SmartFabric Storage Software

Deployment Guide

H19016

Abstract

This guide demonstrates the planning and deployment of SmartFabric Storage Software (SFSS) for NVMe over TCP (NVMe/TCP). Example network topologies are provided, followed by the prerequisite network configuration steps. SFSS is deployed and configured, and the hosts and subsystems are registered with SFSS. Zoning operations such as the creation of a zone group, zone, and the addition of zone members are provided in the deployment example.

Dell Technologies Solutions

February 2022

DELL Technologies

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1

Introduction

Purpose of this guide

This guide demonstrates the planning and deployment of Dell SmartFabric Storage Software (SFSS) for NVMe over TCP (NVMe/TCP) on compatible host and storage systems.

Draft comment: The URL below directs the user to the main support page and not to the specific document. Please provide the URL to the document, or the URL to a location within the product support page.

NOTE: For post-deployment administration tasks such as licensing and life-cycle management, see the SmartFabric Storage Software User Guide.

Dell Technologies

Our vision at Dell Technologies is to be the essential technology company for the data era. Dell ensures modernization for today's applications and for the emerging cloud-native world.

Dell is committed to disrupting the fundamental economics of the market with an open strategy that gives you the freedom of choice for networking operating systems and top-tier merchant silicon. Our strategy enables business transformations that maximize the benefits of collaborative software and standards-based hardware, including lowered costs, flexibility, freedom, and security. Dell provides further customer enablement through validated deployment guides that demonstrate these benefits while maintaining a high standard of quality, consistency, and support.

NVMe and NVMe-oF

The Non-Volatile Memory Express (NVMe) family of specifications defines how host software communicates with nonvolatile memory across multiple transports like PCI Express (PCIe), RDMA, TCP and more. For more information about NVMe specifications, see https://nvmexpress.org/specifications/.

NVMe over Fabrics (NVMe-oF) extends the capabilities of NVMe by enabling NVMe commands to traverse a network to SAN storage, rather than to local disks only.

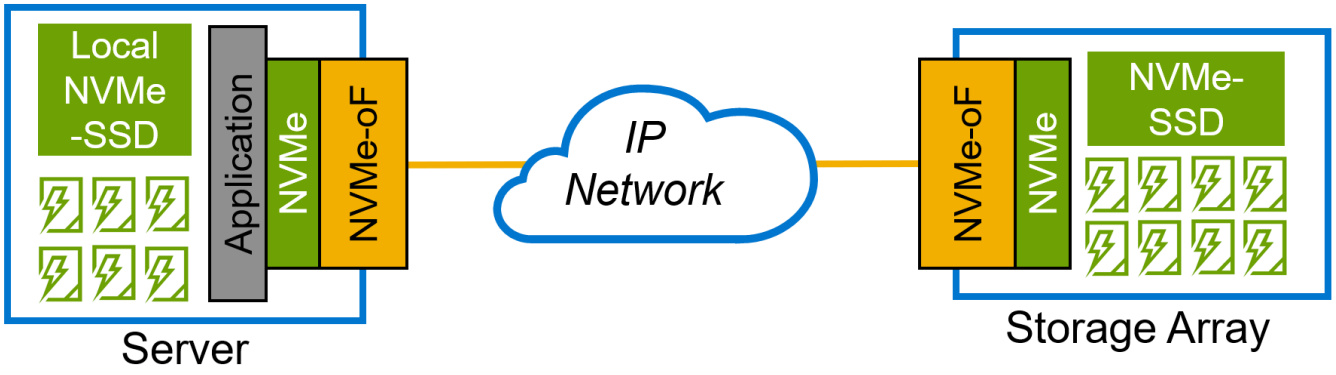


Figure 1. NVMe over Fabrics (NVME-OF)

The different types of NVMe-oF transports include:

- Transmission Control Protocol (TCP)

- Fibre Channel (FC)
- Remote Direct Memory Access (RDMA)
  - iWARP
  - RoCEv2

NOTE: For detailed information about NVMe-oF, see the NVM Express NVMe Over Fabrics White Paper.

This deployment guide focuses on building an end-to-end storage area network solution using NVMe over TCP (NVMe/TCP).

Why NVMe over TCP

NVMe provides superior performance to SCSI in devices such as servers and high-performance storage arrays. NVMe over TCP (NVMe/TCP) uses an Ethernet infrastructure, without the need for specialized network switches or Host Bus Adapters (HBAs). This is more cost effective when compared with an FC storage network. Since an Ethernet network is used, higher bandwidth such as 100 Gb can be leveraged. Compared to FC, the price for Ethernet is also reduced, which provides a significant advantage.

By adopting a standards-based approach to NVMe/TCP, customers can run NVMe/TCP over a standard Ethernet-based infrastructure without the need to configure lossless behavior from end-to-end, as required when using RoCE.

Table 1. Comparison of NVMe-oF features

Feature	NVMe/TCP	Fibre Channel	Ethernet iSCSI	NVMe/RoCEv2
High-Speed Performance	Y	Y		Y
Software Defined Storage	Y		Y	Y
Centralized Provisioning	Y	Y		Y
State Change Notifications	Y	Y		Y
Edge/Distributed System at Scale	Y			
Cloud Operating Model/Automation	Y			
CapEx Cost Advantage	Y		Y	

SmartFabric Storage Software (SFSS)

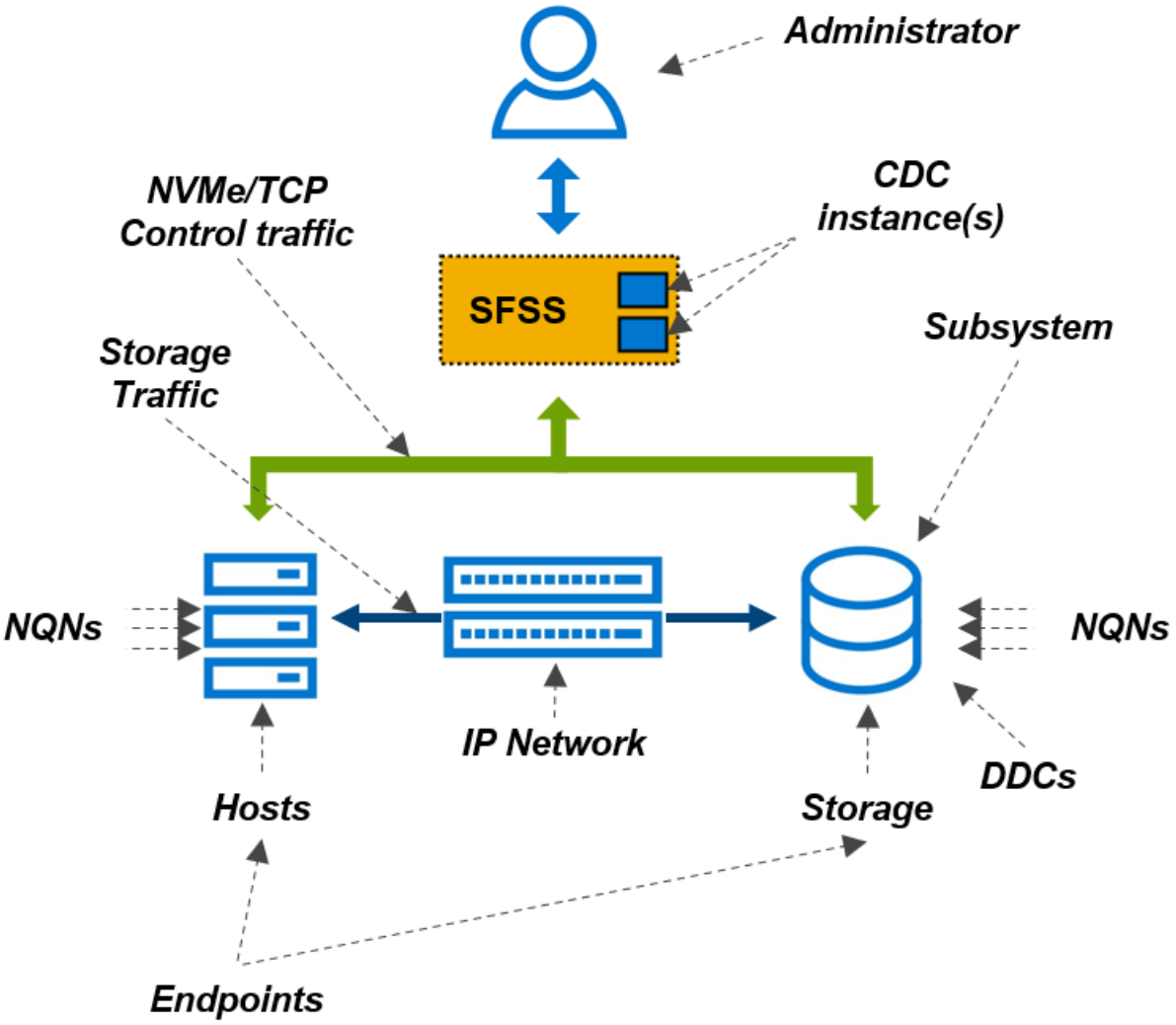


Figure 2. SFSS and NVMe/TCP ecosystem

Dell SmartFabric Storage Software (SFSS) is Dell Technologies implementation of a Centralized Discovery Controller (CDC) that allows administrators to deploy NVMe/TCP at scale. SFSS accomplishes this by providing a Centralized Discovery Service for NVMe/TCP Endpoints that facilitates endpoint discovery, registration, soft zoning, and event notification.

With SFSS, Dell Technologies provides the industry's first comprehensive connectivity automation solution for NVMe/TCP endpoints such as Dell PowerEdge and Dell PowerStore.

You can install SFSS on an ESXi host by deploying an OVA.

NOTE: For more information about SFSS Software models and compatible endpoints, see the Networking Support and Compatibility Matrix.

Before the introduction of the CDC, NVMe/TCP was an end node-centric storage protocol where administrators would manually configure each host to connect to one or more Direct Discovery Controllers (DDCs) on the storage arrays. This manual configuration process was found to be error-prone and time consuming.

SFSS is designed to ensure that hosts can automatically connect to the appropriate NVM subsystem (array) interfaces by:

- Using mDNS to discover the available NVMe Discovery Controllers
- Using get log pages to retrieve a list of IO interfaces that the host has been allowed to access.

Also, SFSS provides features that enable SFSS to provide a fibre channel-like user experience over the NVMe/TCP transport.

Table 2. Comparison of Fibre Channel and SFSS NVMe/TCP terminology

Equivalent of Fibre Channel	Service and notifications	Details of service and notifications
Name Server Database	Discovery Service	NVMe/TCP endpoints dynamically discover the CDC
		Listen and respond to mDNS queries from endpoints in the fabric, where supported
	Endpoint Registration Service	The host and subsystem register their information with the CDC by sending a "Log Page" that includes NQNs, IPs, symbolic names, and other information.
	Endpoint Query Service	NVMe/TCP Hosts query the CDC to discover the NVMe/TCP subsystems they can communicate with
Zone Server Database	Zone Service	Details the soft zoning configured in SFSS. Get Log Page responses only include subsystems zoned for the querying host
Registered State Change Notification (RSCN)	Asynchronous Notifications	Asynchronous Event Registration – subscribe to state change notifications from Endpoints
		Asynchronous Event Notifications – send notifications to Endpoints for state changes

The following terms are used throughout this document.

Endpoints IP addresses on servers and storage that take part in the NVMe/TCP IP SAN.

Centralized Discovery Controller (CDC) Industry term for software that automates registration of NVMe/TCP endpoints.

Subsystems Storage target identified by NQN.

Direct Discovery Controller (DDC) CDC communicates with the DDC on the storage array on the default TCP port 8009.

CDC instance A logical division of interfaces in the SFSS VM. CDCs provide administrative separation.

2

Network Planning

This section covers design considerations for the IP network carrying NVMe/TCP traffic. At a high-level, the network must provide connectivity between SFSS, hosts, and storage as follows:

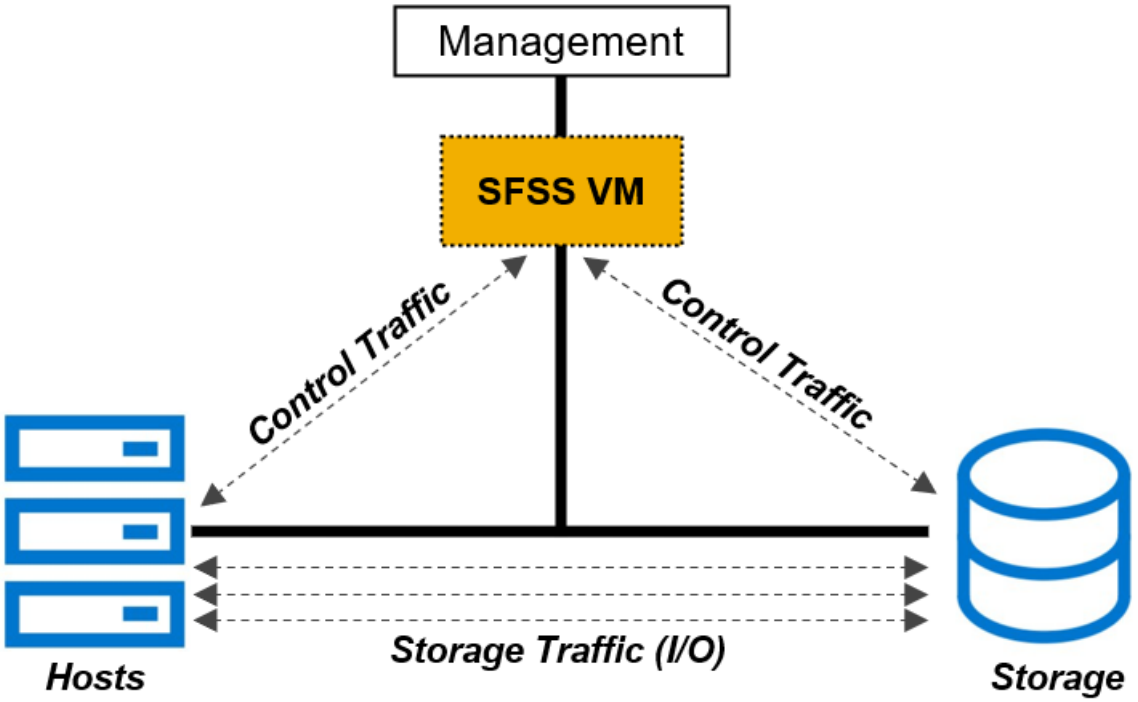


Figure 3. NVMe/TCP and SFSS connectivity requirements

Network design considerations

A key requirement of a storage network is to provide multiple active paths between hosts and storage. This is achieved by creating multiple sources and multiple destinations across separate broadcast domains.

VMware ESXi requirements

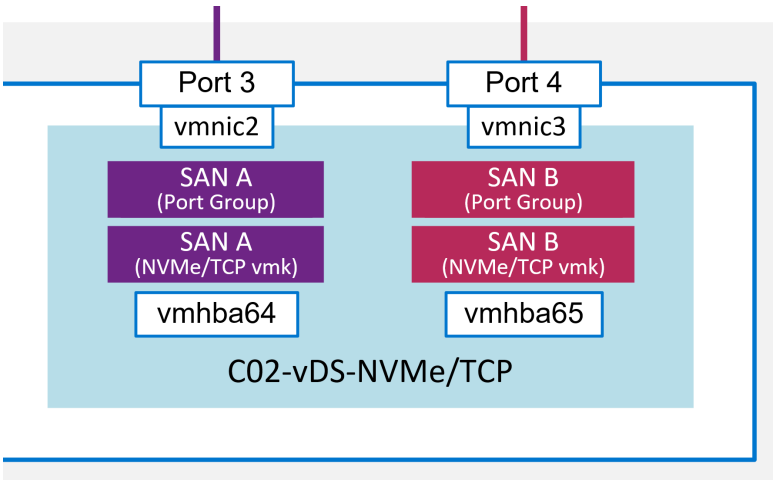


Figure 4. ESXi Host Networking for NVMe/TCP with SFSS

VMware ESXi hosts require the following networking:

- Two ports, preferably dedicated to NVMe/TCP storage traffic
- Two NVMe/TCP Software Storage Adapters (vmhbas)
- Two NVMe/TCP VMKernel Ports (vmks)

NOTE: Two VMKernel ports are required since CDC registrations cannot fail over from one vmhba to another. This differs from iSCSI which does not involve registration and can leverage network port mapping.

- Two Port Groups with different VLANs
- Teaming must not be configured. Each Port Group must have only one Active Uplink. While teaming is possible for ESXi hosts connecting directly to storage, it is not compatible with SFSS.

NOTE: Teaming can be configured on the uplinks of hosts using direct discovery of subsystems, but not on uplinks of hosts leveraging a centralized discovery controller (CDC) such as SFSS.

PowerStore requirements

Use the configuration guidelines information within the Storage Services section in the following documents. The requirements for MLAG, VLAN placement, and port usage are provided.

NOTE: For a current list of the storage subsystems that are interoperable with SFSS, see the Networking Support and Interoperability Matrix regularly.

- Dell PowerStore Networking Guide for PowerStore T Models

These guides each detail the network used for NVMe/TCP as follows:

Figure 5. Storage network in PowerStore guides

NOTE: For more information about the Dell PowerStore systems, see the PowerStore: Info Hub - Product Documentation and Videos page.

SFSS requirements

For full end-to-end operational resiliency and administrative separation, the use of two SFSS instances is recommended, where one instance is for SAN A, and the other instance is for SAN B. However, a single SFSS VM with two CDC instances can provide an improved level of resiliency.

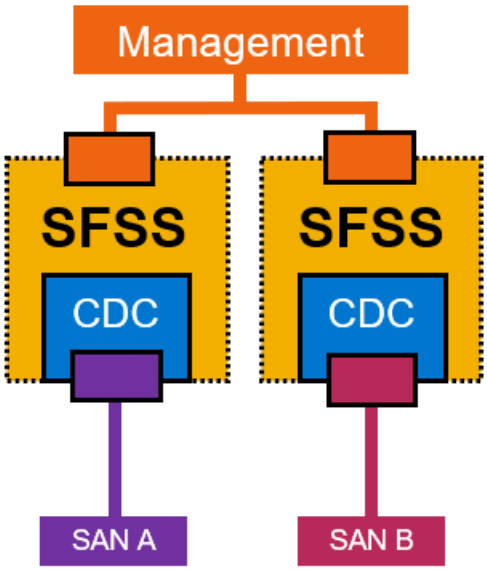


Figure 6. Example of two SFSS VMs, each with one CDC instance

CAUTION: SFSS VMs work independently in Active/Active mode. They are not aware of each other like air-gapped switches are aware of each other. SFSS VMs do not failover to each other as indicated in the figure below.

