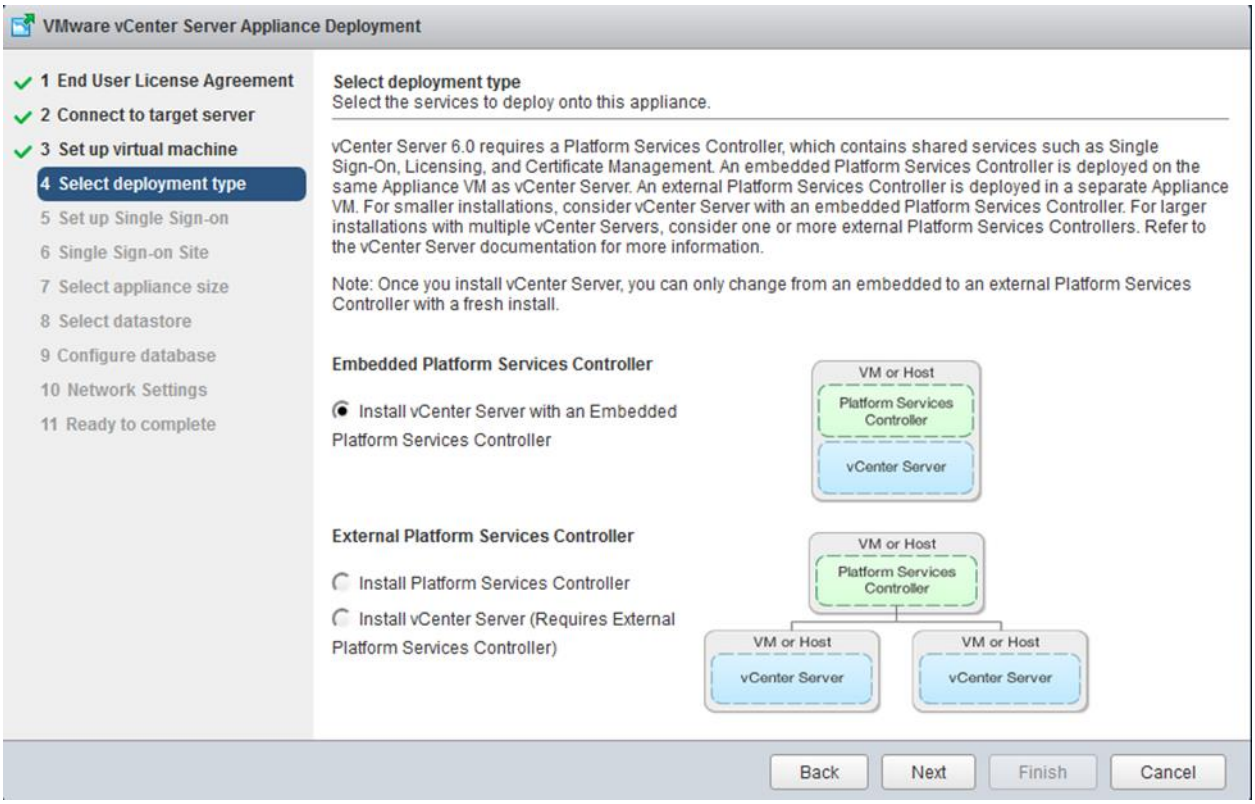
7. Click **Yes** to accept the certificate.

8. Enter the Appliance name and password details in the Set up virtual machine page.

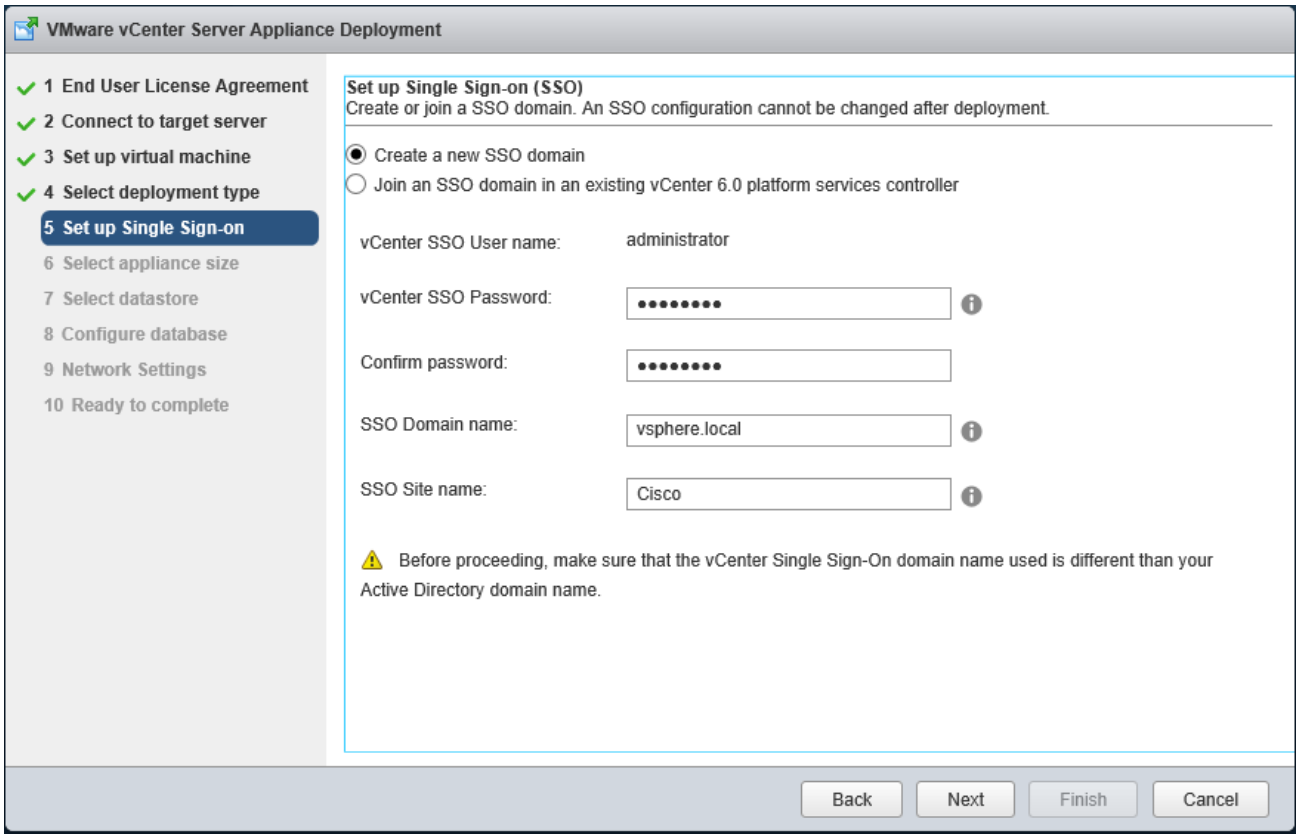


9. Click **Next**.

10. In the Select deployment type page, select the option Install vCenter Server with an embedded Platform Services Controller.

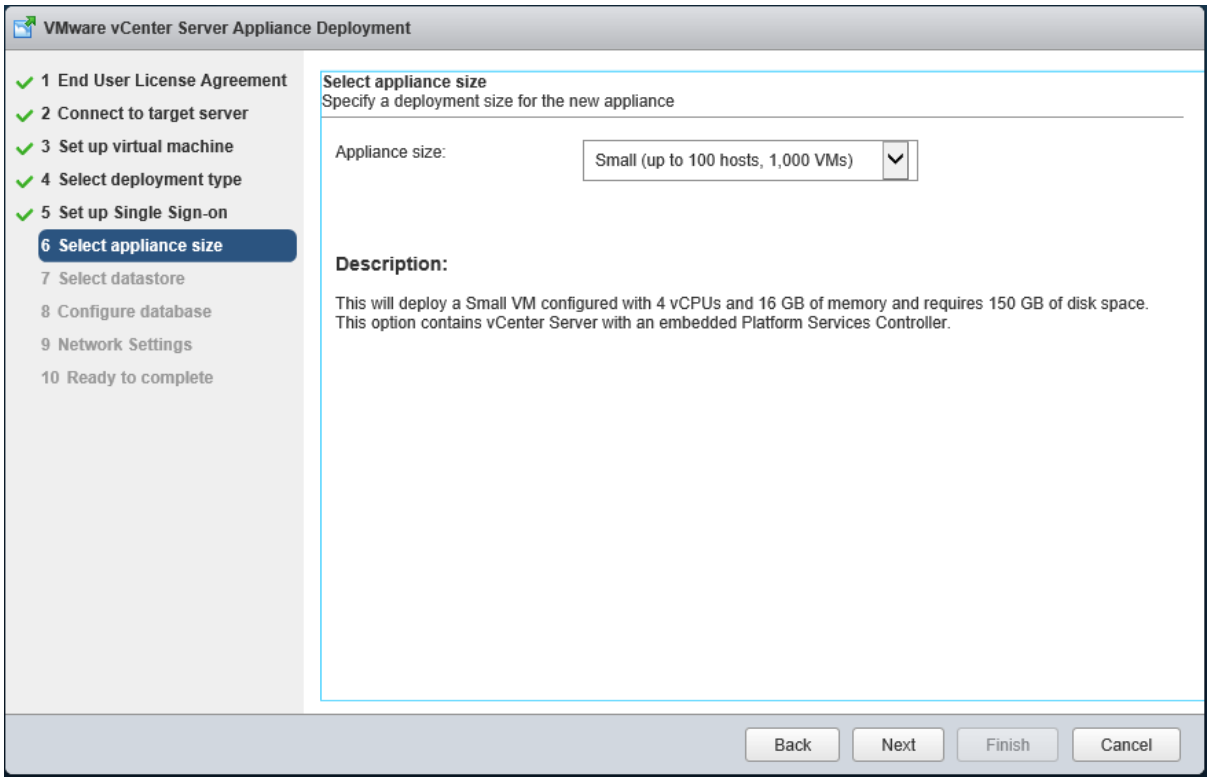


11. Click **Next**.
12. In the Set up Single Sign-On page, select the option Create a new SSO domain.
13. Enter the SSO password, Domain name and Site name.



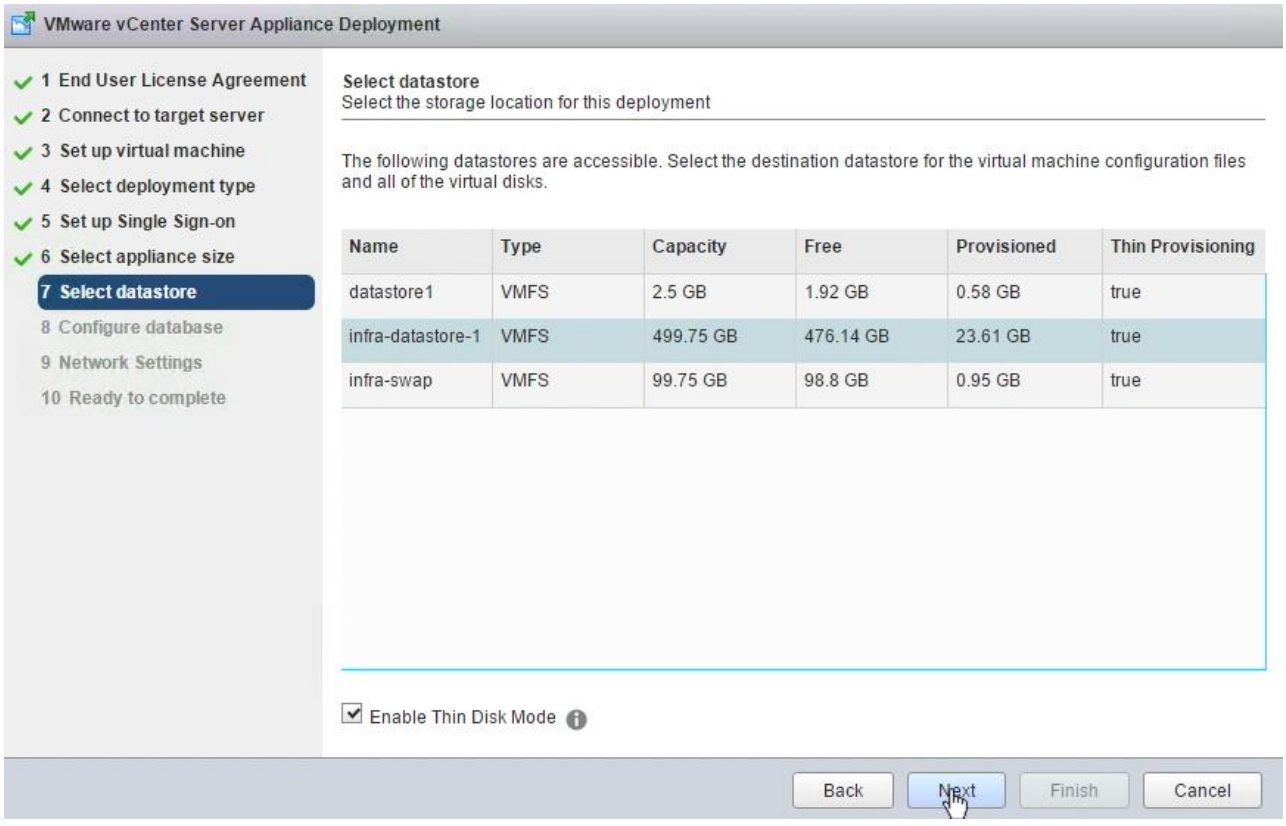
14. Click **Next**.

15. Select the appliance size as Small (up to 100 hosts, 1,000 VMs) as shown in the screenshot.

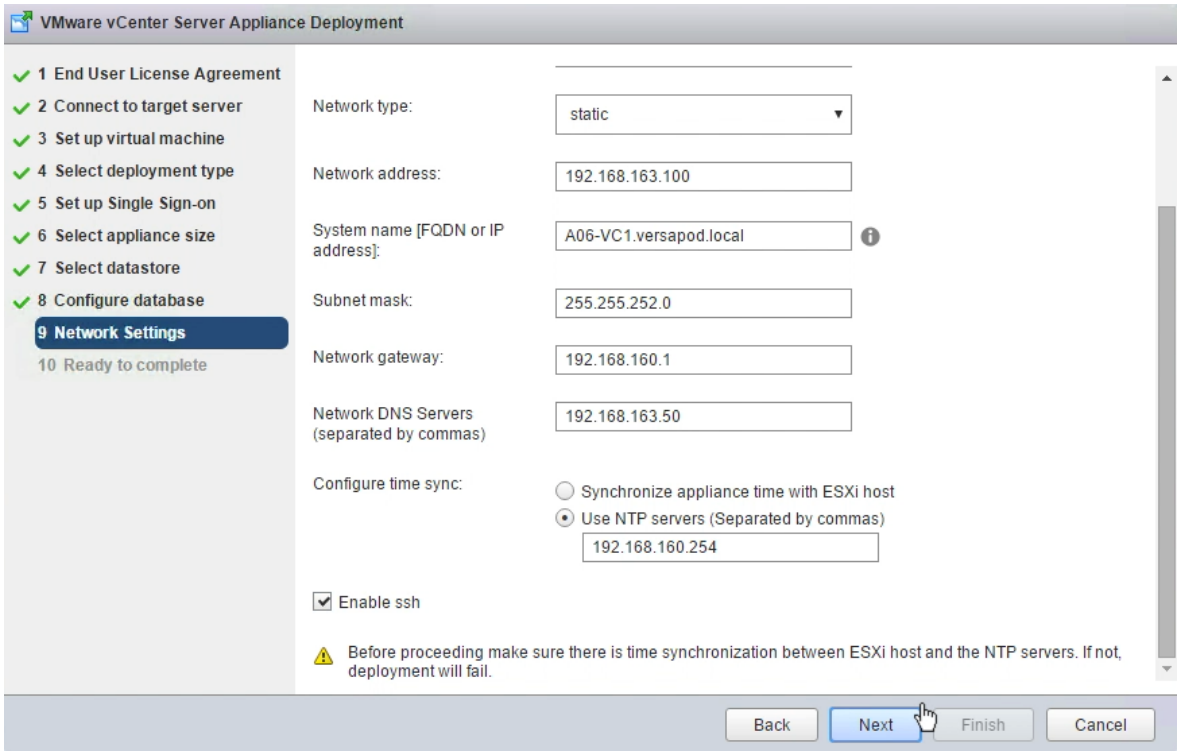


16. Click **Next**.

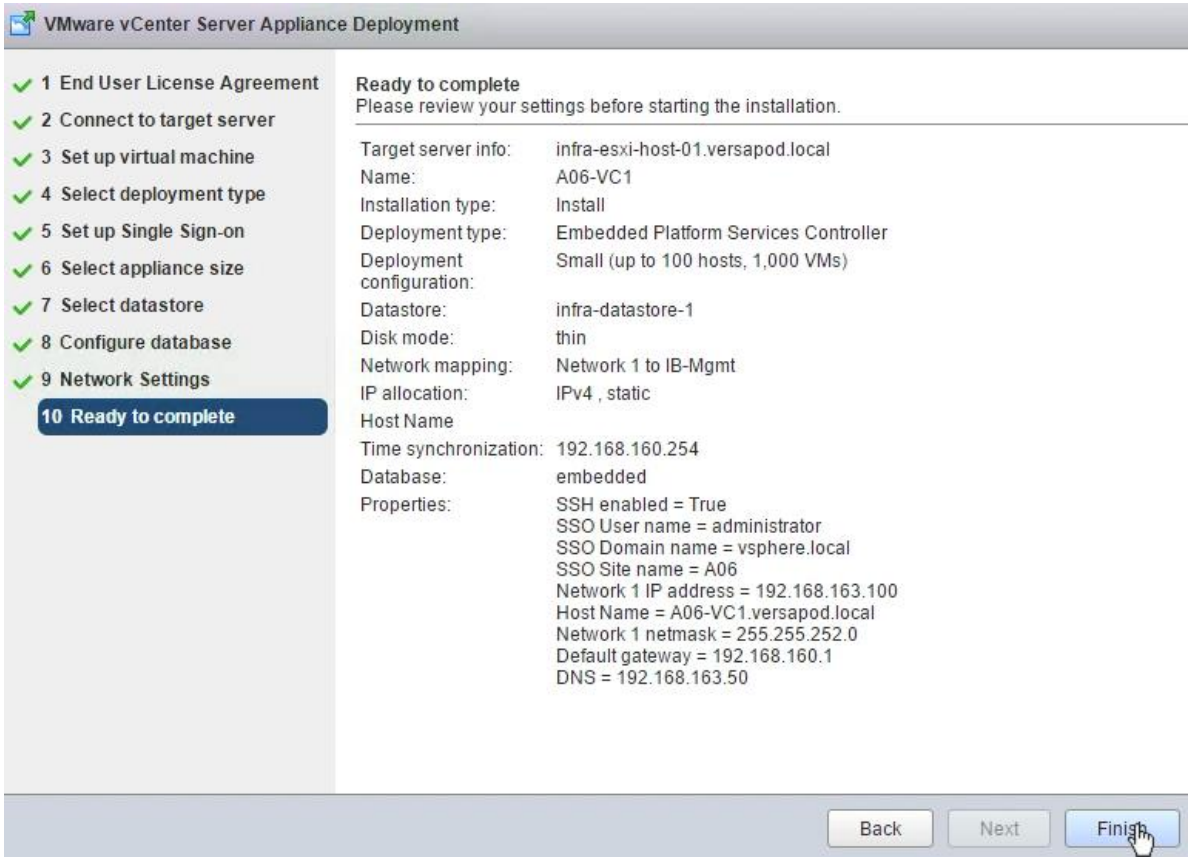
17. In the Select datastore page, select infra-datastore-1. Check the checkbox for Enable Thin Disk Mode.



18. Click **Next**.
19. Select Use an embedded database in the Configure database page. Click **Next**.
20. In the Network Settings page, configure the following:
    - Choose a Network: IB-Mgmt
    - IP address family: IPV4
    - Network type: static
    - Network address: <vcenter-ip>
    - System name: <vcenter-fqdn>
    - Subnet mask: <vcenter-netmask>
    - Network gateway: <vcenter-gateway>
    - Network DNS Servers
    - Configure time sync: Use NTP servers
    - Enable SSH
21. Click **Next**.



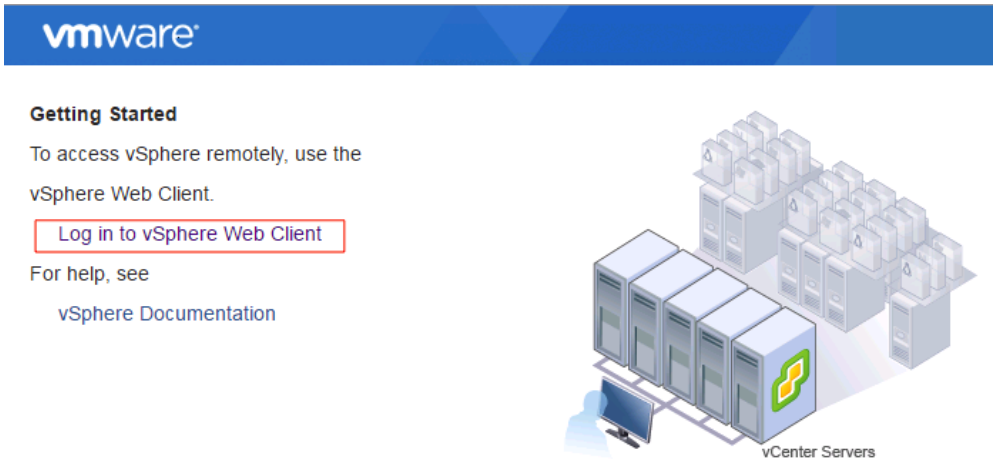
22. Review the configuration and click **Finish**.



23. The vCenter appliance installation will take a few minutes to complete.

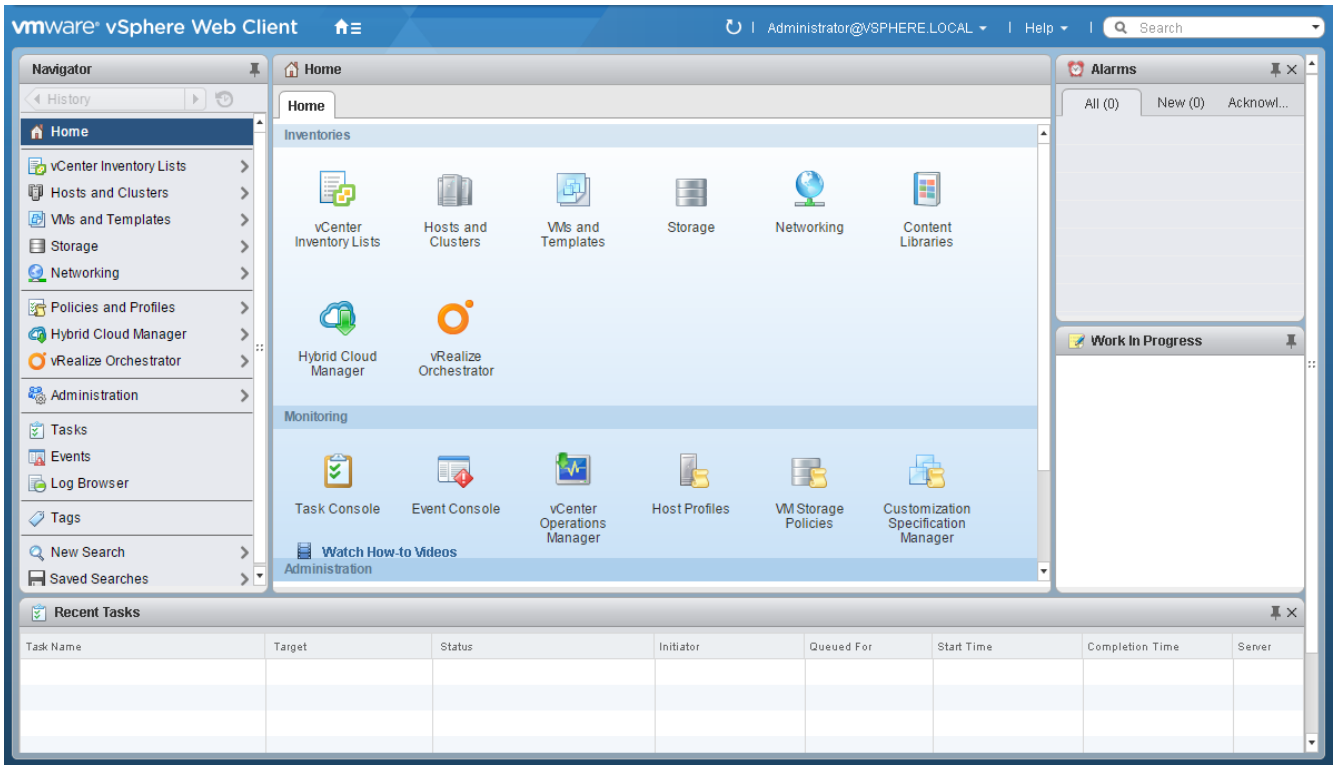
Setup vCenter Server

1. Using a web browser, navigate to <vCenter IP Address>.
2. Click the link Log in to vSphere Web Client.



If prompted, run and install the VMWare Remote Console Plug-in.

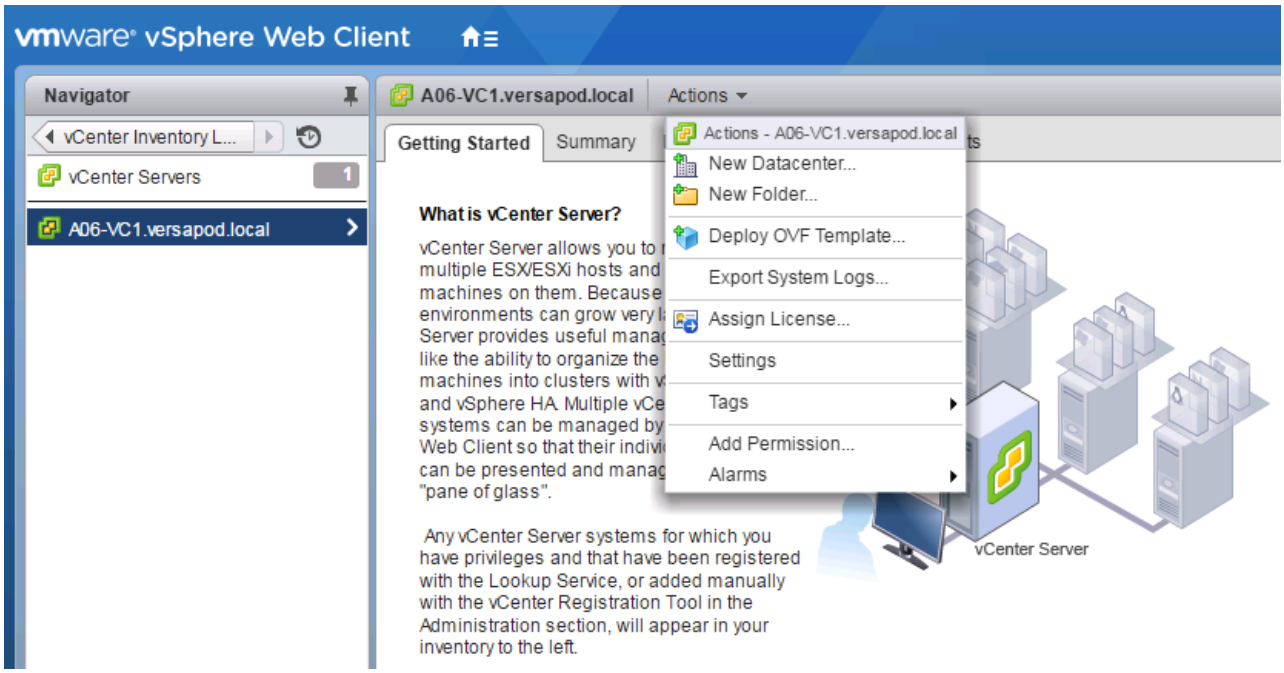
3. Log in as root, with the root password entered above in the vCenter installation.



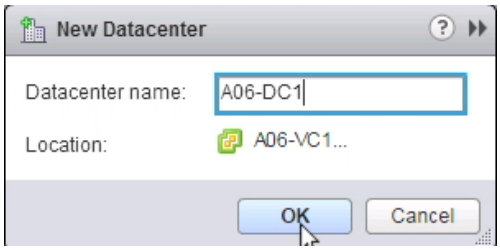
Setup Datacenter, Cluster, DRS and HA

To setup the vCenter Server, complete the following steps:

1. In the vSphere Web Client, navigate to the vCenter Inventory Lists > Resources > vCenter Servers.
2. Select the vCenter instance.
3. Go to Actions in the toolbar and select **New Datacenter** from the drop-down.

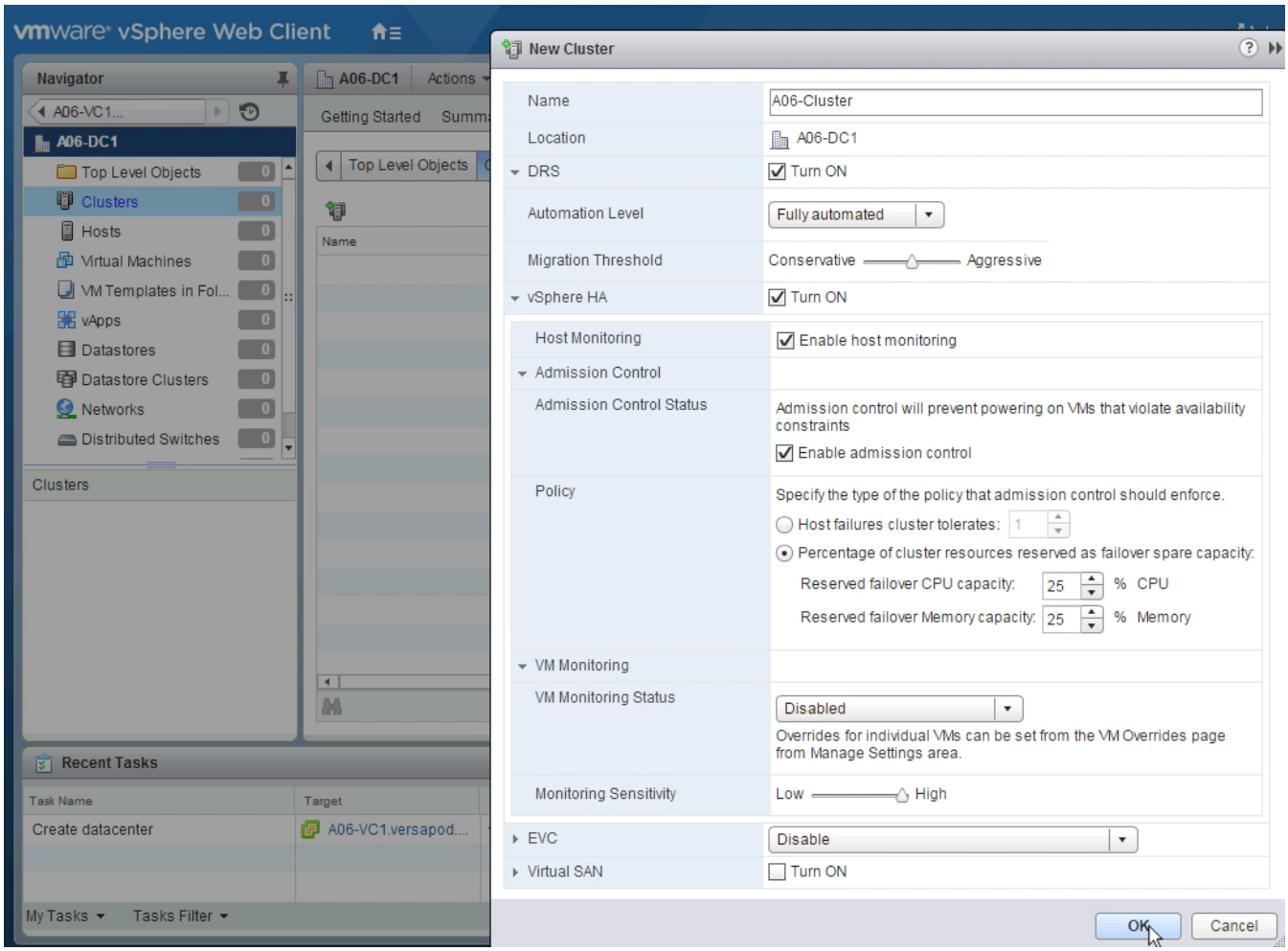


4. Enter a name for the datacenter and click **OK**.



5. Make sure the system takes to the newly created Datacenter. Go to Actions in the toolbar and select **New Cluster** from the drop-down.