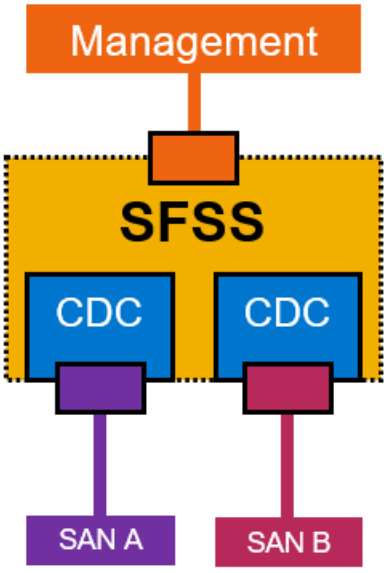


Figure 7. Example of a single SFSS VM with two CDC instances

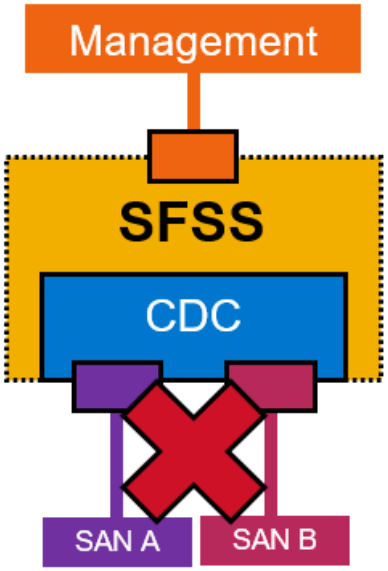


Figure 8. Example of non-best practice use of a single SFSS with two SANs in one CDC instance

When planning the SFSS instances, consider the following prerequisites:

- The necessity of a one-to-one relationship between the CDC instance and storage interface.
- Like any standard application, port groups that you create for SFSS VM interfaces can leverage teaming.
- SFSS should not reside on storage that is registered in its CDC instance.
- Dell Technologies recommends that you install SFSS on a compute and storage system that is external to the SFSS NVMe/TCP endpoints.

NOTE: For SFSS virtual machine requirements, see the SmartFabric Storage Software User Guide.

- By default, the SFSS OVA file comes with three pre-configured interfaces:
  - ens160 for the management interface
  - ens192 for SAN A
  - ens224 for SAN B
- You can add up to 10 adapters to the vApp settings in vCenter, with the remaining interfaces configured as VLAN interfaces in SFSS.

NOTE: See the Create a VLAN interface section in the SmartFabric Storage Software User Guide for more information.

Table 3. Verified scalability limits for SAN topologies

Parameter	Verified limit
Maximum number of CDC instances	16
Maximum number of endpoints (initiators and targets) per SFSS deployment	2048
Maximum number of endpoints per CDC instance	2048[a]
Maximum number of subsystems a host can access	16
Maximum number of hosts that can access a single subsystem	64
Maximum number of zone groups	500
Maximum number of zones per zone group	64
Maximum number of members per zone	65

a. Only one CDC instance is supported in this case because the maximum endpoint limit is reached.

IP network requirements

Special configuration is not required, but there are some recommendations and best practices that will ensure optimal performance of an NVMe/TCP network.

- An Ethernet network consists of validated or interoperable switches as indicated in the Networking Support and Interoperability Matrix.
- Where PowerSwitch systems are used, additional automation can be leveraged:
  - SmartFabric Services (SFS) can be used to automate the deployment and operations of Top of Rack switches. See the Dell SmartFabric Services with PowerEdge Servers, PowerStore Storage Appliance, and Isilon Storage guide for more information which also includes the deployment steps.
  - OpenManage Network Integration (OMNI) can provide a single pane of glass for multiple SFSS VMs. Within vCenter, the administrator can access multiple SFSS and SFS instances. For an introduction to OMNI, see the OpenManage Network Integration (OMNI) software section.

Maximum Transmission Unit (MTU)

In most solutions, the use of jumbo frames improves the performance of IP SAN traffic. In lieu of analyzing the application that will use NVMe/TCP storage, an MTU of 9000 is recommended.

CAUTION: The CDC registration fails if there is an MTU mismatch. If any of the devices in the end-to-end path has an MTU of 1500 and cannot be increased, use an MTU of 1500 in all components.

The following is a list of points where MTU may be configured and should be aligned.

Table 4. MTU recommendations

Point	Alignment
SFSS	The global setting applies to all storage interfaces. The default is 1500.
vSphere	vSwitch properties, vDS Advanced Settings, and VMkernels.
Switches	Interface and global level, depending on the vendor, model, and operating system.
PowerStore	Cluster level and storage network level.

Multichassis Link Aggregation (MLAG)

The following are MLAG best practices for NVMe/TCP endpoints.

Table 5. MLAG recommendations

Port	Recommendation
Ports that connect to ESXi hosts	The NVMe/TCP vmhba cannot fail over, therefore teaming is not used on these ports. Do not configure LAG or MLAG on the switch ports.
Ports that connect to PowerStore	Follow the guidelines provided in the Networking Guide for PowerStore T models on the PowerStore: Info Hub - Product Documentation and Videos page.
Ports connecting to the SFSS ESXi Host	These ports can be Active/Active or Active/Standby, with MLAG as optional.

Flow control

For ports connected to NVMe/TCP Endpoints, flow control should be off for receive and transmit.

VLAN tagging

Table 6. VLAN tagging recommendations

Port	Recommendation
Ports connecting to ESXi hosts	NVMe/TCP VLANs are tagged.
Ports connecting to PowerStore	Follow the guidelines provided in the Networking Guide for PowerStore T models on the PowerStore: Info Hub - Product Documentation and Videos page.
Ports connecting to the SFSS Host	NVMe/TCP VLANs are tagged.

Congestion

Avoid congestion by leveraging the following:

- Dedicated switches
- Separate broadcast domains
- Dedicated NVMe/TCP ports on hosts
- No oversubscription
- Traffic should ingress and egress at line rate

NOTE: Dropping packets by leveraging QoS configuration is not recommended as a solution for congestion. The cause of congestion should be discovered and rectified.

NOTE: DTCP and ECN are not currently available in PowerStore or VMware ESXi.

Network firewall

Storage traffic and SFSS control traffic are not firewalled. Administrators may want to firewall administrator traffic to the SFSS management interface.

Table 7. Open Ports Required for SFSS

Port	Protocol	Purpose	Description	Source	Destination
22	SSH	ESXi console access through SSH	ESXi console access through SSH	Admin	SFSS Management Interface
49	TCP	TACACS+	Remote user authentication	SFSS Management	TACACS+ Server
443	HTTPS	HTTPS access to SFSS UI, RestAPI	User access to SFSS through web UI or RestAPI	Admin	SFSS Management Interface
1812	UDP	RADIUS	Remote user authentication	SFSS Management	RADIUS Server
4420	TCP	NVMe TCP I/O Controller	Data traffic between the host and the subsystem	Host NVMe/TCP Interface	Dell PowerStore Storage Networks
8009	TCP	NVMe TCP Discovery	Host registration	Host NVMe/TCP Interface	SFSS CDC Interface
8009	TCP	NVMe TCP Discovery	Subsystem registration	SFSS CDC Interface	All Subsystems

Example network topologies

Many network topologies work well for NVMe/TCP traffic. This section covers three of the most popular production topologies along with a fourth example topology used in the Deploy and configure SFSS section of this guide.

Dual SAN with dedicated, air-gapped SAN switches

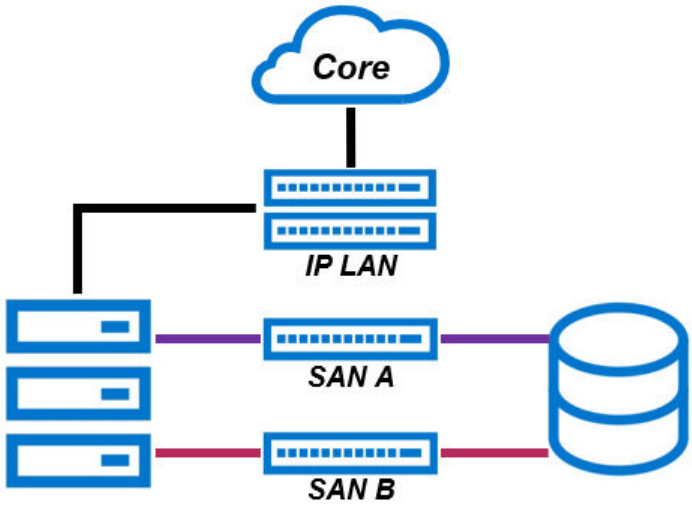


Figure 9. Dedicated dual SAN switch topology - Layer 1

The dedicated, air-gapped dual SAN switch topology has two isolated SAN switches with two isolated Layer 2 networks dedicated to NVMe/TCP traffic. This is similar to a dual SAN FC topology. One switch carries SAN A, and the other carries SAN B.

Advantages

The following examples are advantages of this topology:

- Dual SAN creates an Active/Active resilient solution.
- This topology removes the risk of contention with LAN traffic by:
  - Dedicating ports on Hosts to NVMe/TCP traffic.
  - Dedicating ports on Subsystems to NVMe/TCP traffic.
  - Dedicating entire switches to NVMe/TCP traffic
- Provides an additional level of security:
  - NVMe/TCP traffic is Layer 2 only, resulting in Layer 3 isolation from the rest of the network.
- This topology is familiar to fibre channel SAN administrators.

Attributes

Taking a closer look at the dedicated dual SAN topology as shown in the figure below, the following should be noted:

- There are two SFSS Virtual Machines, providing end-to-end administrative and operational resiliency.
- Each SFSS has one CDC instance with one storage interface in each.
- On the ESXi hosts in the workload cluster, ports 1 and 2 are for management and guest traffic only. Port 3 is dedicated to SAN A and port 4 is dedicated to SAN B.
- The PowerStore ports are configured according to the PowerStore Networking Guide. See the Plan and Install section of the PowerStore: Info Hub - Product Documentation and Videos page for the documentation.
- LAG is not configured on the PowerStore T storage ports. Port 2 on each PowerStore node is dedicated to SAN A, and port 3 on each PowerStore node is dedicated to SAN B.
- The SAN switches are not connected (air-gapped) to each other, therefore MLAG is not used on the SAN A or SAN B interfaces.
- The SAN switches do not have uplinks to the rest of the network.

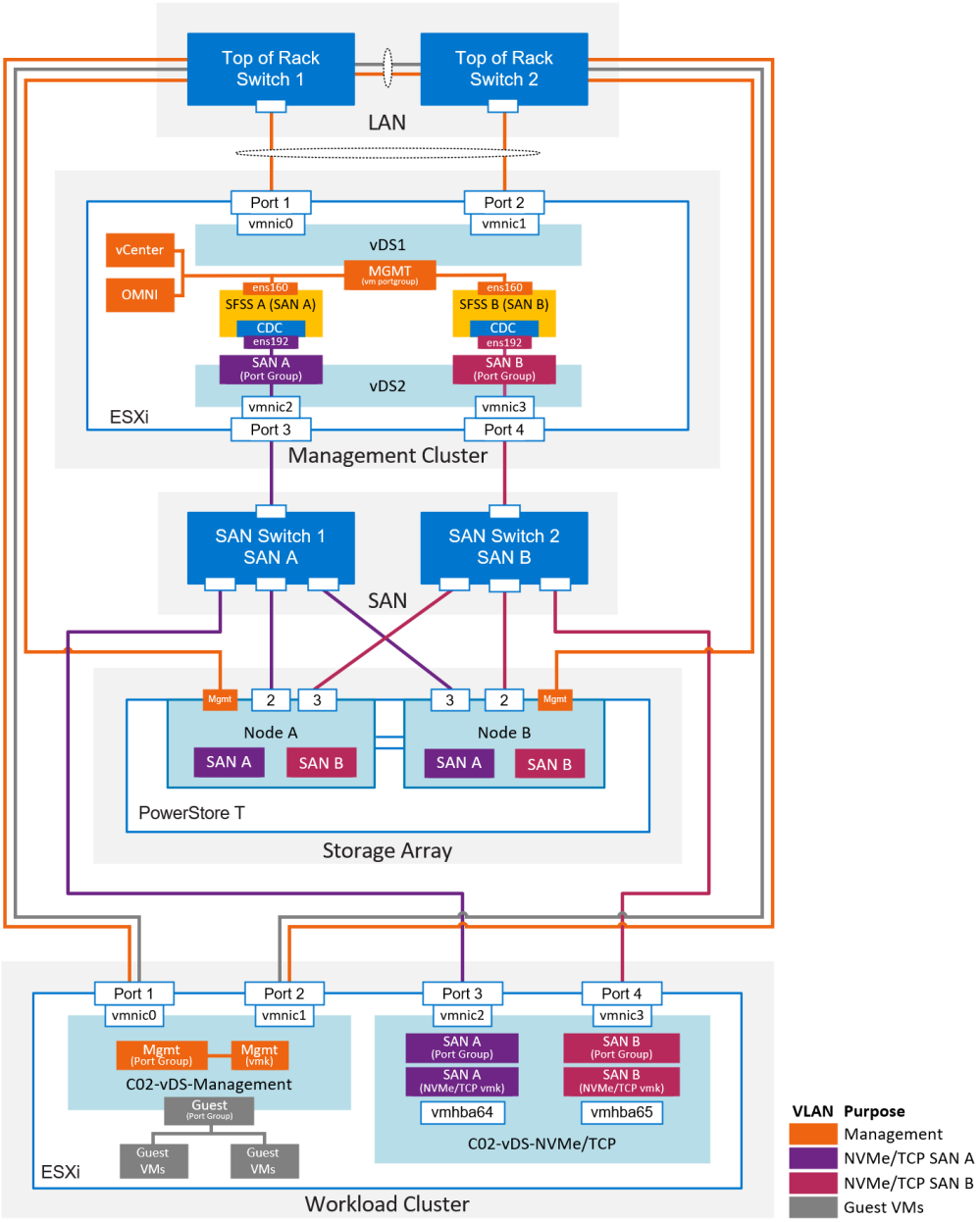


Figure 10. Dedicated dual SAN switch topology - Layer 1 through Layer 3

Adjustments

Some of the possible modifications to this topology include:

- Though the presence of two SFSS VMs most closely emulates the services provided by physically separate switches in different SAN instances, the administrator can choose to deploy a single SFSS VM containing two CDC Instances instead.
- See the Dual SAN with dedicated air-gapped SAN spine/leaf fabrics over Layer 3 section for a large-scaled variation of this topology.
- SFSS and endpoints can be on different subnets. See the Dual SAN with dedicated air-gapped SAN spine/leaf fabrics over Layer 3 section for more information.

Sample switch configuration

The following table shows the switch interface configuration for a pair of dedicated, air-gapped SAN PowerSwitch systems running SmartFabric OS10 in full switch mode. Notice that there are no uplinks to the rest of the network, and there are no connections between the switches.

SAN switch 1 - SAN A	SAN Switch 2 - SAN B
default mtu 9216 interface vlan1821 description **SAN-A** no shutdown ! ! Interface descriptions interface ethernet1/1/1 description esxi01-port3 interface ethernet1/1/2 description esxi02-port3 interface ethernet1/1/3 description esxi03-port3 interface ethernet1/1/4 description esxi04-port3 interface ethernet1/1/41:1 description PowerStoreT-NodeA-Port0 interface ethernet1/1/42:1 description PowerStoreT-NodeB-Port0 ! ! ESXi Host Interfaces interface range ethernet1/1/1-1/1/4 no shutdown switchport mode trunk switchport trunk allowed vlan **1821** flowcontrol receive off flowcontrol transmit off ! ! PowerStore interfaces interface range ethernet1/1/41:1-1/1/42:1 no shutdown switchport mode trunk switchport trunk allowed vlan **1821** flowcontrol receive off flowcontrol transmit off !	default mtu 9216 interface vlan1822 description **SAN-B** no shutdown ! ! Interface descriptions interface ethernet1/1/1 description esxi01-port4 interface ethernet1/1/2 description esxi02-port4 interface ethernet1/1/3 description esxi03-port4 interface ethernet1/1/4 description esxi04-port4 interface ethernet1/1/41:1 description PowerStoreT-NodeA-Port1 interface ethernet1/1/42:1 description PowerStoreT-NodeB-Port1 ! ! ESXi Host Interfaces interface range ethernet1/1/1-1/1/4 no shutdown switchport mode trunk switchport trunk allowed vlan **1822** flowcontrol receive off flowcontrol transmit off ! ! PowerStore interfaces interface range ethernet1/1/41:1-1/1/42:1 no shutdown switchport mode trunk switchport trunk allowed vlan **1822** flowcontrol receive off flowcontrol transmit off !

Converged LAN and SAN topology

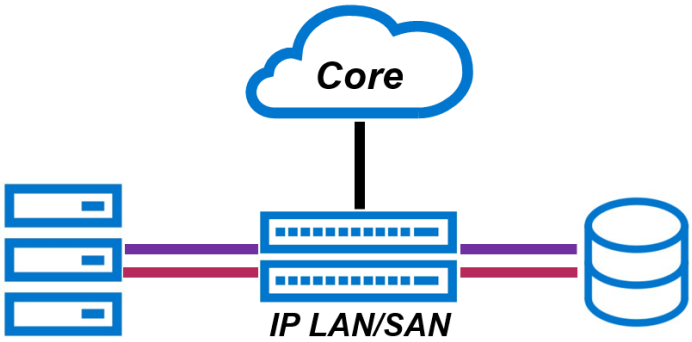


Figure 11. Converged LAN and SAN Topology - Layer 1

Advantages

The converged LAN/SAN topology uses the same switches for application (LAN) and storage (SAN) traffic. The advantages of this topology are as follows:

- You can use Top-of-Rack switches for LAN and SAN traffic, so more switches are not required.
- This topology is ideal for smaller environments.

NOTE: See the Congestion section for converged LAN/SAN best practices.

Attributes

The converged LAN/SAN topology shown in the figure below, is a more detailed look at the topology. Note the following:

- There is a single SFSS VM with two CDC instances, each with one storage interface.
- On the ESXi hosts in the workload cluster, ports 1 and 2 are for management and guest traffic only. Port 3 is dedicated to SAN A, and port 4 is dedicated to SAN B.
- The PowerStore ports are configured according to the PowerStore Networking Guide. See the Plan and Install section of the PowerStore: Info Hub - Product Documentation and Videos page for the documentation.
- LAG is configured on the PowerStore T storage ports.