6. In the New Cluster window, provide a cluster name, enable DRS, vSphere HA and Host monitoring.



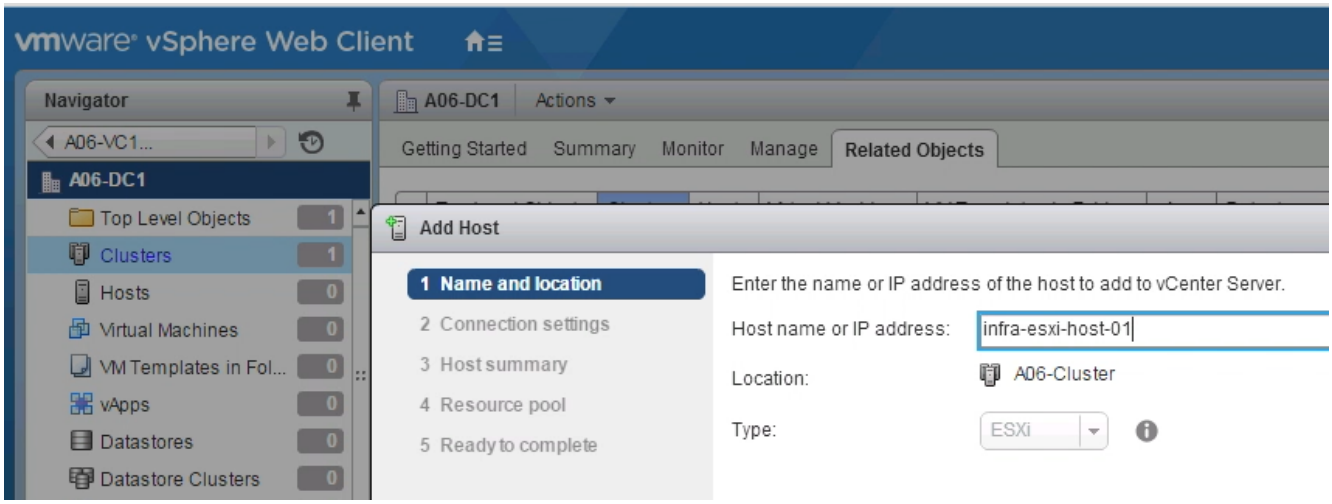
7. Click **OK**.

If mixing Cisco UCS B or C-Series M2, M3 or M4 servers within a vCenter cluster, it is necessary to enable VMware Enhanced vMotion Compatibility (EVC) mode. For more information about setting up EVC mode, refer to Enhanced vMotion Compatibility (EVC) Processor Support.

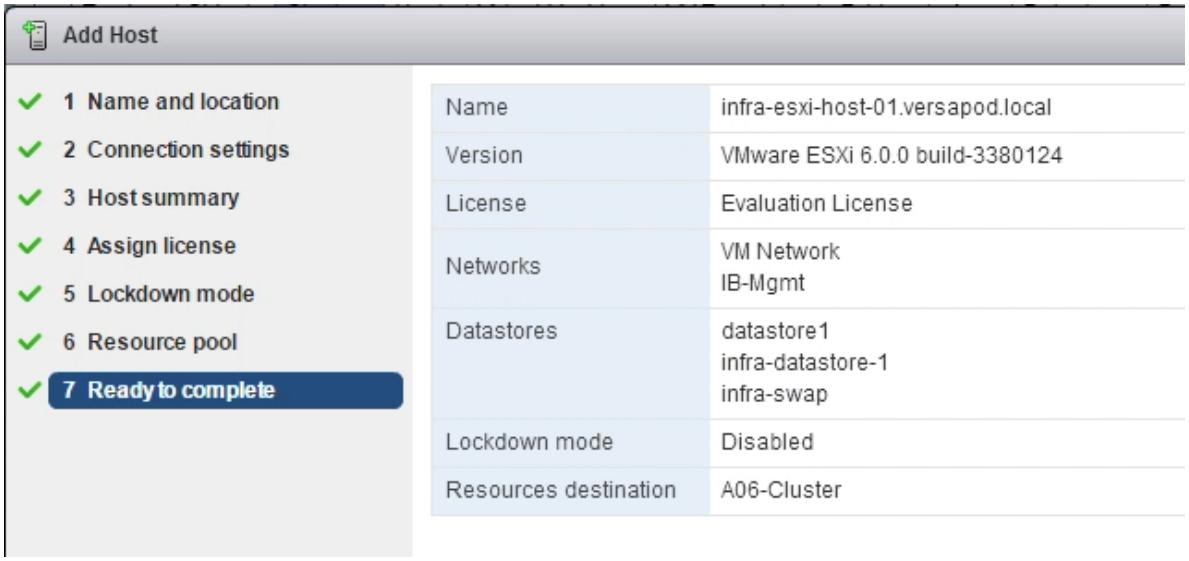
Add Hosts to the Cluster

To add a host to the newly created Cluster, complete the following steps:

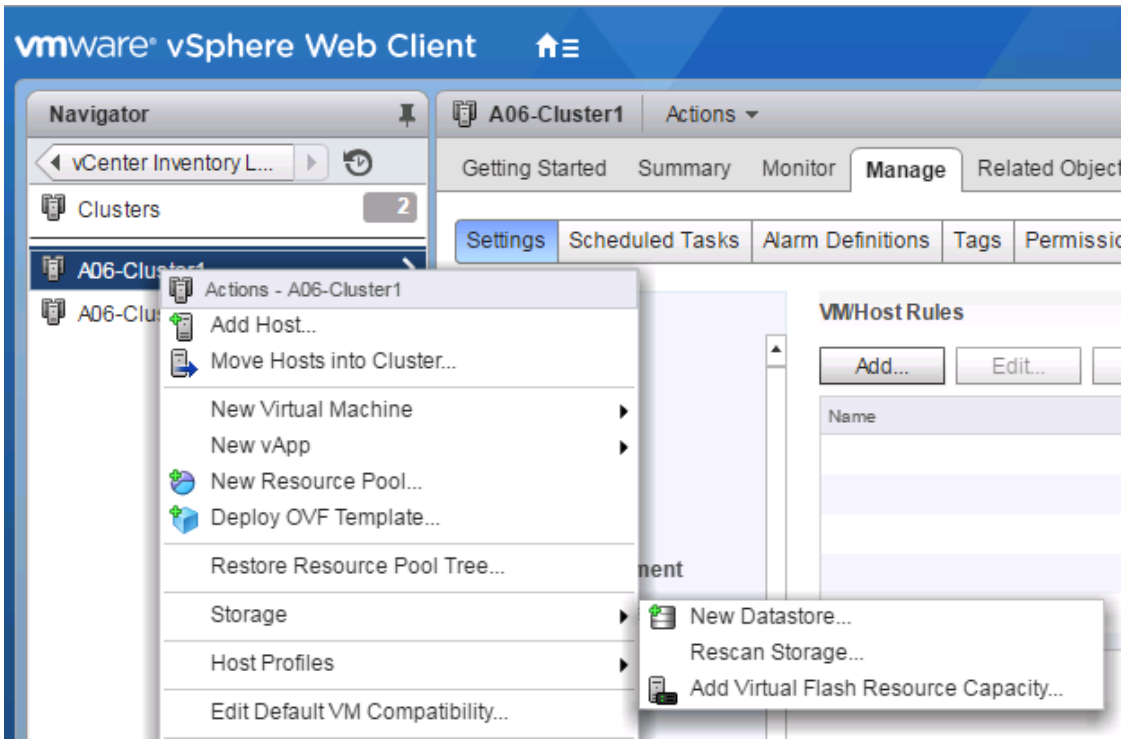
1. Select the newly created cluster in the left.
2. Go to Actions in the menu bar and select **Add Host** from the drop-down list.
3. In the Add Host window, in the Name and Location screen, provide the IP address or FQDN of the host.



4. In the Connection settings screen, provide the root access credentials for the host.
5. Click **Yes** to accept the certificate.
6. In the Host summary screen, review the information and click **Next**.
7. Assign a license key to the host Click **Next**.
8. In the Lockdown mode screen, select the appropriate lockdown mode. For this validation, the lockdown mode was set to Disabled. Click **Next**.
9. In the Resource pool screen, click **Next**.
10. In the Ready to complete screen, review the summary and click **Finish**.



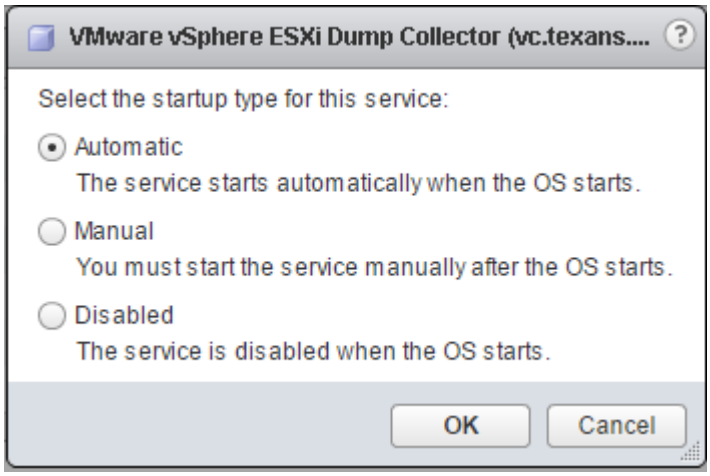
11. Repeat this procedure to add other Hosts to the cluster.
12. In vSphere, in the left pane right-click the newly created cluster, and under Storage click **Rescan Storage**.



ESXi Dump Collector Setup for iSCSI Hosts (IBM V9000 Only)

ESXi hosts booted with iSCSI need to be configured with ESXi dump collection. The Dump Collector functionality is supported but the vCenter but is not enabled by default on the vCenter Appliance.

1. In the vSphere web client, select **Home**.
2. In the center pane, click **System Configuration**.
3. In the left hand pane, select Services and select **VMware vSphere ESXi Dump Collector**.
4. In the Actions menu, choose **Start**.
5. In the Actions menu, click **Edit Startup Type**.
6. Select **Automatic**.



7. Click **OK**.

8. Select Home > Hosts and Clusters.

9. Expand the DataCenter and Cluster.

10. For each ESXi host, right-click the host and select **Settings**. Scroll down and select **Security Profile**. Scroll down to Services and select **Edit**. Select **SSH** and click **Start**. Click **OK**.

11. SSH to each ESXi hosts and use root for the user id and the associated password to log into the system. Type the following commands to enable dump collection:

```
esxcli system coredump network set --interface-name vmk0 --server-ipv4
<vcenter-ip> --server-port 6500
esxcli system coredump network set --enable true
esxcli system coredump network check
```

12. **Optional**: Turn off SSH on the host servers.

Cisco ACI – Virtual Machine Networking

This deployment guide covers both APIC-controlled VMware VDS as well as APIC-controlled Cisco AVS in VXLAN switching mode. Customers can choose to deploy any of these two distributed switching architecture and the customers can also choose to deploy both the switching architectures preferable on different ESXi hosts at the same time. In this deployment, both Cisco AVS and VMware VDS were deployed at the same time on different ESXi hosts.

Deploying VM Networking for vSphere Distributed Switch (VDS)

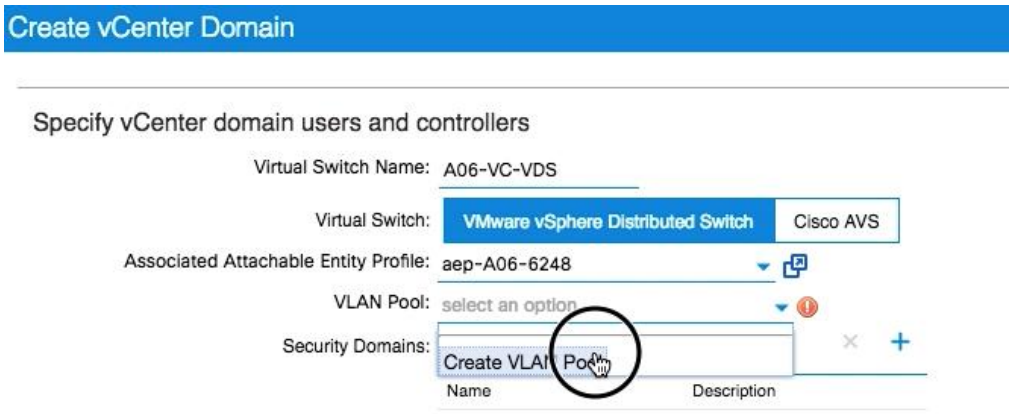
The VMware VDS is a distributed Virtual Switch (DVS) that uses VLANs for network separation and is included in vSphere with Enterprise Plus licensing. For installing the VDS in this VersaStack, complete the following steps:

To add the VDS in the APIC Advanced GUI, complete the following steps:

1. Log into the APIC Advanced GUI using the admin user.
2. At the top, click **VM Networking**.
3. In the left pane, select **VMware**.
4. In the right pane, click **+** to add a vCenter Domain.
5. In the Create vCenter Domain window, enter a Virtual Switch Name. The name used in the deployment below is A06-VC-VDS.
6. Make sure VMware vSphere Distributed Switch is selected.
7. Select the aep-<UCS> (aep-A06-6248) from the Associated Attachable Entity Profile drop-down list to associate the VDS with the UCS Physical Domain.

Create VLAN Pool

1. From the VLAN Pool drop-down list select **Create VLAN Pool**.

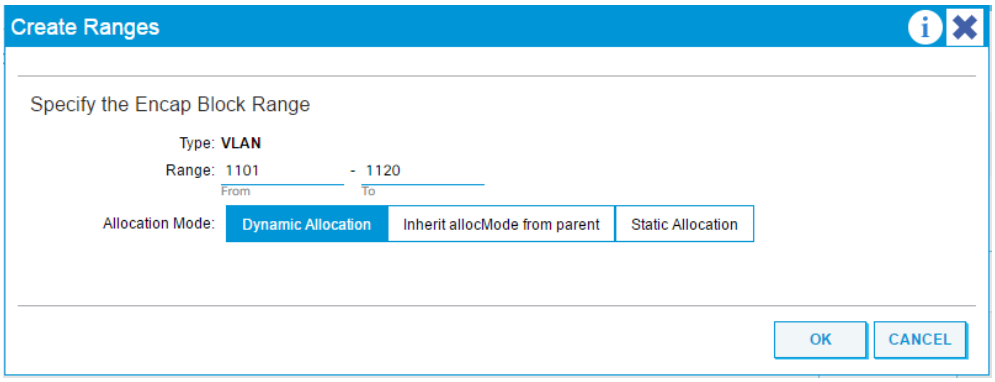


2. In the Create VLAN Pool window, name the pool vp-<Virtual Center>-VDS-Pool. The name used in this deployment is vp-A06-VDS-Pool.

3. Make sure Dynamic Allocation is selected. Click **+** to add a VLAN range.

4. In the Create Ranges window, enter the VLAN range that was entered in the Cisco UCS for the APIC-VDS VLANs. Refer to Table 12 to find the range.

5. Select the option **Dynamic Allocation** for Allocation Mode.



6. Click **OK** to create the VLAN range.

7. Click **SUBMIT** to create the VLAN Pool.

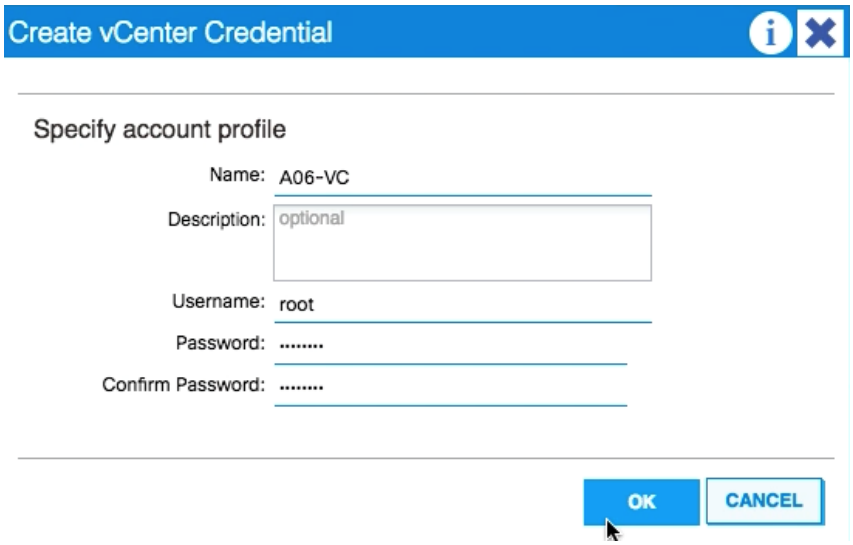
Create vCenter Credentials

1. Click the **+** sign to the right of vCenter Credentials.

2. In the Create vCenter Credential window, for vCenter Credential Name, <vcenter-name>-VDS-Creds. The name used for this deployment is A06-VC.

3. For Username enter root.

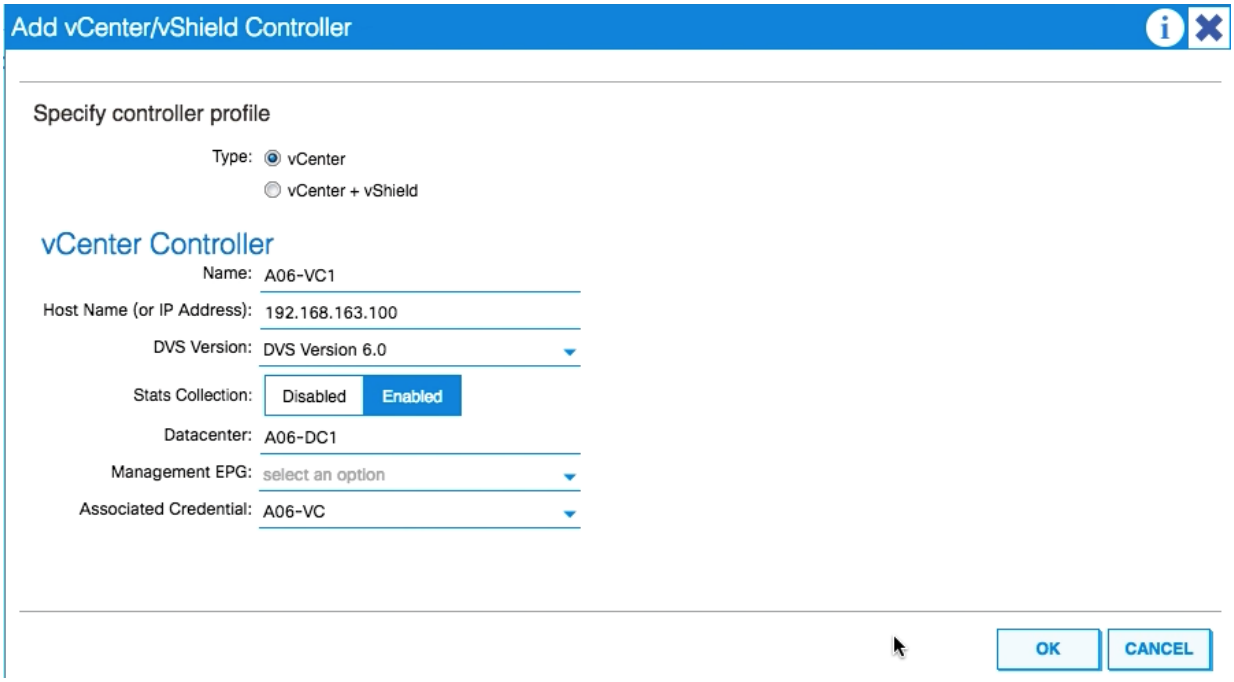
4. Enter and confirm the password for root.



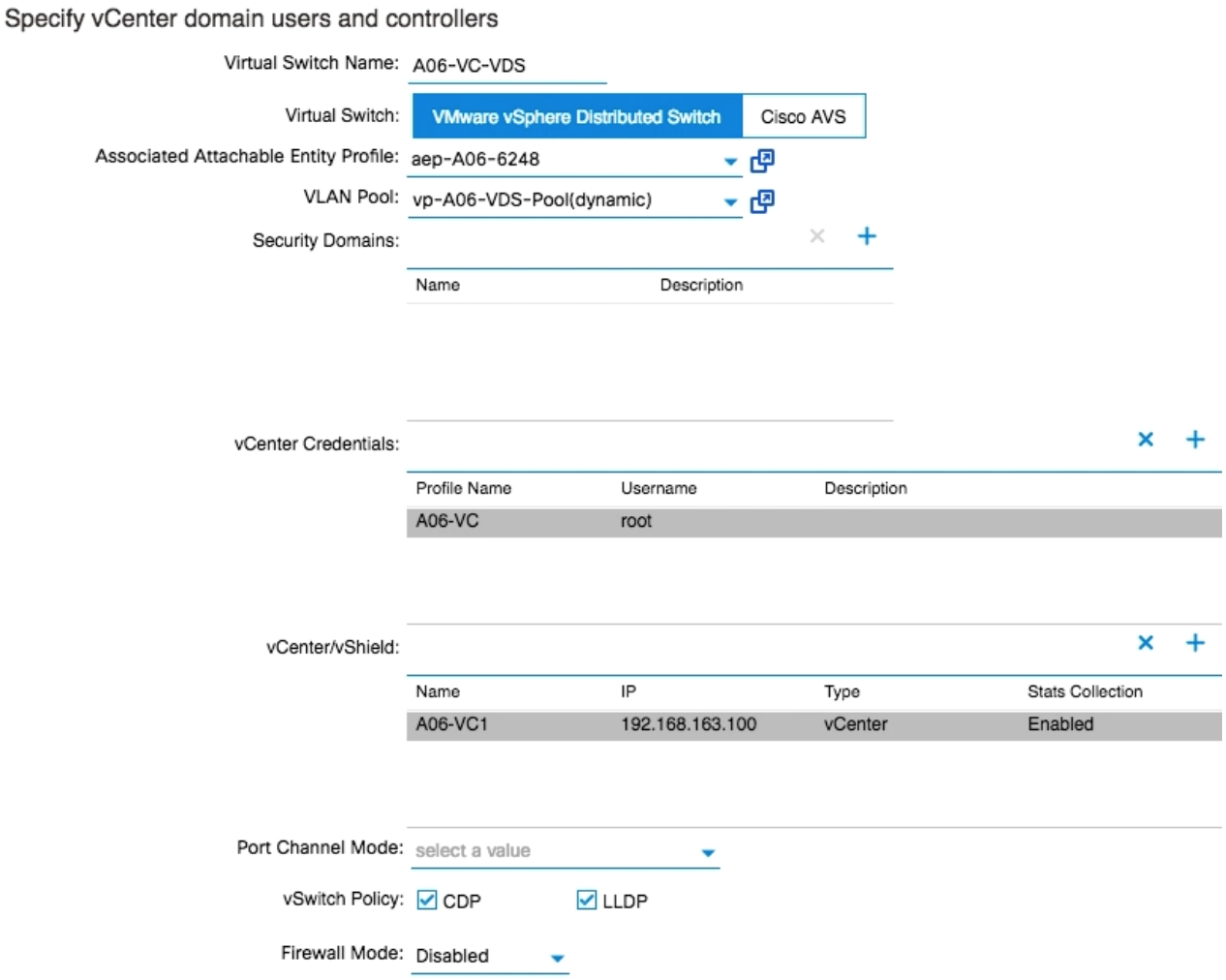
5. Click **OK** to complete adding the credential.

Add vCenter Server

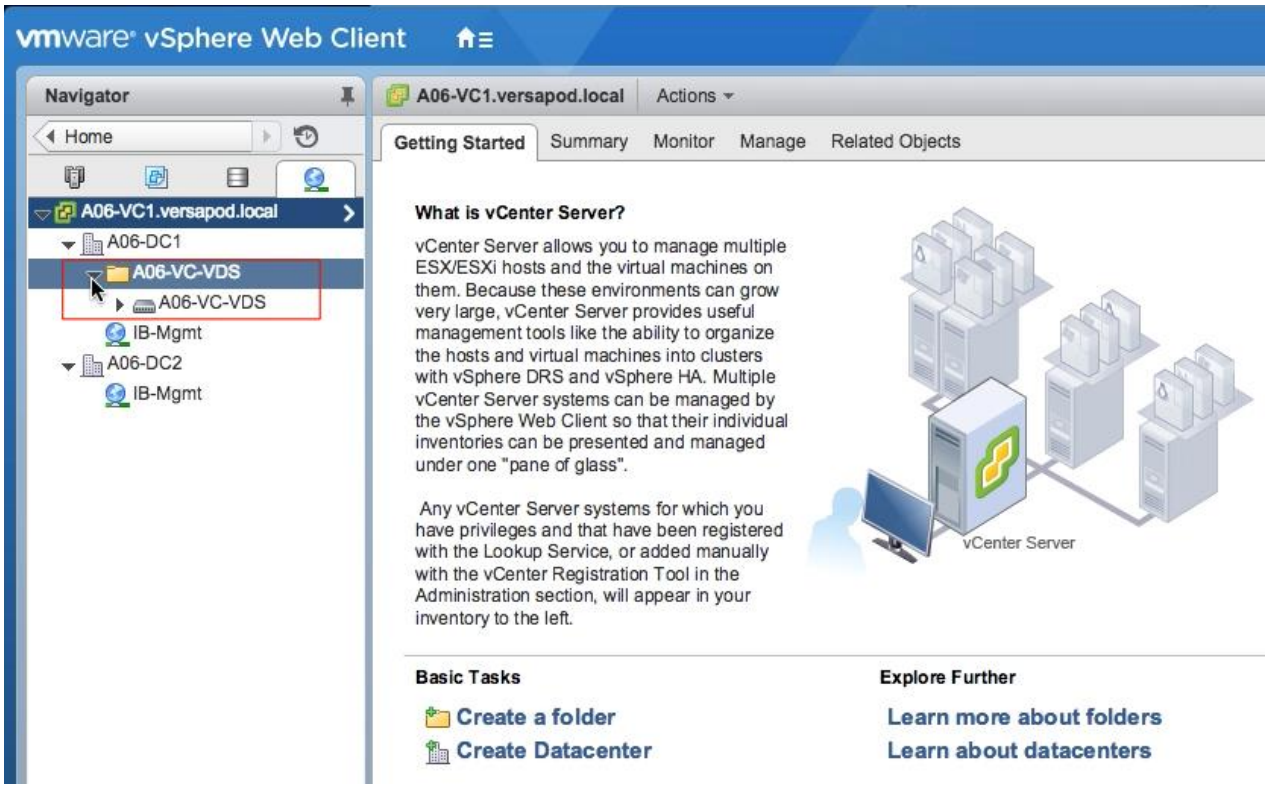
1. Click **+** on the right of vCenter/vShield to add the vCenter server for APIC.
2. In the Add vCenter/vShield Controller window, select **Type vCenter**.
3. Enter a name for the vCenter. The name used in this deployment is A06-VC1.
4. Enter the vCenter IP Address or Host Name.
5. For DVS Version, select DVS Version 6.0
6. Enable Stats Collection.
7. For Datacenter, enter the exact vCenter Datacenter name (A06-DC1).
8. Do not select a Management EPG.
9. For vCenter Credential Name, select the vCenter credentials created in the last step (A06-VC).



10. Click **OK** to add the vCenter Controller.
11. In the Create vCenter Domain Window, select the MAC Pinning+ as the Port Channel Mode.
12. Check the check boxes for both CDP and LLDP vSwitch Policy.
13. Select the **Disabled** for the Firewall Mode.



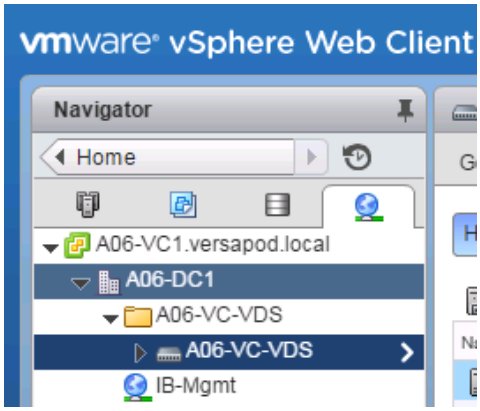
14. Click **SUBMIT** to complete creating the vCenter Domain and adding the VDS.
15. Log into the vCenter vSphere Web Client and navigate to Networking.
16. A distributed switch should have been added.



Add VMware ESXi Host Servers to VDS

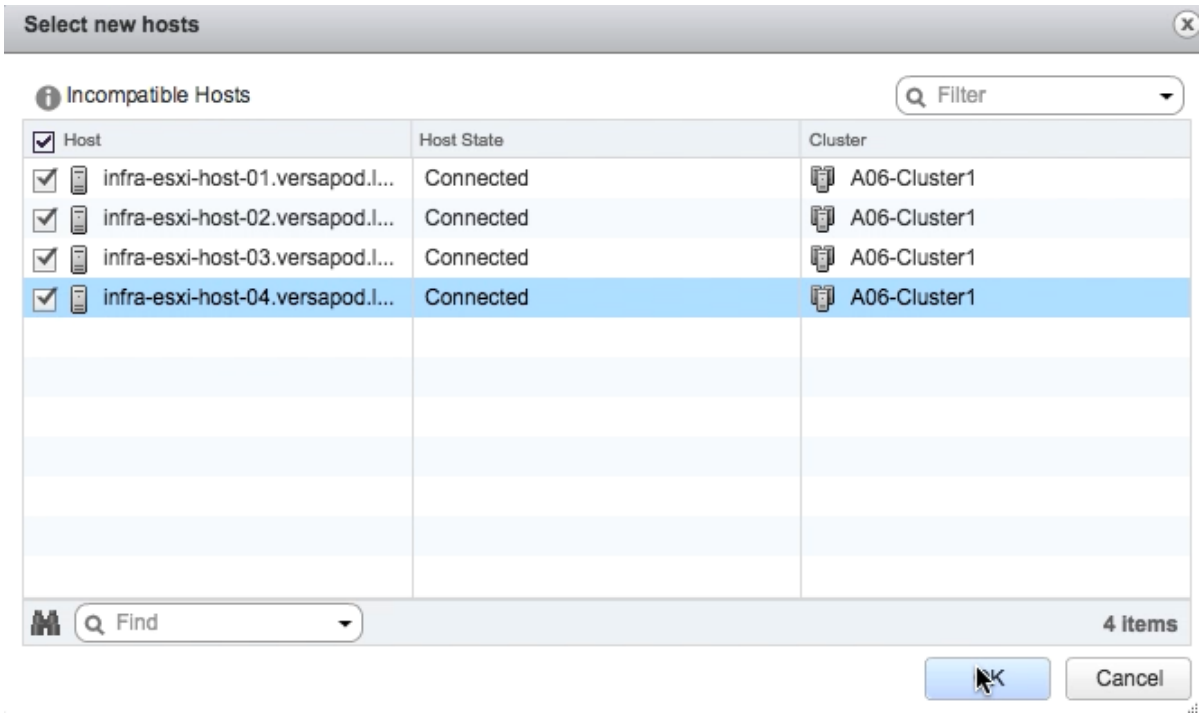
To add the VMware ESXi Hosts to the VDS, complete the following steps:

1. Log into the vSphere Web Client.
2. From the Home screen, select **Networking** under Inventories.
3. In the left, expand the Datacenter and the VDS folder. Select the **VDS switch**.



4. Right-click on the VDS switch and select **Add and manage hosts**.
5. In the Add and Manage Hosts window, make sure the option **Add hosts** is selected; click **Next**.
6. Click **+** to add New hosts.

7. In the Select new hosts window, select all of the relevant ESXi hosts.



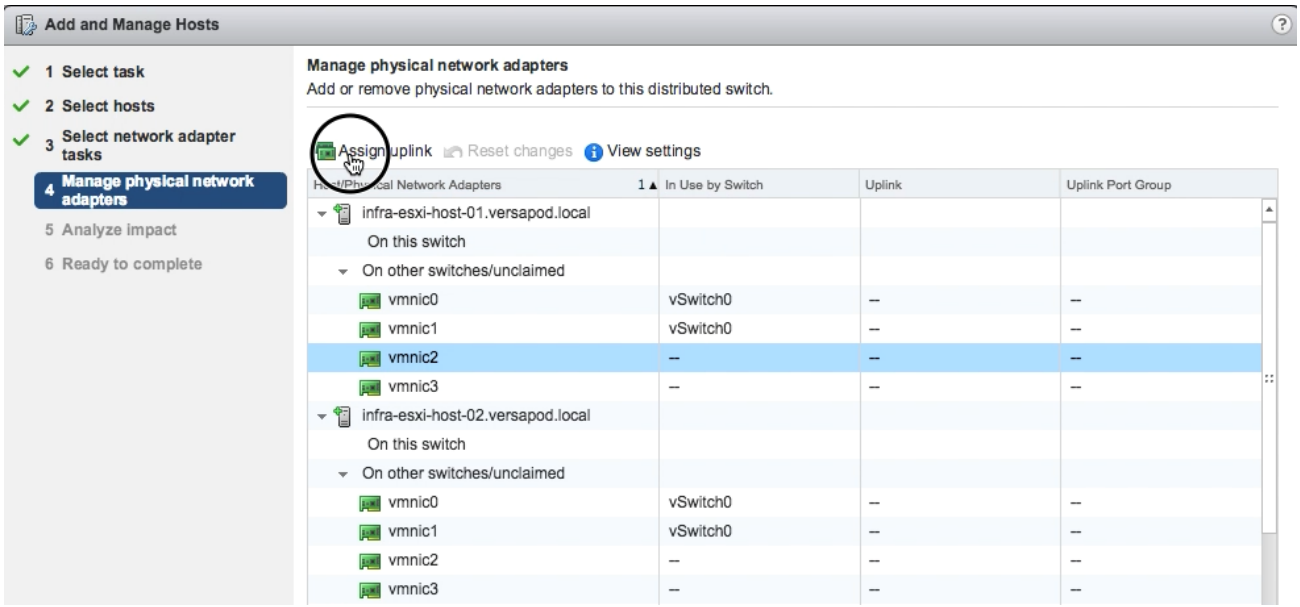
8. Click **OK** to complete the host selection.

9. Click **Next**.

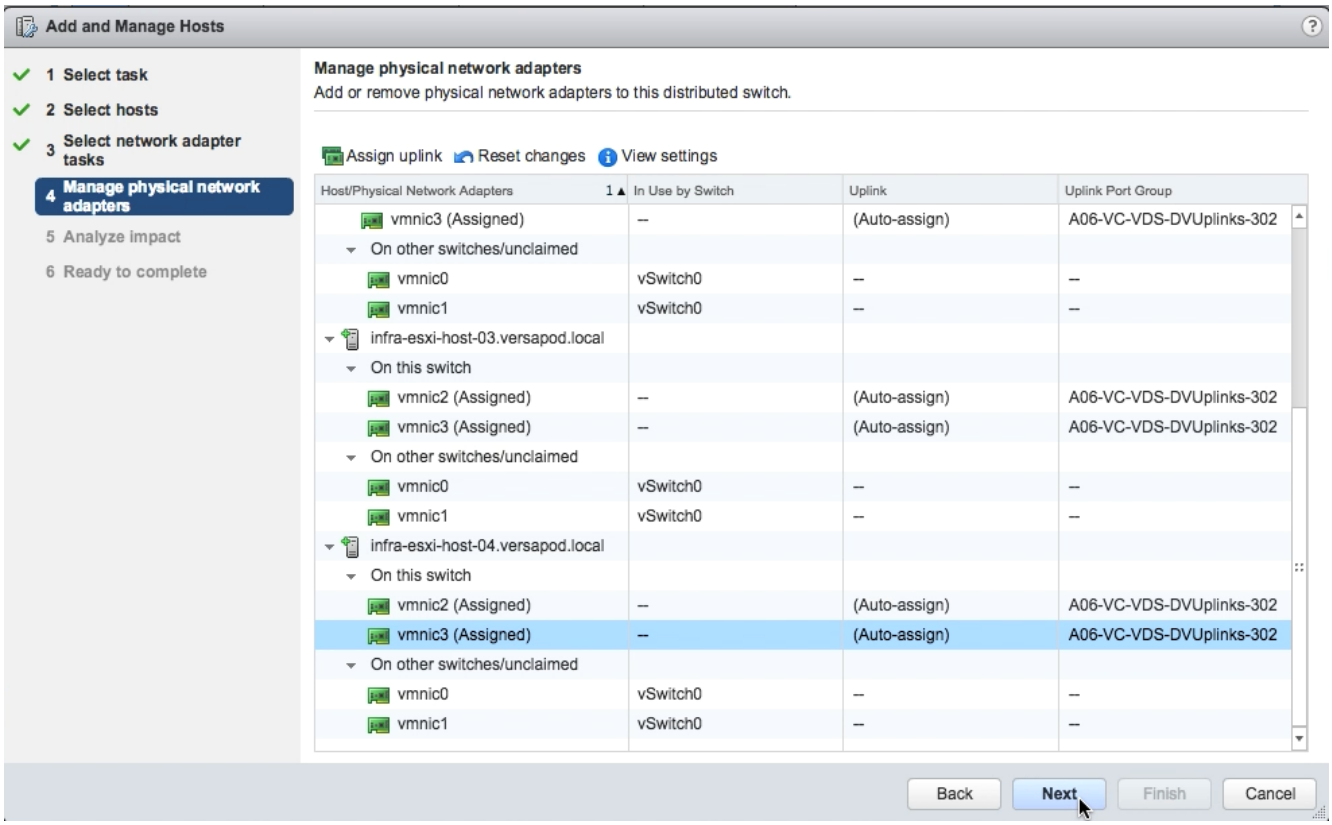
10. Select Manage physical adapters.

11. Click **Next**.

12. On the hosts, select the appropriate vmnics (vmnic2 and vmnic3), click **Assign uplink**, and then click **OK**.



13. Repeat this process until all vmnics (2 per host) have been assigned.



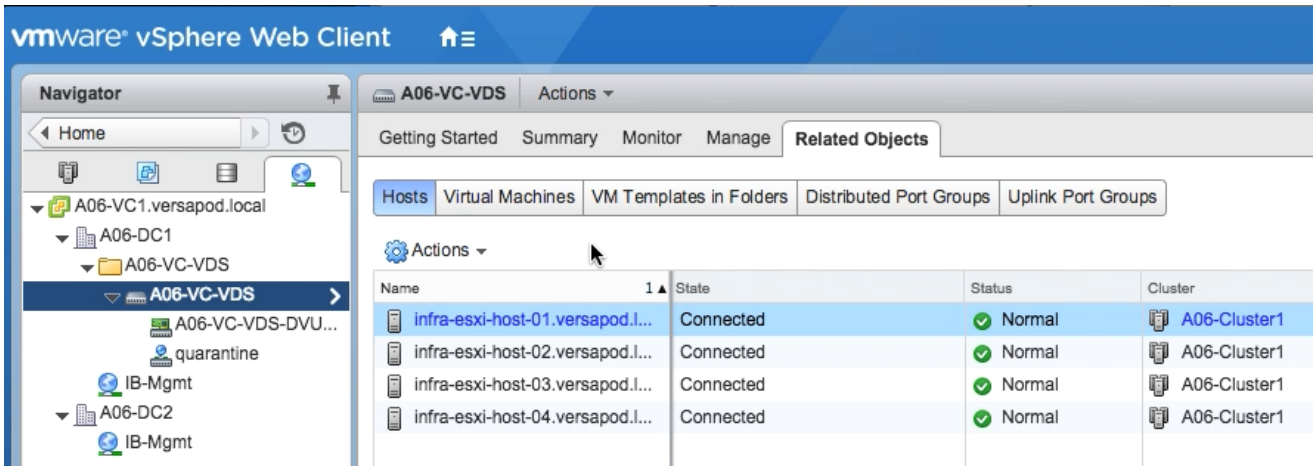
14. Click **Next**.

15. Verify that these changes will have no impact and click **Next**.

16. Click **Finish** to complete adding the ESXi hosts to the VDS.

17. With the VDS selected, in the center pane select the Related Objects tab.

18. Under Related Objects, select the **Hosts** tab. Verify the ESXi hosts are now part of the VDS.



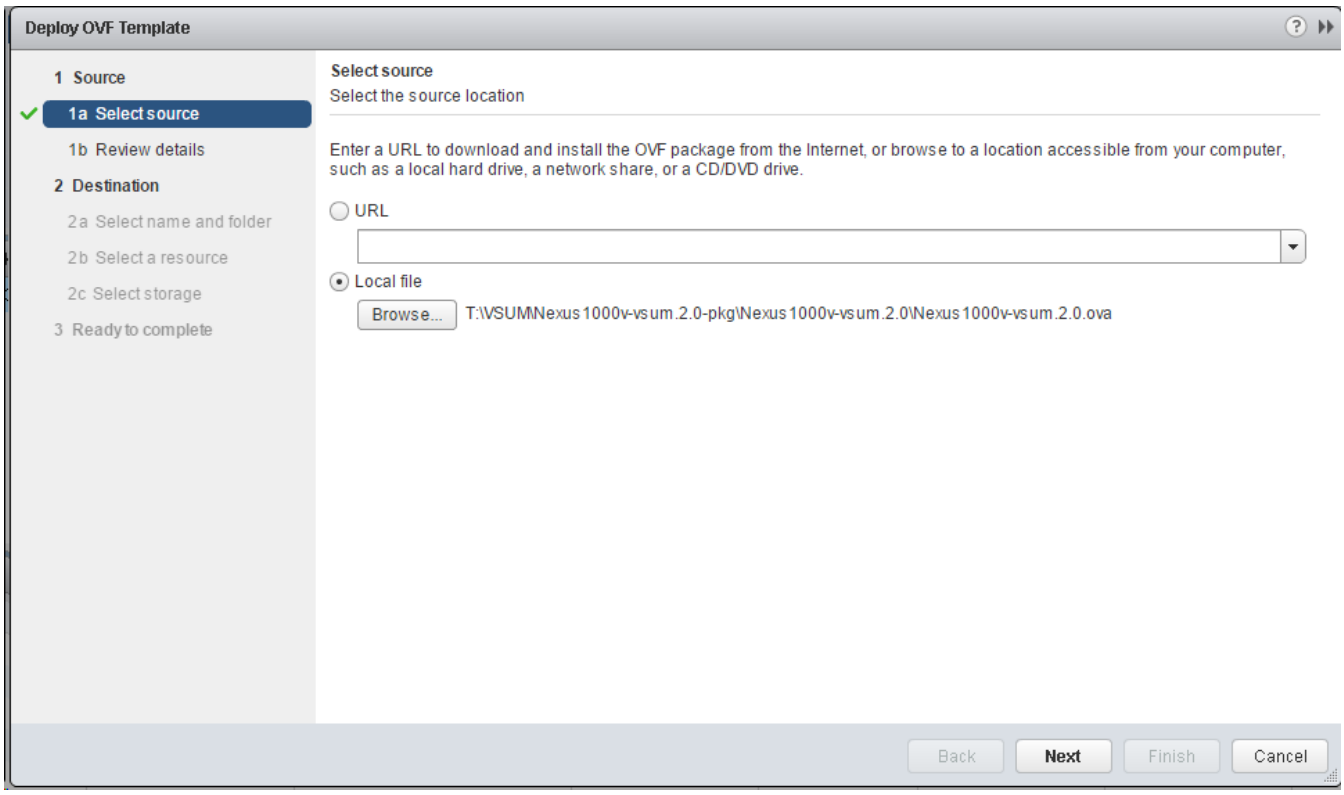
Deploying VM Networking for Cisco Application Virtual Switch (AVS)

The AVS in VXLAN switching mode uses VXLANs for network separation. For installing the AVS in this VersaStack environment, complete the following steps:

Install Cisco Virtual Switch Update Manager (VSUM) Virtual Appliance

To install VSUM into your VersaStack Management Cluster, complete the following steps:

1. Download and unzip the VSUM Release 2.0 .zip file from Cisco VSUM 2.0 Download.
2. In the Nexus1000v-vsum.2.0.pkg folder that is unzipped from the downloaded zip, unzip the Nexus1000v-vsum.2.0.zip file.
3. Log into vSphere Web Client as the VersaStack Admin user.
4. From the Home screen, in the left pane, select **VMs and Templates**.
5. Select the vCenter in the left and using the Actions pulldown in the center pane, select **Deploy OVF Template**.
6. If a Security Prompt pops up, click **Allow** to allow the Client Integration Plugin to run.
7. In the Deploy OVF Template window, select Local file, then Browse and browse to the Nexus1000v-vsum.2.0.ova file downloaded and unzipped above.
8. Select the file and click **Open**.

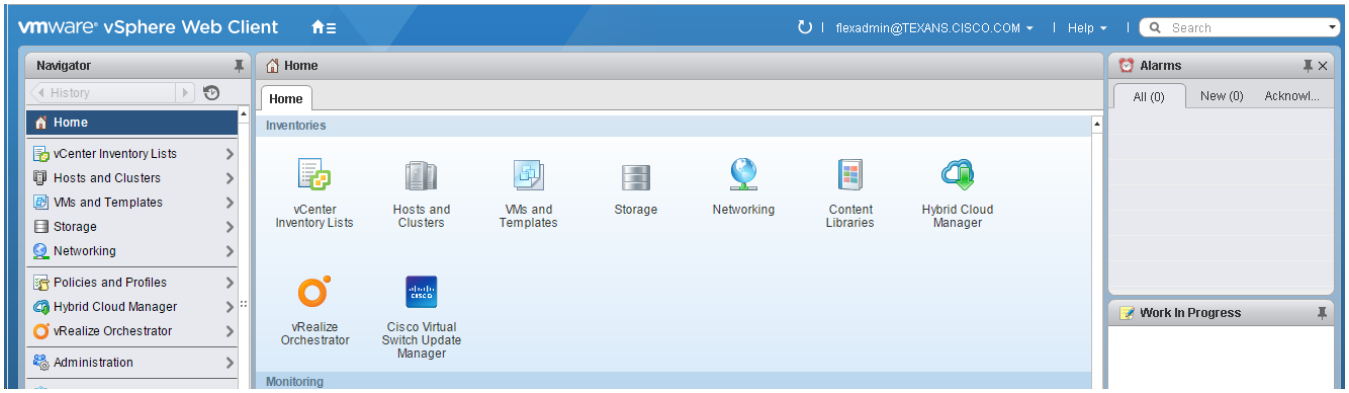


9. Click **Next**.

10. Review the details and click **Next**.
11. Click **Accept** to accept the License Agreement and click **Next**.
12. Give the VM a name and select the appropriate Datacenter (A06-DC1).
13. Click **Next**.
14. Select the appropriate Cluster (A06-Cluster1) and click **Next**.
15. Select infra-datastore-1 and make sure the **Thin Provision virtual disk format** is selected. Click **Next**.
16. Make sure the **IB-Mgmt Network** is chosen and click **Next**.
17. Fill in all IP, DNS, and vCenter properties for the VSUM Appliance and click **Next**.

The VSUM IP address should be in the IB-MGMT subnet.

18. Review all the values and click **Finish** to complete the deployment of the VSUM Appliance.
19. In the left pane, expand the vCenter and Datacenter. Right-click the **VSUM VM** and select Power > Power On.
20. Right-click the VSUM VM again and select **Open Console**. When a login prompt appears, close the console.
21. Log out and Log back in to the vSphere Web Client.
22. Verify that Cisco Virtual Switch Update Manager now appears in the center pane under Inventories.



Add VM Networking for AVS in APIC

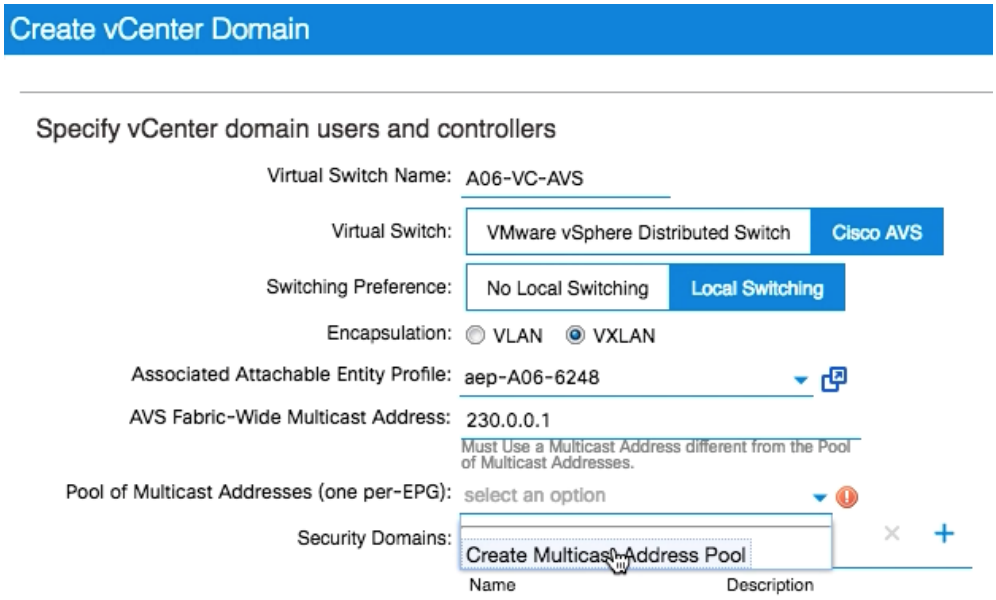
To add the AVS in the APIC Advanced GUI, complete the following steps:

1. Log into the APIC Advanced GUI using the admin user.
2. At the top, select **VM Networking**. In the left pane, select **VMware**.
3. From VM Networking > Inventory > VMware, on the right, click + to add a vCenter Domain.
4. In the Create vCenter Domain window, enter a Virtual Switch Name. A suggested name is <vcenter-name>-AVS. Select the **Cisco AVS**.

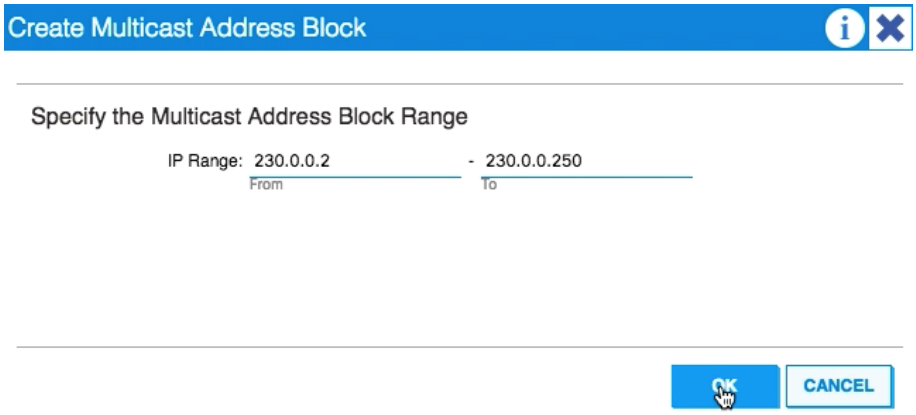
5. For Switching Preference, select **Local Switching**.
6. For Encapsulation, **select VXLAN**.
7. For Associated Attachable Entity Profile, select aep-<UCS Name> (aep-A06-6248).
8. For the AVS Fabric-Wide Multicast Address, enter a Multicast Address. For this deployment, 230.0.0.1 was used.

Create VxLAN Pool

1. For the Pool of Multicast Addresses (one per-EPG), use the drop-down list to select **Create Multicast Address Pool**.



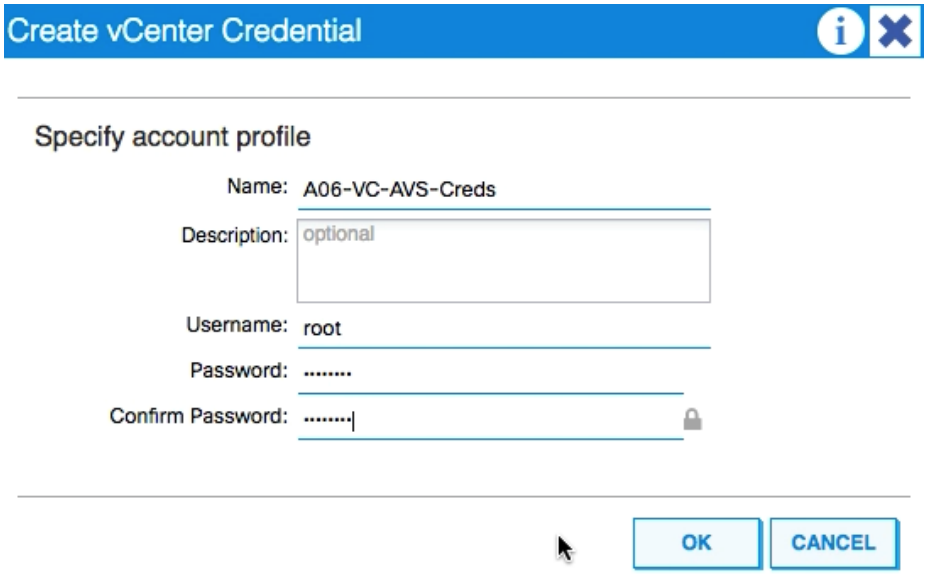
2. Name the pool map-<vcenter-name>-AVS.
3. Click **+** to create an Address Block.
4. Enter a multicast address IP Range. The range used in this validation is 230.0.0.2 to 230.0.0.250.



5. Click **OK** to complete creating the Multicast Address Block.
6. Click **SUBMIT** to complete creating the Multicast Address Pool.

Create vCenter Credentials

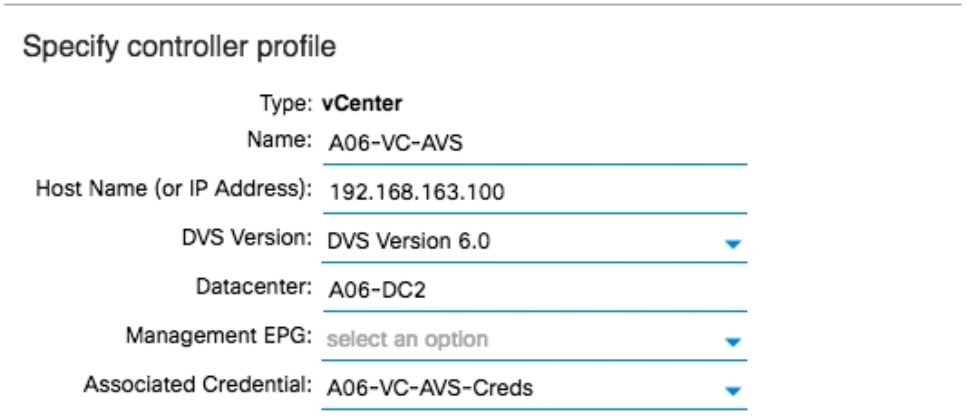
1. Click **+** to add vCenter Credentials.
2. In the Create vCenter Credential window, name the account profile <vcenter-name>-AVS-Creds. Name used in this deployment is A06-VC-AVS-Creds.
3. For Username, enter root.
4. Enter and confirm the use root password.



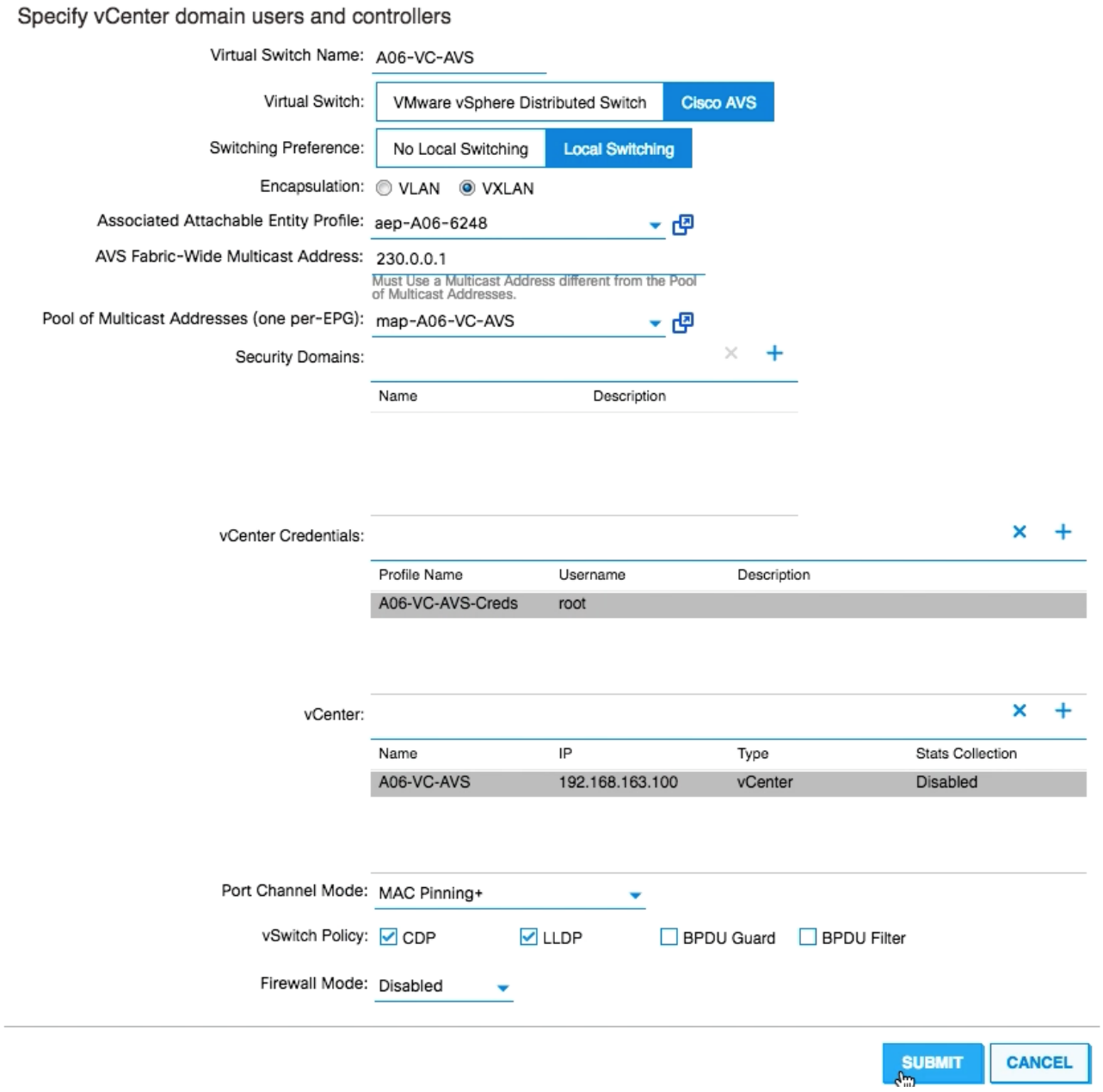
5. Click **OK** to complete adding the vCenter credentials.

Add vCenter Server

1. Click **+** to add the vCenter server for APIC to vCenter communication.
2. In the Create vCenter Controller window, enter <vcenter-name>-AVS for Name. Name used in this deployment is A06-VC-AVS.
3. Enter the vCenter IP Address or Host Name.
4. For DVS Version, select DVS Version 6.0.
5. For Datacenter, enter the exact vCenter Datacenter name. vCenter Datacenter used in this deployment is A06-DC2.
6. Do not select a Management EPG.
7. For Associated Credential, select <vcenter-name>-AVS-Creds.



8. Click **OK** to complete adding the vCenter Controller.
9. For Port Channel Mode, select MAC Pinning+.
10. For vSwitch Policy, select both CDP and LLDP. Do not select BPDU Guard or BPDU Filter.
11. For Firewall Mode, select Disabled.



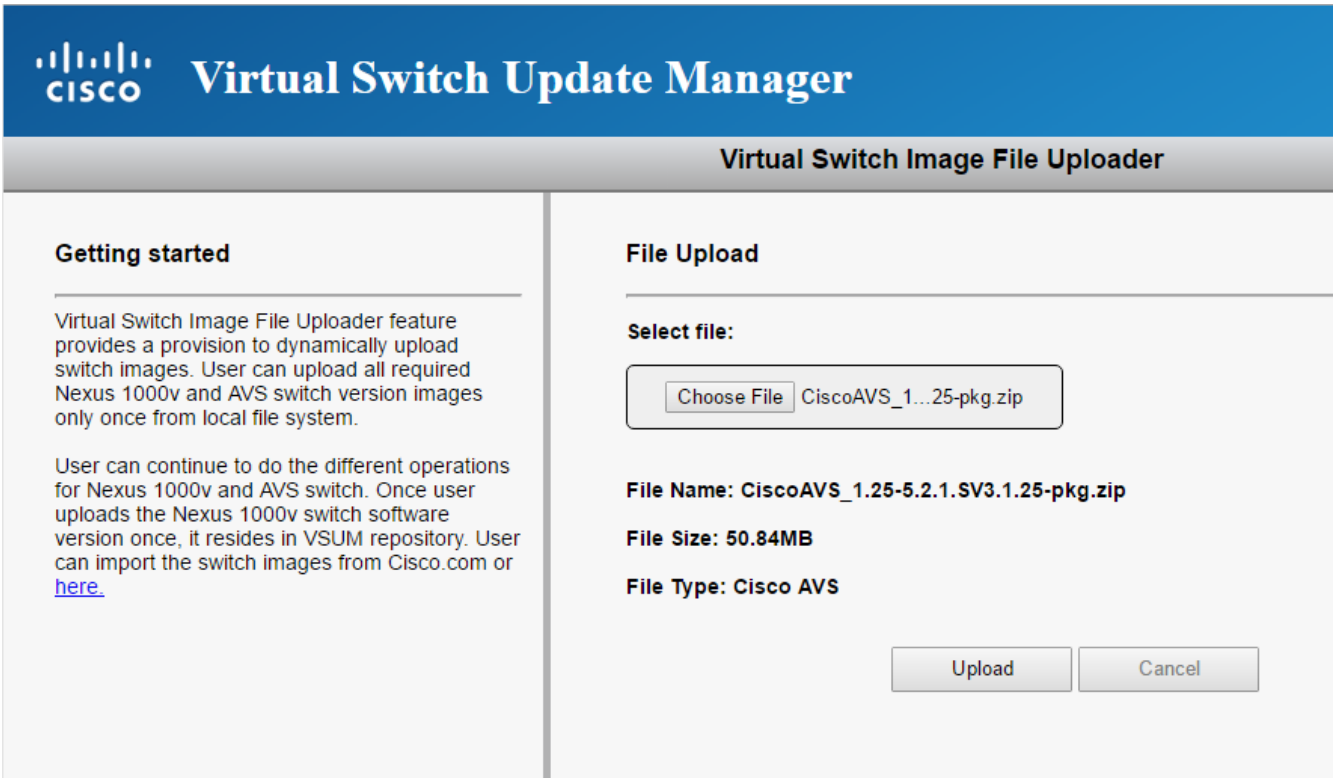
12. Click **SUBMIT** to add Cisco AVS.

Add VMware ESXi Host Servers to AVS

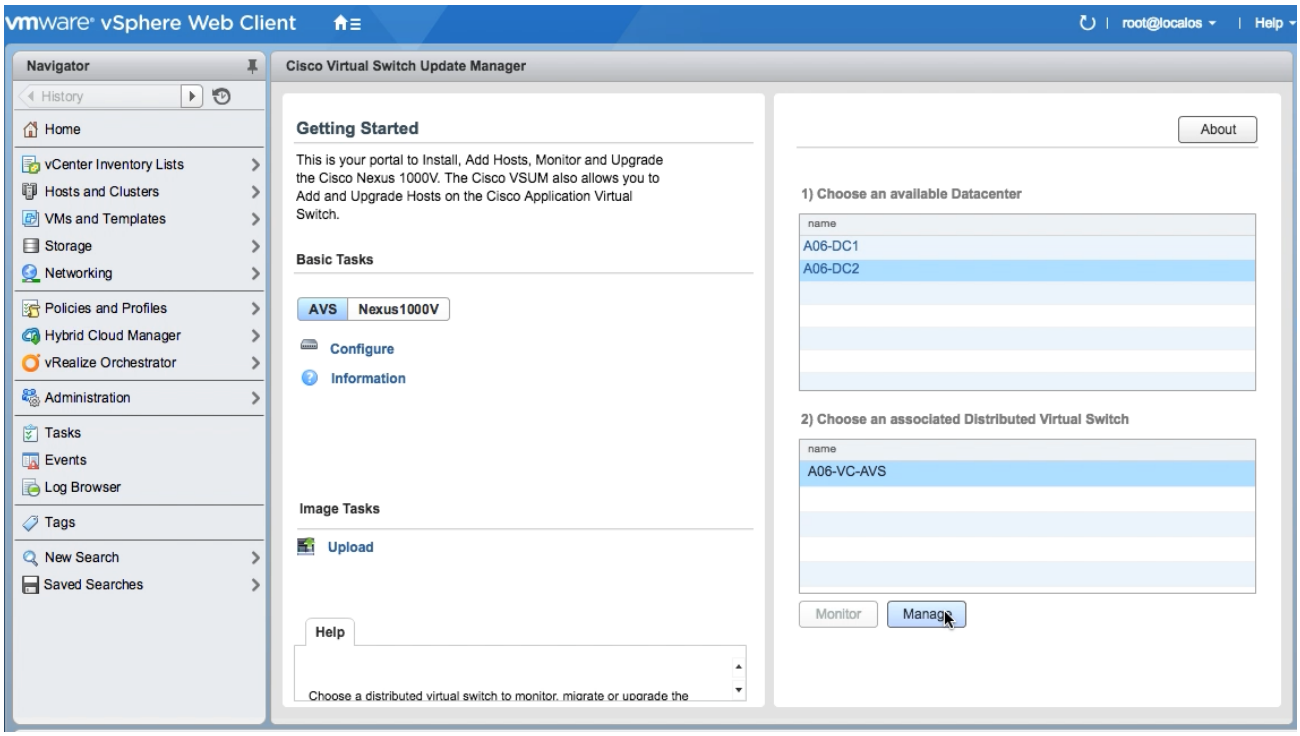
To add the VMware ESXi Hosts to the AVS, complete the following steps:

1. Download Cisco AVS version 5.2(1)SV3(1.25), by going to Cisco AVS Download and navigating to version 5.2(1)SV3(1.25). Download the CiscoAVS_1.25-5.2.1.SV3.1.25-pkg.zip file, but do not unzip it.
2. Log into the vSphere Web Client as the VersaStack Admin.
3. From the Home screen, select **Cisco Virtual Switch Update Manager** under Inventories.
4. Under Basic Tasks, select AVS.

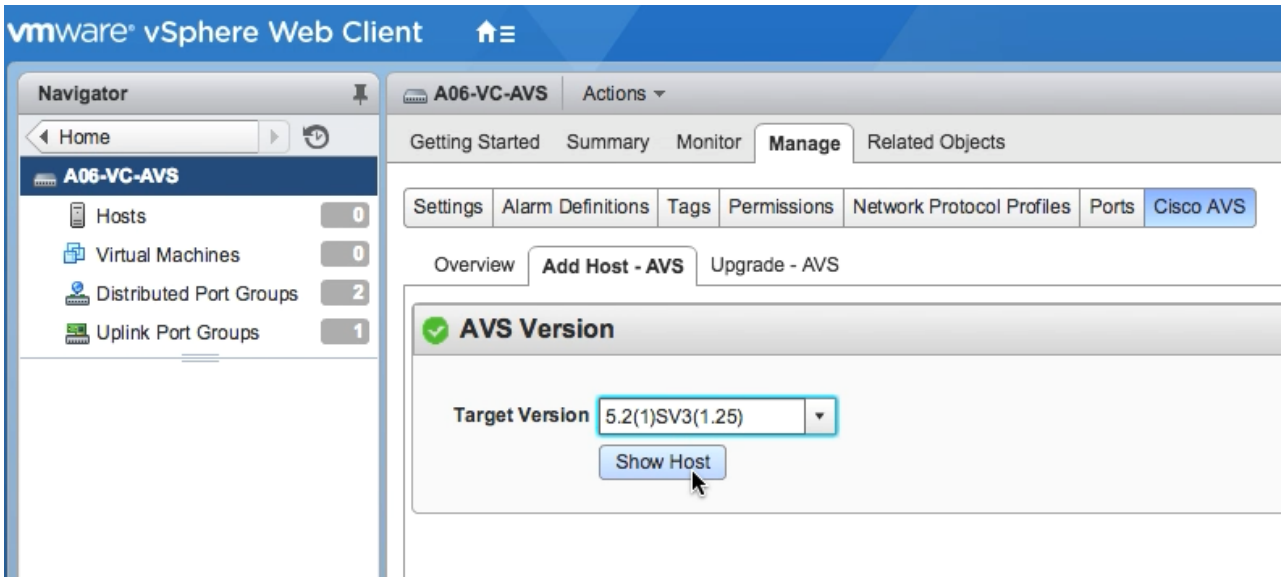
5. Under Image Tasks, select Upload.
6. On the right under Upload switch image, click **Upload**.
7. Click Choose File.
8. Navigate to the CiscoAVS_1.25-5.2.1.SV3.1.25-pkg.zip file, select it and click **Open**.