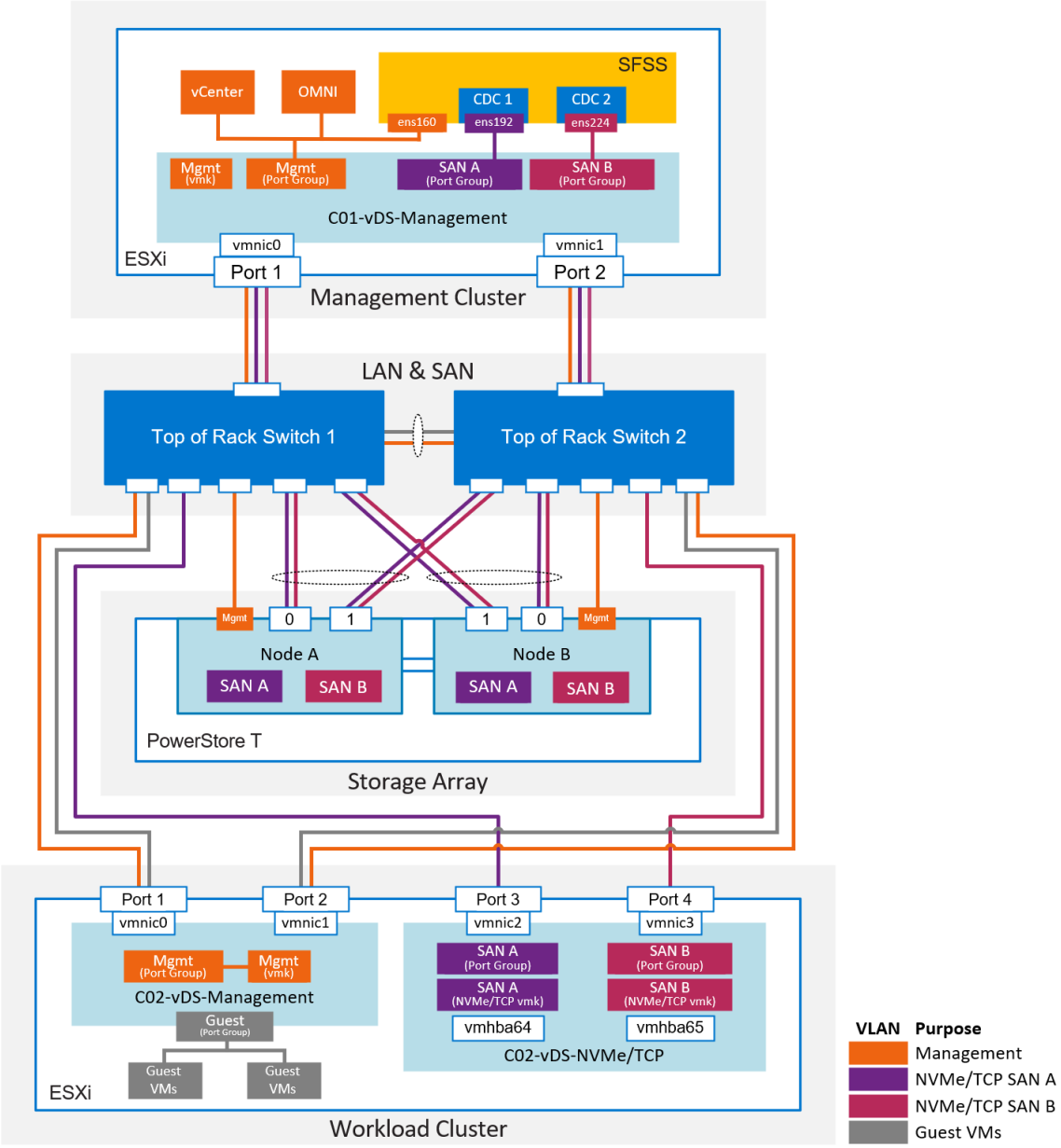


Figure 12. Converged LAN and SAN topology – Layer 1 through Layer 3

Adjustments

Some of the possible modifications to this topology include

- Replace the switch pair with a Spine/Leaf fabric, significantly increasing capacity.
- Though not recommended, the ESXi host may use two ports to carry all traffic. Teaming cannot be configured on these ports. See the VMware ESXi requirements section for more information.
- SFSS and endpoints can be on different subnets. See the Dual SAN with dedicated air-gapped SAN spine/leaf fabrics over Layer 3 section for more information.

Dual SAN with dedicated air-gapped SAN spine/leaf fabrics over Layer 3

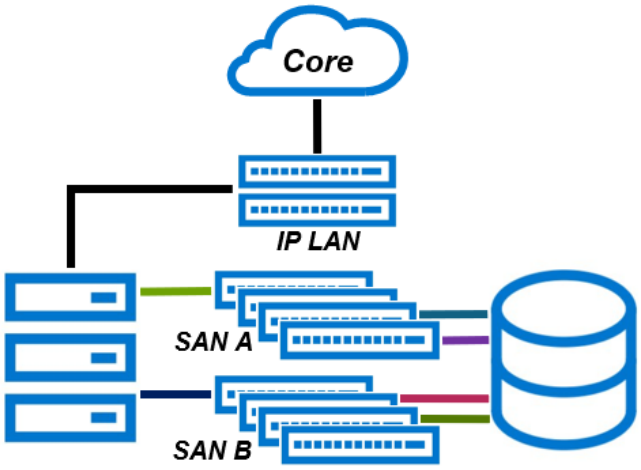


Figure 13. Dedicated dual fabric SAN over Layer 3

Advantages

The dedicated, air-gapped, dual SAN fabric topology has a dedicated spine/leaf fabric for SAN A, and a separate dedicated spine/leaf fabric for SAN B. This example topology leverages Layer 3 between endpoints and SFSS. The advantages of this topology are as follows:

- The environment can scale up to multiple racks.
- SFSS, hosts, and subsystems can be on separate VLANs and separate subnets.
- Multiple storage networks can be configured on the storage array.

Attributes

When looking at the dedicated dual SAN fabric topology example in the figure below, note the following:

- There are two SFSS Virtual Machines, providing end-to-end administrative and operational resiliency.
- Each SFSS has one CDC instance with one storage interface in each.
- To avoid the need for static or dynamic routing configuration in SFSS, each SFSS VM has only one network interface. The interface used for management in other topologies is inactive.

  NOTE: A future release of SFSS allows you to configure static and dynamic routing on multiple interfaces.
- A jump box is required to administer the SFSSs using the storage interfaces.
- On the ESXi hosts in the workload cluster, ports 1 and 2 are for management and guest traffic only. Port 3 is dedicated to SAN A, and port 4 is dedicated to SAN B.
- The PowerStore ports are configured according to the PowerStore Networking Guide. See the Plan and Install section of the PowerStore: Info Hub - Product Documentation and Videos page for the documentation.
- The SAN fabrics are not connected to each other (air-gapped), therefore LAG is not configured on the PowerStore T storage ports.
- Routing configuration is required in the spine/leaf fabrics to facilitate communication between SFSS and endpoints, and between hosts and subsystems.

- There are more than two storage networks. See the Plan and Install section of the PowerStore: Info Hub - Product Documentation and Videos page for the documentation.

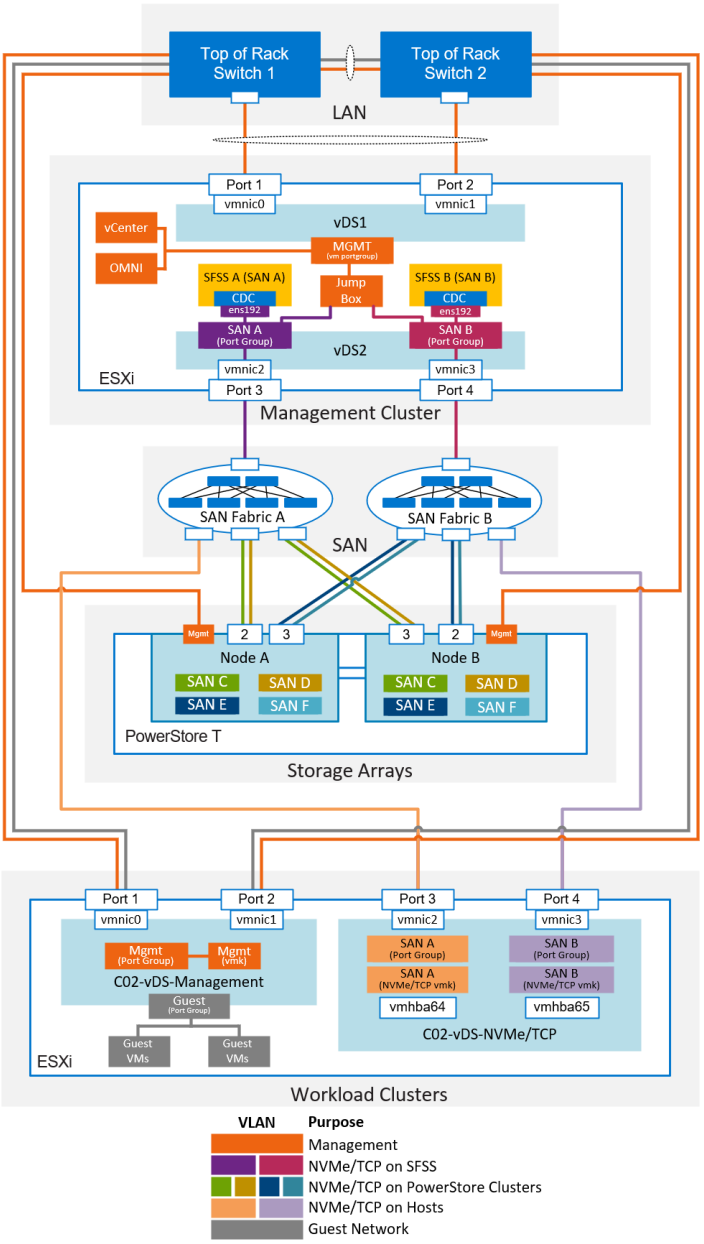


Figure 14. Dedicated dual fabric SAN over Layer 1 through Layer 3

Initial configuration worksheet template

Before you proceed with the solution deployment, plan and record the necessary configuration values in the tables below. for a fully populated example, see the Initial configuration worksheet for this guide section.

SFSS configuration data

NOTE: Duplicate this table for each SFSS instance.

Table 8. SFSS configuration table

SFSS Configuration Item	Value
Hostname (cannot contain ".")	
Default Username	
Default Password	
Management Interface IP	
Management Mask/Prefix	
Management Gateway	
Associated CDC Instance(s)	
Storage interface MTU	
IPv4 Internal Network	172.18.0.0/16[a]
IPv6 Internal Network	fe01::0/64[b]

a. Default value shown for IPv4 Internal Network can be modified.
b. Default value shown for IPv6 Internal Network can be modified.

CDC instance configuration data

NOTE: Duplicate this table for each SFSS instance.

Table 9. CDC instance configuration data

CDC Instance ID(s) configuration item	CDC 1	CDC 2
Storage interface IP		
Storage subnet mask/prefix length		
Storage subnet default gateway[a]		
Associated storage VLAN ID		
Zone Group Name		
Zone Name		

a. Only required if Layer 3 routing is required to reach endpoints.

VMware vSphere configuration data

Table 10. VMware vSphere configuration data

vCenter Configuration Item	Value
vCenter Hostname / IP	
Data Center	
SFSS's Host Cluster name	
SFSS's Host Cluster vDS/vSwitch	
SFSS's Host Cluster Management Port Group	
Workload Management Port Group	
Workload Cluster name	
Workload Cluster Management vDS	

Table 10. VMware vSphere configuration data (continued)

vCenter Configuration Item	Value
Workload Cluster NVMe/TCP vDS	
NVMe/TCP Datastore name	

ESXi Hosts/Cluster SAN Configuration Item	SAN A	SAN B
SFSS VM storage Port Group		
SFSS VM storage Port Group VLAN		
Workload Cluster storage Port Group		
Workload Cluster storage Port Group VLAN		
Workload Cluster storage network mask/prefix length		
Workload Cluster storage network gateway[a]		
Workload Cluster storage network vmk interface IPs		
Workload Cluster Storage Software Adapter		
Port Number		
VM NIC name		

a. Only required if Layer 3 routing is required to reach SFSS or subsystems.

PowerStore

Table 11. PowerStore configuration data

PowerStore Configuration Item	Value
PowerStore Cluster FQDN/IP	
Volume Group name(s)	
Volume Name(s)	
DDC Port Number[a]	8009

a. Default value shown can be modified

PowerStore Storage Network Configuration Item	SAN A	SAN B
Storage network name		
Storage network VLAN ID		
Storage network address		
Storage network mask/prefix length		
Storage network gateway[a]		
Storage network interface IPs		

a. Only required if Layer 3 routing is required to reach SFSS or subsystems.

Network VLANs and subnets

VLAN ID	Description	Network	Gateway	Tagged or untagged edge ports
	Management			Tagged
	vMotion			Tagged
	Guest Network			Tagged
	NVMe/TCP traffic for SAN A		See Footnote[a]	Tagged
	NVMe/TCP traffic for SAN B		See Footnote[b]	Tagged

a. Only required if Layer 3 routing is required for NVMe/TCP communication between SFSS and Endpoints
b. Only required if Layer 3 routing is required for NVMe/TCP communication between SFSS and Endpoints

Hosts and VMs

FQDN	Management IP address	Description
		ESXi Host, Mgmt Cluster
		ESXi Initiator, Workload
		vCenter
		OMNI
		SFSS vApp

3

Deploy and Configure SFSS and Configure NVMe/TCP Endpoints

This section provides the necessary configuration steps for the implementation of the topology below. Using the values from your Initial Configuration Worksheet, adjust the number of times to repeat the steps in this section as necessary to accommodate your topology.

NOTE: If the outcome of a step is not as expected, see the SmartFabric Storage Software Troubleshooting Guide for assistance.

Topology overview

The purpose of this section is to provide the set of configuration steps required to set up the below topology. Follow the steps using the values in your Initial Configuration Worksheet, adjusting the number of times to repeat steps accordingly. If the outcome of a step is not as expected, see the SmartFabric Storage Software Troubleshooting Guide for assistance.

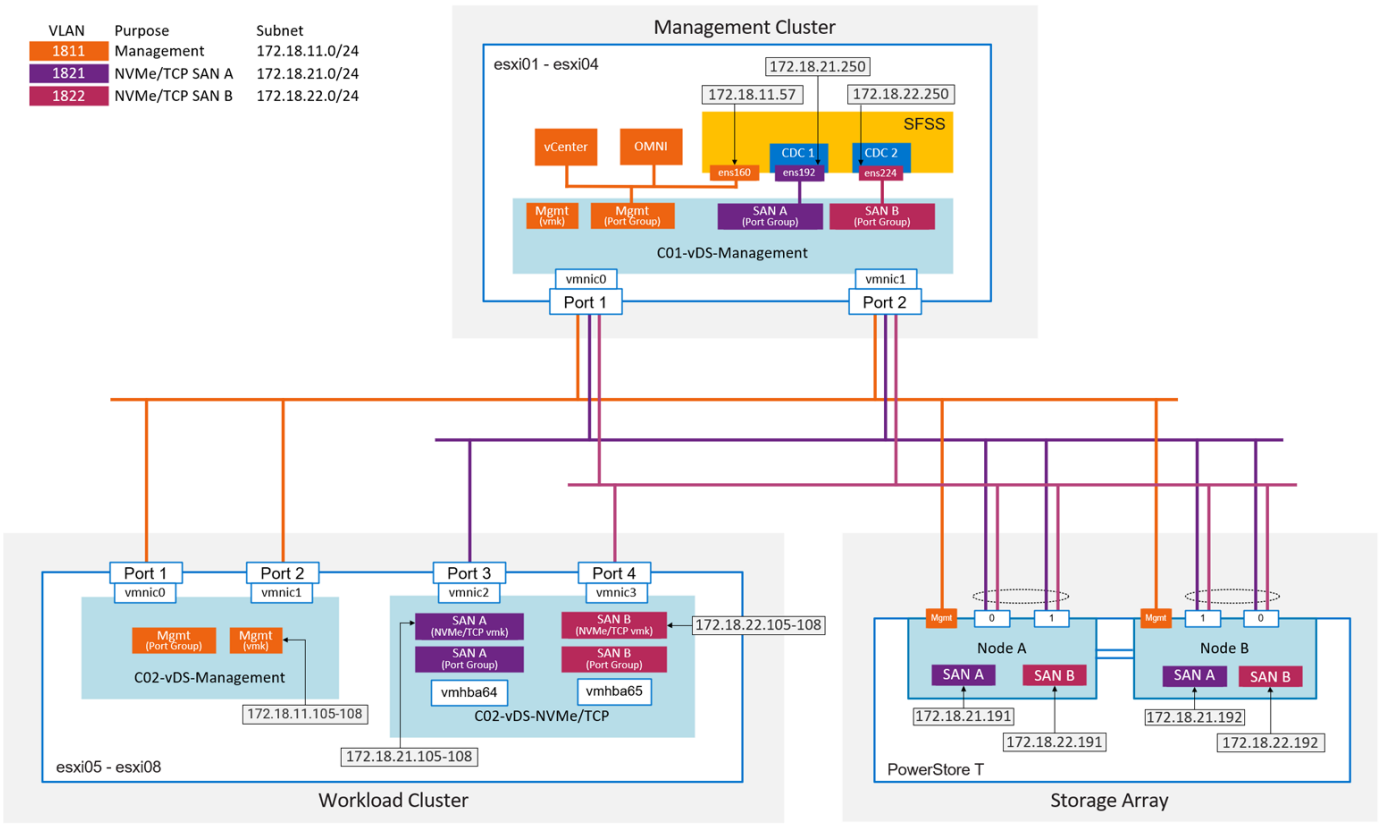


Figure 15. Topology used in this guide - Layers 2 to 3

The deployment example illustrated in this guide is a variation of a dual SAN with dedicated SAN switch topology.

Component attributes

Table 12. Hardware and roles

Component purpose	Dell product	Port usage	Number of ports
Management Cluster	PowerEdge Servers	vSphere Management and SFSS Control Traffic	2 per host
Workload Cluster	PowerEdge Servers	ESXi Management	2 per host
Workload Cluster	PowerEdge Servers	NVMe/TCP Control and Data Traffic	2 per host
Storage Subsystem	PowerStore T	Out of Band Management Ports	1 per node
Storage Subsystem	PowerStore T	NVMe/TCP Control and Data Traffic	2 per node
Centralized Discovery Controller	SFSS	Out of Band Management Port	1
Centralized Discovery Controller	SFSS	NVMe/TCP Control Traffic	1 per CDC
SFSS and SFS Administration	OMNI	Out of Band management	1

NOTE: The topology used in this guide has the same PowerStore configuration as the converged LAN and SAN topology, the same SFSS host configuration as the dual SAN with dedicated, air-gapped SAN switches, and dual SAN with dedicated air-gapped SAN spine/leaf fabrics over Layer 3 topologies, and the same ESXi host configuration as all three example network topologies. The only difference is where the ports are used.

The following image shows the same solution with the switches included.