9. Click **Upload** to upload the file.
10. Click **OK**.
11. Close the Cisco Virtual Switch Update Manager tab in the browser and return to vSphere Web Client.
12. Click Refresh at the lower right. CiscoAVS_1.25 should now appear in the list of Manage Uploaded switch images.
13. In the left pane under the Basic Tasks, select AVS.
14. Click Configure.
15. On the right, select the A06-DC2 Datacenter.
16. Select the AVS for the Distributed Virtual Switch.

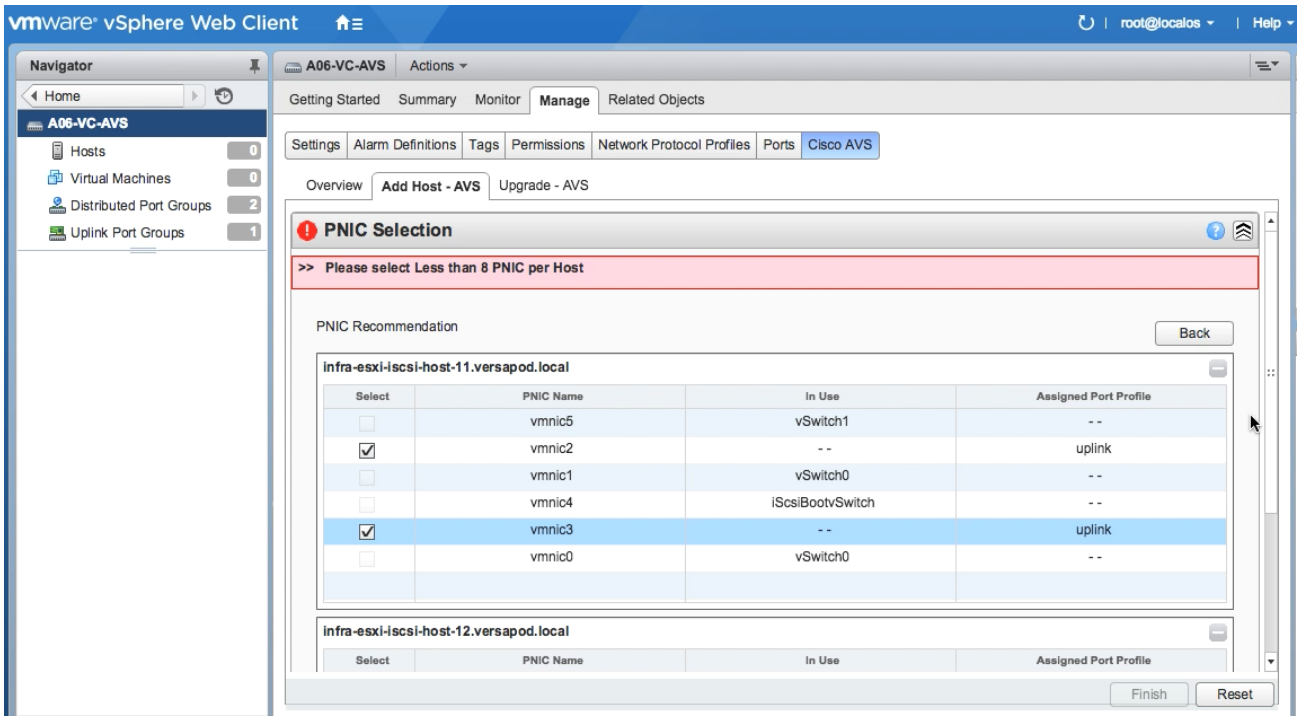


17. Click **Manage**.
18. In the center pane, under Manage, select the Cisco AVS tab.
19. In the center pane, select the Add **Host – AVS** tab.
20. Using the pulldown, select the 5.2(1)SV3(1.25) Target Version. Click **Show Host**.



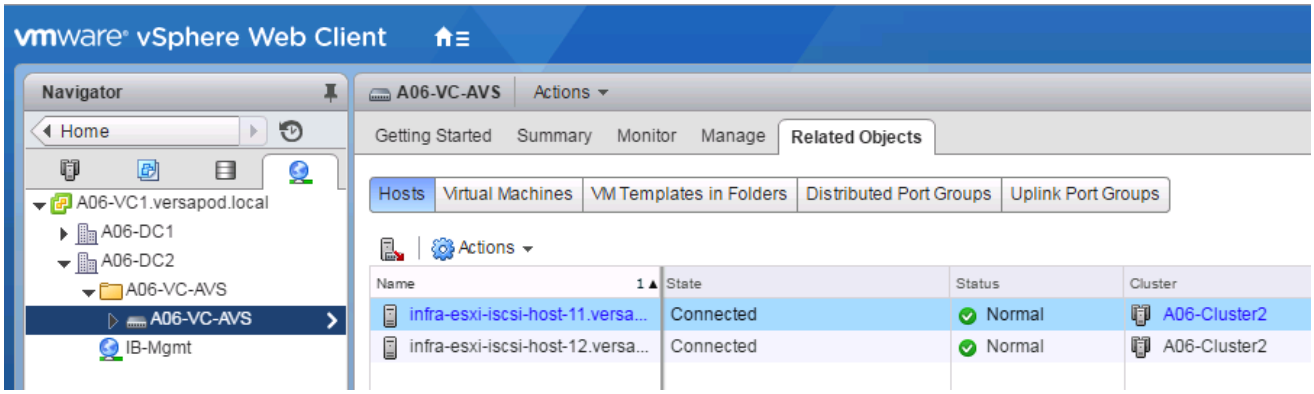
21. Expand VMware Cluster (A06-Cluster2) and select all the relevant ESXi hosts.
22. Click **Suggest**.

23. Under PNIC Selection, select the two vmnics per host set up for AVS. Make sure to select the vmnics for all the hosts.



24. Click **Finish** to install the Virtual Ethernet Module (VEM) on each host and add the host to the AVS. The process might take a few minutes.

25. In the left pane, select Hosts. The ESXi hosts should now show up as part of the AVS.



Add Second VXLAN Tunnel Endpoint (VTEP) to Each ESXi Host for Load Balancing

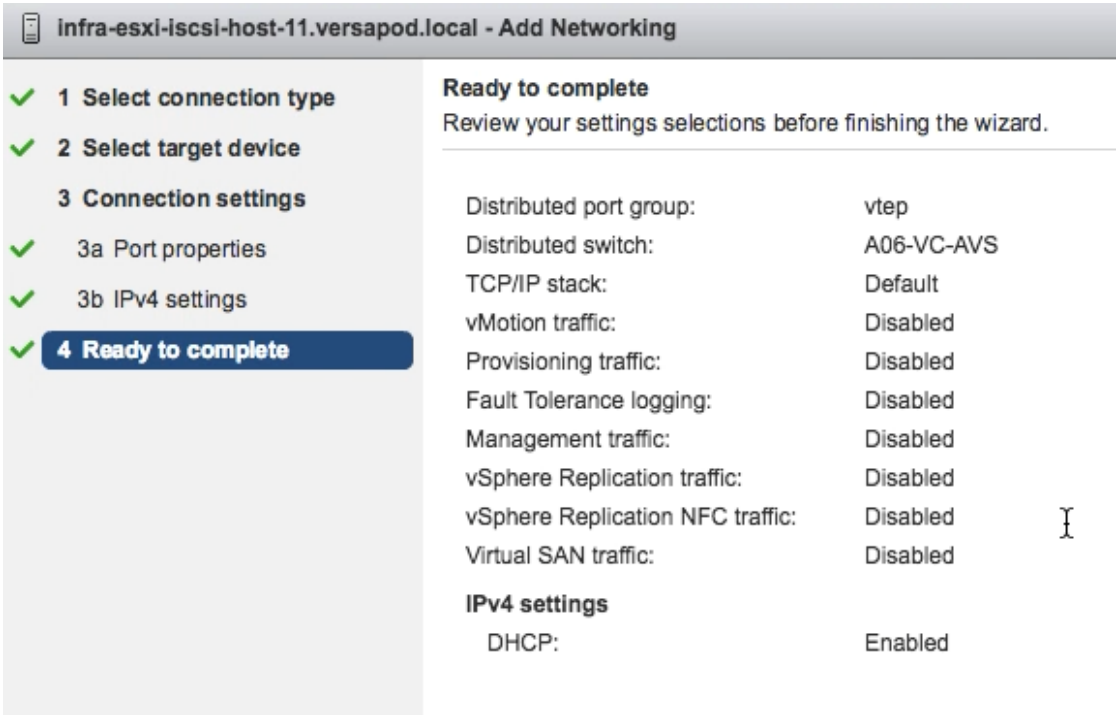
To add a second VTEP to each ESXi host in the Cisco AVS for load balancing, complete the following steps:

1. In the vSphere Web Client, from the Home screen, select **Hosts and Clusters**.

2. In the left pane, expand vCenter, Datacenter, and Cluster. Select the first ESXi host.

3. In the center pane, under the Manage tab, select the Networking tab. Select VMkernel adapters.

4. In the list of VMkernel ports, make sure the vtep VMkernel port has been assigned an IP address in the ACI Fabric system subnet (10.0.0.0/16 by default).
5. Click **+** to add a VMkernel port.
6. In the Add Networking window, make sure VMkernel Network Adapter is selected and click **Next**.
7. Leave Select an existing network selected and click **Browse**.
8. Select vtep and click **OK**.
9. Make sure vtep is now in the text box and click **Next**.
10. Make sure the Default TCP/IP stack is selected. Do not enable any services. Click **Next**.
11. Leave Obtain IPv4 settings automatically selected and click **Next**.



12. Click **Finish** to complete adding the VTEP.
13. Verify that the just added VTEP obtains an IP address in the same subnet as the first VTEP.
14. Repeat this procedure to add a VTEP to all the remaining ESXi hosts.

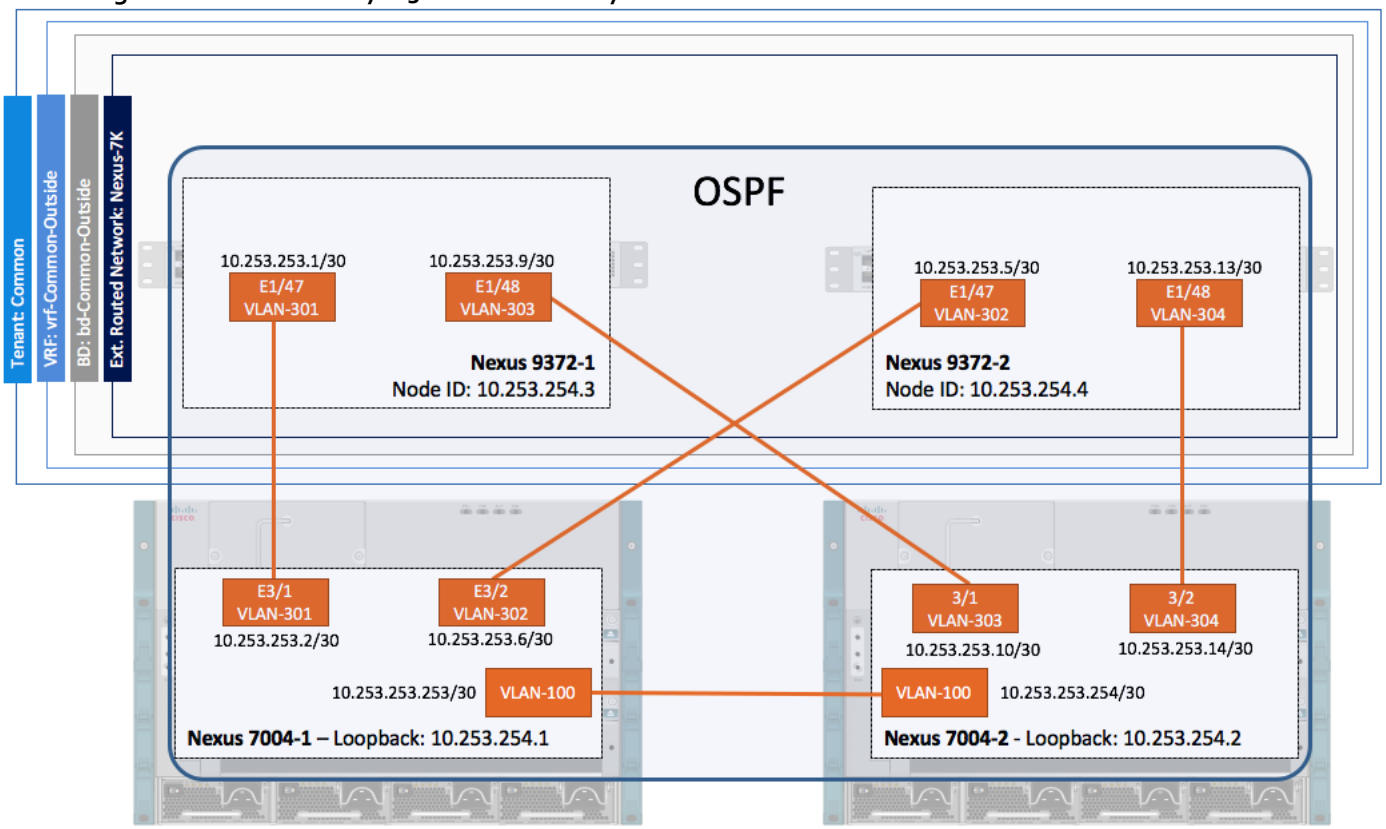
Connectivity to Existing Infrastructure – Shared L3 Out

ACI Shared Layer 3 Out Setup

This section provides a detailed procedure for setting the Shared Layer 3 Out in tenant "common" to connect to Nexus 7000 core switches. The configuration utilizes four interfaces between the pair of the ACI leaf switches and the pair of Nexus 7000 switches. The routing protocol being utilized is OSPF. Some highlights of this connectivity are:

- A dedicated bridge domain bd-Common-Outside and associated dedicated VRF vrf-Common-Outside is configured in tenant common for external connectivity.
- The shared Layer 3 Out created in Tenant common "provides" an external connectivity contract that can be "consumed" from any tenant.
- Each of the two Nexus 7000s is connected to each of the two Nexus 9000 leaf switches.
- Sub-interfaces are configured and used for external connectivity.
- The Nexus 7000s are configured to originate and send a default route to the Nexus 9000 leaf switches using OSPF.
- ACI leaf switches advertise tenant subnet back to Nexus 7000 switches
- The physical connectivity is shown in the Figure 10 ACI Shared Layer 3 Out Connectivity Details

Figure 10 ACI Shared Layer 3 Out Connectivity Details



Nexus 7000 – Sample Configuration

The following configuration is a sample from the virtual device contexts (VDCs) of two Nexus 7004s.

The Nexus 7000 configuration below is not complete and is meant to be used only as a reference

Nexus 7004-1

```
feature ospf
feature interface-vlan
!
vlan 100
  name OSPF-Peering
!
interface Vlan100
  no shutdown
  mtu 9216
  no ip redirects
  ip address 10.253.253.253/30
  ip ospf mtu-ignore
  ip router ospf 10 area 0.0.0.0
!
interface Ethernet3/1
  description To A06-9372-1 E1/47
  no shutdown
!
interface Ethernet3/1.301
  description To A06-9372-1 E1/47
  encapsulation dot1q 301
  ip address 10.253.253.2/30
  ip ospf network point-to-point
  ip ospf mtu-ignore
  ip router ospf 10 area 0.0.0.10
  no shutdown
!
interface Ethernet3/2
  description To A06-9372-2 E1/47
  no shutdown
!
interface Ethernet3/2.302
  description To A06-9372-2 E1/47
  encapsulation dot1q 302
  ip address 10.253.253.6/30
  ip ospf network point-to-point
  ip ospf mtu-ignore
  ip router ospf 10 area 0.0.0.10
  no shutdown
!
interface Ethernet3/5
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 100
  mtu 9216
!
interface loopback0
  ip address 10.253.254.1/32
  ip router ospf 10 area 0.0.0.0
```

```
!
router ospf 10
  router-id 10.253.254.1
  area 0.0.0.10 nssa no-summary no-redistribution default-information-originate
!
```

Nexus 7004-2

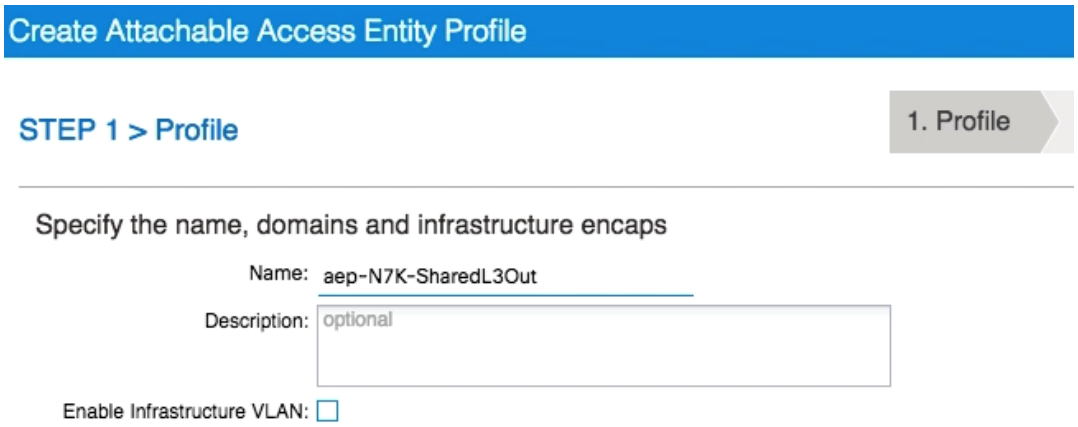
```
feature ospf
feature interface-vlan
!
vlan 100
  name OSPF-Peering
!
interface Vlan100
  no shutdown
  mtu 9216
  no ip redirects
  ip address 10.253.253.254/30
  ip ospf mtu-ignore
  ip router ospf 10 area 0.0.0.0
!
 interface Ethernet3/1
  description To A06-9372-1 E1/48
  no shutdown
!
interface Ethernet3/1.303
  description To A06-9372-1 E1/48
  encapsulation dot1q 303
  ip address 10.253.253.10/30
  ip ospf network point-to-point
  ip ospf mtu-ignore
  ip router ospf 10 area 0.0.0.10
  no shutdown
!
interface Ethernet3/2
  description To A06-9372-2 E1/48
  no shutdown
!
interface Ethernet3/2.304
  description To A06-9372-2 E1/48
  encapsulation dot1q 304
  ip address 10.253.253.14/30
  ip ospf network point-to-point
  ip ospf mtu-ignore
  ip router ospf 10 area 0.0.0.10
  no shutdown
!
interface Ethernet3/5
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 100
  mtu 9216
!
interface loopback0
  ip address 10.253.254.2/32
  ip router ospf 10 area 0.0.0.0
```

```
!
router ospf 10
  router-id 10.253.254.2
  area 0.0.0.10 nssa no-summary no-redistribution default-information-originate
!
```

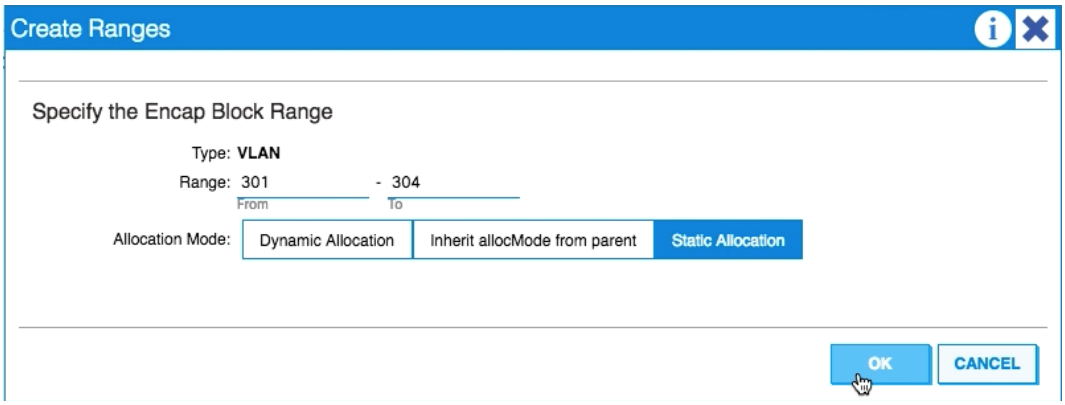
Configuring ACI Shared Layer 3 Out in Tenant Common

Configure External Routed Domain

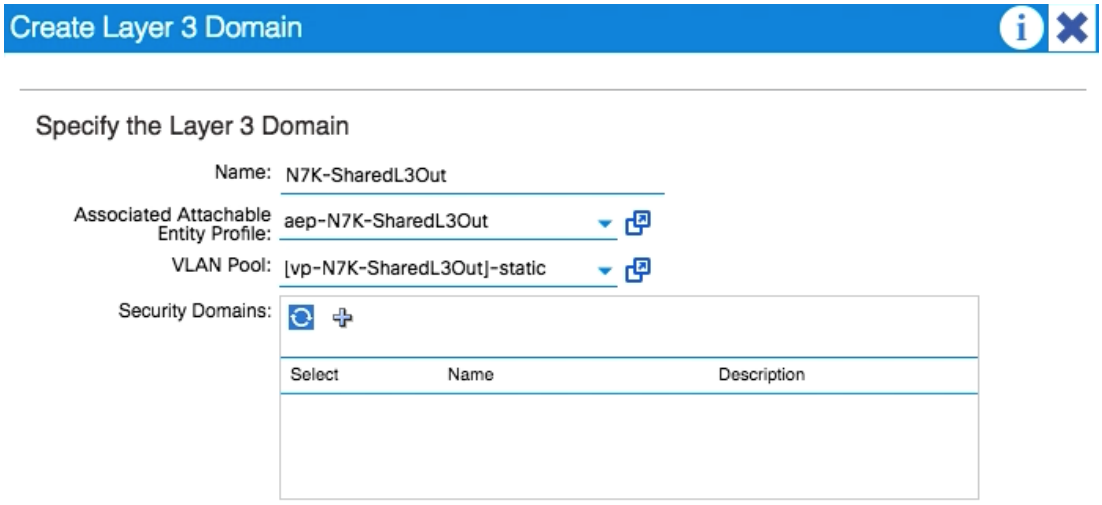
1. At the top, select Fabric > Access Policies.
2. In the left pane, expand Physical and External Domains.
3. Right-click External Routed Domains and select Create Layer 3 Domain.
4. Name the Domain N7K-SharedL3Out.
5. From the Associated Attachable Entity Profile drop-down list, select **Create Attachable Entity Profile**.
6. Name the Profile aep-N7K-SharedL3Out and click **NEXT**.



7. Click **FINISH** to continue without specifying interfaces.
8. Back in the Create Layer 3 Domain window, use the VLAN Pool drop-down list to select Create VLAN Pool.
9. Name the VLAN Pool vp-N7K-SharedL3Out
10. Select Static Allocation.
11. Click **+** to add an Encap Block.
12. In the Create Ranges window, enter the VLAN range as shown in Figure 10 (301-304).
13. Select Static Allocation.



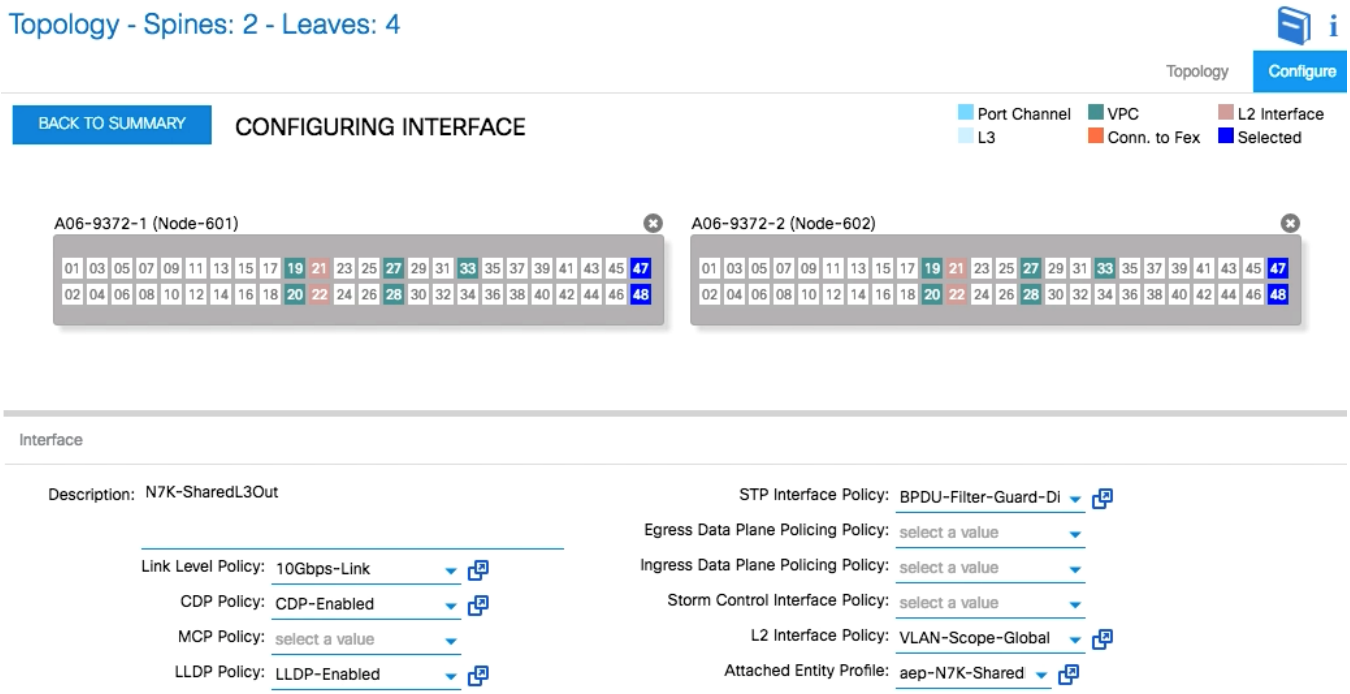
14. Click **OK** to complete adding the VLAN range.
15. Click **SUBMIT** to complete creating the VLAN Pool.



16. Click **SUBMIT** to complete creating the Layer 3 Domain.

Configure Leaf Switch Interfaces

1. At the top, select Fabric > Inventory.
2. In the left pane, select **Topology**. On the right pane, select **Configure**.
3. In the center pane, select **ADD SWITCHES**.
4. Using the shift key, select the two leaf switches connected to Nexus 7000s and select **ADD SELECTED**.
5. On the two switches, select the 4 ports connected to the Nexus 7000s.
6. On the lower right, select **CONFIGURE PORT**.
7. Select the appropriate policies as shown below.

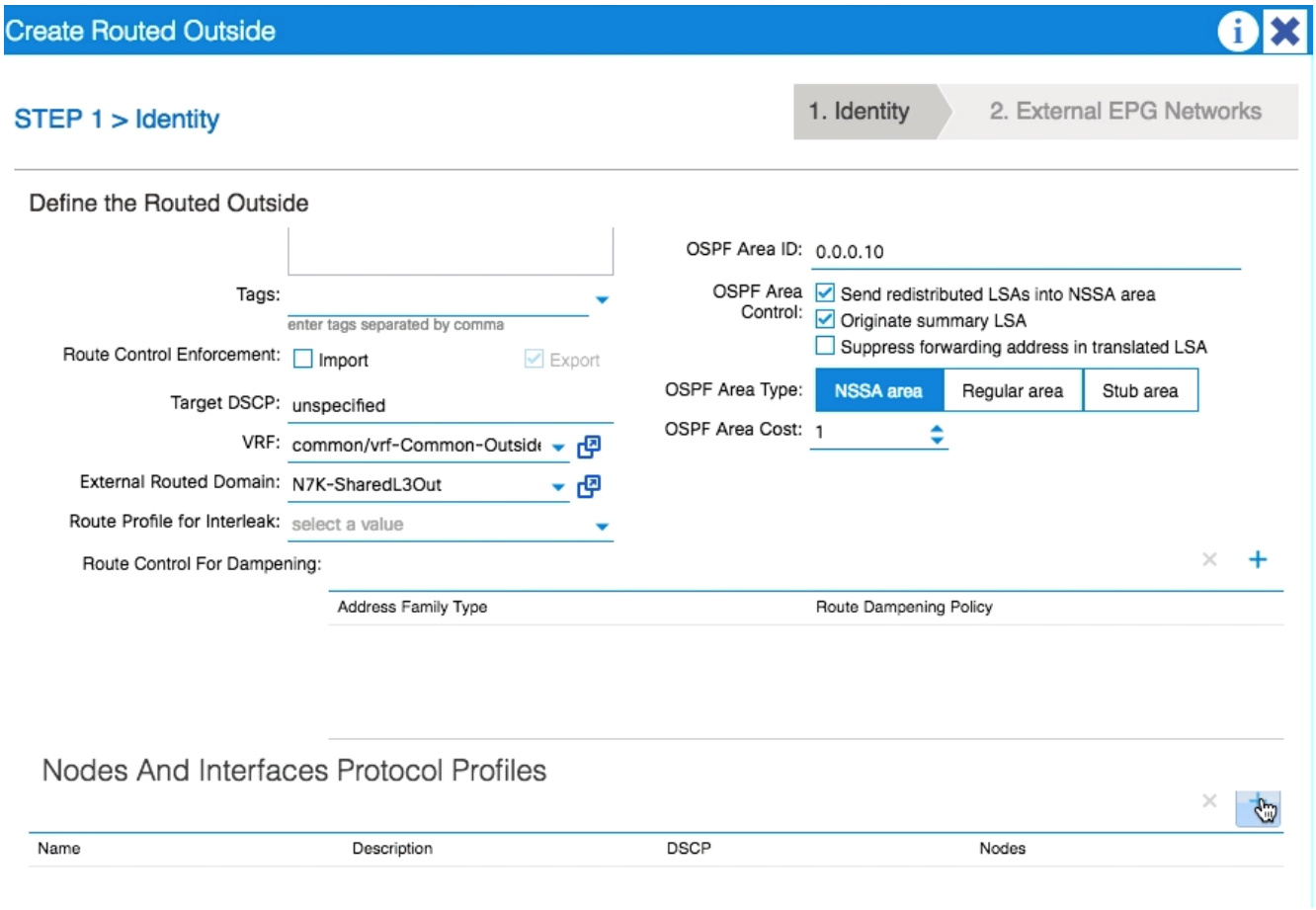


The STP Interface Policy selected in the figure above is BPDU-Filter-Guard-Disabled

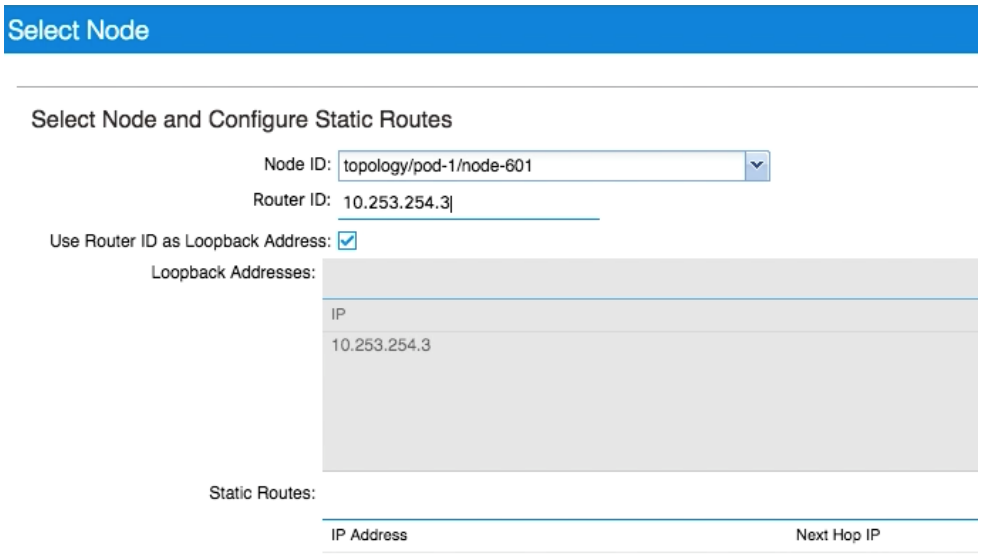
8. Select **APPLY CHANGES** to configure the ports. Click **OK** for the Success confirmation.

Configure External Routed Networks under Tenant common

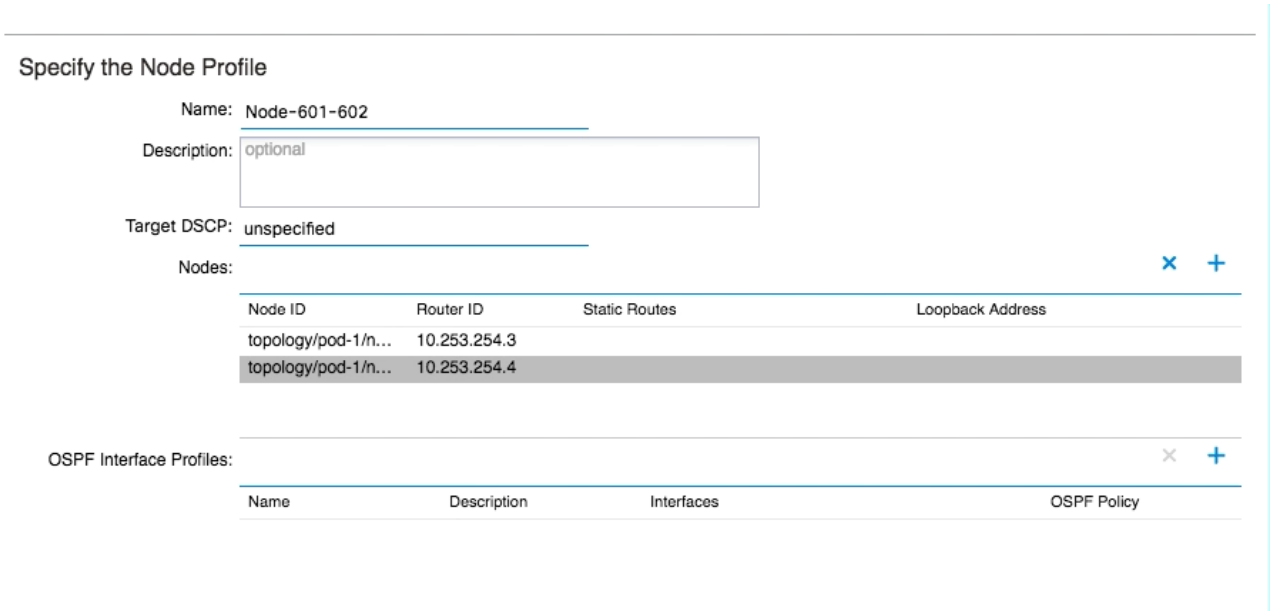
1. At the top, select Tenants > common.
2. In the left pane, expand Tenant common and Networking.
3. Right-click External Routed Networks and select **Create Routed Outside**.
4. Name the Routed Outside Nexus-7K-Shared.
5. Check the check box next to OSPF.
6. Enter 0.0.0.10 (configured in the Nexus 7000s) as the OSPF Area ID.
7. From the VRF drop-down list, select common/Common-Outside.
8. From the External Routed Domain drop-down list, select N7K-SharedL3Out.
9. Click **+** to add a Node Profile.



10. Name the Node Profile Node-601-602 (601 and 602 are Node IDs of leaf switches connected to Nexus 7000).
11. Click **+** to add a Node.
12. In the select Node and Configure Static Routes window, select Leaf switch 601 from the drop-down list.
13. Provide a Router ID IP address – this address will be configured as the Loopback Address. The address used in this deployment is 10.253.254.3.

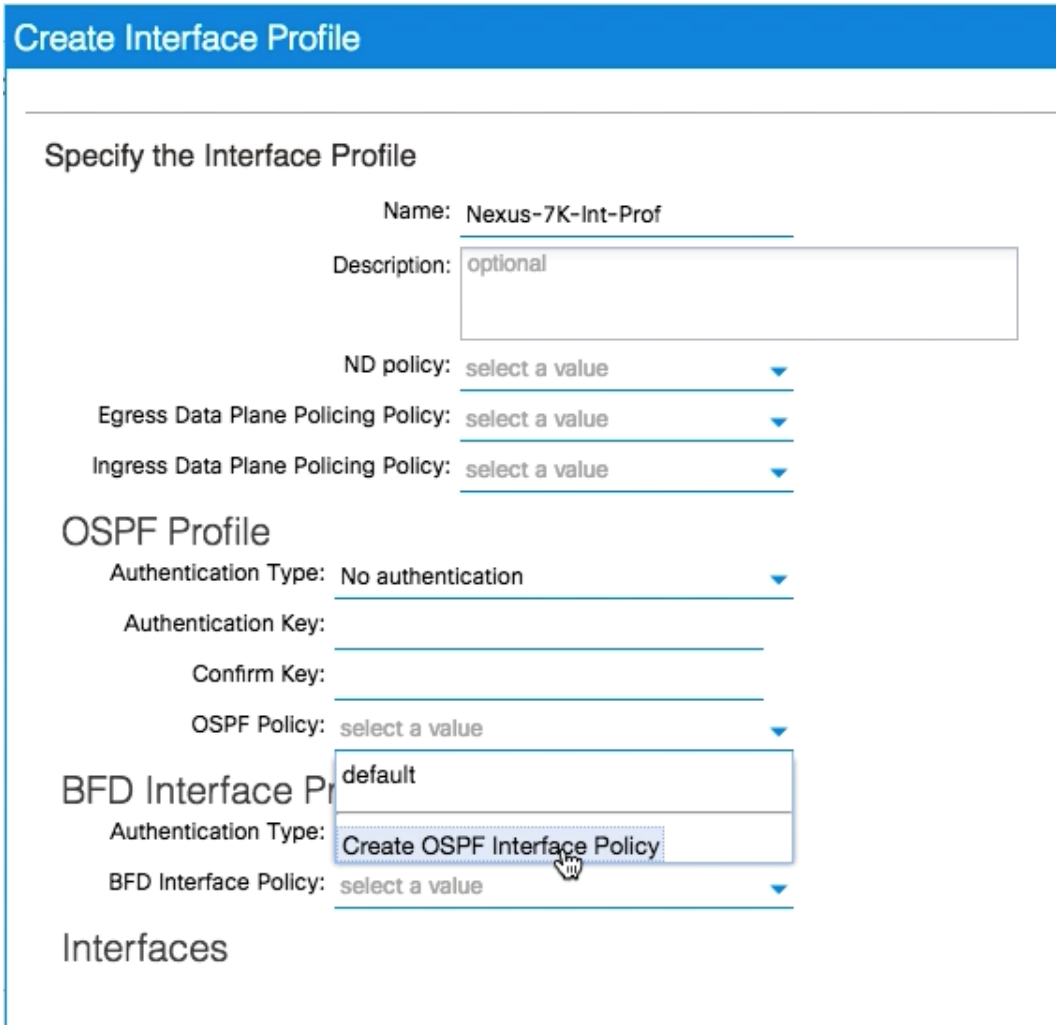


14. Click **OK** to complete selecting the Node.
15. Click **+** to add another Node.
16. In the select Node window, select Leaf switch 602.
17. Provide a Router ID IP address – this address will be configured as the Loopback Address. The address used in this deployment is 10.253.254.4.
18. Click **OK** to complete selecting the Node.

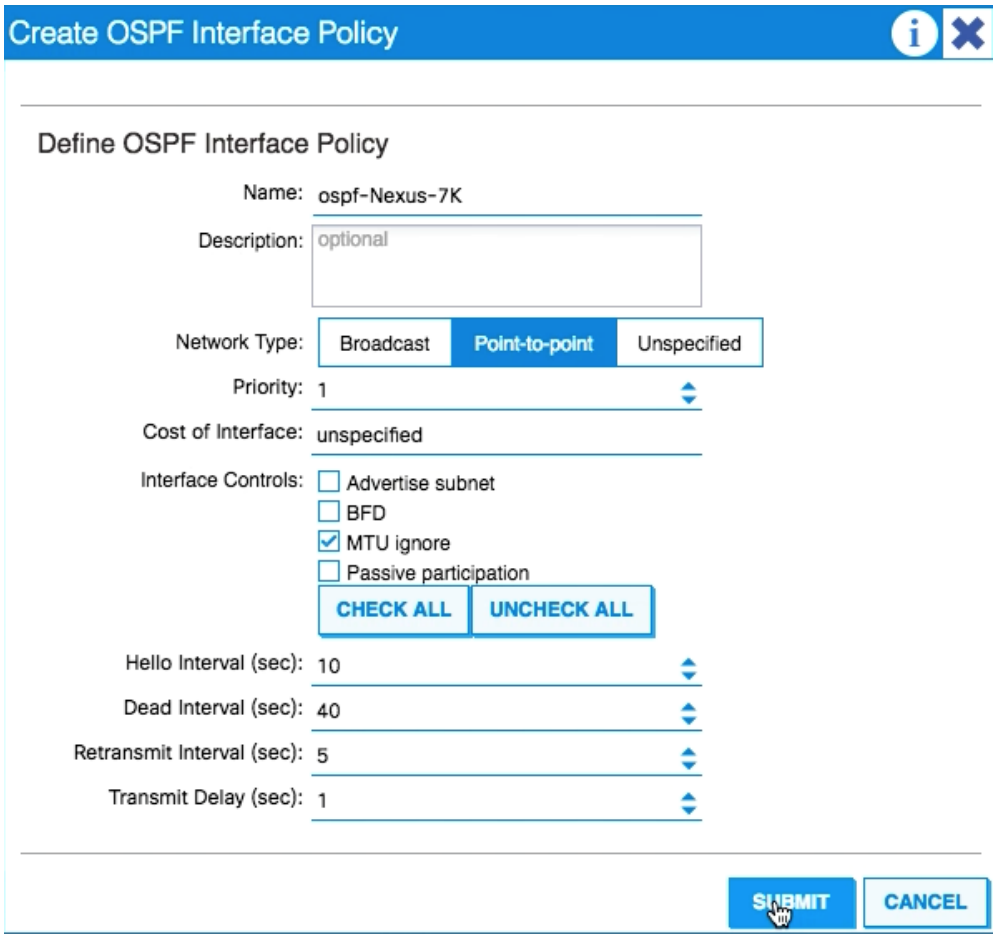


19. Click **+** to create an OSPF Interface Profile.
20. Name the profile Nexus-7K-Int-Ptof.

21. Using the OSPF Policy pulldown, select Create OSPF Interface Policy.



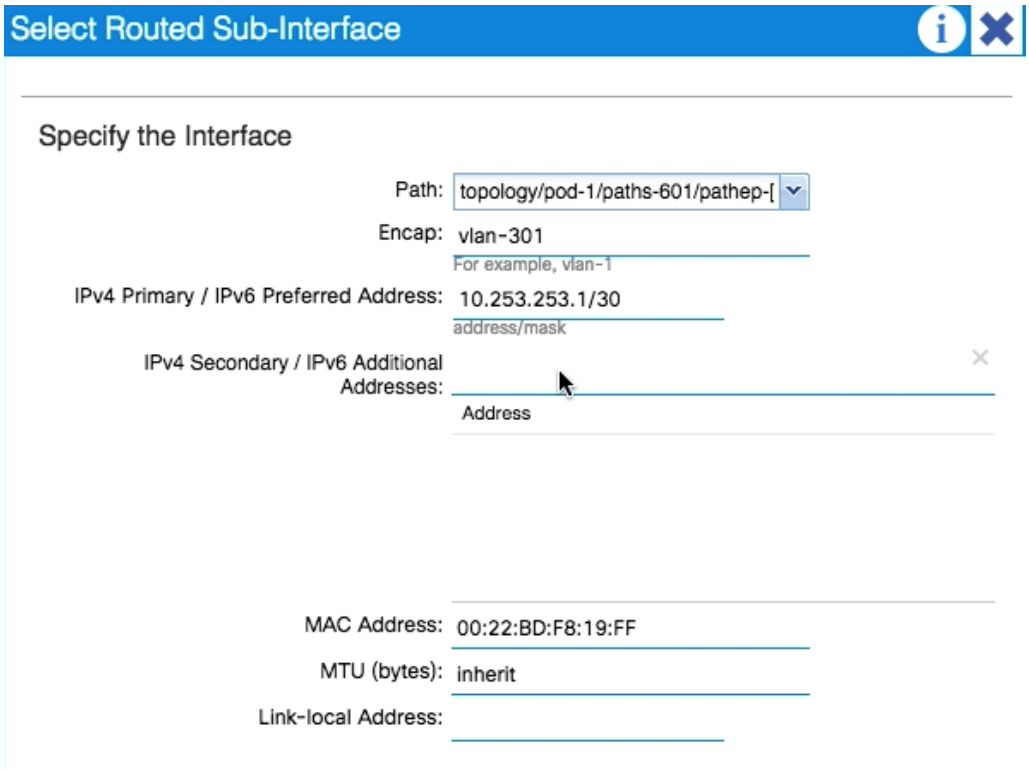
22. Name the policy ospf-Nexus-7K.
23. Select the Point-to-Point Network Type.
24. Select the MTU ignore Interface Controls.



25. Click **SUBMIT** to complete creating the policy.
26. Select Routed Sub-Interface under Interfaces.
27. Click **+** to add a routed sub-interface.

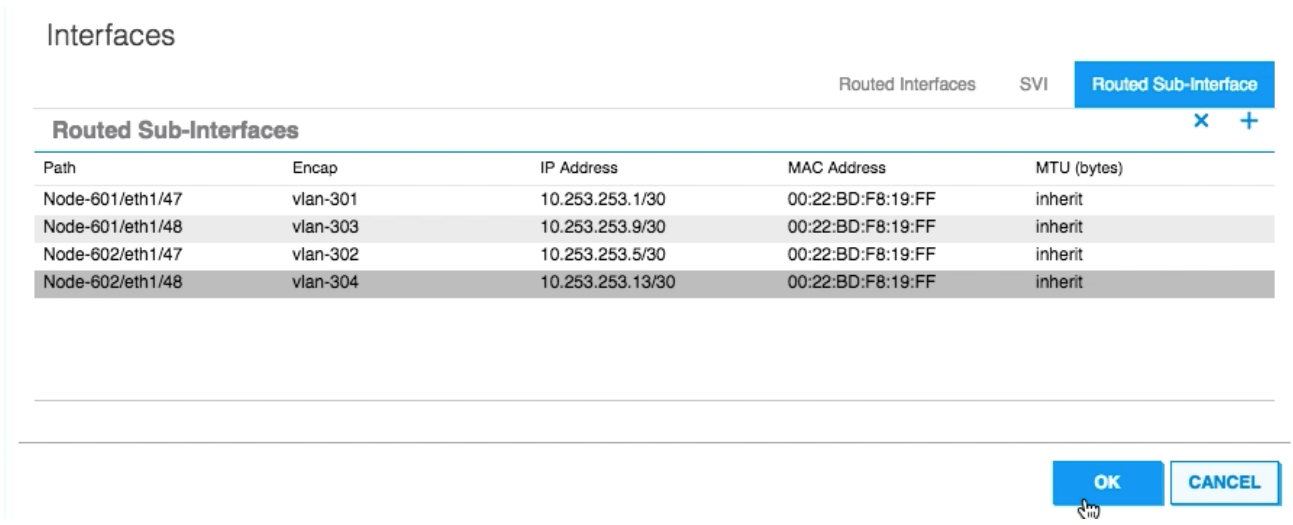
> For adding Routed Sub-interfaces, refer to Figure 10 for Interface, IP and VLAN details

28. In the Select Routed Sub-Interface window, select the interface on Nexus 9372-1 (Node 601) that is connected to Nexus 7004-1.
29. Enter vlan-<interface vlan> (301) for Encap.
30. Enter the IPv4 Address as shown in Figure 10 (10.253.253.1/30)
31. Leave the MTU set to inherit.

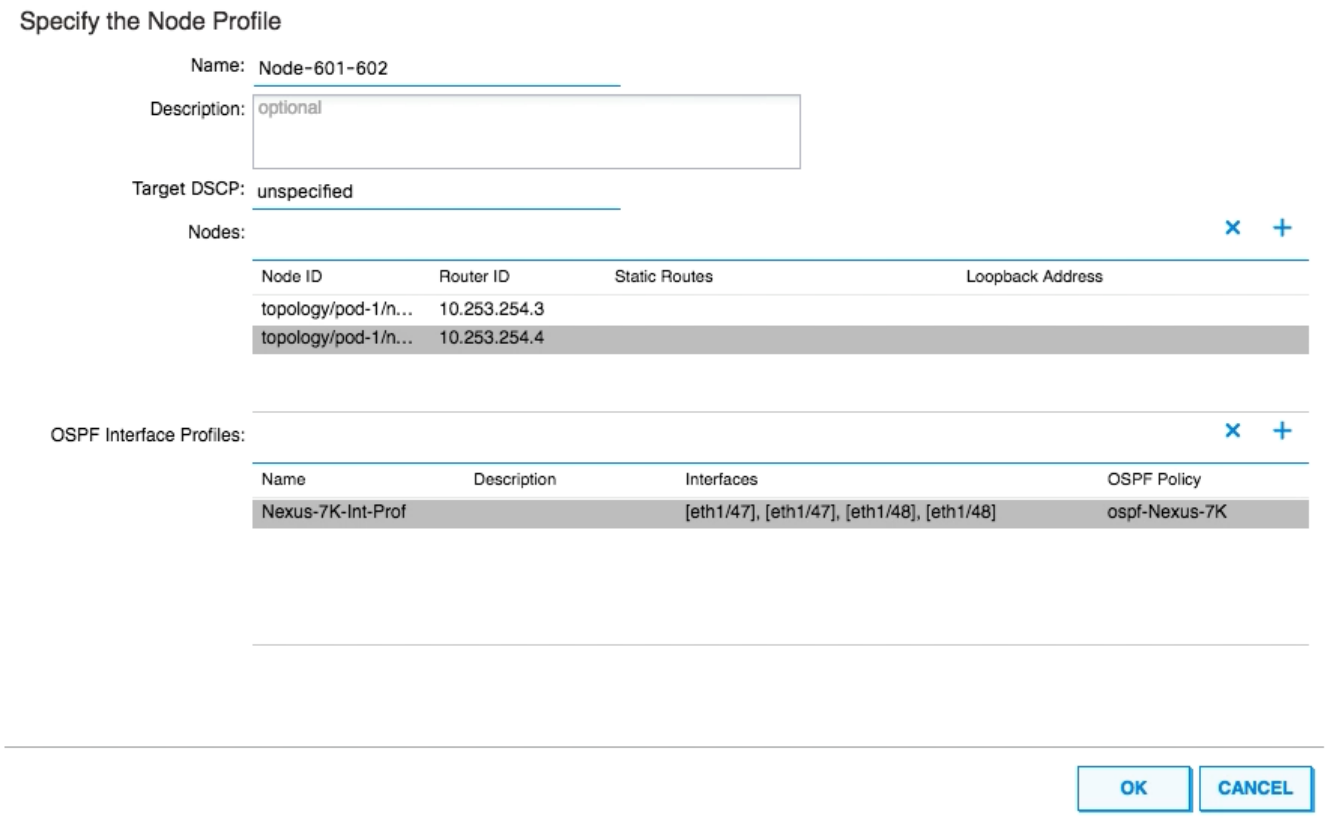


32. Click **OK** to complete creating the routed sub-interface.

33. Repeat these steps to all four sub-interfaces shown in Figure 10. The Routed Sub-Interfaces will be similar to the figure shown below.

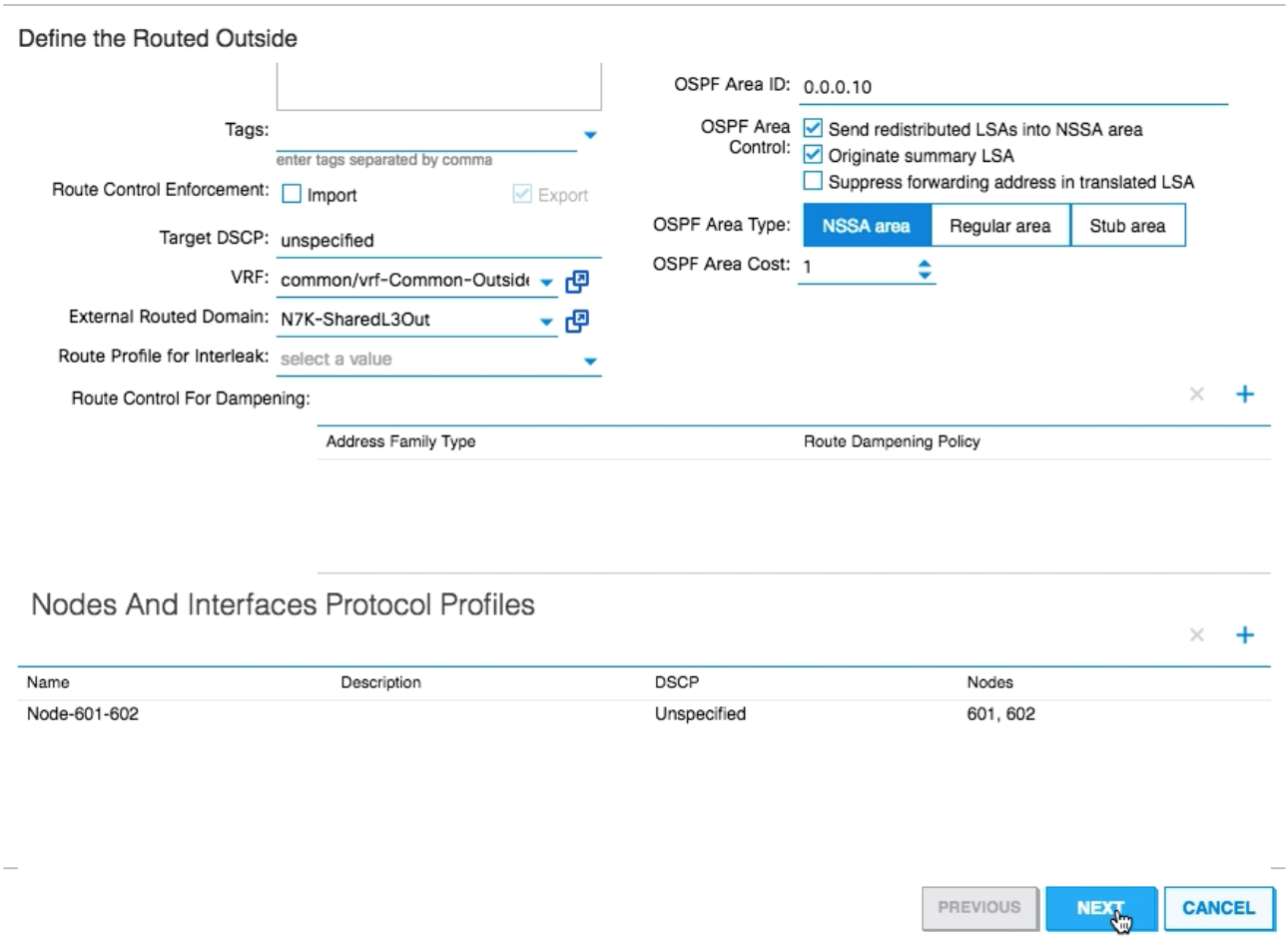


34. Click **OK** to complete creating the Node Interface Profile.

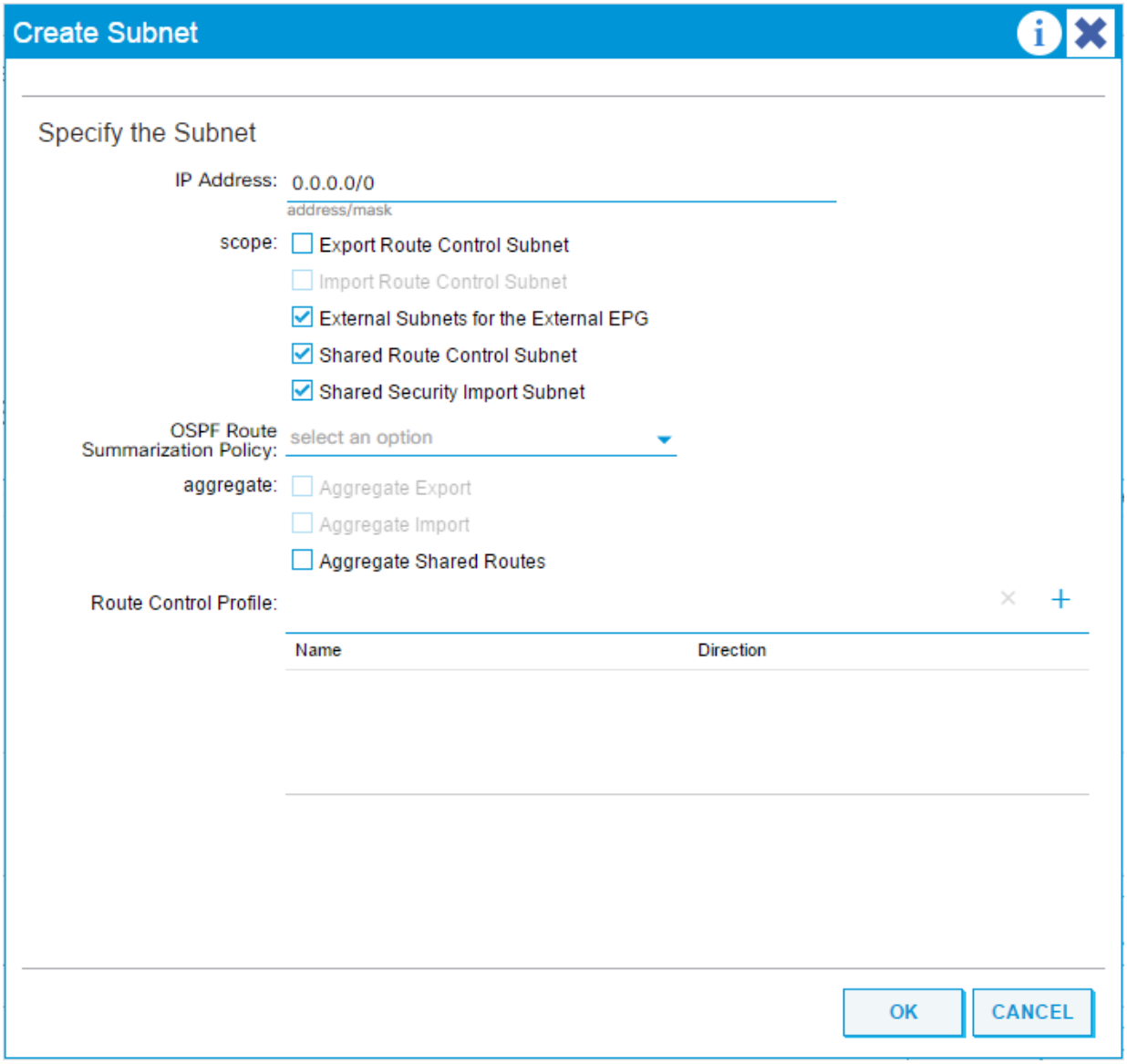


35. Click **OK** to complete creating the Node Profile.

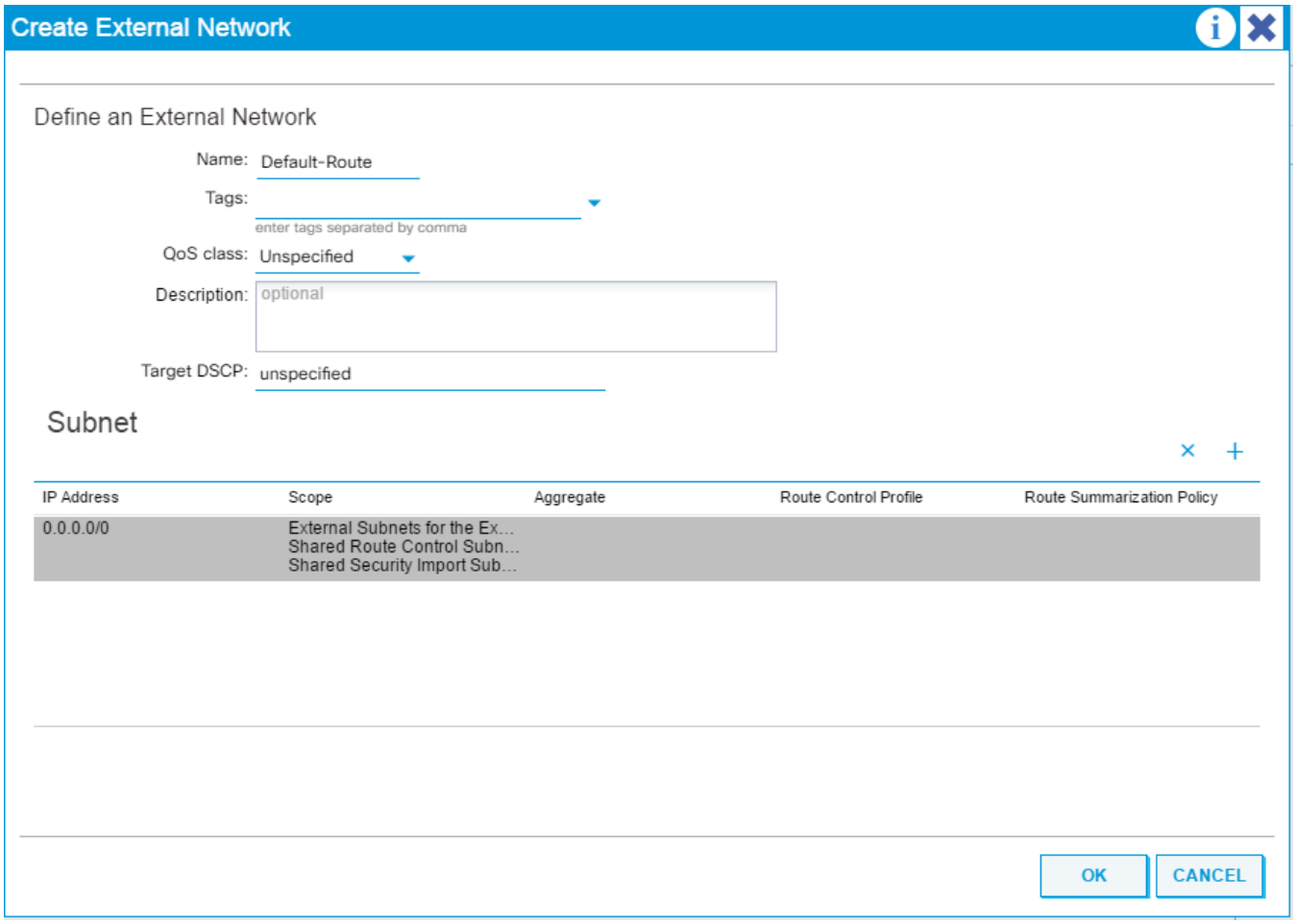
36. Click **NEXT** on Create Routed Outside Screen.



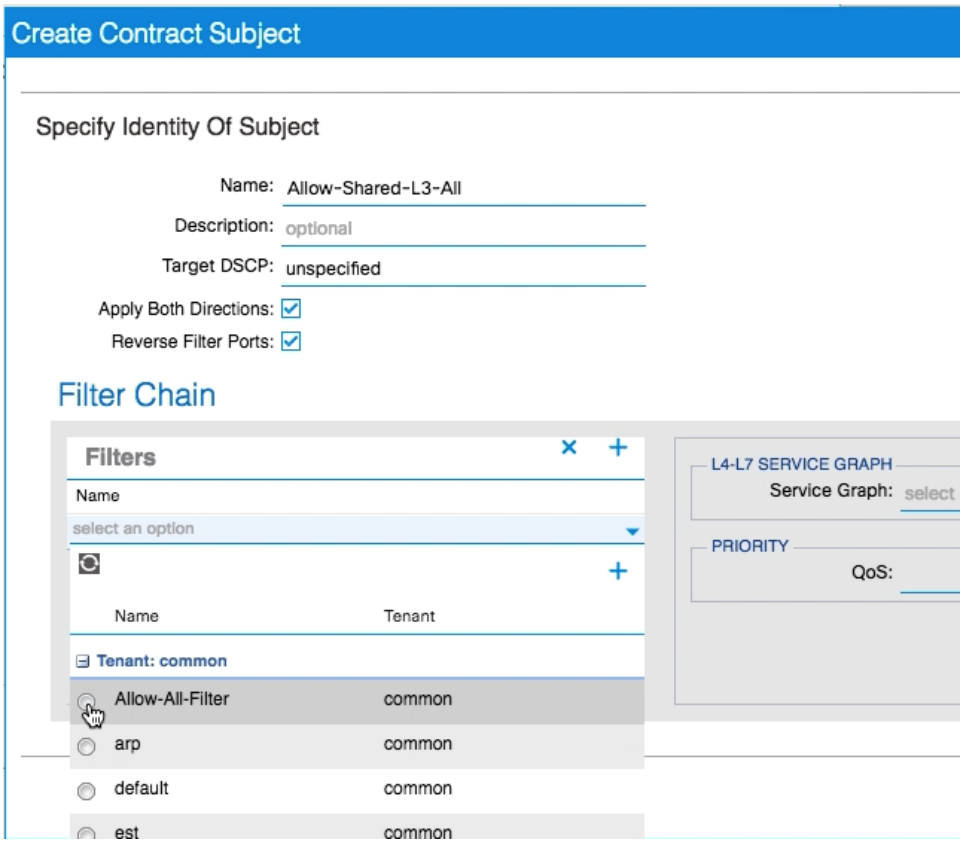
37. Click **+** to create an External EPG Network.
38. Name the External Network Default-Route.
39. Click **+** to add a Subnet.
40. Enter 0.0.0.0/0 as the IP Address. Select the checkboxes for External Subnets for the External EPG, Shared Route Control Subnet, and Shared Security Import Subnet.



41. Click **OK** to complete creating the subnet.



42. Click **OK** to complete creating the external network.
43. Click **FINISH** to complete creating the External Routed Networks.
44. In the left pane, expand Security Policies, Right-click on Contracts and select **Create Contract**.
45. Name the contract Allow-Shared-L3-Traffic.
46. Select the Global Scope to allow the contract to be consumed from all tenants.
47. Click **+** to add a contract subject.
48. Name the subject Allow-Shared-L3-Out.
49. Click **+** to add a filter.
50. From the drop-down list, select the Allow-All-Filter from Tenant common.