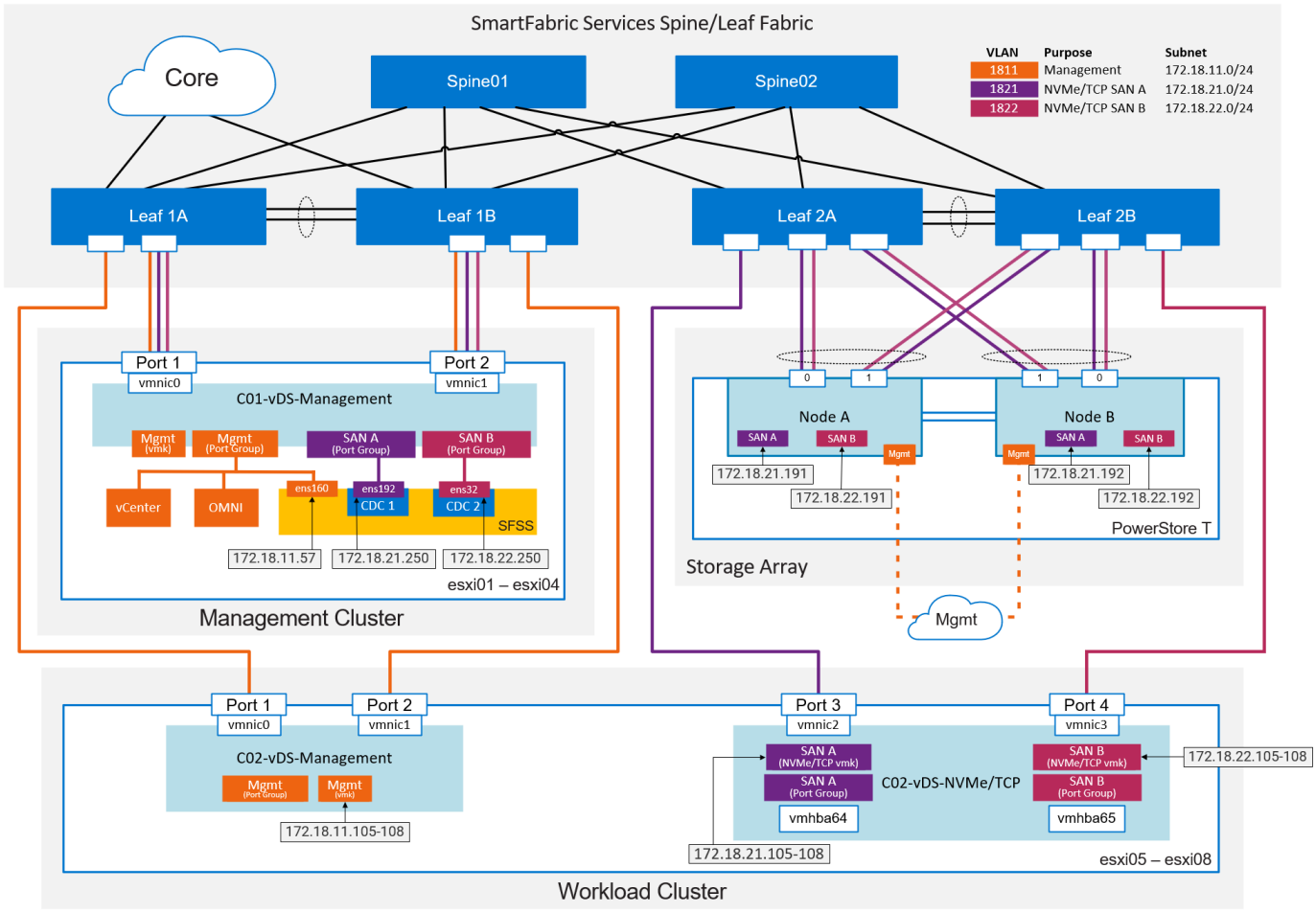


Figure 16. Topology used in this guide - Layers 1 to 3

Network attributes

Table 13. Hardware and roles

Dell product		Role
PowerSwitch switches	Leafs 1A and 1B	Top of Rack (ToR) switches for the ESXi hosts
PowerSwitch switches	Leafs 2A and 2B	Top of Rack (ToR) switches for the PowerStore T
PowerSwitch switches	Spines 1 and 2	Connecting ToRs in a SmartFabric spine/leaf topology.[a] Control traffic from SFSS to the endpoints and traverses the spines.

a. See the SFS configuration section for more details.

Table 14. VLANs and subnets

VLAN ID	Description	Network	Gateway	Server interfaces
1811	Management	172.18.11.0/24	172.18.11.254	Tagged
1812	vMotion	172.18.12.0/24	None	Tagged
1814	Guest Network	172.18.14.0/24	172.18.14.254	Tagged

Table 14. VLANs and subnets (continued)

VLAN ID	Description	Network	Gateway	Server interfaces
1821	NVMe/TCP traffic for SAN A	172.18.21.0/24	172.18.21.254	Tagged
1822	NVMe/TCP traffic for SAN B	172.18.22.0/24	172.18.22.254	Tagged

Table 15. Hosts and VMs

FQDN or Hostname	Management IP address	Description
esxi01.dell.lab	172.18.11.101	ESXi Host, Mgmt Cluster
esxi02.dell.lab	172.18.11.102	ESXi Host, Mgmt Cluster
esxi03.dell.lab	172.18.11.103	ESXi Host, Mgmt Cluster
esxi04.dell.lab	172.18.11.104	ESXi Host, Mgmt Cluster
esxi05.dell.lab	172.18.11.105	ESXi Host, Workload Cluster
esxi06.dell.lab	172.18.11.106	ESXi Host, Workload Cluster
esxi07.dell.lab	172.18.11.107	ESXi Host, Workload Cluster
esxi08.dell.lab	172.18.11.108	ESXi Host, Workload Cluster
vcenter.dell.lab	172.18.11.62	vCenter VM
omni.dell.lab	172.18.11.56	OpenManage Network Integration software VM
sfss.dell.lab	172.18.11.57	SmartFabric Storage Software VM
PowerStore-Cluster-01	100.67.108.190	PowerStore T Appliance

Table 16. Infrastructure services

Infrastructure services	IP address
DNS	172.18.11.50
NTP	172.18.11.50

Initial State

This section shows the configuration state of the ecosystem before beginning the deployment steps in this guide.

VMware vSphere

This guide begins with vSphere vCenter and hosts deployed with the data center, clusters, and management virtual networking in place. The screens below depict the settings used.

In vSphere, configure your clusters, hosts, and VMs before deploying SFSS. The figure below shows the configuration used for the example in this guide.

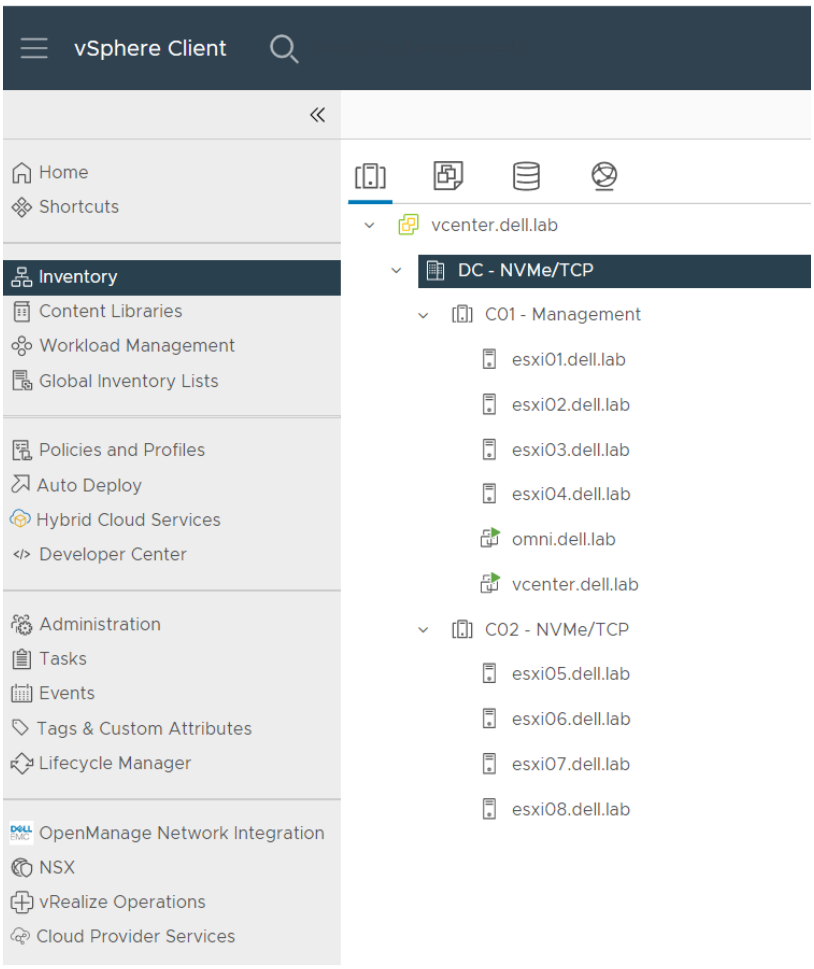


Figure 17. vSphere Clusters, hosts, and VMs before SFSS Deployment

NOTE: The OpenManage Network Integration (OMNI) software is optional. See the OpenManage Network Integration section for information about adding SFSS to the OMNI UI. See the OpenManage Network Integration section for an introduction to OMNI.

The figure below shows the virtual networking configuration.

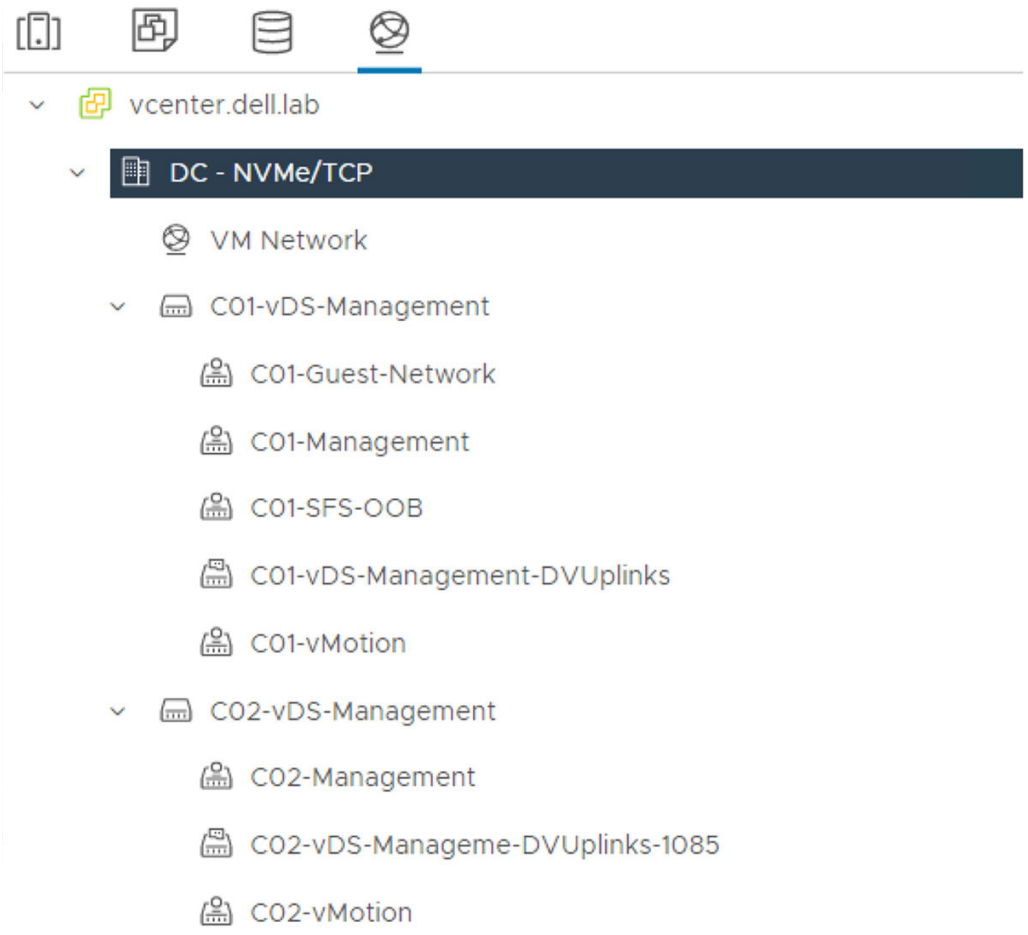


Figure 18. vSphere virtual networking before SFSS deployment

The figure below shows the topology of the virtual distributed switch of the Management Cluster.

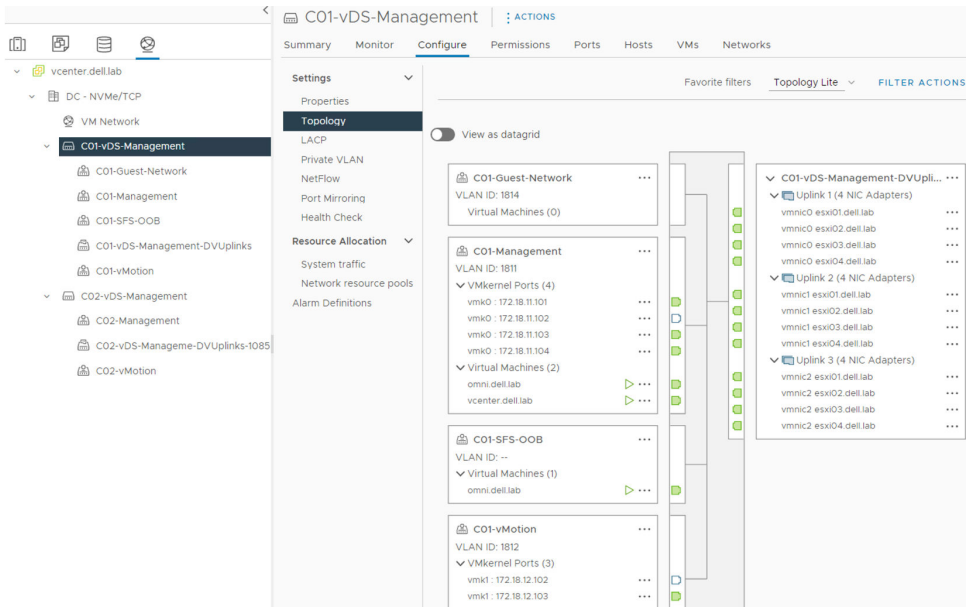


Figure 19. Distributed switch of Management cluster

The figure below shows the configuration used for vDS for the workload cluster's management uplink ports.

NOTE: There are two management uplinks.

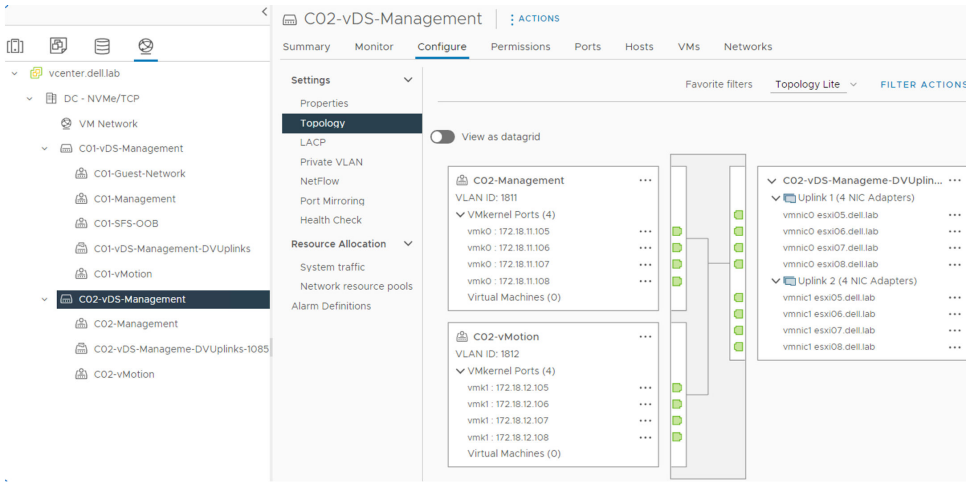


Figure 20. Distributed switch for workload cluster management uplinks

PowerStore T

Before using the steps in this guide to deploy SFSS, deploy a single PowerStore T appliance with PowerStore Manager v2.1 as instructed in the Setting up PowerStore Manager Guide.

The following figure shows the PowerStore Manager dashboard for the deployed PowerStore T used in this guide.

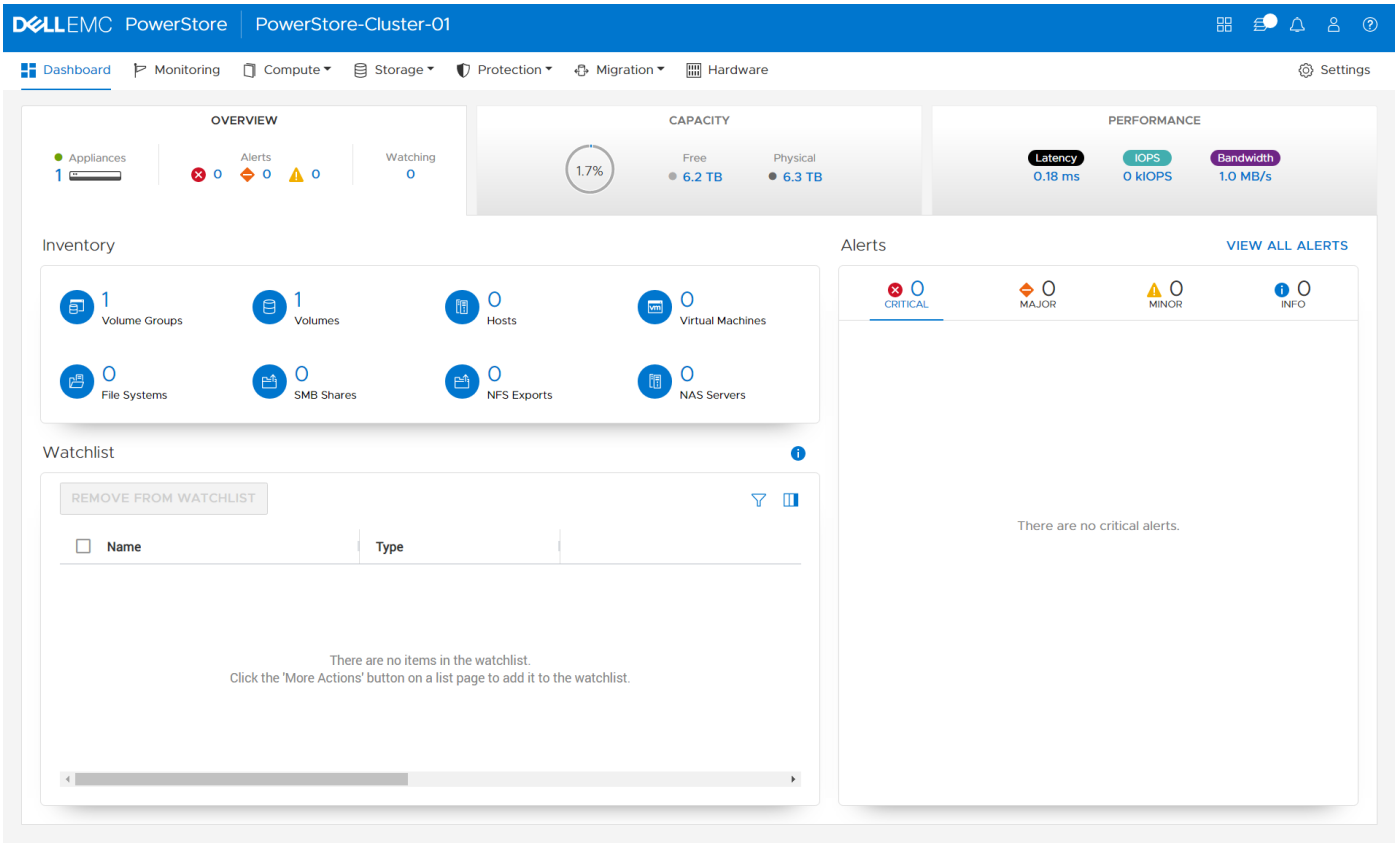


Figure 21. PowerStore dashboard

The MTU is set to 9000 across the storage network, which is done during cluster deployment.

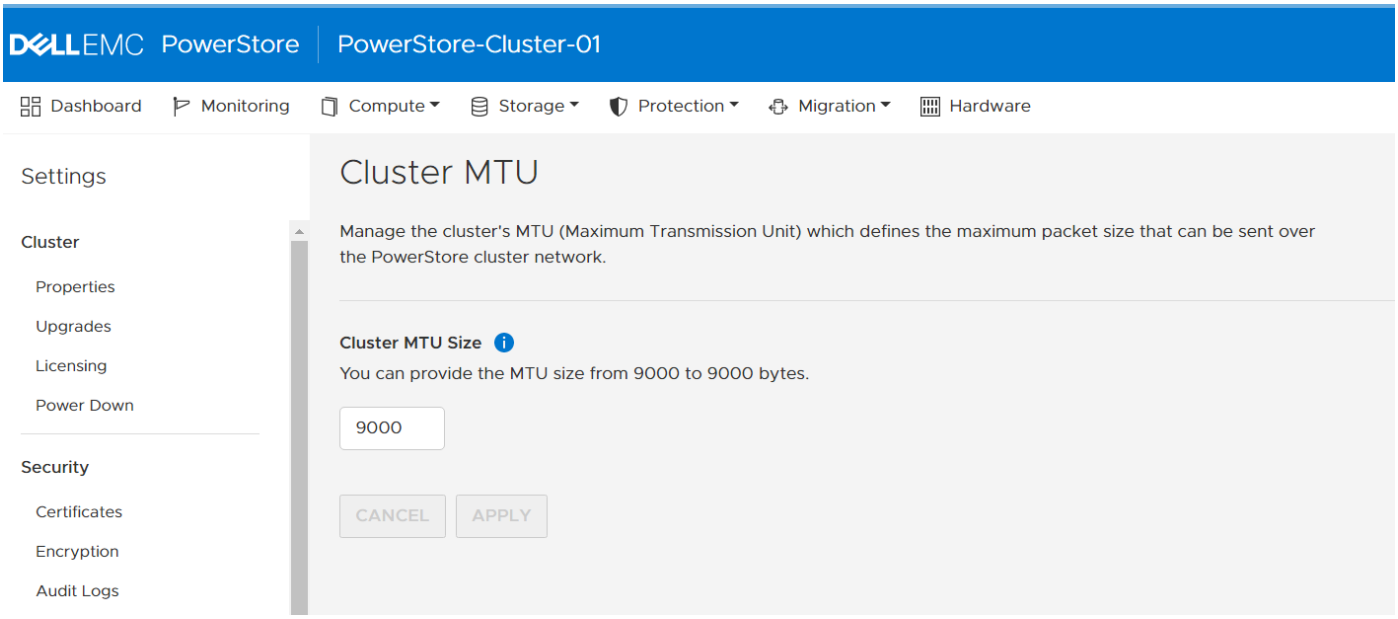


Figure 22. PowerStore Cluster MTU set to 9000

A PowerStore Management network was configured during initialization. The figure below shows the configuration used for the example in this guide.

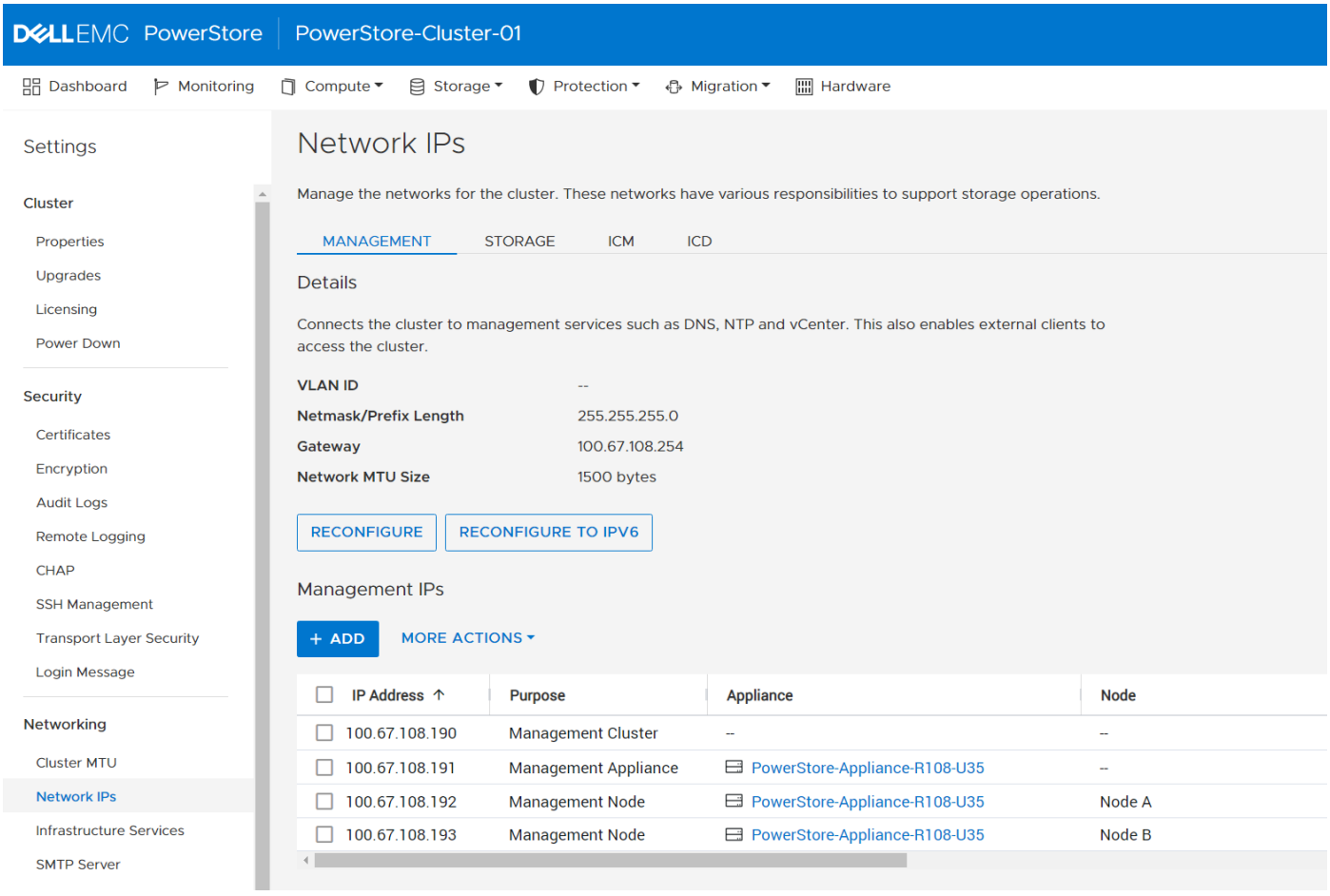


Figure 23. PowerStore Management Network

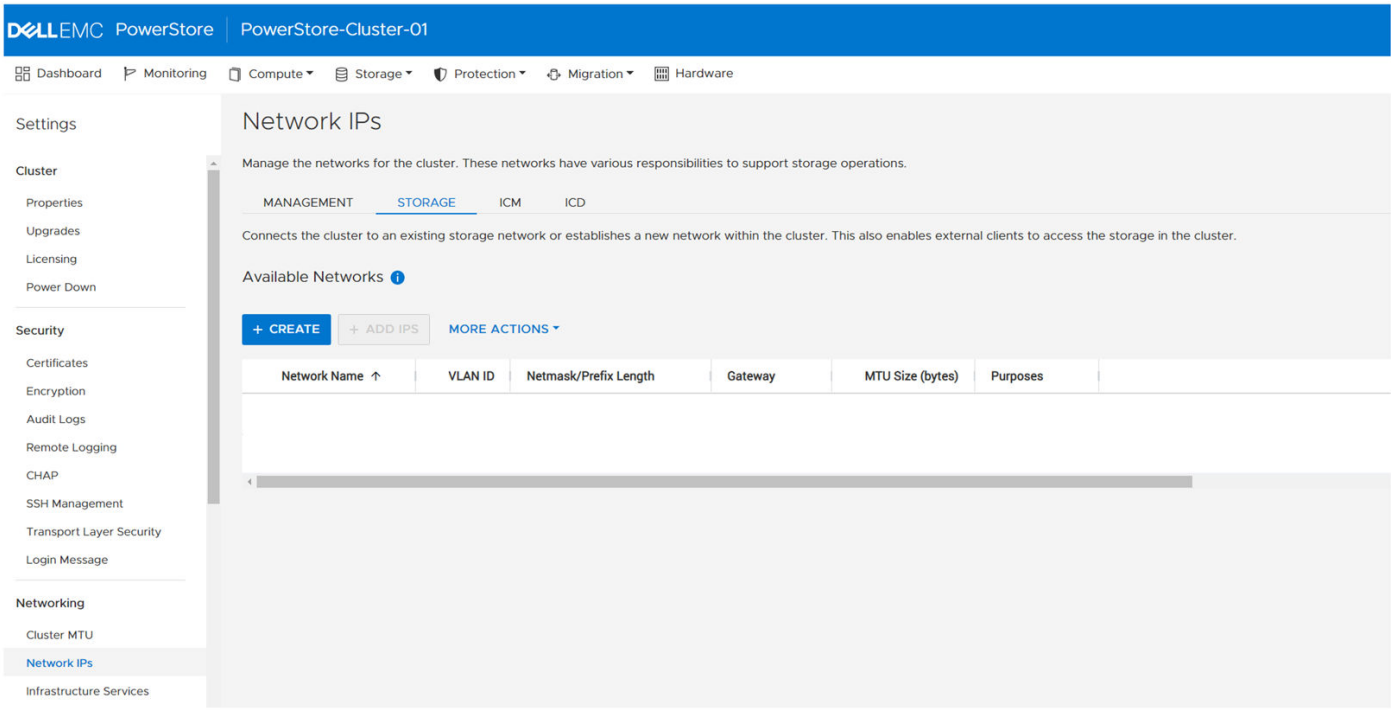


Figure 24. Storage networks before SFSS deployment

IP network

The network in this guide is configured using SmartFabric Services (SFS) automation. SFS is included with SmartFabric OS10. With SFS, you can easily deploy and automate data center networking fabrics. SFS automatically builds an L3 leaf-spine fabric which accelerates time to production while being fully interoperable with the existing data center infrastructure.

SFS configuration

The deployment of a multirack SmartFabric with two spines and four leafs, is done using the information provided in the Dell SmartFabric Services with PowerEdge Servers, PowerStore Storage Appliance, and Isilon Storage Guide.

The process for the SFS fabric build is performed as follows:

1. Rack and cable the leaf and spine switches.
2. Enable SFS from the OS10 command-line interface (CLI) using the `smartfabric l3fabric enable` command on each switch.
3. Specify Virtual Link Trunking interconnect (VLTi) ports on leafs.
4. Verify that the switches boot in SmartFabric mode.
5. Ensure that the switches discover each other using Link Layer Discovery Protocol (LLDP).
6. Check that the leaf and spine connections are established using private IP addresses and external Border Gateway Protocol (eBGP).
7. Confirm that leaf nodes are configured as hardware Virtual Tunnel End Points (VTEPs) for the infrastructure network overlay using BGP EVPN.
8. When configuring links to the external network, keep in mind that they can be Layer 2 or Layer 3.

After the deployment is complete, use the OpenManage Network Integration vCenter plugin to perform additional configurations.

OpenManage Network Integration software

The OMNI vCenter plugin makes vCenter a single pane of glass for administration of SFS and SFSS. For SFS, OpenManage Network Integration (OMNI) enables configuration and management of Dell PowerSwitch systems running Dell SmartFabric OS10 in VMware vCenter. With OMNI, networks created in vCenter are automatically configured in the fabric.

You can perform the following tasks in the OMNI plugin within vCenter:

- View the leaf-spine topology
- View switch status
- Configure server-facing interfaces and port channels
- Configure uplinks to external networks
- Create networks
- Configure routing
- Upgrade SmartFabric OS10

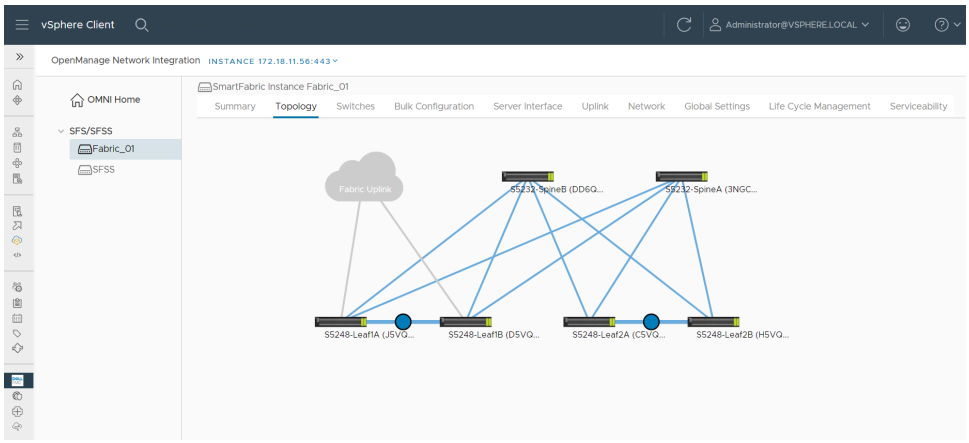


Figure 25. View of SFS spine/leaf topology in OMNI vCenter plugin

NOTE: Uplink connections from the SmartFabric to the external switches are Layer 2. You can find examples of the configuration of uplinks and external switches in the Dell SmartFabric Services with PowerEdge Servers, PowerStore Storage Appliance, and Isilon Storage Guide.

Initial configuration worksheet for this guide

The initial configuration worksheet for the example topology is shown in the preview section.

Table 17. SFSS configuration data

SFSS configuration item	Value
Hostname (cannot contain a period)	sfss
Default Username	admin
Default Password	admin
Management Interface IP	172.18.11.57
Management Mask/Prefix	255.255.255.0/24
Management Gateway	172.18.11.254
Associated CDC Instances	1, 2
Storage interface MTU	9000
IPv4 Internal Network	172.16.0.0/16
IPv6 Internal Network	fe01::/64

NOTE: See the Sample Initial Configuration Worksheet for Dual SFSS section for examples that have dual SFSS values.

Table 18. CDC instance configuration data

CDC instance ID configuration item	CDC 1	CDC 2
Storage interface IP	172.18.21.250	172.18.22.250
Storage subnet mask/prefix length	255.255.255.0/24	255.255.255.0/24
Storage subnet default gateway (L3 topology only)	None	None
Associated storage VLAN ID	1821	1822
Zone Group Name	ZG-NVMe-SAN-A	ZG-NVMe-SAN-B
Zone Name	Z-NVMe-SAN-A	Z-NVMe-SAN-B

Table 19. VMware vSphere configuration data

vCenter configuration item	Value
vCenter Hostname / IP	vcenter.dell.lab / 172.18.11.62
Data Center	DC - NVMe/TCP
SFSS's Host Cluster name	C01 - Management
SFSS's Host Cluster vDS/vSwitch	C01-vDS-Management
SFSS's Host Cluster Management Port Group	C01-Management
Workload Management Port Group	C02-Management
Workload Cluster name	C02 - NVMe/TCP
Workload Cluster Management vDS	C02-vDS-Management
Workload Cluster NVMe/TCP vDS	C02-vDS-NVMeTCP
NVMe/TCP Datastore name	PowerStore-NVMeTCP-DS

Table 20. ESXi host or cluster SAN configuration

ESXi host or cluster configuration item	SAN A	SAN B
SFSS VM storage Port Group	C01-NVMeTCP-SAN-A-SFSS	C01-NVMeTCP-SAN-B-SFSS
SFSS VM storage Port Group VLAN	1821	1822
Workload Cluster storage Port Group	C01-NVMeTCP-SAN-A	C01-NVMeTCP-SAN-B
Workload Cluster storage Port Group VLAN	1821	1822
Workload Cluster storage network mask/prefix length	255.255.255.0/24	255.255.255.0/24
Workload Cluster storage network gateway (L3 only)	None	None
Workload Cluster storage network vmk interface IPs	172.18.21.105-108	172.18.22.105-108
Workload Cluster Storage Software Adapter	vmhba64	vmhba65
Port Number	3	4
VM NIC name	vmnic2	vmnic3

Table 21. PowerStore configuration

Configuration item	Value
PowerStore cluster FQDN or IP	PowerStore-Cluster-01
Volume Group names	VG-NVMe
Volume Names	V-NVMe
DDC Port Number	8009 (Default)

Table 22. PowerStore networking

Configuration item	SAN A	SAN B
Storage network name	NVMeTCP-SAN-A	NVMeTCP-SAN-B
Storage network VLAN ID	1821	1822
Storage network mask and prefix length	255.255.255.0/24	255.255.255.0/24
Storage network gateway (L3 only)	None	None
Storage network interface IPs	172.18.21.191-192	172.18.22.191-192

Configure virtual networking on endpoints and SFSS host operating system

The following section shows how to set up the virtual networking on the NVMe/TCP endpoints.

Create port groups for the SFSS VM NVMe/TCP control traffic

This example uses distributed port groups, but standard port groups can also be used.

1. Log in to the vSphere web client.
2. Click the **Networking** option.
3. Select the vDS used for the SFSS VM's NVMe/TCP Control traffic. This example uses the **C01-vDS-Management** vDS.
4. Right-click the vDS listing and select **Distributed Port Group**.
5. Click **New Distributed Port Group**.