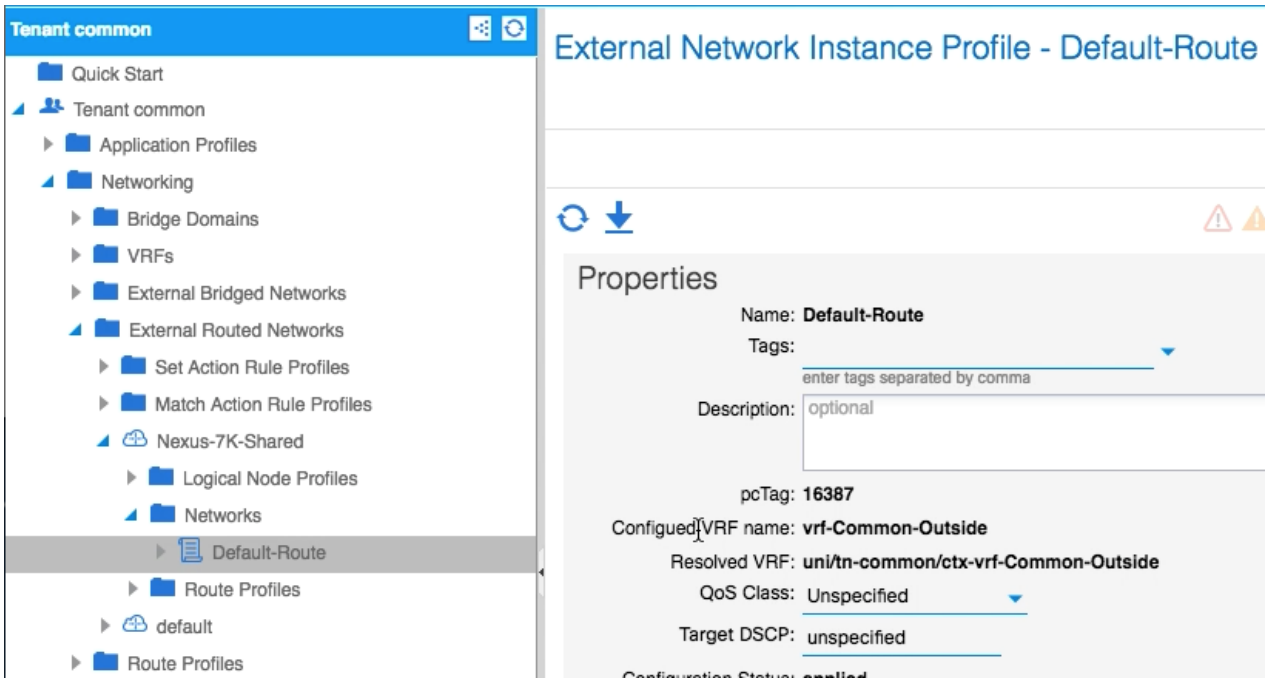


51. Click **UPDATE**.

52. Click **OK** to complete creating the contract subject.

53. Click **SUBMIT** to complete creating the contract.

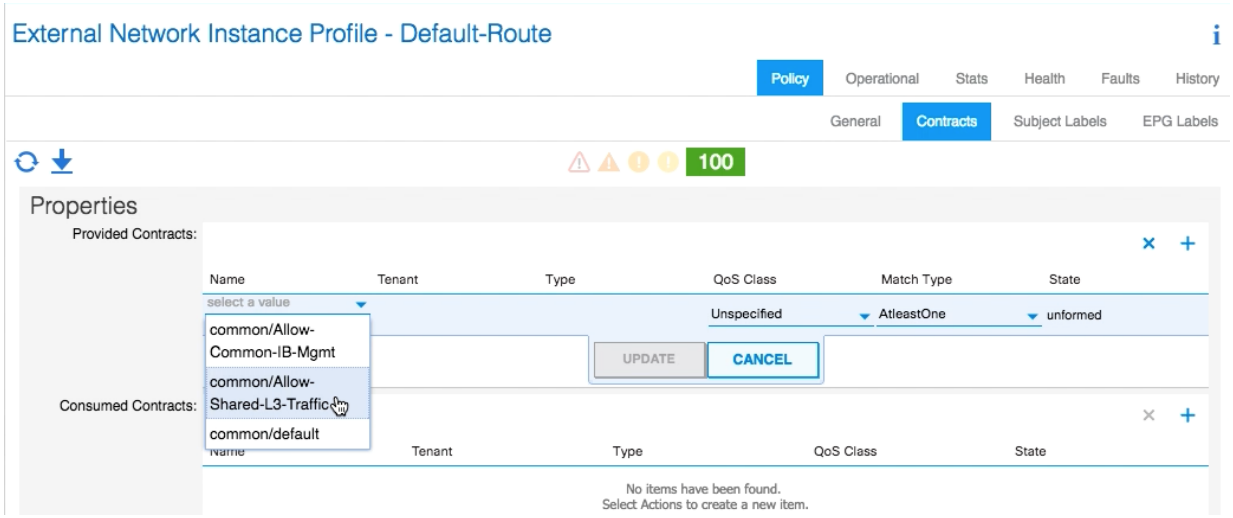
54. In the left pane expand Tenant common, Networking, External Routed Networks, Nexus-7K-Shared, and Networks. Select Default-Route.



55. In the right pane under Policy, select Contracts.

56. Click **+** to add a Provided Contract.

57. Select the common/Allow-Shared-L3-Traffic contract.



58. Click **UPDATE**.

Tenant EPGs can now consume the Allow-Shared-L3-Traffic contract and route traffic outside fabric. This deployment example shows Allow-All filters. More restrictive contracts can be created for more restrictive access outside the Fabric.

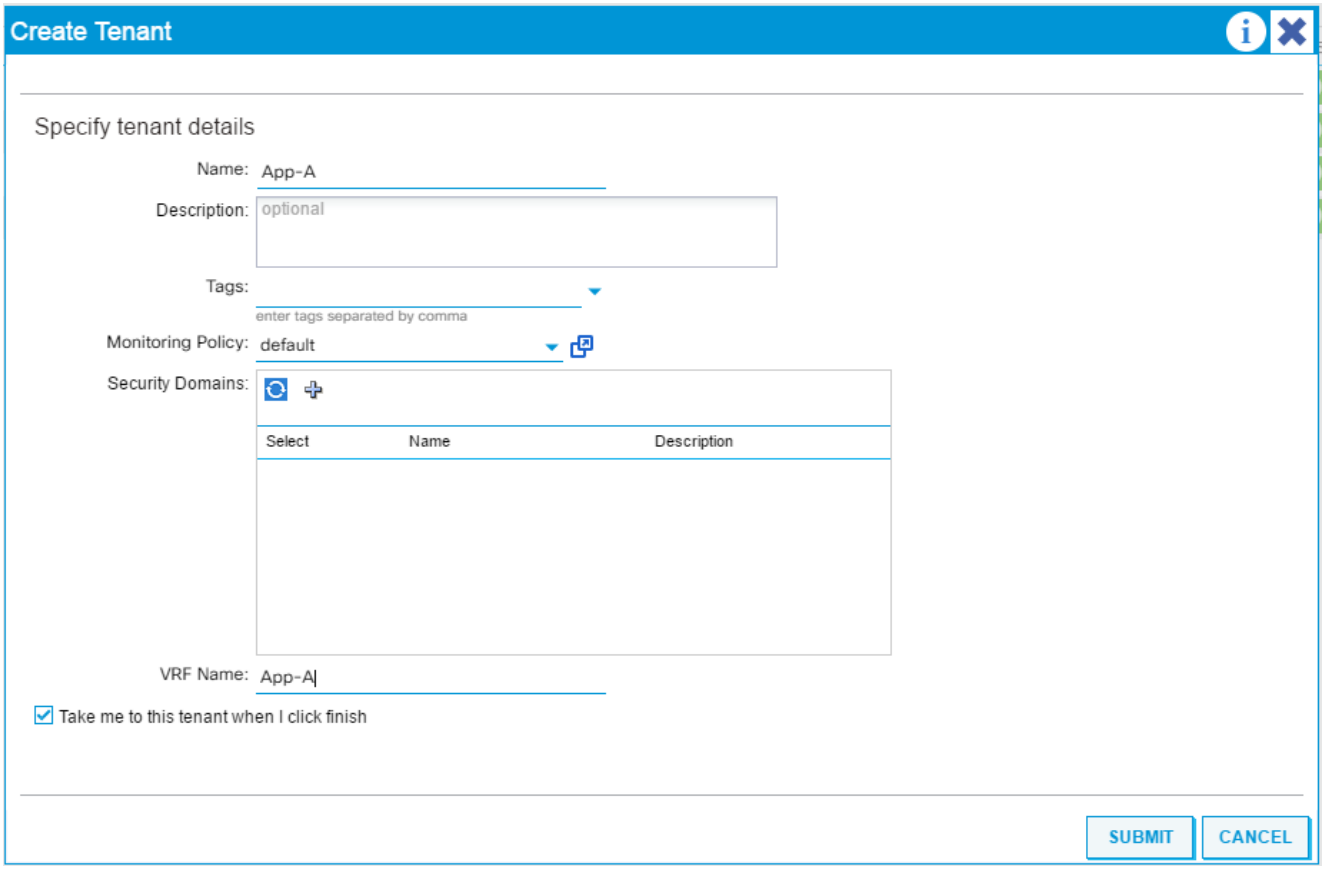
Onboarding an Application Tenant

This section details the steps for creating a sample two-tier application called App-A. This tenant will comprise of a Web and App tier which will be mapped to relevant EPGs on the ACI fabric.

To deploy the Application Tenant and associate it to the VM networking, complete the following steps:

Configure Tenant

1. In the APIC Advanced GUI, select Tenants.
2. At the top select Tenants > Add Tenant.
3. Name the Tenant App-A.
4. For the VRF Name, also enter App-A. Leave the Take me to this tenant when I click finish checkbox checked.



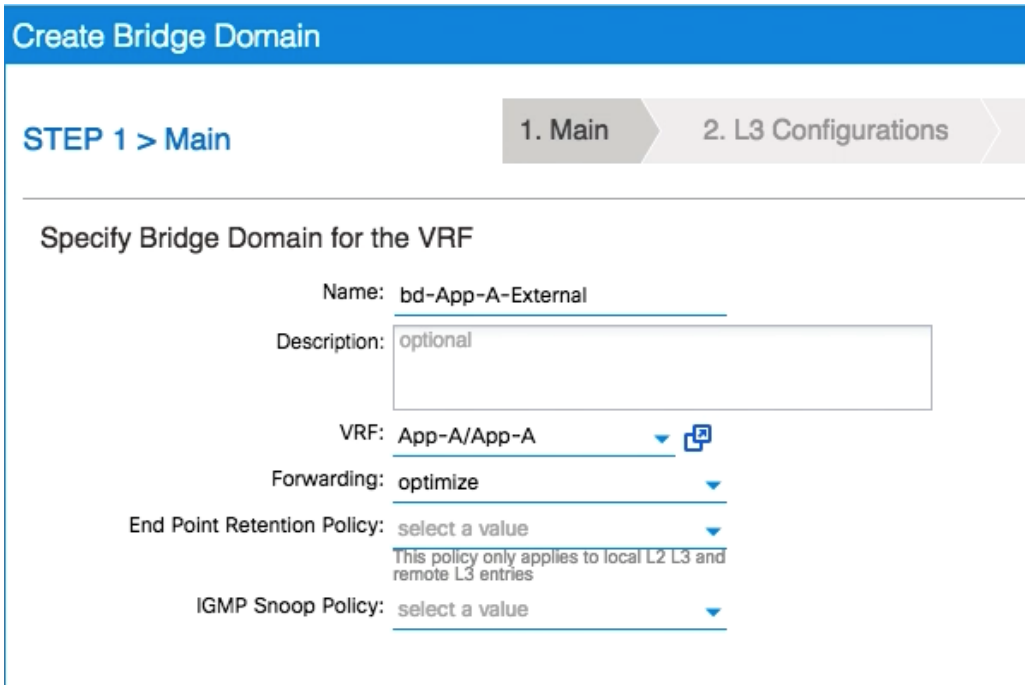
5. Click **SUBMIT** to finish creating the Tenant.

Configure Bridge Domains

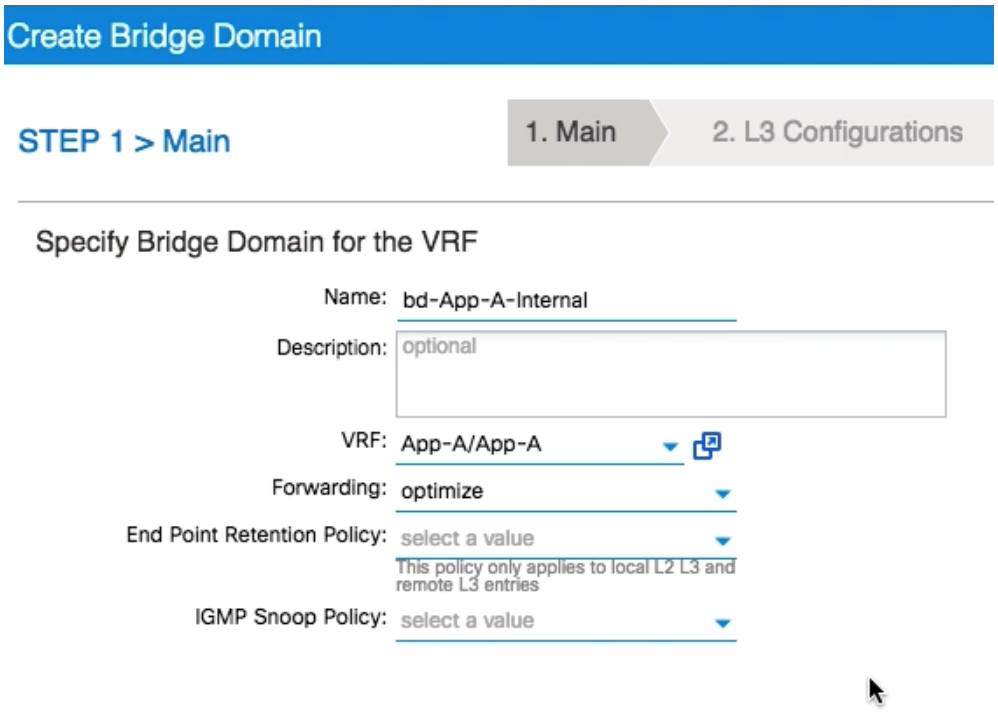
1. In the left pane expand Tenant App-A > Networking.
2. Right-click on the Bridge Domain and select **Create Bridge Domain**.

In this deployment, two different bridge domains will be created to host Web and App application tiers to keep the external and application-internal traffic separated. Customers can choose to create a single Bridge Domain to host both.

3. Name the Bridge Domain bd-App-A-External, leave the Forwarding set at optimize, and click **NEXT**, **NEXT** and click **SUBMIT** to complete adding the Bridge Domain.

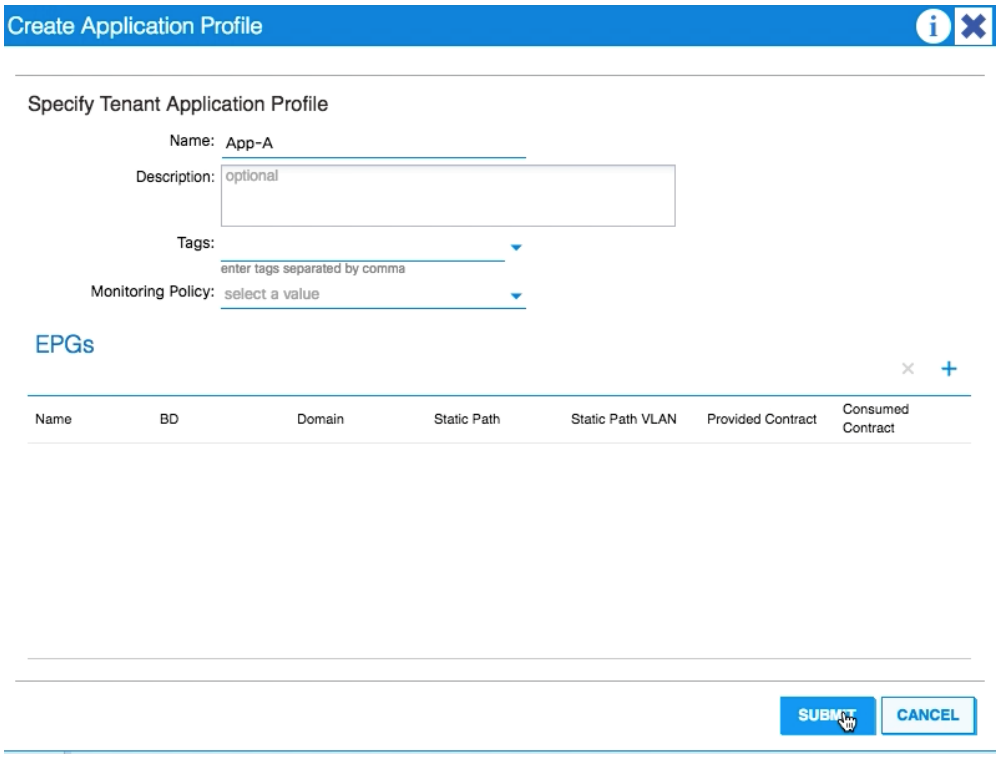


4. Repeat the steps above to add another Bridge Domain called bd-App-A-Internal.



Configure Application Profile

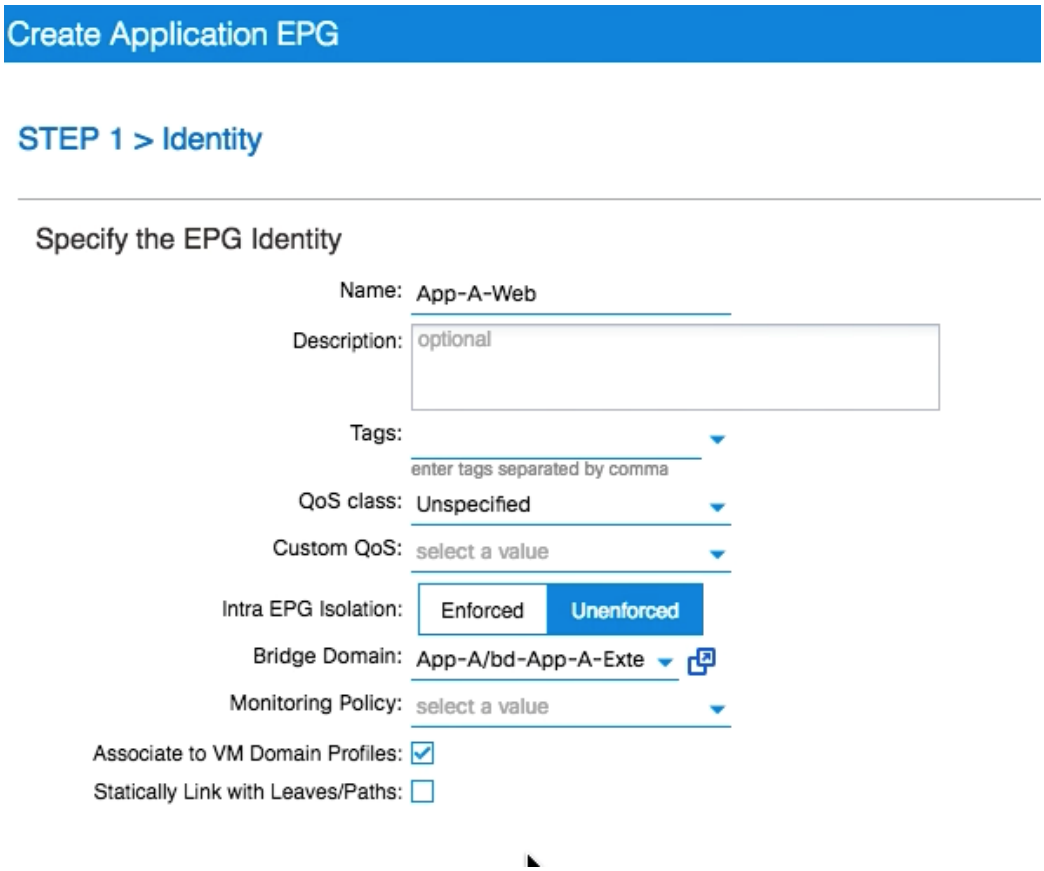
1. In the left pane, right-click Application Profiles and select **Create Application Profile**.
2. Name the Application Profile App-A and click **SUBMIT**.



Configure End Point Groups

EPG App-A-Web

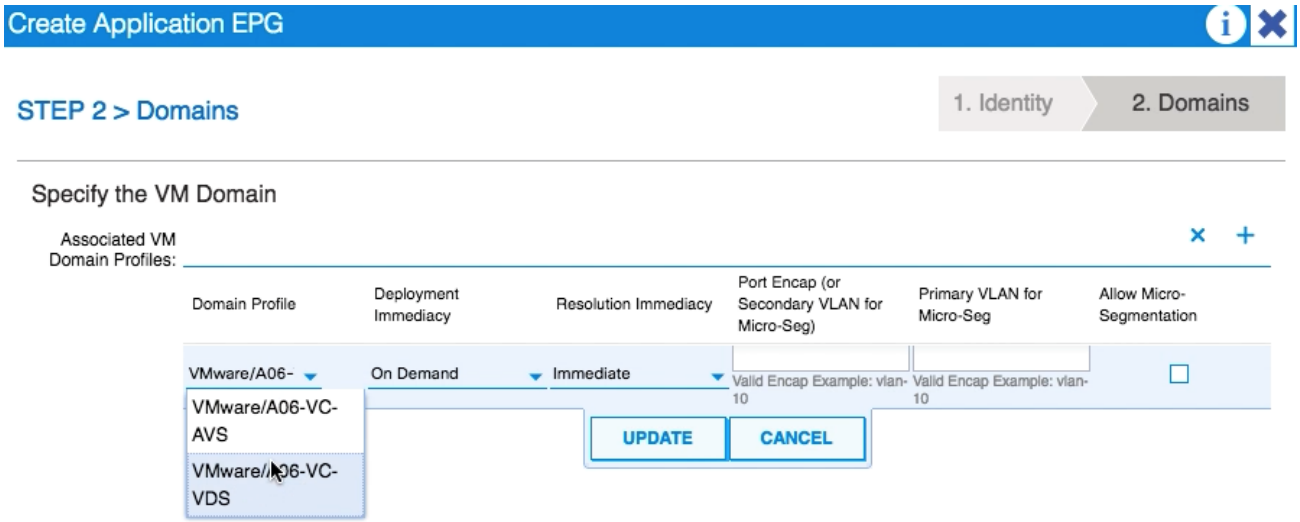
1. In the left pane expand Application Profiles > App-A.
2. Right-click Application EPGs and select **Create Application EPG**.
3. Name the EPG App-A-Web. Leave Intra EPG Isolation Unenforced.
4. From the Bridge Domain drop-down list, select App-A/bd-App-A-External.
5. Check the check box next to Associate to VM Domain Profiles.



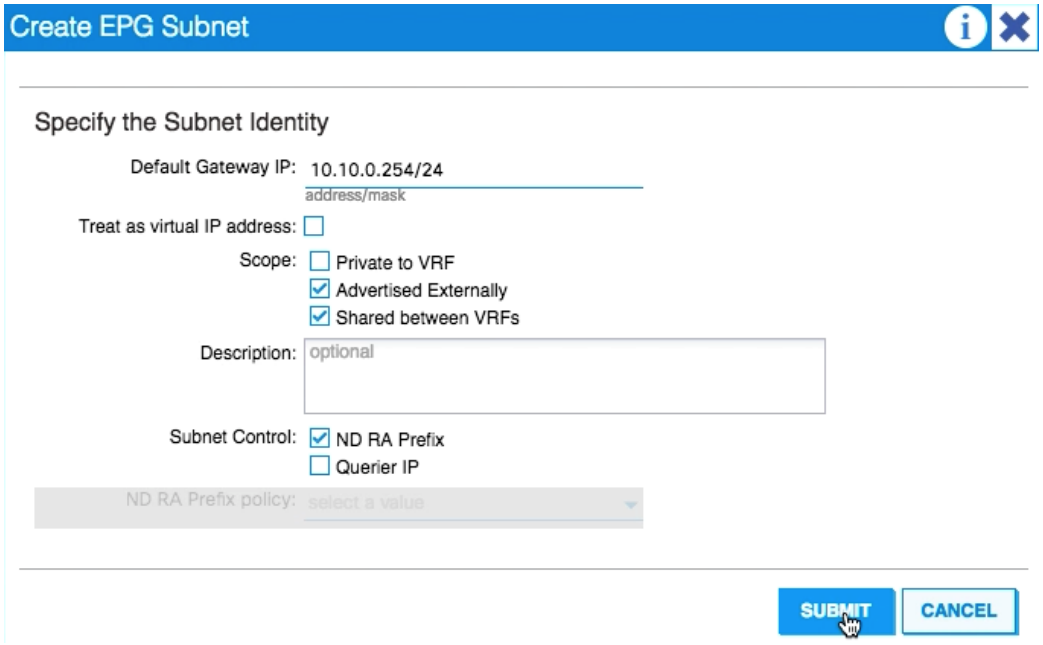
6. Click **NEXT**.

7. Click **+** to Associate VM Domain Profiles.

8. From the Domain Profile drop-down list, select VMware domain. If customers have deployed both VDS and AVS domains, both the domain will be visible in the drop-down list as shown below. In this example, VMware domain for VDS is selected to deploy the EPG.

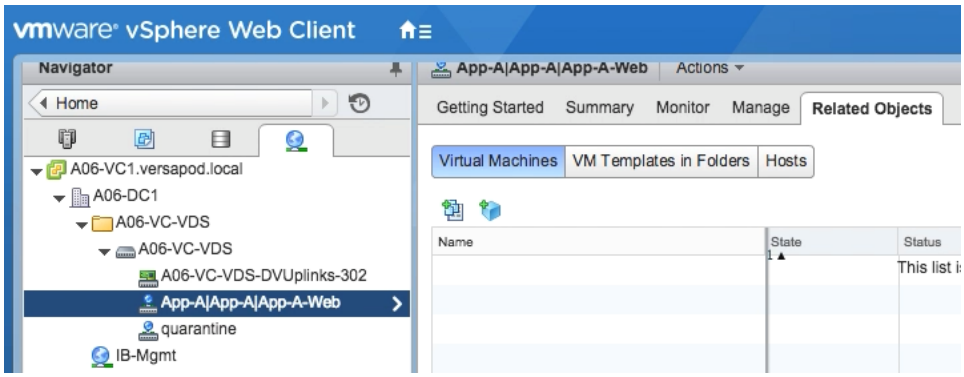


9. Change the Deployment Immediacy and Resolution Immediacy to Immediate.
10. Click **UPDATE**.
11. Click **FINISH** to complete creating the EPG.
12. In the left pane expand EPG App-A-Web, right-click on the Subnets and select **Create EPG Subnet**.
13. For the Default Gateway IP, enter a gateway IP address and mask. In this deployment, the GW address configured for Web VMs is 10.10.0.254/24.
14. Since the Web VM Subnet is advertised to Nexus 7000s and to App EPG, select Advertise Externally and Shared between the VRFs.



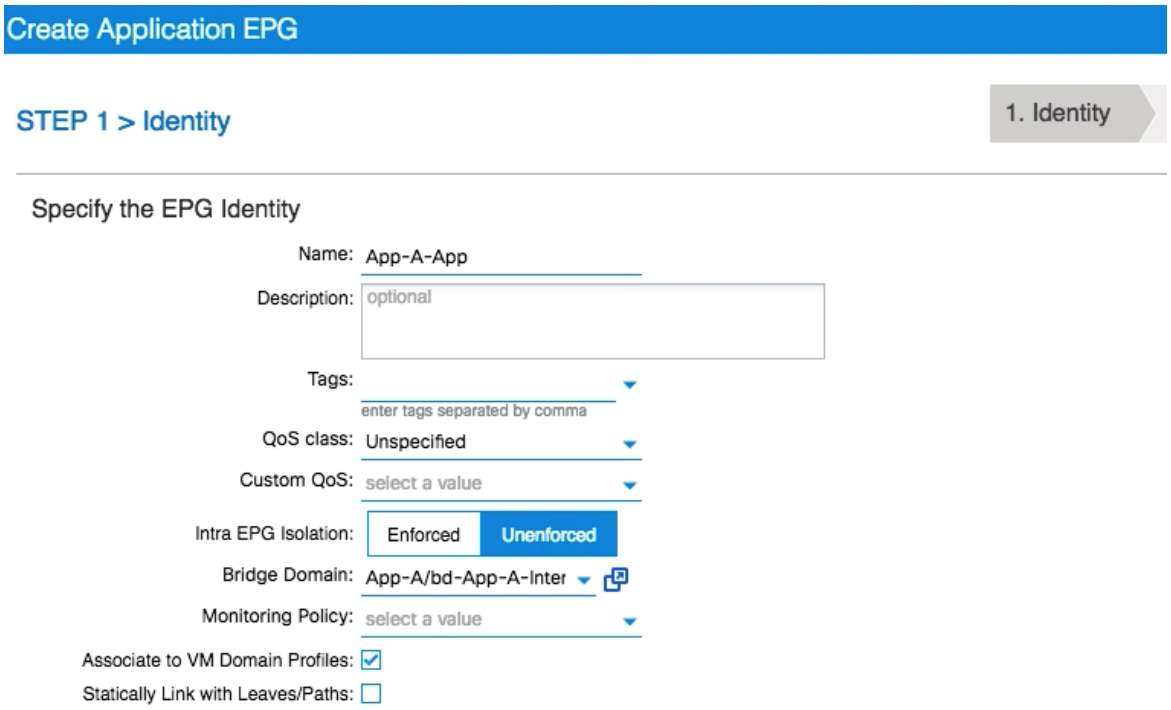
15. Click **SUBMIT**.

At this point, a new port-group should have been created on the VMware VDS. Log into the vSphere Web Client, browse to Networking > VDS and verify.

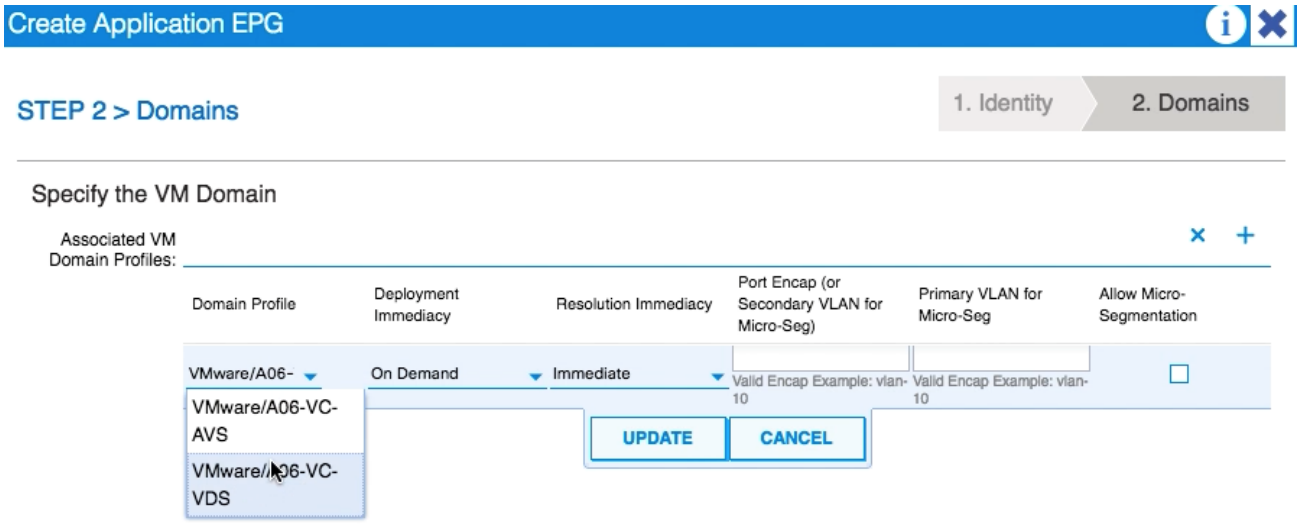


EPG App-A-App

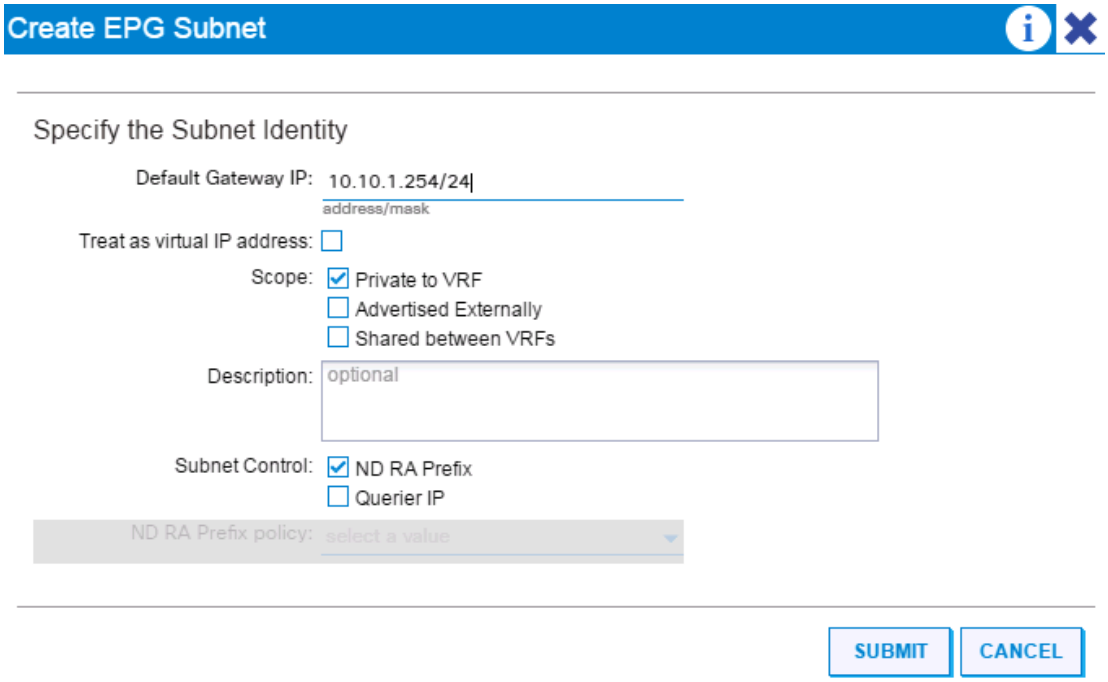
1. In the left pane expand Application Profiles > App-A.
2. Right-click Application EPGs and select **Create Application EPG**.
3. Name the EPG App-A-App. Leave Intra EPG Isolation Unenforced.
4. From the Bridge Domain drop-down list select App-A/bd-App-A-Interna.
5. Check the check box next to Associate to VM Domain Profiles.