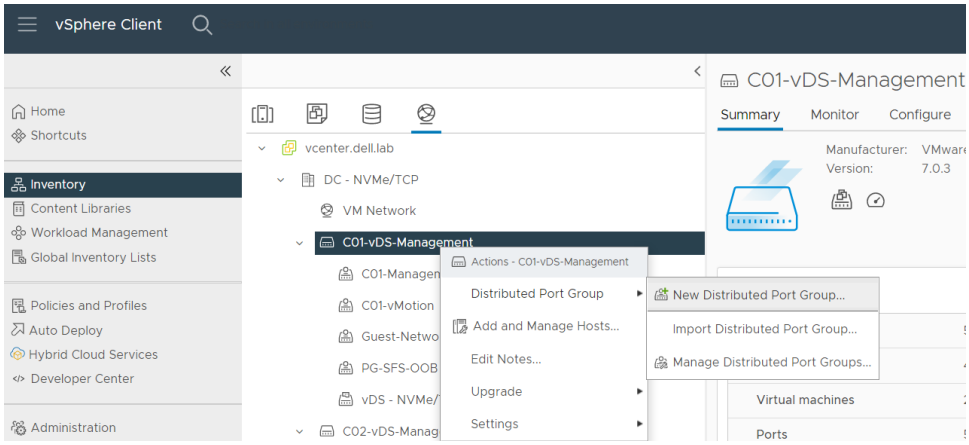


Figure 26. Add New Distributed Port Group

6. Provide a name for the first port group. This example uses the **C01-NVMeTCP-SAN-A-SFSS** port group.

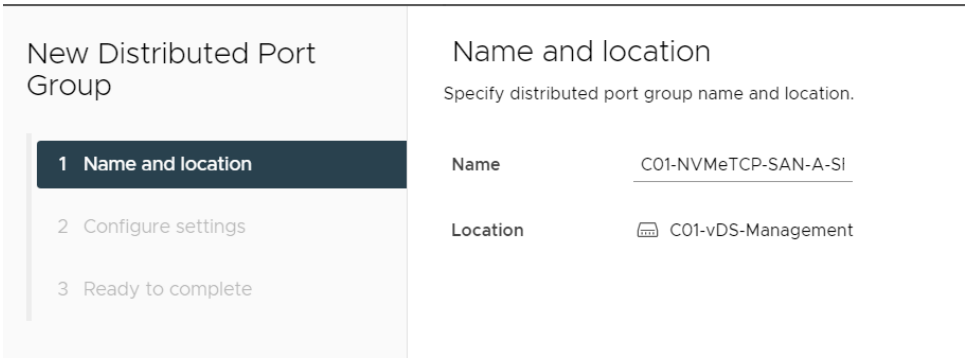


Figure 27. Provide a Name for the port group

7. Click **NEXT.**
8. On the **Configure Settings** page, select **VLAN** from the **VLAN type** field.
9. Enter the **VLAN ID** in the field provided. This example uses VLAN ID **1821**.
10. From the **Configure settings** screen, click to select the box next to **Customize default policies configuration**, and then click **NEXT**.

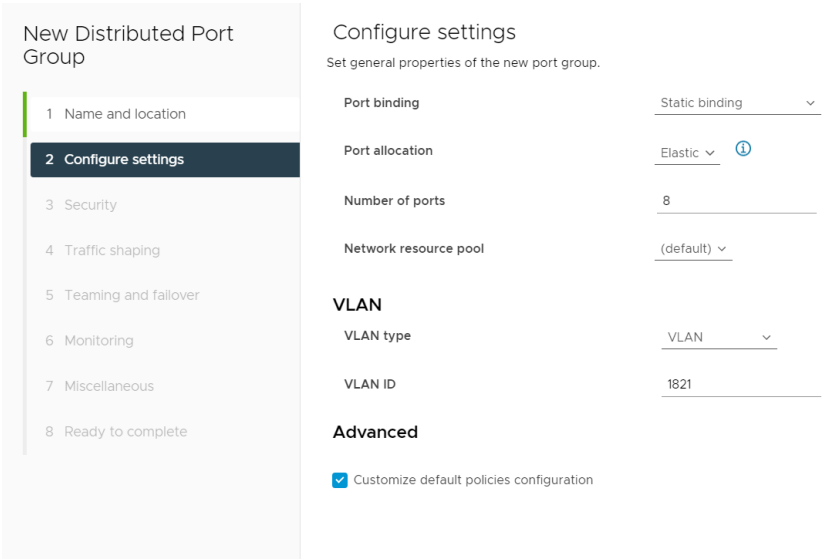


Figure 28. Distributed Port Group Settings

11. From the **Security** page, click **NEXT** to accept the default options.
12. On the **Traffic shaping** page, click **NEXT** to accept the **Disabled** default options.
13. From the **Teaming and failover** page, select and move the uplinks individually so that there is one **Active uplink**, and one **Standby uplink**, as shown in the figure below.

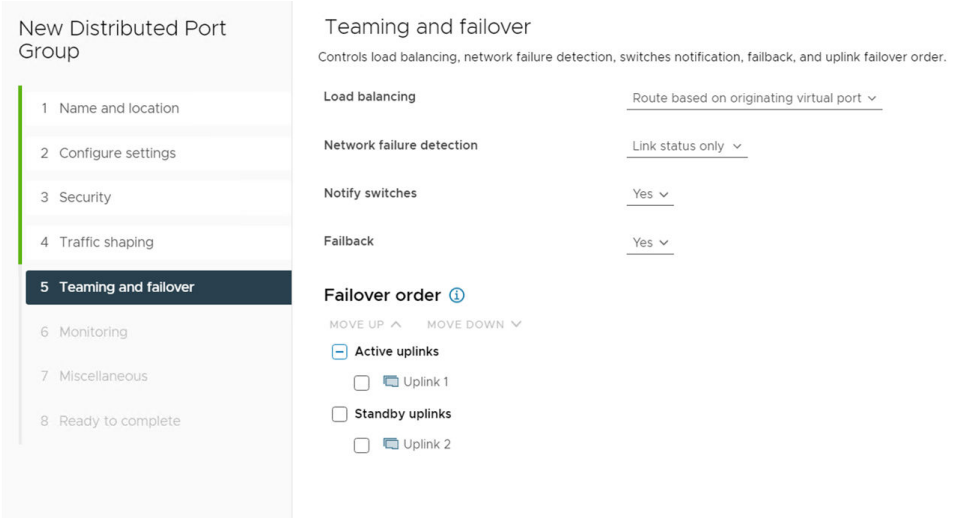


Figure 29. Teaming and failover page

14. Click **NEXT. Note:** Once selected, you can move an uplink to a different category using the **MOVE UP** and **MOVE DOWN** buttons.
15. Click **NEXT** to accept the **NetFlow – Disabled** default setting on the **Monitoring** screen.
16. Click **NEXT** to accept the **Block All Ports – No** default setting on the **Miscellaneous** screen.
17. Review the **Ready to complete** screen, and then click **FINISH**.

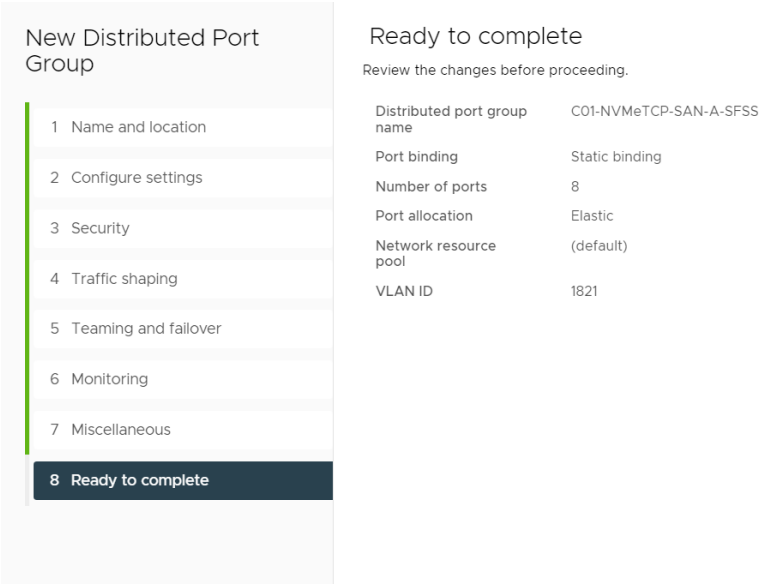


Figure 30. Ready to complete confirmation screen

The new **Distributed Port Group** is configured and displays under the **C01-vDS-Management** vDS.

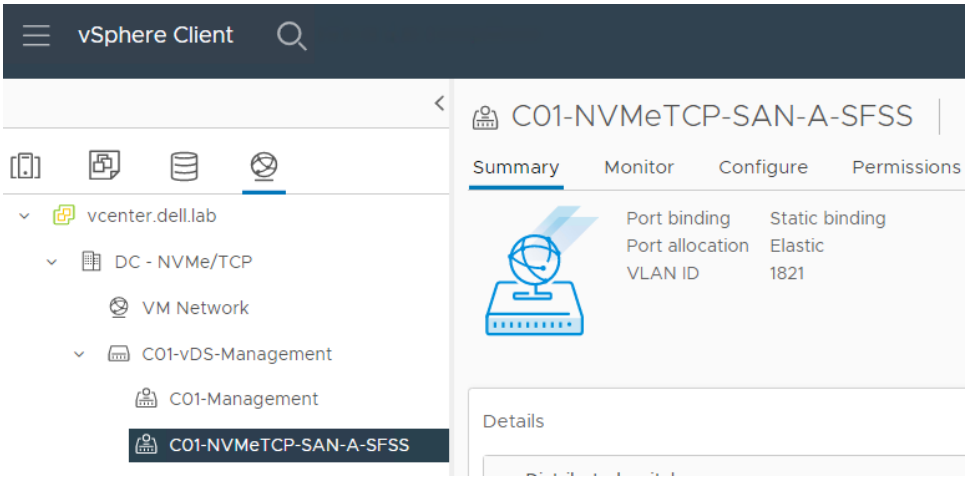


Figure 31. New Distributed Port Group created

To create the SFSS VM SAN B Control Traffic distributed port group, perform the following steps:

18. Select the **vDS.** In this example, **C01-vDS-Management** is selected.
19. Right-click and select **Distributed Port Group**.
20. Click **New Distributed Port Group**.
21. Provide a name for the second port group. In this example, **C01-NVMeTCP-SAN-B-SFSS** is used.

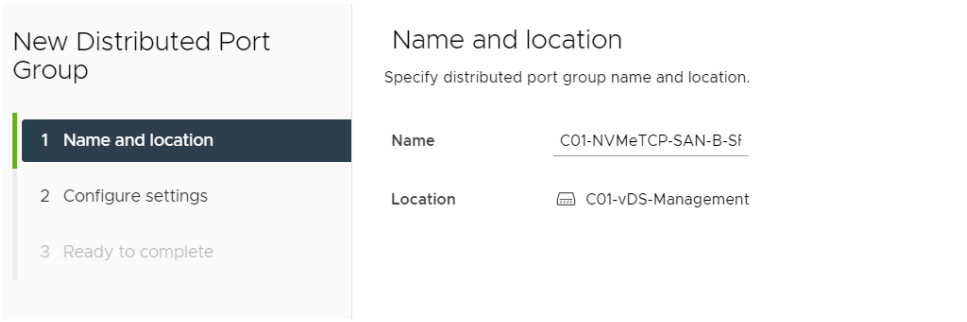


Figure 32. Provide a Name for the Port Group

22. Click **NEXT**.
23. On the **Configure Settings** page, select **VLAN** from the VLAN type field.
24. Enter **1822** as the VLAN ID for this example.
25. Check the box next to **Customize default policies configuration**.

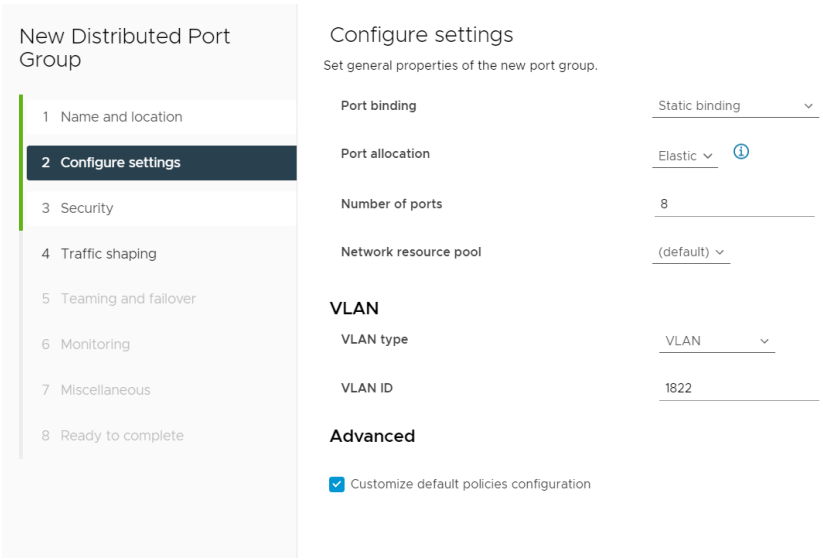


Figure 33. Distributed Port Group settings

26. Click **NEXT**.
27. On the **Security** page, leave the options at their default settings, and then click **NEXT**.
28. From the **Traffic shaping** page, leave the default **Disabled** settings, and then click **NEXT**.
29. On the **Teaming and failover** page, select and move the uplinks individually so that there is one **Active uplink**, and one **Standby uplink**, as MLAG is not used on the connected switch ports.

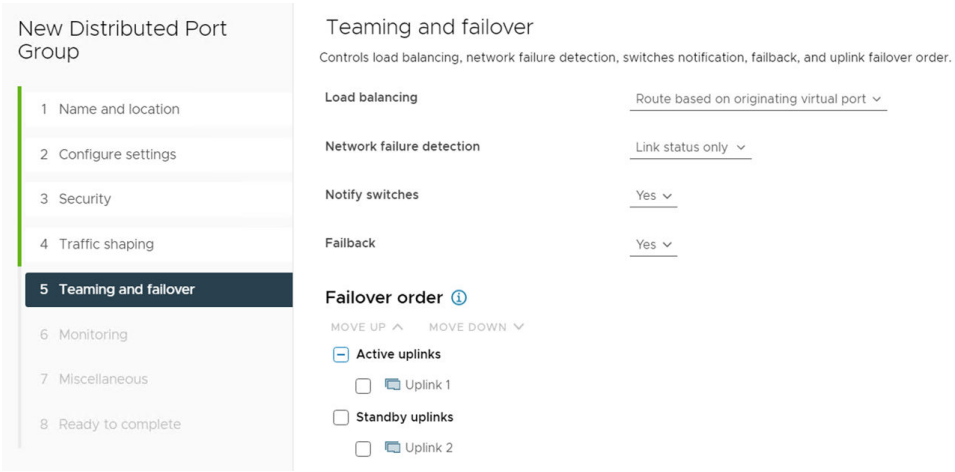


Figure 34. Teaming and failover page

30. On the **Monitoring** screen, leave the **Netflow** option at its default **Disabled** setting, and then click **NEXT**.
31. From the **Miscellaneous** screen, leave the **Block All Ports** option at its default **No** setting, and then click **NEXT**.
32. Review the **Ready to complete** screen, and click **FINISH**.

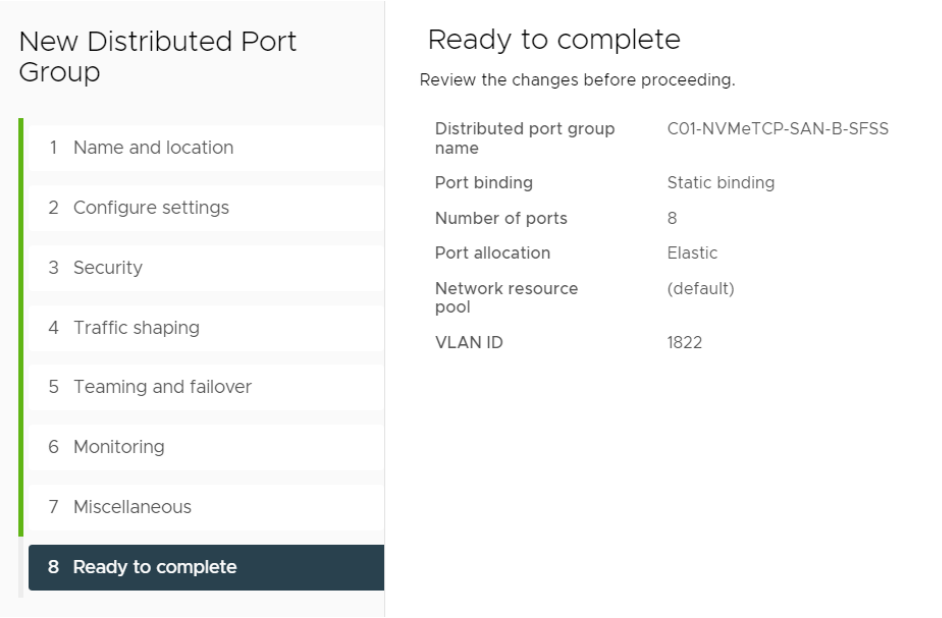


Figure 35. Ready to complete confirmation screen

The second Distributed Port Group is configured and displays under the **C01-vDS-Management** vDS.

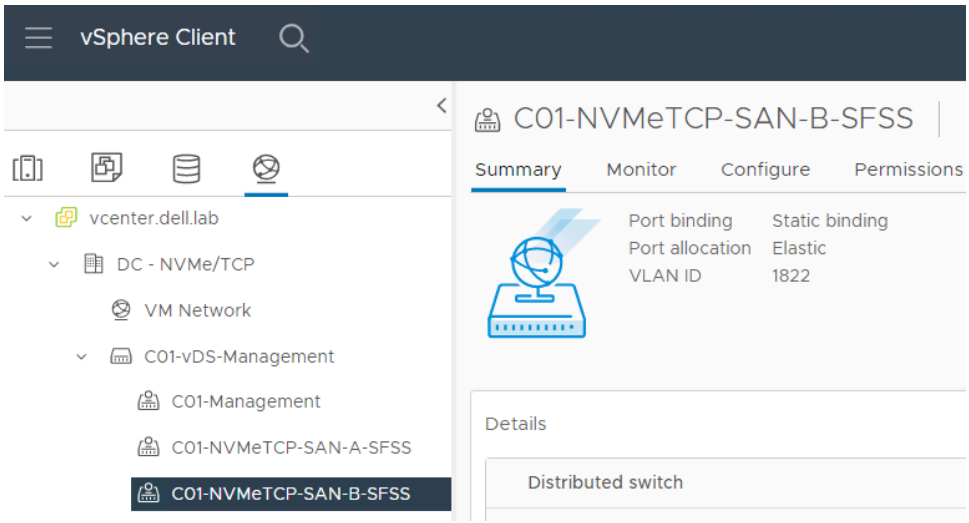


Figure 36. Configuration confirmation of Distributed Port Groups

VMware ESXi hosts

The following steps prepare the ESXi hosts for NVMe/TCP connectivity.

Create and configure vDS for host NVMe/TCP storage I/O traffic

In this example, the **C02-vDS-NVMeTCP** distributed switch is created for NVMe/TCP host traffic. For other virtual switch configurations, you can use an existing vDS or standard switches.

You will configure two port groups on this vDS to accommodate SAN-A and SAN-B traffic.

To create a vDS:

1. From the vSphere client, locate the **Networking** listing, and then right-click the **DC-NVMeTCP** virtual data center.
2. Click **Distributed Switch** > **New Distributed Switch**.

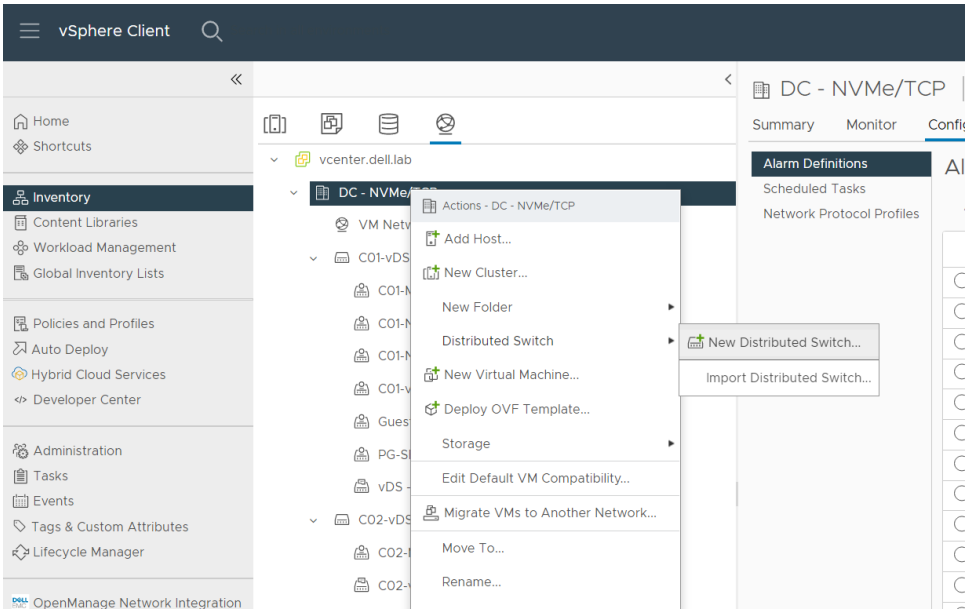


Figure 37. Select New Distributed Switch

3. In the **Name** field, enter a name for the vDS.

   NOTE: In this example, **C02-vDS-NVMeTCP** is used.

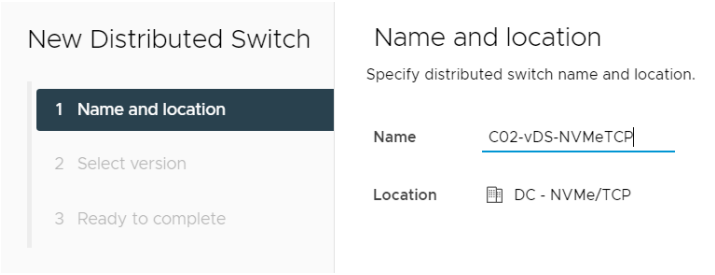


Figure 38. Provide Name for vDS

4. From the **Select version** option, select the version 7.0.3.

   NOTE: In this example, **7.0.3 - ESXi 7.0.3 and later** is used.

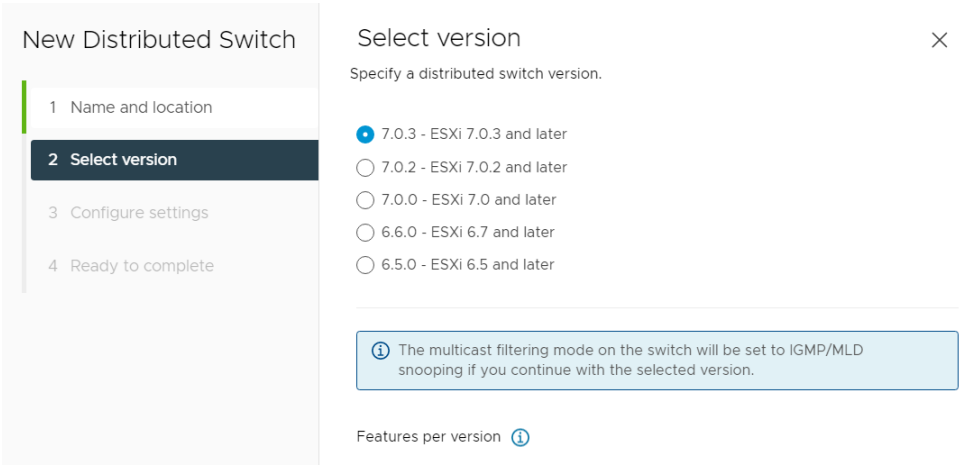


Figure 39. Select ESXi version

5. Click **Next.**
6. Specify the number of uplinks. This example uses **2** of the four uplinks for this vDS.
7. Click to clear the check from **Create a default port group**.

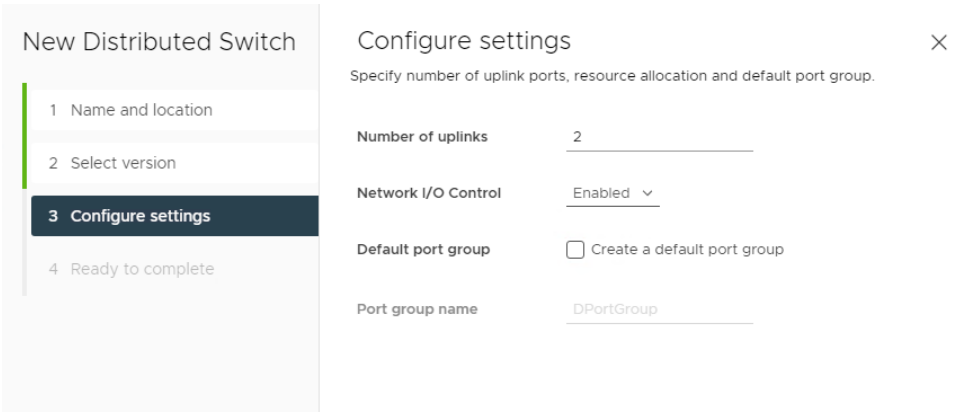


Figure 40. Number of uplinks

8. Click **Next.**
9. Review the **Ready to complete** screen and then click **FINISH.**

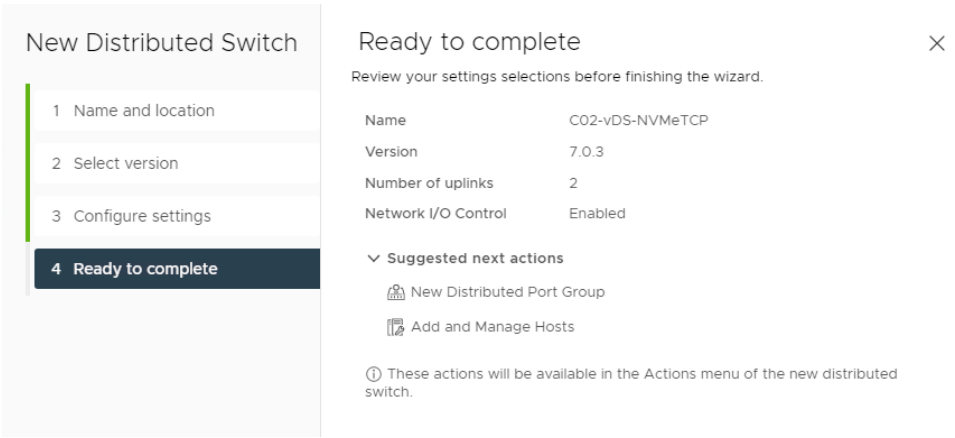


Figure 41. Ready to complete confirmation screen

10. Right-click the new **C02-vDS-NVMeTCP** vDS and then click **Settings** > **Edit Settings**.

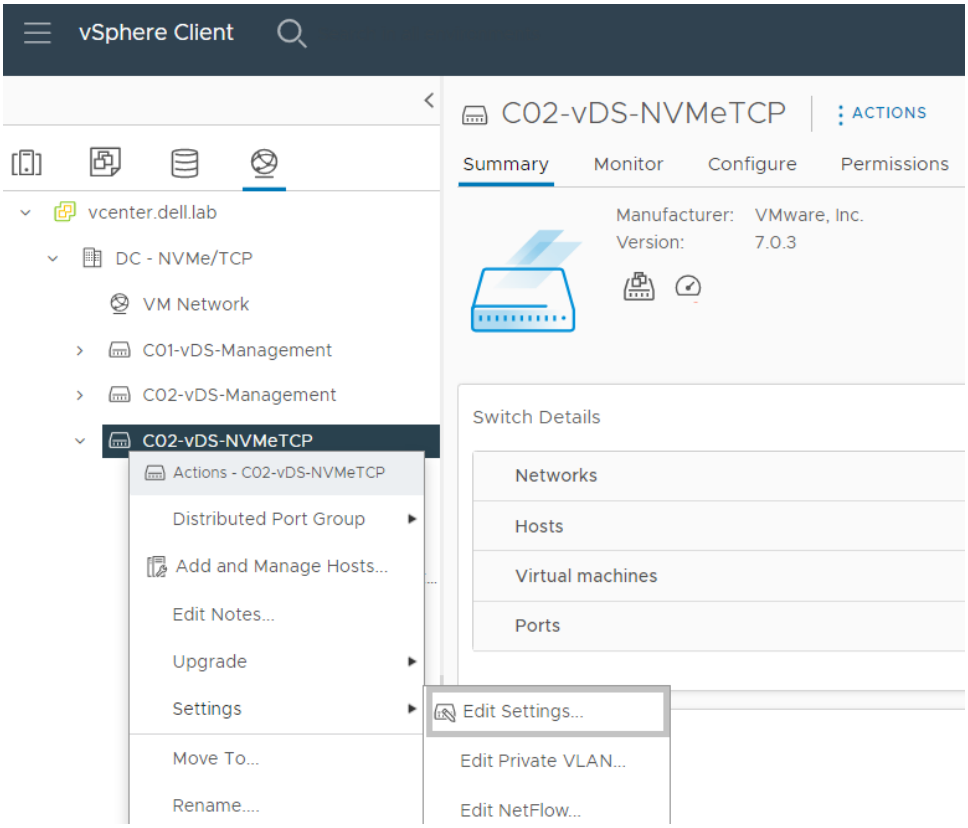


Figure 42. Edit Settings location

11. Click the **Advanced** tab and modify the following parameters:
    a. **MTU (Bytes)** – Change the MTU to match the end-to-end network. In this example, **9000** is used.
    NOTE: See the Maximum Transmission Unit section for more information.
    b. Under **Discovery protocol**, change the **Type** to **Link Layer Discovery Protocol**, and the **Operation** to **Both**.

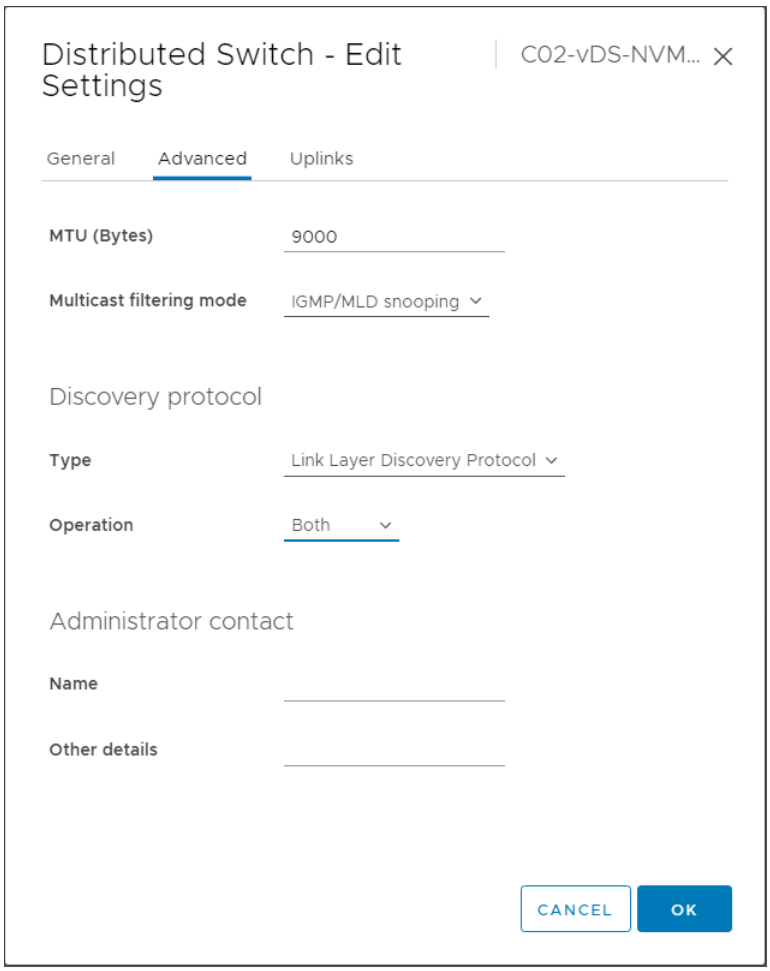


Figure 43. Distributed Switch - Edit settings

12. Click the **Uplinks** tab to confirm the correct number of uplinks.

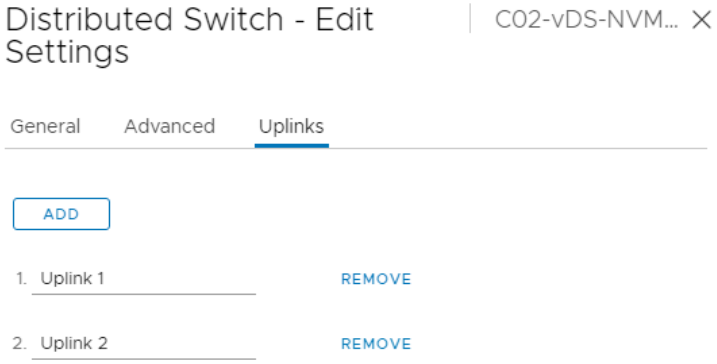


Figure 44. Edit Uplinks

13. Click **OK**.
14. From the **Configure** tab, verify that the **Properties** page displays the updated configuration.

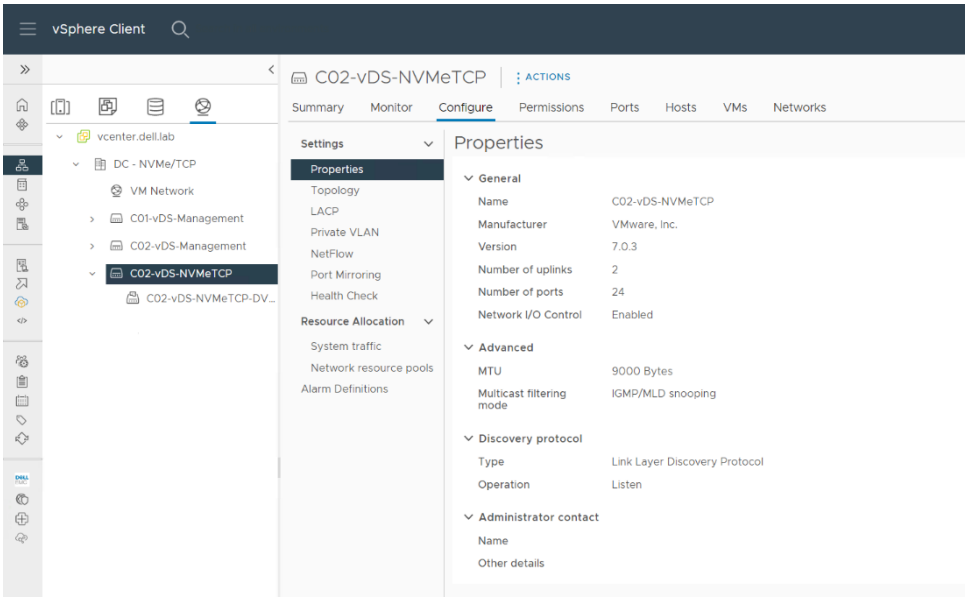


Figure 45. vDS Properties

Add hosts to vDS

To add the hosts to the vDS, perform the following steps:

1. Right-click the new vDS and select **Add and Manage Hosts**.

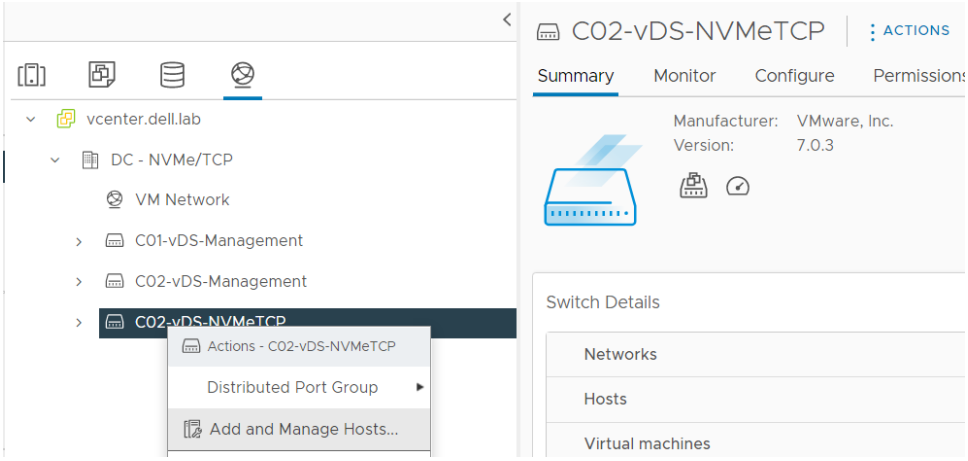


Figure 46. Add and Manage hosts

2. Select **Add hosts** and click **NEXT**.

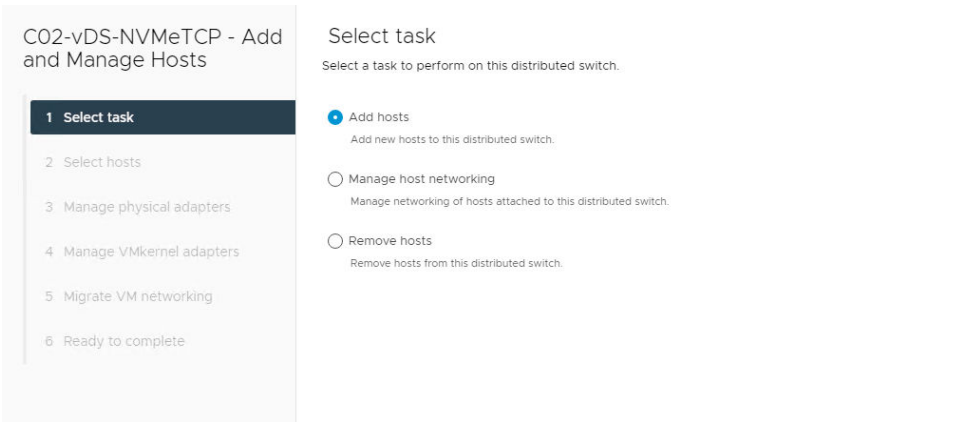


Figure 47. Add Hosts

3. From the listing, click to select the hosts that will participate in NVMe/TCP.

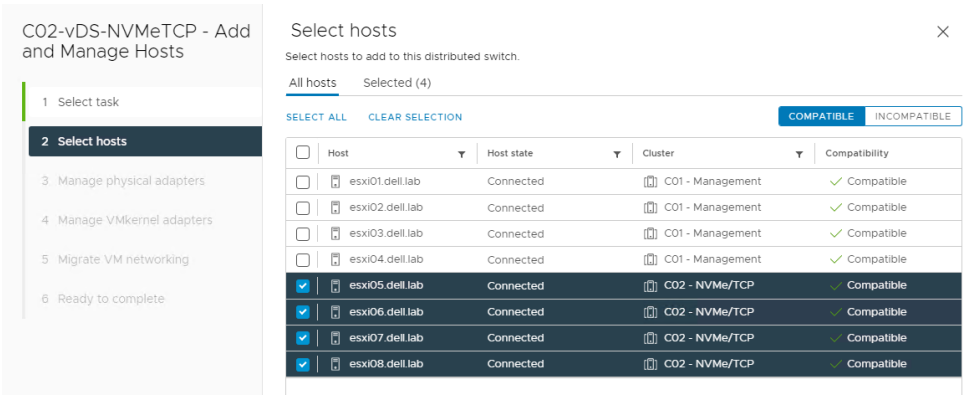


Figure 48. Select Hosts

4. In **Manage physical adapters**, click to select and assign which of the host vmnics will map to the vDS uplinks. In this example, **Uplink 1** and **Uplink 2** are assigned to **vmnic 2** and **vmnic3**.