6. Click **NEXT**.
7. Click **+** to Associate VM Domain Profiles.
8. From the Domain Profile drop-down list, select VMware domain. If customers have deployed both VDS and AVS domains, both the domain will be visible in the drop-down list as shown below. In this example, VMware domain for VDS is selected to deploy the EPG.

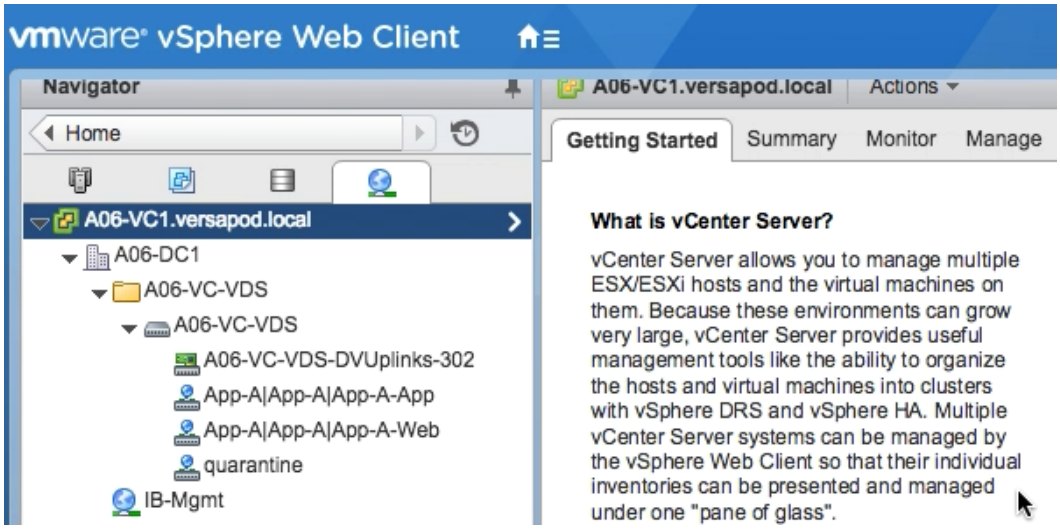


9. Change the Deployment Immediacy and Resolution Immediacy to Immediate.
10. Click UPDATE.
11. Click **FINISH** to complete creating the EPG.
12. In the left pane expand EPG App-A-App, right-click on the Subnets and select **Create EPG Subnet**.
13. For the Default Gateway IP, enter a gateway IP address and mask. In this deployment, the GW address configured for App VMs is 10.10.1.254/24.
14. Since the App VMs only need to communicate with Web VMs EPG, select Private to VRFs.



15. Click **SUBMIT**.

At this point, a new port-group should have been created on the VMware VDS. Log into the vSphere Web Client, browse to Networking > VDS and verify.

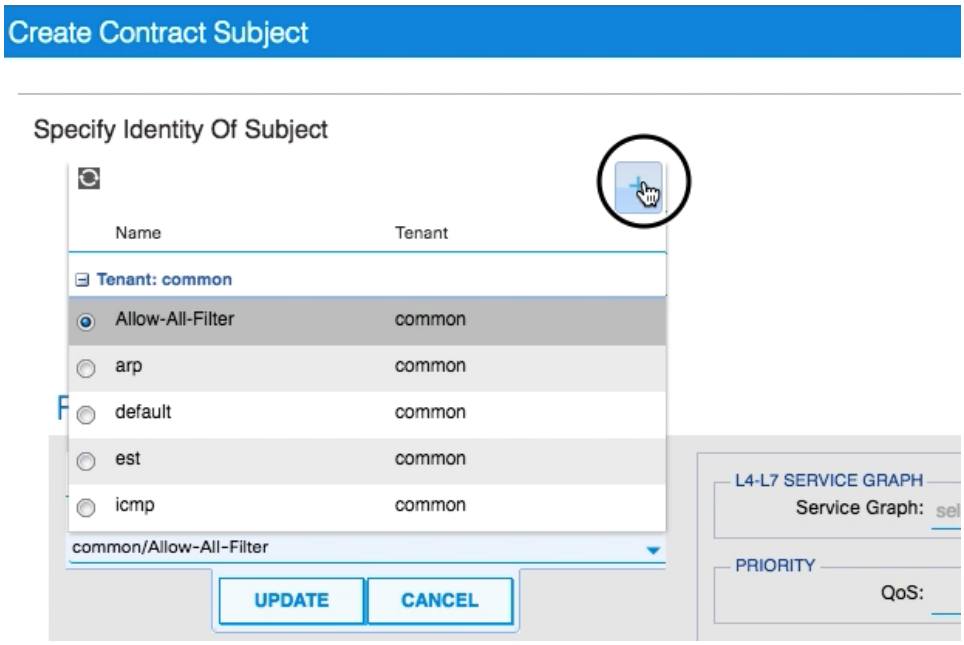


Configure Contracts

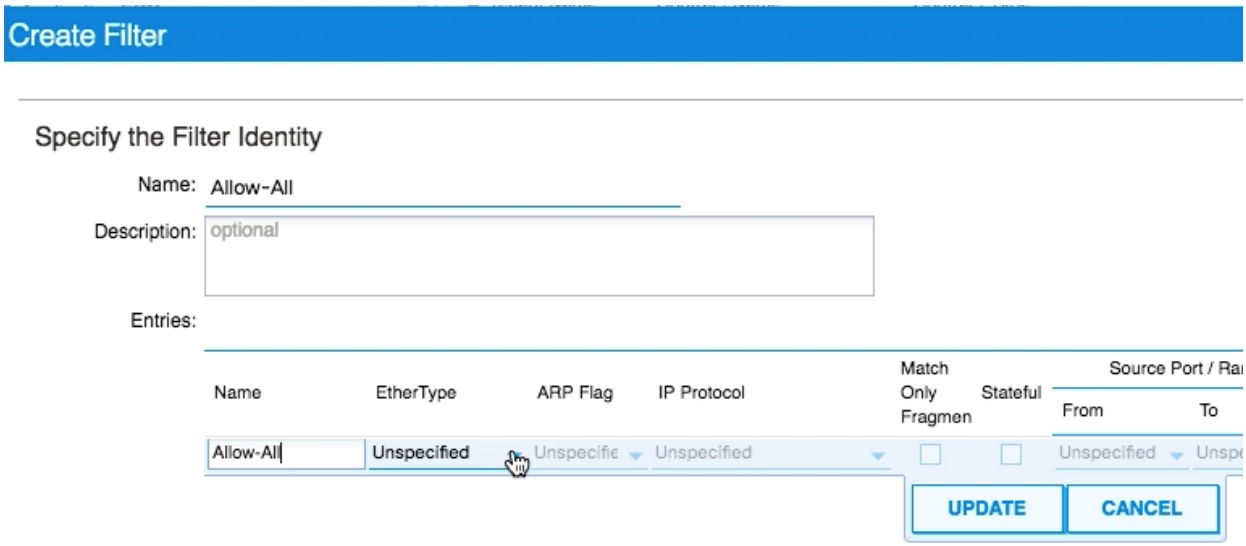
App-Tier to Web-Tier Contract

Provided Contract in EPG App-A-App

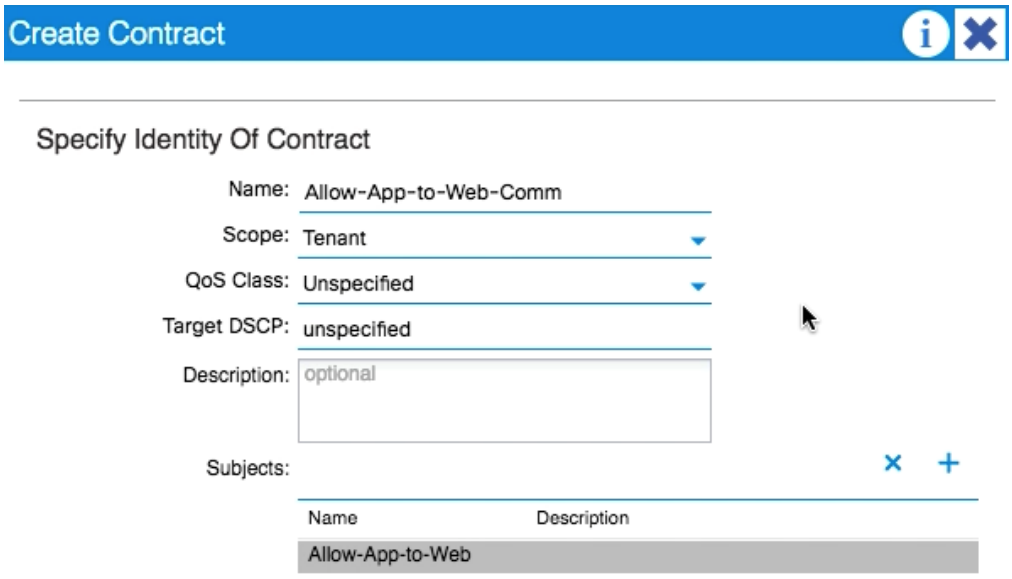
1. In the APIC Advanced GUI, select Tenants > App-A.
2. In the left pane, expand Tenant App-A > Application Profiles > App-A > Application EPGs > EPG App-A-App.
3. Right-click on Contract and select **Add Provided Contract**.
4. In the Add Provided Contract window, from the Contract drop-down list, select **Create Contract**.
5. Name the Contract Allow-App-to-Web-Comm.
6. Select Tenant for Scope.
7. Click **+** to add a Contract Subject.
8. Name the subject Allow-App-to-Web.
9. Click **+** to add a Contract filter.
10. Click **+** to add a new Subject.



11. For Filter Identity Name, enter Allow-All.
12. Enter Allow-All as the name of Entries.



13. From the EtherType drop-down list, select IP.
14. Click **UPDATE**.
15. Click **SUBMIT**.
16. Click **UPDATE** in the Create Contract Subject window.
17. Click **OK** to finish creating the Contract Subject.



18. Click **SUBMIT** to complete creating the Contract.
19. Click **SUBMIT** to complete adding the Provided Contract.

Consumes Contract in EPG App-A-Web

1. In the left pane expand Tenant App-A > Application Profiles > App-A > Application EPGs > EPG App-A-Web.
2. Right-click on Contracts and select **Add Consumed Contract**.
3. In the Add Consumed Contract window, use the drop-down list to select the contract defined in the last step, App-A/Allow-App-to-Web-Comm.

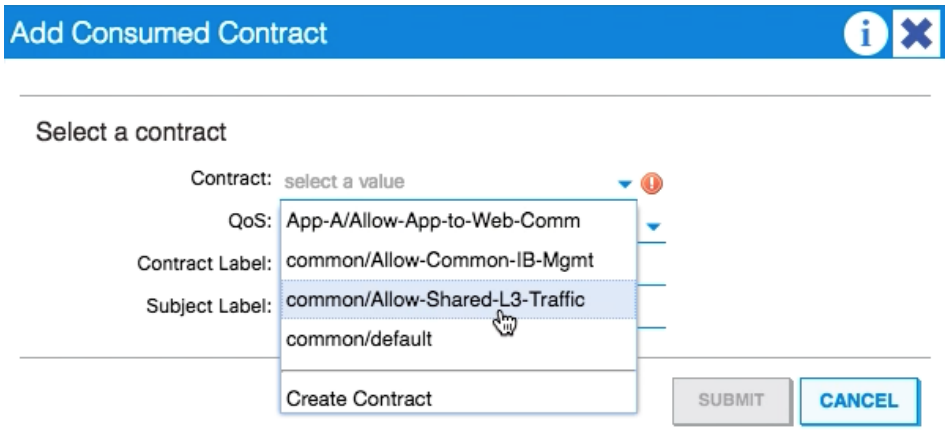
4. Click **SUBMIT** to complete adding the Consumed Contract.

The communication between Web and App tiers of the application should be enabled now. Customers can use more restrictive contracts to replace the Allow-All contract defined in this example.

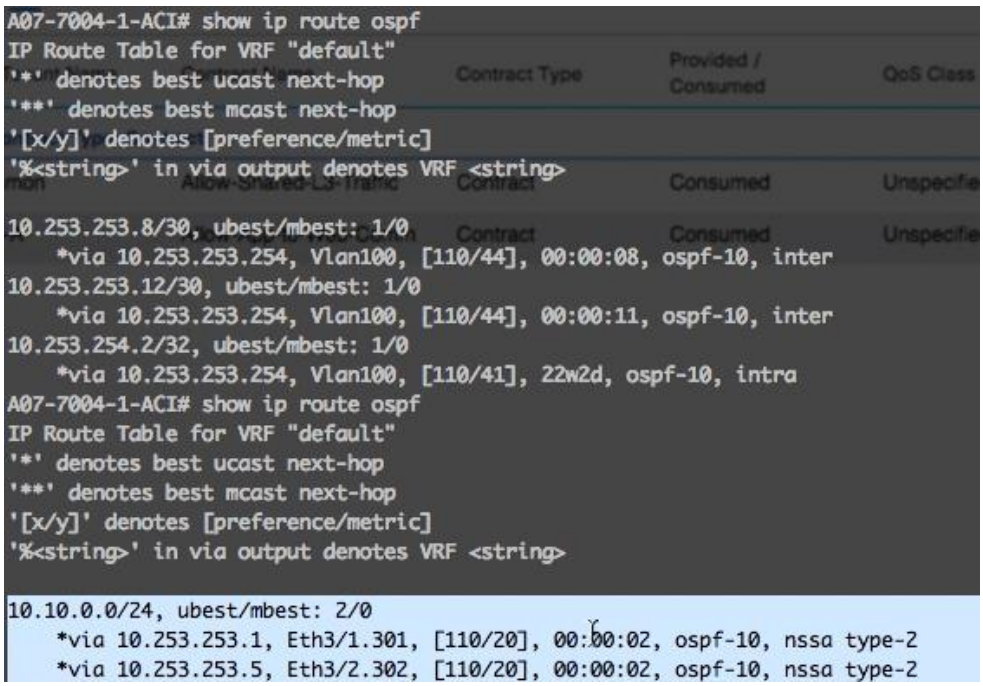
Web-Tier to Shared L3 Out Contract

To enable App-A's Web VMs to communicate outside the Fabric, Shared L3 Out contract defined in the Common Tenant will be consumed in the App-A-Web EPG. Complete the following steps to enable traffic rom Web VMs to outside the fabric:

1. In the APIC Advanced GUI, select Tenants > App-A
2. In the left pane, expand Tenant App-A > Application Profiles > App-A > Application EPGs > EPG App-A-Web
3. Right-click on Contracts and select **Add Consumed Contract**.
4. In the Add Consumed Contract window, use the drop-down list to select Common/Allow-Shared-L3-Traffic.



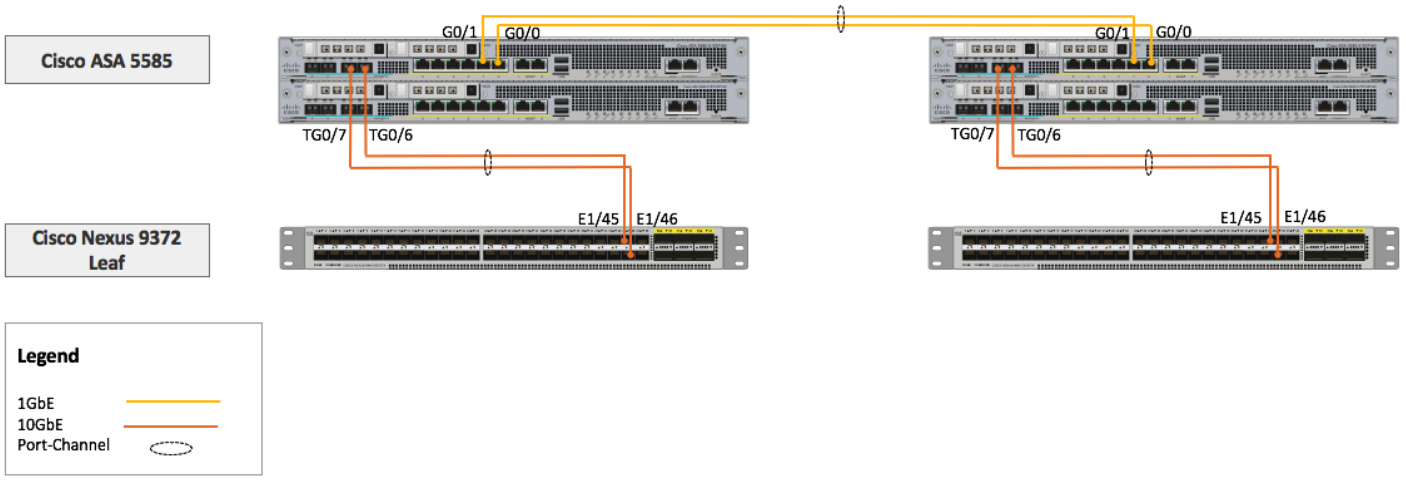
5. Click SUBMIT to complete adding the Consumed Contract.
6. Log into the core Nexus 7000 switch to verify App-A-Web EPG's subnet (10.10.0.0/24) is being advertised



Configuring L4-L7 Services – Network Only Stitching Mode

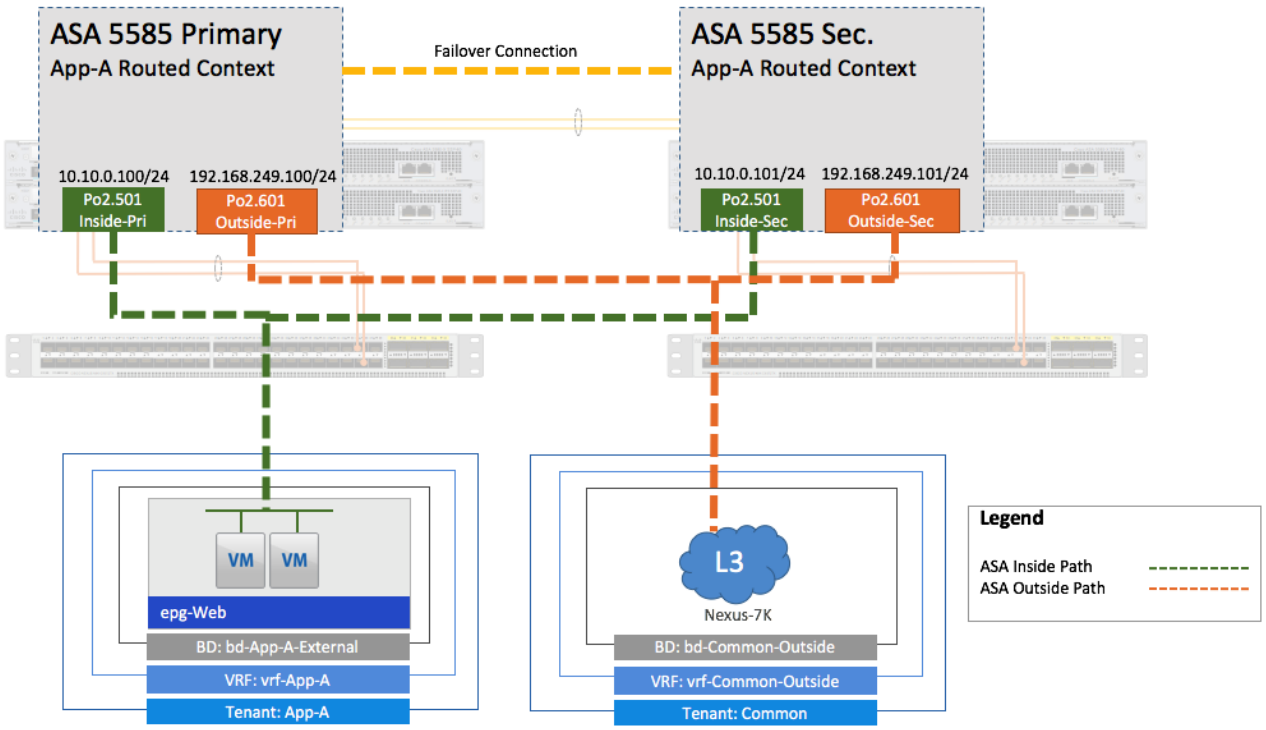
This procedure details an ACI L4-L7 VLAN Stitching feature. In this design, a pair of Cisco ASA-5585 firewall devices in a High Availability configuration is connected to the ACI Fabric. The firewalls are connected to Cisco Nexus 9372 leaf switches as shown in Figure 11.

Figure 11 – Cisco ASA Physical Connectivity



VLAN Stitching does not make use of device packages therefore ASA devices need to be configured using CLI or ASDM. However, Cisco ACI fabric will configured as shown in this section to provide the necessary traffic/VLAN "stitching". The VLANs and IP subnet details utilized in this setup are shown in Figure 12.

Figure 12 – Cisco ASA Logical Connectivity



Cisco ASA – Sample Configuration

The following configuration is a sample from the ASA devices.

The Cisco ASA configuration below is not complete and is meant to be used only as a reference.

Cisco ASA System Context

```
interface TenGigabitEthernet0/6
 channel-group 2 mode active
!
interface TenGigabitEthernet0/7
 channel-group 2 mode active
!
interface Port-channel2
 description To Nexus 9K Leaf
 lacp max-bundle 8
!
interface Port-channel2.501
 description Inside Interface for Context N1
 vlan 501
!
interface Port-channel2.601
 description Outside Interface for Context N1
 vlan 601
!
context N1
  allocate-interface Port-channel2.501
  allocate-interface Port-channel2.601
```

```
  config-url disk0:/N1.cfg
  join-failover-group 1
!
```

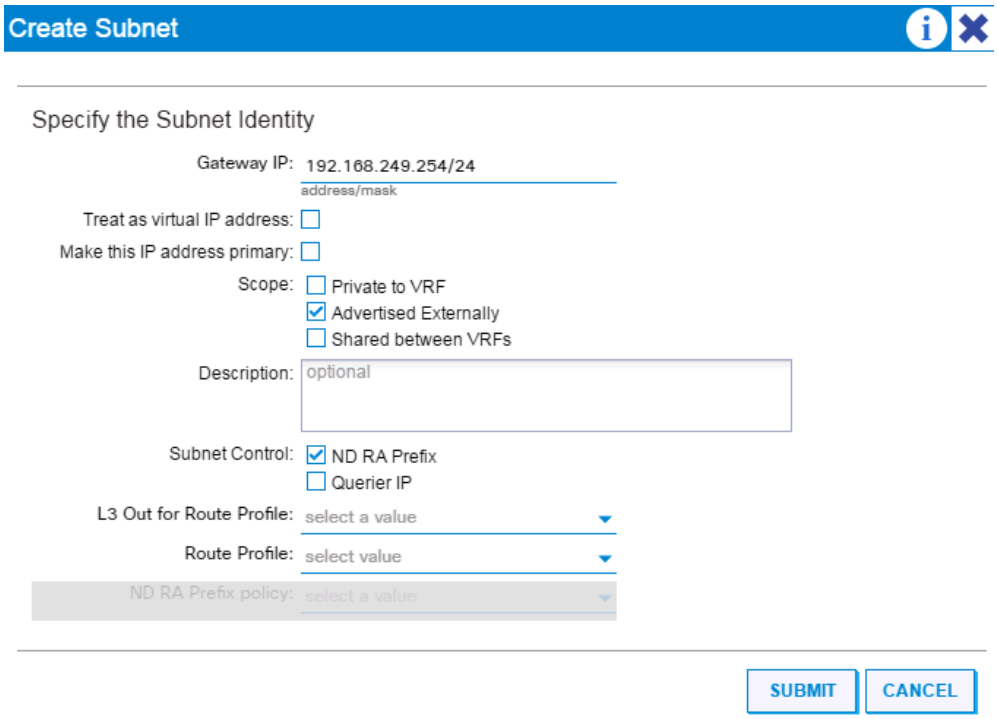
Cisco ASA Context for Application App-A

```
!
interface Port-channel2.501
 nameif inside
 security-level 100
 ip address 10.10.0.100 255.255.255.0 standby 10.10.0.101
!
interface Port-channel2.601
 nameif outside
 security-level 0
 ip address 192.168.249.100 255.255.255.0 standby 192.168.249.101
!
object network Inside-Net
 subnet 10.10.0.0 255.255.255.0
!
access-list permit-all extended permit ip any any
access-list outside_access_in extended permit ip any any
!
object network Inside-Net
 nat (any,outside) dynamic interface
!
access-group outside_access_in in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.249.254 1
!
```

Create Gateway for ASA Outside interfaces in tenant common

Create Subnet under Bridge Domain

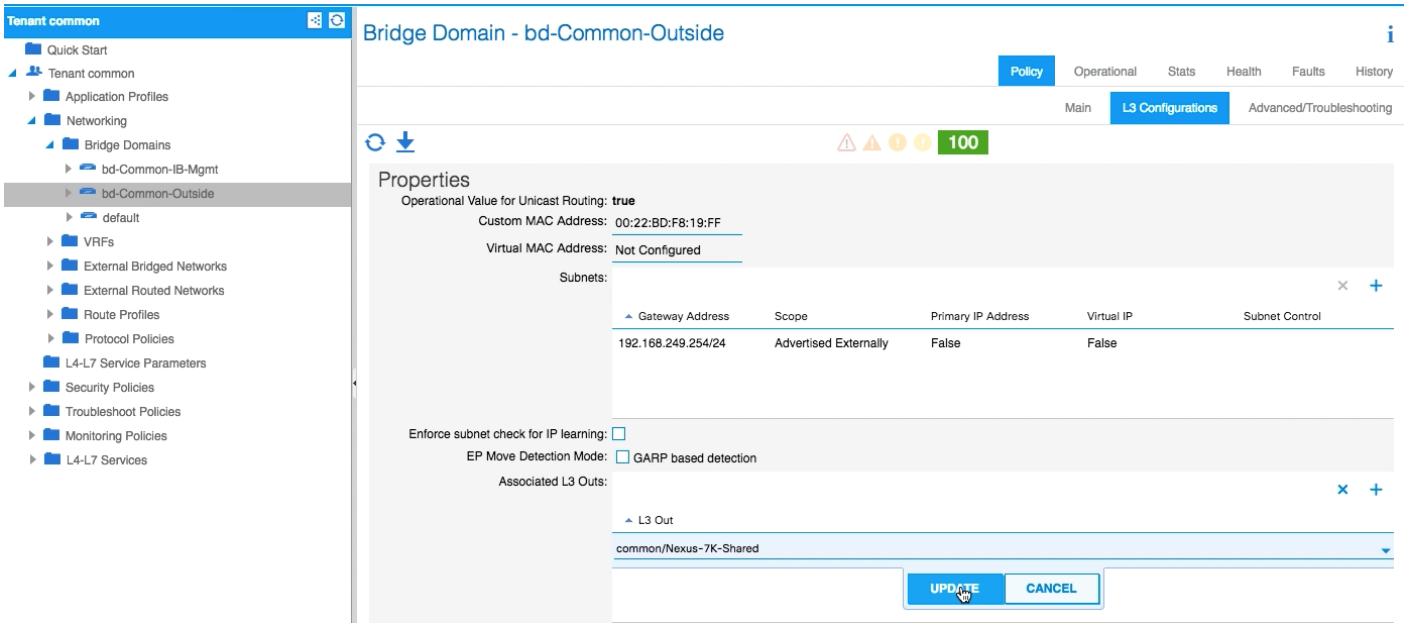
1. In APIC advanced GUI, click on Tenant > Common.
2. Expand Tenant Common > Networking > Bridge Domain > bd-Common-Outside.
3. Right-click on the Subnets and select **Create Subnet**.
4. Enter the gateway IP address and subnet and set the scope as shown in the figure below. The GW IP address used in this validation is 192.168.249.254/24.



5. Click **SUBMIT**.

Create Subnet under Bridge Domain

1. Click the **Bridge Domain bd-Common-Outside** and in the right pane under Policy, select **L3 Configurations**.
2. Click **+** to Associate L3 Out.
3. From the drop-down list, select common-7K-Shared and click **UPDATE**.

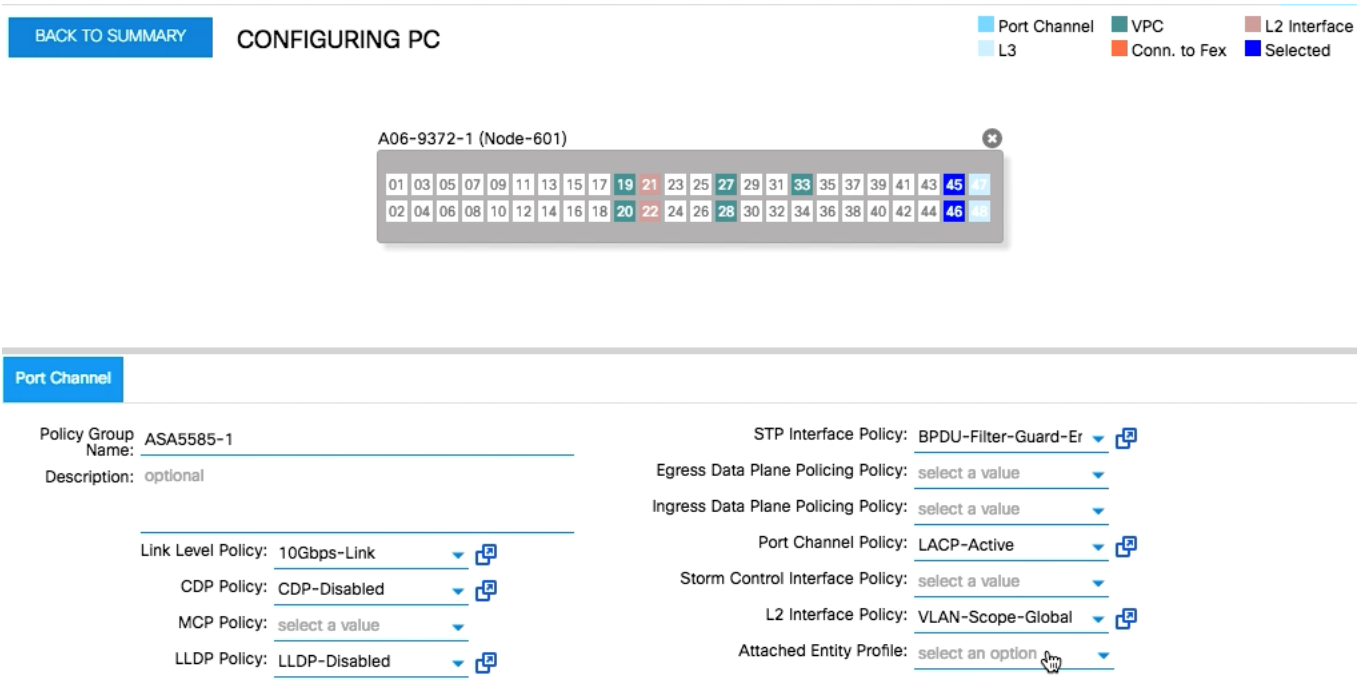


4. Click **SUBMIT**.

Create Port-Channels for Cisco ASA Devices

This section details setup of port-channels for the Cisco ASA-5585 devices as shown in Figure 11.

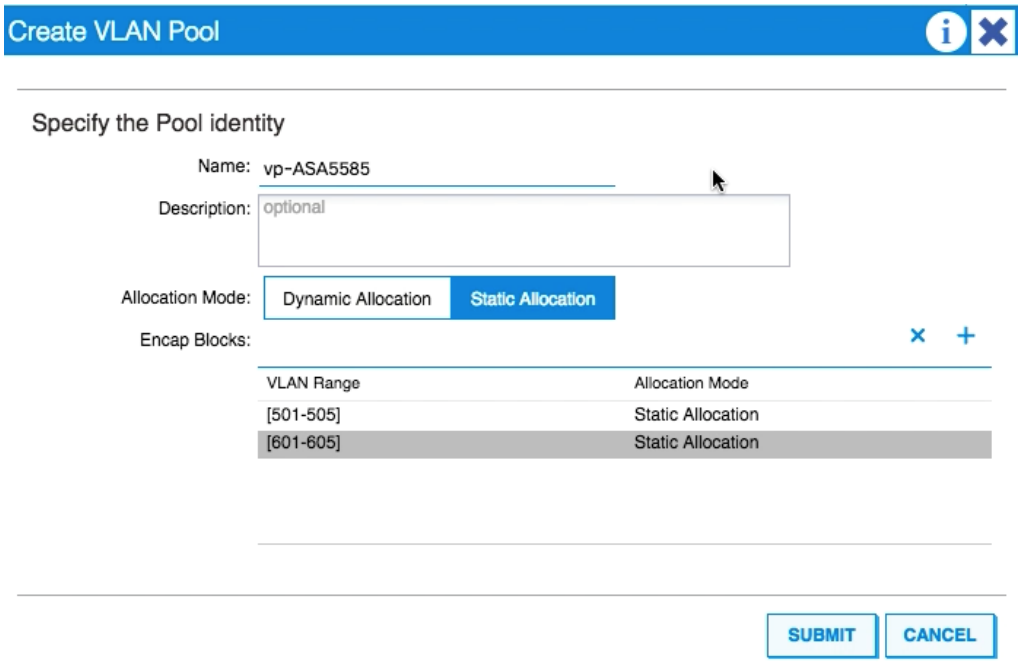
1. From the Cisco APIC Advanced GUI, at the top, select Fabric > Inventory.
2. In the left pane select Topology and then select **Configure**.
3. Select ADD SWITCHES.
4. Select the leaf switch the first ASA is attached to. Click **ADD SELECTED**.
5. Select the ports (45 and 46) that are connected the first ASA. On the lower right, click **CONFIGURE PC**.
6. Name the Policy Group ASA5585-1.
7. Select the appropriate policies as shown in the screenshot.



The STP interface Policy in the figure above is set to BPDU-Filter-Guard-Enabled

8. From the Attached Entity Profile drop-down list, select **Create Attachable Access Entity Profile**.
9. Name the profile aep-ASA5585. Click **+** to add a Domain.
10. From the drop-down list, select **Create Physical Domain**.
11. In the Create Physical Domain window, name the Domain pd-ASA5585.

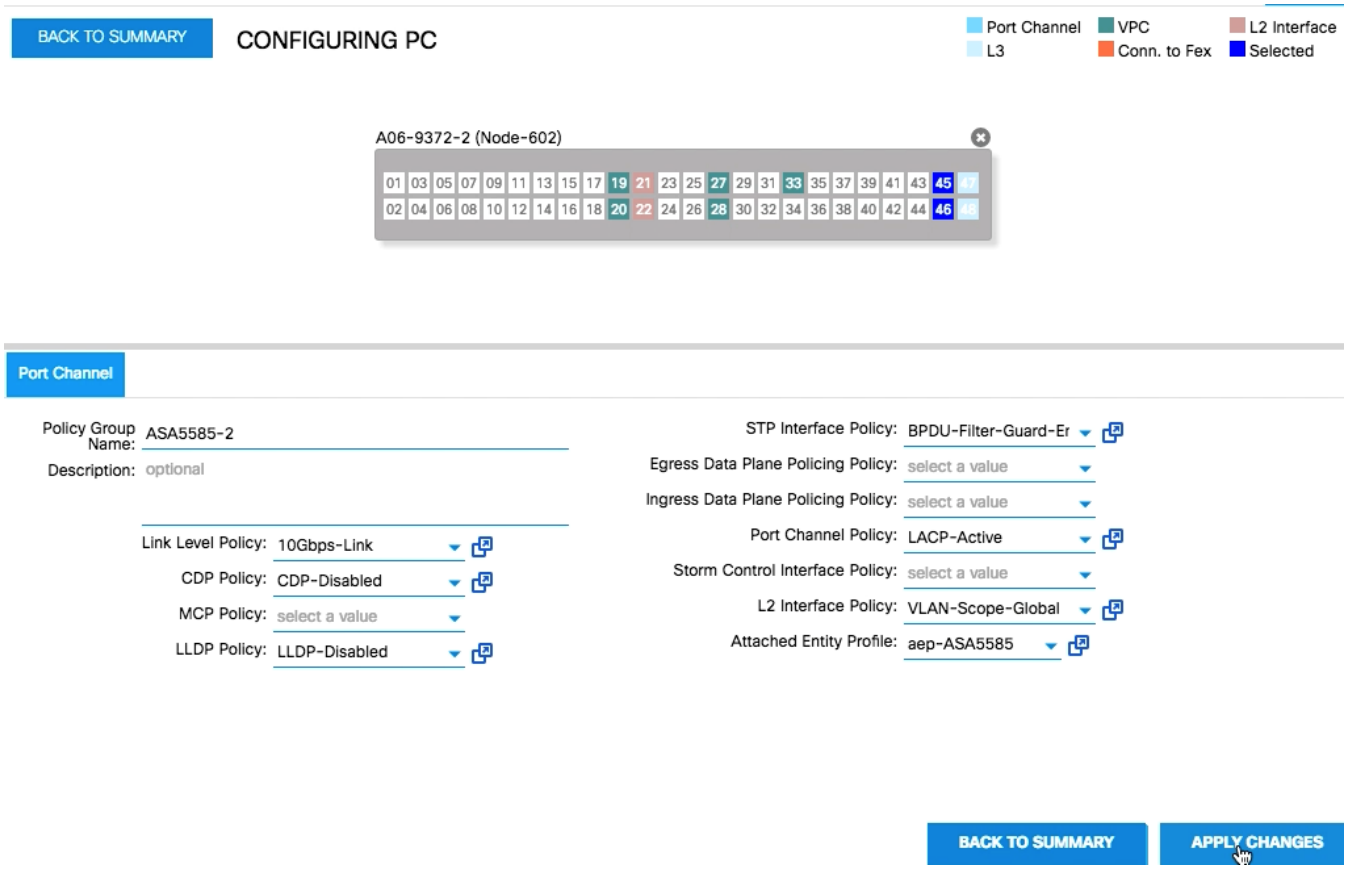
12. From the VLAN Pool drop-down list, select **Create VLAN Pool**.
13. In the Create VLAN Pool window, name the VLAN Pool VP-ASA.
14. Select **Static Allocation**. Click **+** to add a VLAN range to the pool.
15. In the Create Ranges window, input the From and To values for VLANs to be used for the firewall Inside and Outside VLANs. Select **Static Allocation**.
16. Click **OK** to complete creating the VLAN range.



In this validation, two different ranges of 5 VLANs (total 10 VLANs) are added to the pool. VLANs 501-505 are to be used to configure up to 5 tenant context inside interfaces. VLANs 601-605 are to be used for up to 5 tenant context outside interfaces. Customers can adjust these ranges based on number of tenants.

17. Click **SUBMIT** to complete creating the VLAN Pool.
18. Click **SUBMIT** to complete creating the Physical Domain.
19. Click **UPDATE**.
20. Click **SUBMIT** to complete creating the Attachable Access Entity Profile.
21. Click **APPLY CHANGES** to complete creating the Port-Channel.
22. Click **OK** for the confirmation.
23. On the second leaf switch, select the ports that are connected the second ASA.
24. Repeat the above procedure to configure the port-channel to second ASA.

There is no need to create a new Attached Entity Profile. From the drop-down list, select the aep-ASA5585 configured in the last step.



Create Tenant L4-L7 Device and Service Graph

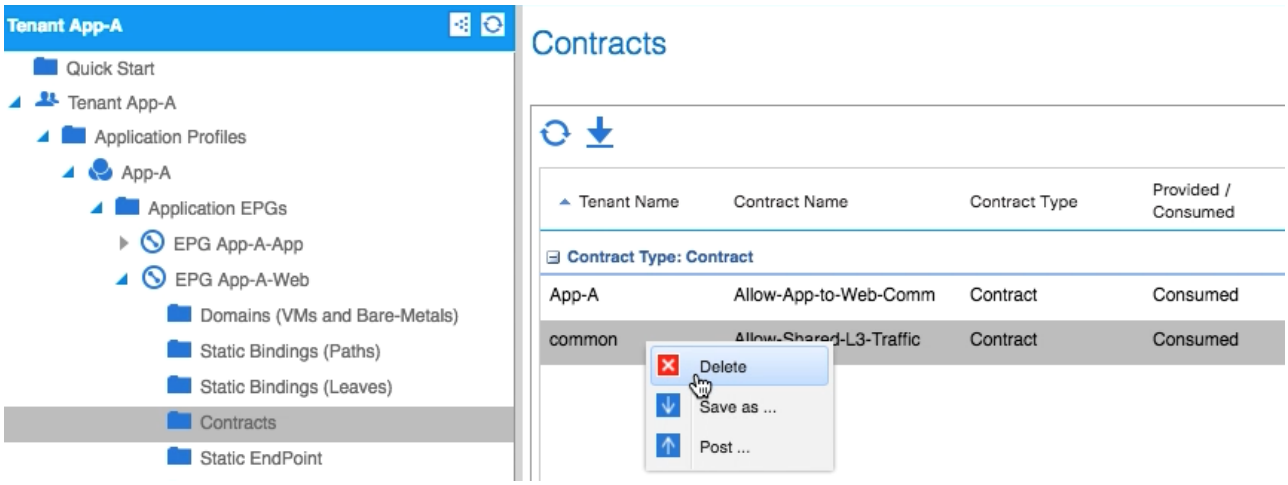
This section covers L4-L7 Device and Service Graph setup for tenant App-A.

1. From the Cisco APIC Advanced GUI, select Tenants > App-A.
2. In the left pane expand Tenant App-A, Application Profiles, Three-Tier-App, Application EPGs, and EPG Web.

Remove the Existing Connectivity through L3 Out

The Shared L3 connectivity configured previously must be removed and replaced by ASA Firewall contracts.

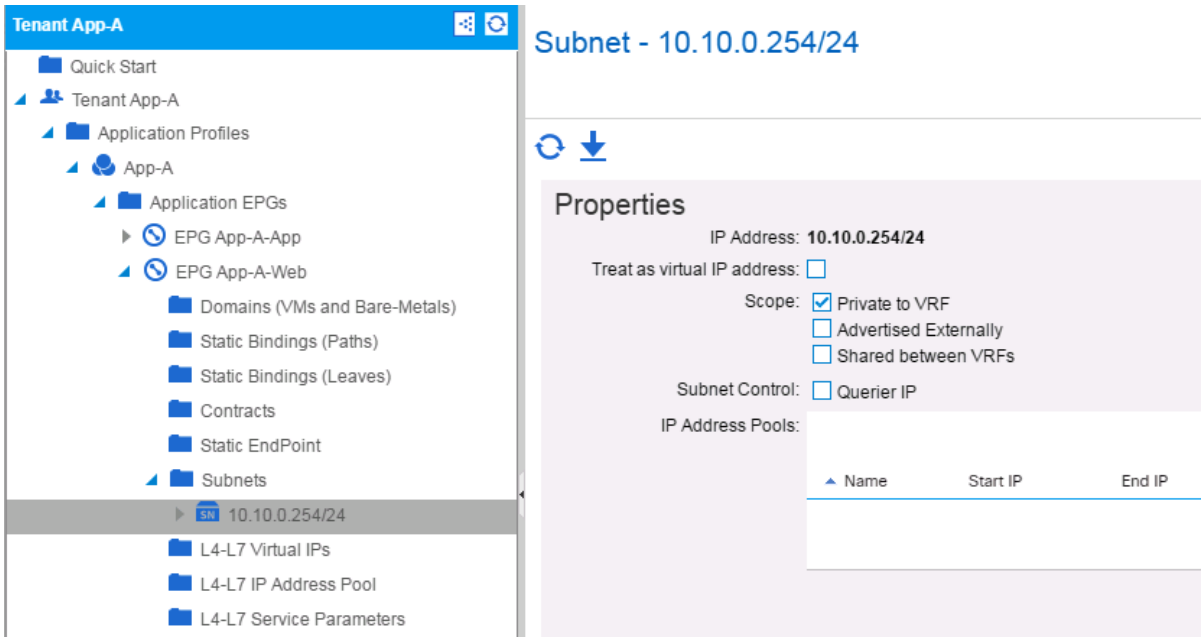
1. Under EPG Web, select **Contracts**.
2. Right-click on the Allow-Shared-L3-Traffic contract and select **Delete** to remove this contract association.



3. Click **YES** for the confirmation.

4. In the left pane, expand Subnets and select **EPG subnet**.

5. Under the Properties area, uncheck the check box Advertised Externally. If the Web EPG is connected to the Core-Services, then keep the option Shared between VRFs selected. Otherwise, select Private to VRF.



6. Click **SUBMIT** to complete modifying the subnet.

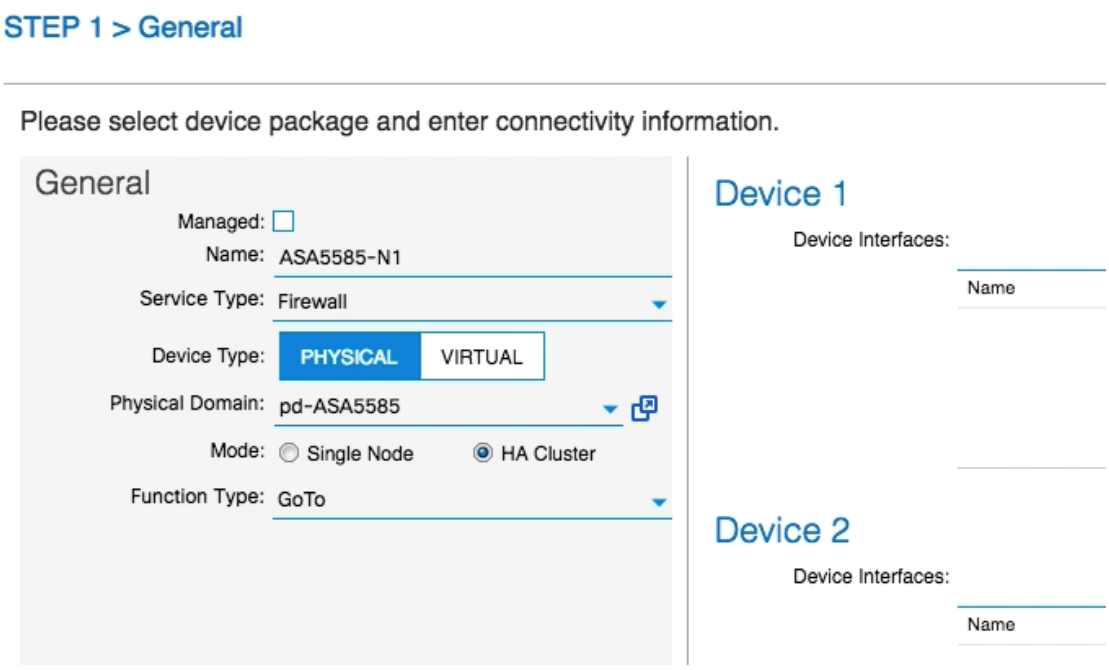
At this point, log into the Nexus 7000 and verify the subnet defined under the EPG has disappeared from the routing table and is not learnt via OSPF anymore.

Create L4-7 Devices

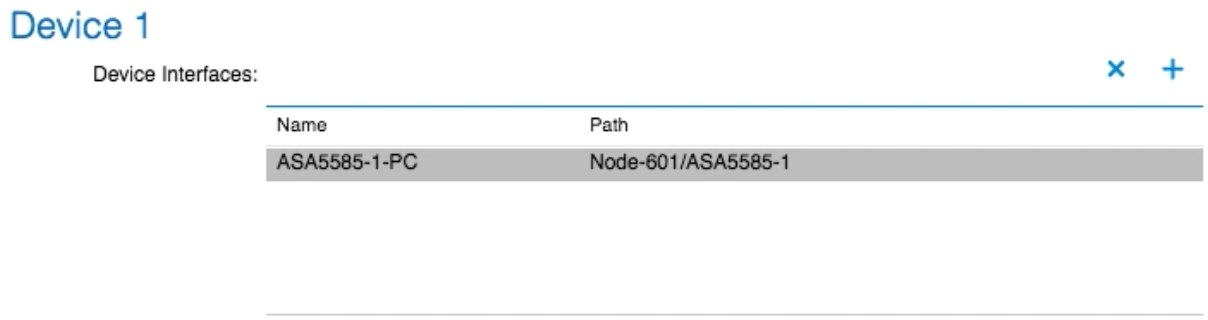
1. In the left pane expand Tenant App-A and L4-L7 Services.

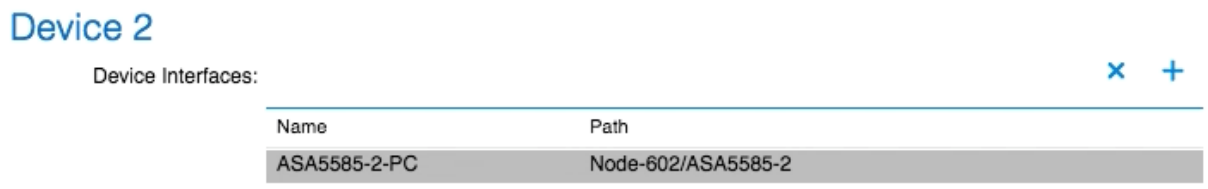
2. Right-click on the L4-L7 Devices and select **Create L4-L7 Devices**.

3. In the Create L4-L7 Devices window, uncheck the Managed check box.
4. Name the Device ASA5585-<context name>. This deployment uses the ASA5585-N1 as the name.
5. Select the Firewall as Service Type.
6. For the Physical Domain, select pd-ASA5585.
7. Select the HA Cluster Mode.
8. For the Function Type, select GoTo.

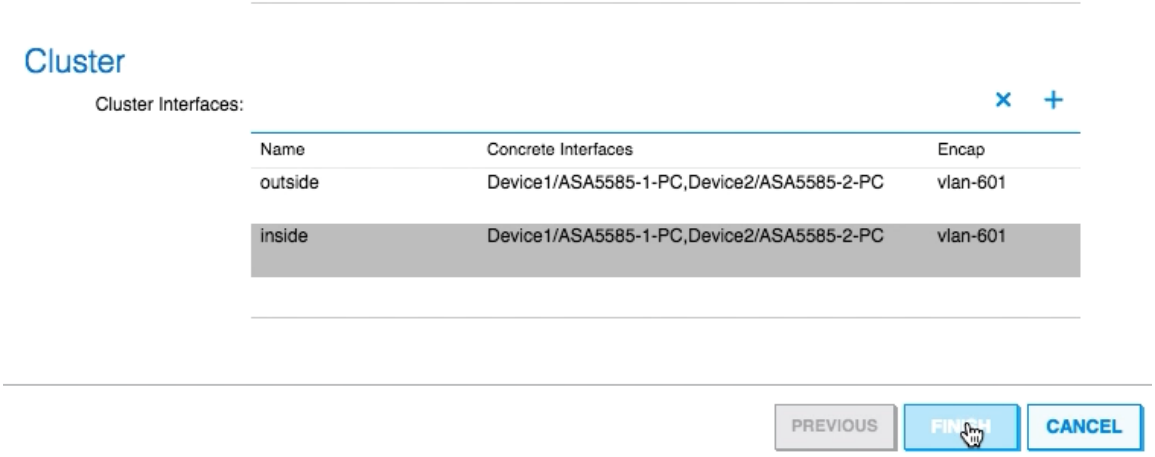


9. Under Device 1, Click **+** to add the Device Interface.
10. Name the Device Interface ASA5585-1-PC.
11. From the drop-down list, select Path Type PC.
12. Select the PC for the first ASA.
13. Click **UPDATE**.
14. Under Device 2, click **+** to add the Device Interface.
15. Name the Device ASA5585-2-PC.
16. From the drop-down list, select **Path Type PC**.
17. Select the PC for the second ASA.
18. Click **UPDATE**.





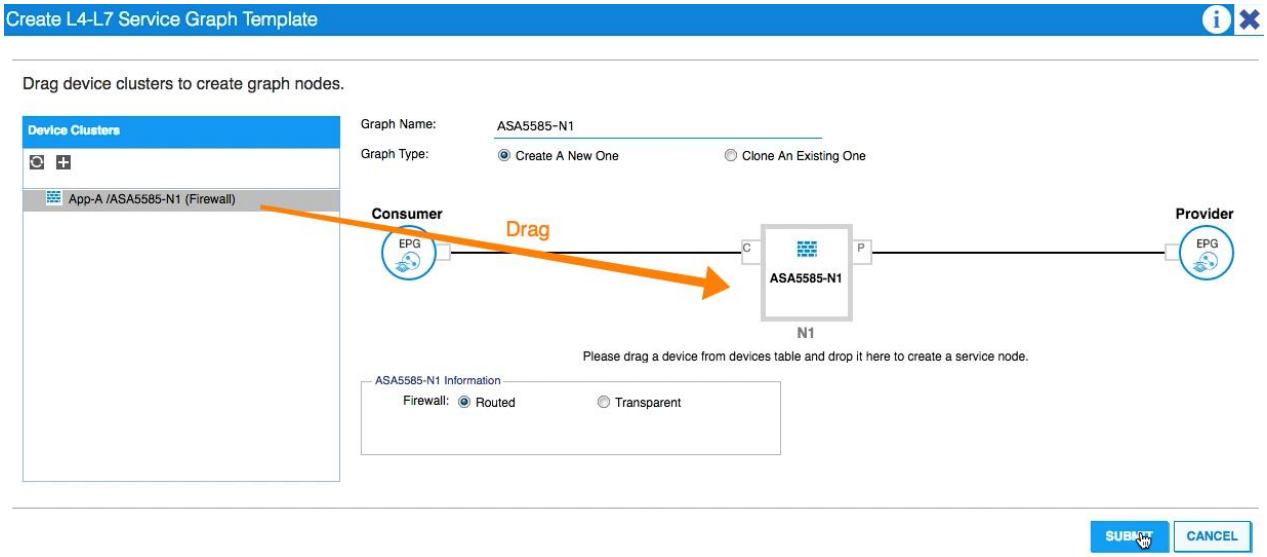
19. Under Cluster, click **+** to add a Concrete Interface.
20. Name the interface outside.
21. From the drop-down list, select both the ASA-1 and ASA-2 devices.
22. For Encap, input vlan<App-A-outside-VLAN-ID> (Vlan-601).
23. Click **UPDATE**.
24. Under Cluster, click **+** to add a second Concrete Interface.
25. Name the interface inside.
26. From the drop-down list, select both the ASA-1 and ASA-2 devices.
27. For Encap, input vlan<App-A-inside-VLAN-ID> (VLAN 501).
28. Click **UPDATE**.



29. Click **FINISH** to complete creating the L4-L7 Device.

Create L4-L7 Service Graph Template

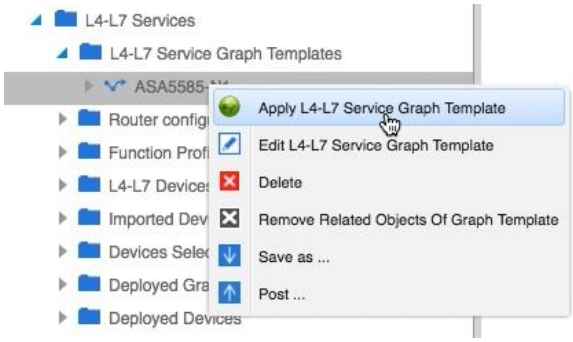
1. Right-click L4-L7 Service Graph Templates and select Create L4-L7 Service Graph Template.
2. In the Create L4-L7 Service Graph Template window, name the Graph ASA-5585-N1-Context.
3. Make sure Graph Type is set to Create A New One.
4. Drag the ASA5585-N1 Firewall icon to between the two EPGs.
5. Select the Routed Firewall.



6. Click **SUBMIT** to complete creating the Service Graph Template.

Apply Service Graph Template

7. In the left, expand L4-L7 Service Graph Templates and select the ASA5585-N1 Template.
8. Right-click the ASA-App-A-Context Template and select Apply L4-L7 Service Graph Template.

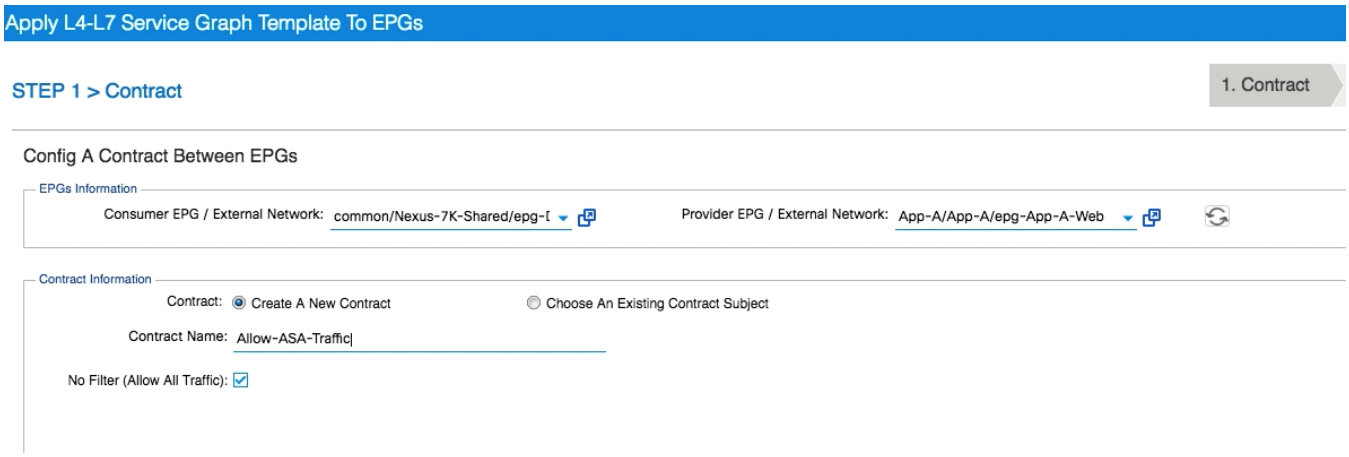


9. In the Apply L4-L7 Service Graph Template to EPGs window, from the Consumer EPG drop-down list, select common/Nexus-7K-Shared/epg-Default-Route.

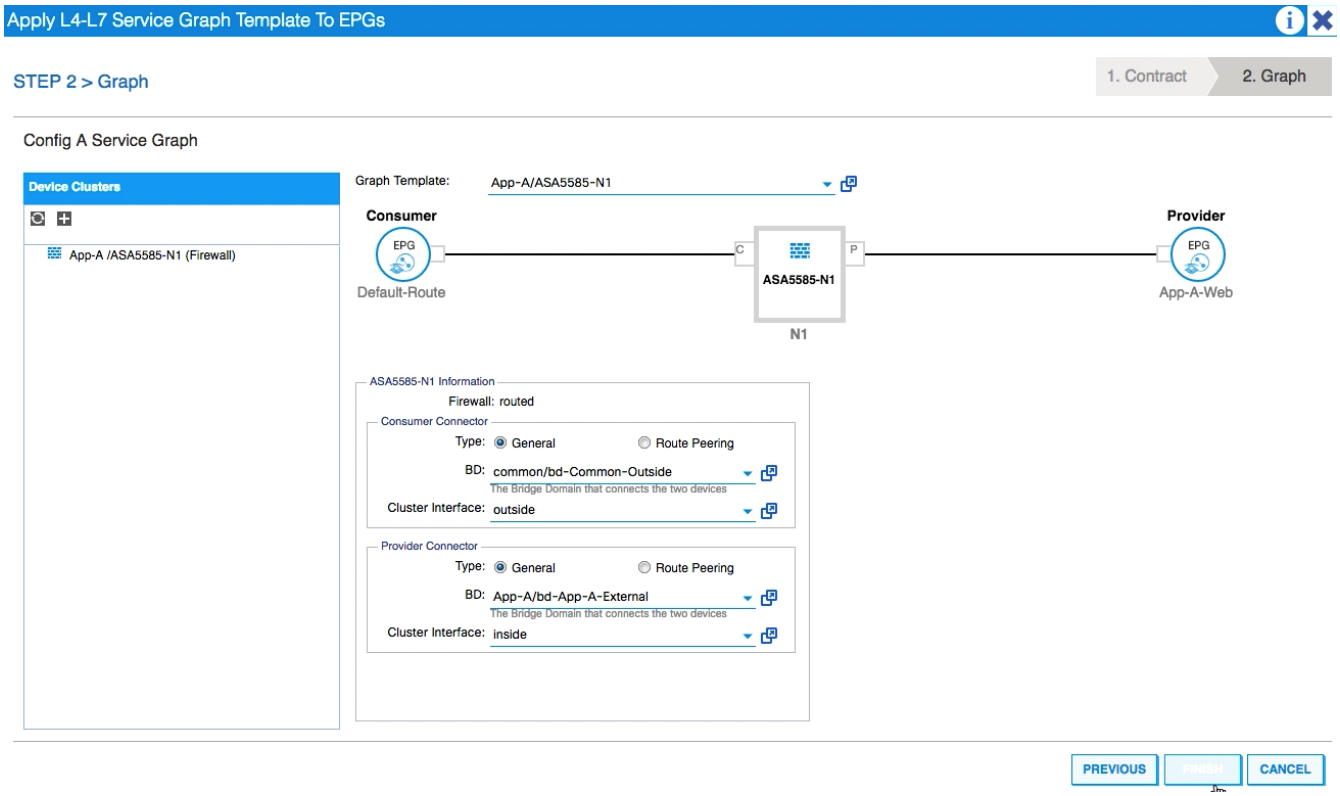
10. From the Provider EPG drop-down list, select App-A/App-A/epg-App-A-Web.

These EPG selections place the firewall between the Shared-L3-Out and App-A Web EPGs.

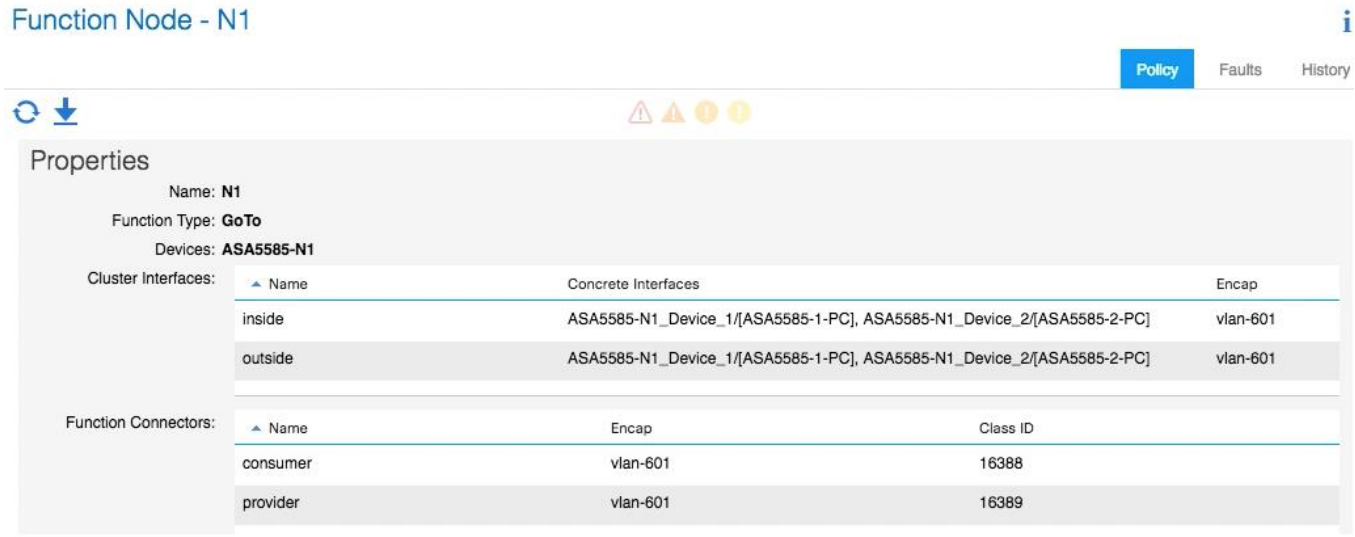
11. Under Contract Information, leave Create A New Contract selected and name the contract Allow-ASA-Traffic.



12. Click **NEXT**.
13. Under Consumer Connector, from the BD drop-down list, select common/bd-Common-Outside.
14. Under Consumer Connector, from the Cluster Interface drop-down list, select outside.
15. Under Provider Connector, from the BD drop-down list, select App-A/bd-App-A-External.
16. Under Provider Connector, from the Cluster Interface drop-down list, select inside.



17. Click **FINISH** to compete applying the Service Graph Template.
18. In the left pane expand Deployed Graph Instances and Allow-ASA-Traffic-ASA5585-N1.
19. Select Function Node – N1.
20. Verify that the Function Connectors display values for Encap and interfaces.



21. For VMs with interfaces in the Web EPG, set the default gateway to the ASA's inside interface IP (10.10.0.100/24).

22. The ASA in this deployment was configured to NAT all the Web tier traffic to ASA's outside interface IP address.

23. Log into the Nexus 7000 and verify the 192.168.249.0/24 subnet is not being advertised from the leaf switches.

```
A07-7004-1-ACI# show ip route 192.168.249.0/24
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

192.168.249.0/24, ubest/mbest: 2/0
    *via 10.253.253.1, Eth3/1.301, [110/20], 4d17h, ospf-10, nssa type-2
    *via 10.253.253.5, Eth3/2.302, [110/20], 4d17h, ospf-10, nssa type-2
```

About the Authors

Haseeb Niazi, Technical Marketing Engineer, Computing Systems Product Group, Cisco Systems, Inc.

Haseeb Niazi has over 17 years of experience at Cisco in the Data Center, Enterprise and Service Provider solutions and technologies. As a member of various solution teams and Advanced Services, Haseeb has helped many enterprise and service provider customers evaluate and deploy a wide range of Cisco solutions. As a technical marking engineer at Cisco UCS solutions group, Haseeb currently focuses on network, compute, virtualization, storage and orchestration aspects of various Compute Stacks. Haseeb holds a master's degree in Computer Engineering from the University of Southern California and is a Cisco Certified Internetwork Expert (CCIE 7848).

Adam H. Reid, Test Specialist, Systems & Technology Group, IBM

Adam H. Reid is a published author with more than 15 years of Computer Engineering experience. Focused more recently on IBM's Spectrum Virtualize, he's been deeply involved with the testing and configuration of virtualized environments pivotal to the future of software defined storage. Adam has designed, tested and validated systems to meet the demands of a wide range of mid-range and enterprise environments.

Acknowledgements

Following individual(s) contributed to building this solution and participated in writing of this design document:

- Sreenivasa Edula, Technical Marketing Engineer, Cisco Systems, Inc.
- John George, Technical Marketing Engineer, Cisco Systems, Inc.