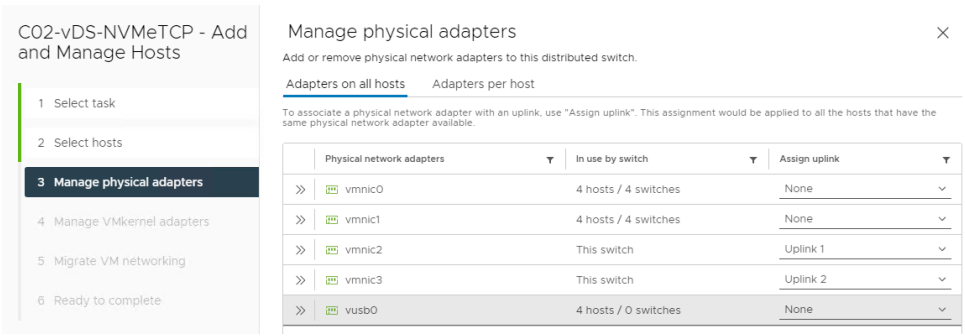


Figure 49. Manage physical adapters

5. Click **NEXT**.
6. From the **Manage VMkernel adapters** section, click **NEXT**. **Note:** The NVMe/TCP VMkernel adapters are created later in this process.
7. On the **Migrate VM networking** screen, click **NEXT**, and then click **FINISH**.

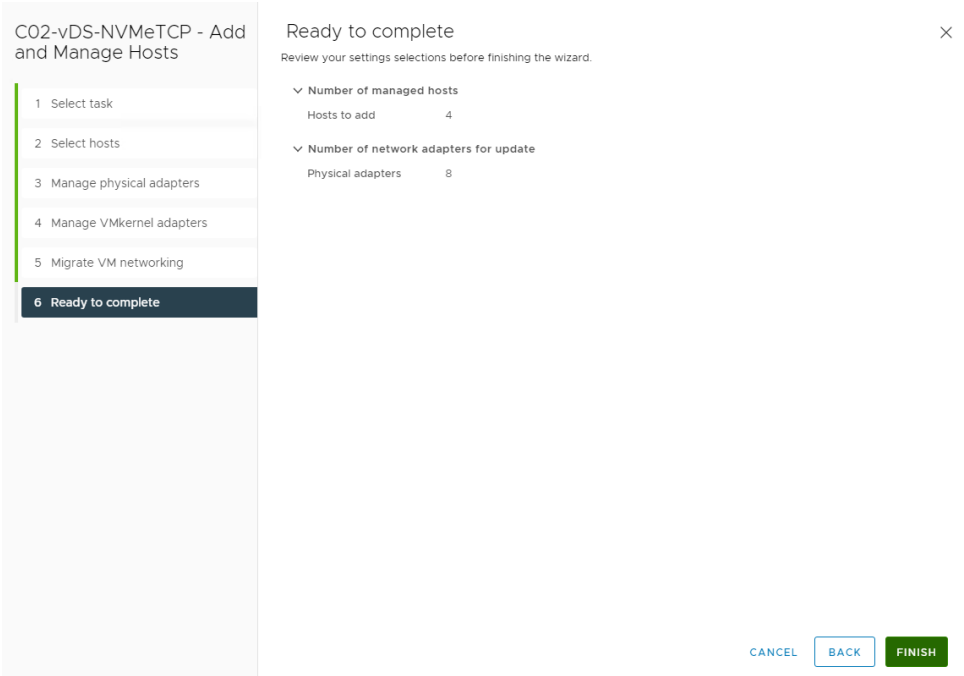


Figure 50. Ready to Complete host addition

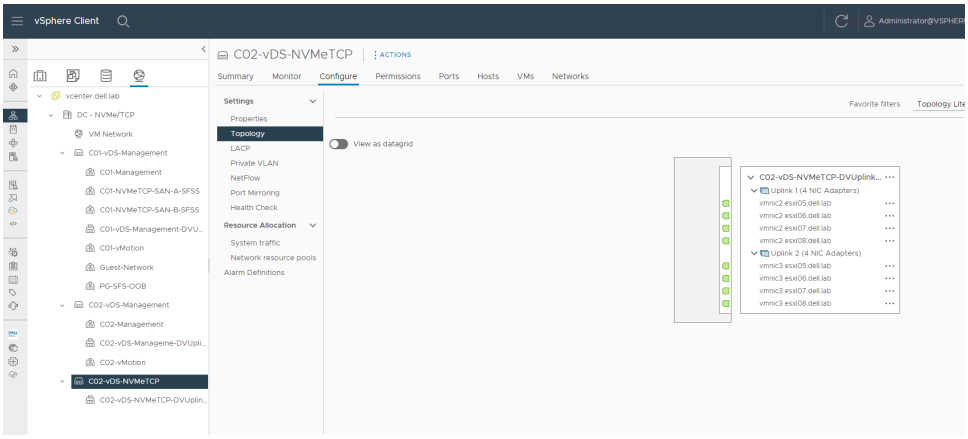


Figure 51. New vDS Topology View

Create host NVMe/TCP storage I/O traffic port groups

In this section, two port groups for NVMe/TCP storage traffic are created on the virtual distributed switch. In this example, **C02-NVMeTCP-SAN-A** and **C02-NVMeTCP-SAN-B** are created on the **C02-vDS-NVMeTCP** distributed switch.

Configure SAN A Port Group for NVMe/TCP VMkernels

To configure the SAN A port group for the NVMe/TCP VMkernels, perform the following steps:

1. Right-click the distributed switch for NVMe/TCP traffic.
   This example uses **C02-vDS-NVMeTCP**.
2. Select **Distributed Port Group**, and then click **New Distributed Port Group**.

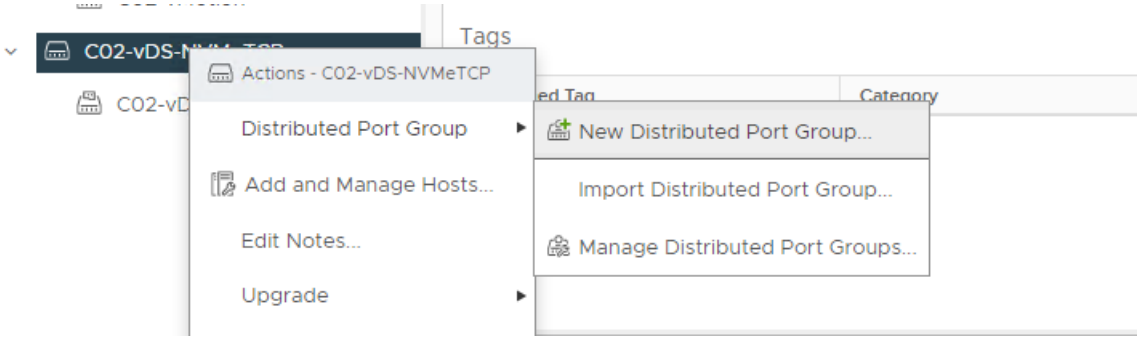


Figure 52. Create Port Group

3. From the **Name and location** screen, enter a **Name** for the port group in the field provided.

   NOTE: In this example, **C02-NVMeTCP-SAN-A** is used.

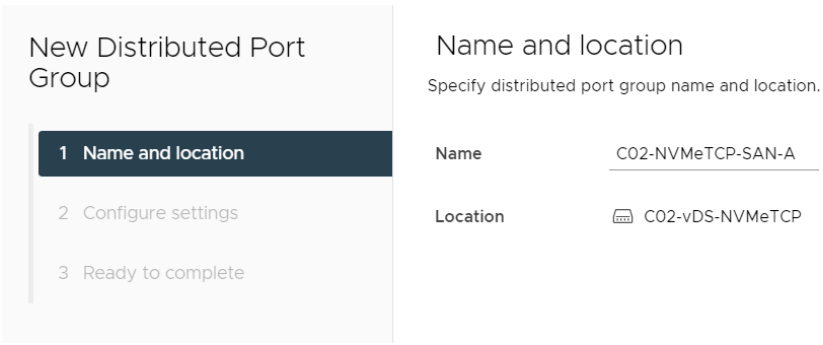


Figure 53. Specify name for port group

4. Click **Next**.
5. On the **Configure settings** screen, select **VLAN** as the **VLAN type**, and enter the **VLAN ID** in the field provided.

NOTE: This example uses **1821**.

6. Click to select the **Customize default policies configuration** box.

NOTE: Other tasks display in the left column.

7. Click **NEXT**.

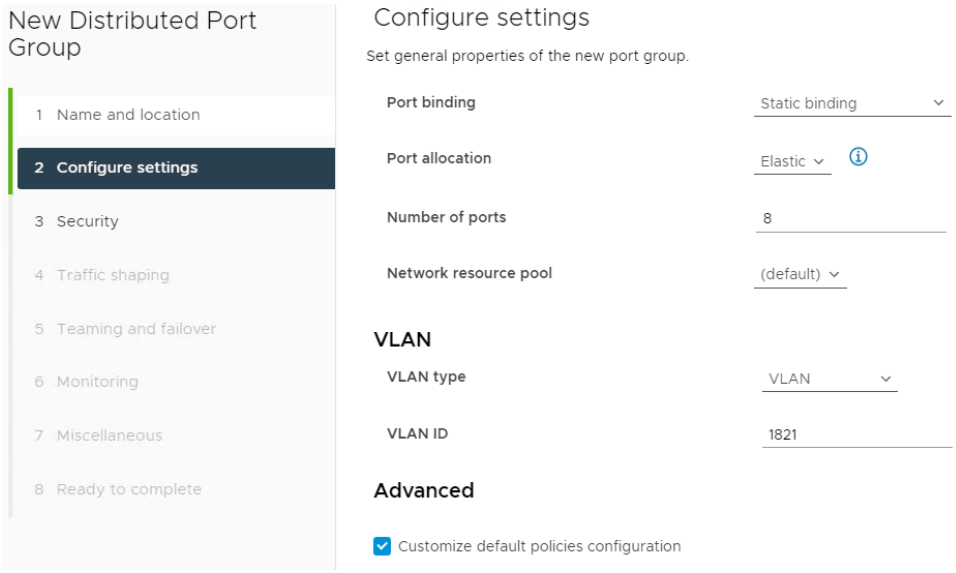


Figure 54. Configure settings for port group

8. Click **Next** to accept the **Security** screen defaults.
9. Click **Next** to accept the **Traffic shaping** defaults.
10. From the **Teaming and Failover** screen, set **Notify switches** to **No**, and the **Failback** option to **No**.

NOTE: Set only one Active uplink. Other **Active** or **Standby** links are not possible because the storage adapter cannot failover. In this example, **Uplink 1** is the **Active** uplink for **C02-NVMeTCP-SAN-A**, **Uplink 1**. In this example, **Uplink 2** is moved to **Unused uplinks**, where **Uplink 2** will be active for **SAN B**.

NOTE: See the VMware ESXi requirements section for further details.

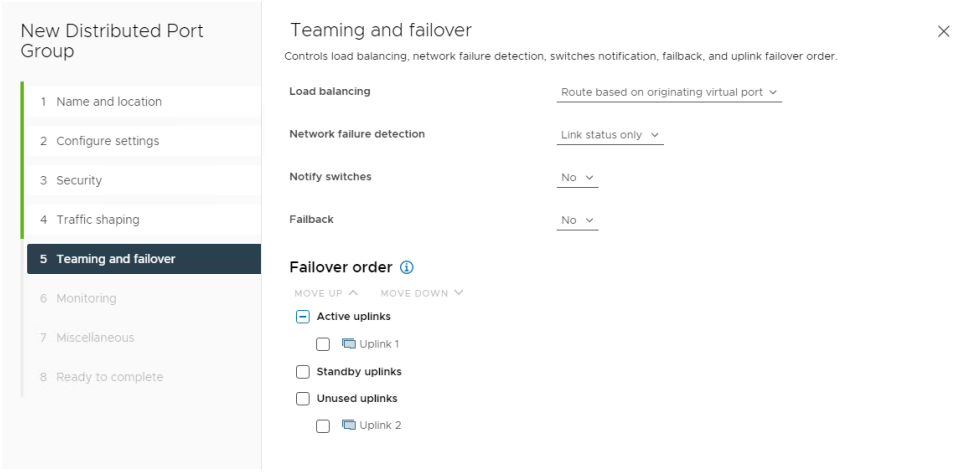


Figure 55. Port group Teaming and failover screen

11. From the **Monitoring** screen, leave the default settings as they are and click **NEXT**.
12. On the **Miscellaneous** screen, leave the default settings as they are and then click **NEXT**.
13. On the **Ready to complete** screen, review the information, and then click **Finish**.

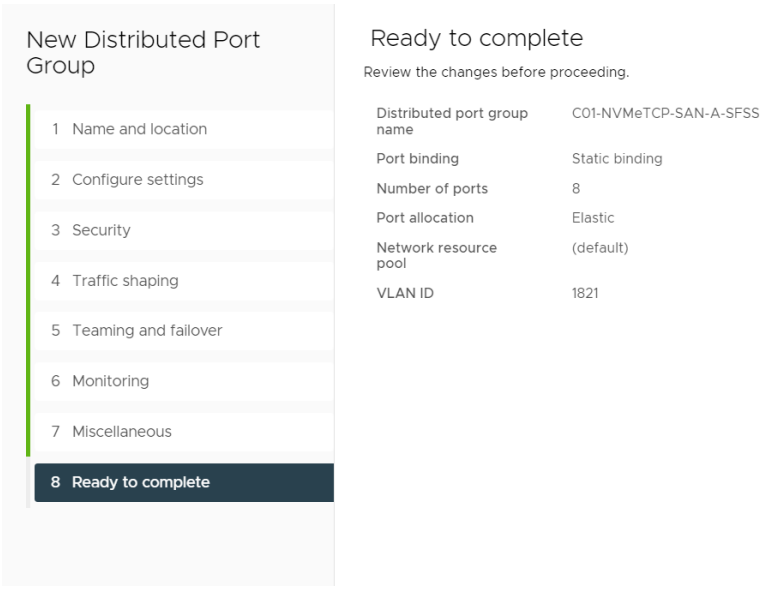


Figure 56. Ready to complete confirmation screen

Configure SAN B Port Group for NVMe/TCP VMkernels

To configure the SAN A port group for the NVMe/TCP VMkernels, perform the following steps:

1. Right-click the distributed switch for NVMe/TCP traffic. In this example, **C02-vDS-NVMeTCP** is used**.**
2. Select **Distributed Port Group** > **New Distributed Port Group**.
3. On the **Name and location** screen, enter a **Name** for the Port Group. In this example, **C02-NVMeTCP-SAN-B** is used.
4. Click **Next.**
5. In the **Configure settings** screen, select **VLAN type** as VLAN, and set the **VLAN ID**.
   This example uses **1822**.
6. Click to select the **Customize default policies** configuration box.
7. Click **Next** to accept **Security** screen defaults.
8. Click **Next** to accept the **Traffic shaping** defaults.
9. On the **Teaming and Failover** screen, set Notify switches to No, and Failback to No.

   NOTE: Set only one **Active uplink**. Other Active or Standby links are not possible because the storage adapter cannot failover. In this example, for **C02-NVMeTCP-SAN-B**, **Uplink 2** is the Active uplink. In this example, move **Uplink 1** to **Unused uplinks**.

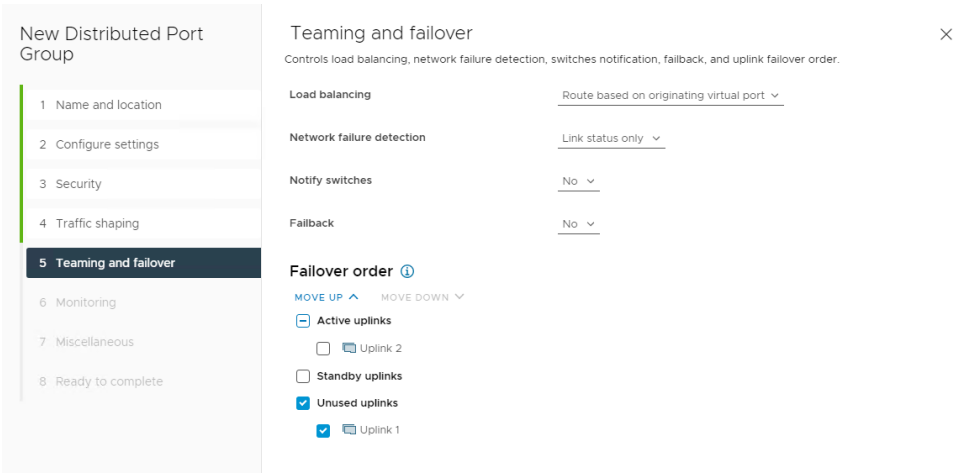


Figure 57. Teaming and Failover settings on SAN B Port Group

10. Click **Next** to accept **Monitoring** screen defaults.
11. Click **Next** to accept the **Miscellaneous** defaults.

12. On the **Ready to complete** screen, review the information, and then click **Finish**.
13. To view the topology of the vDS, right-click the distributed switch, go to the **configure** tab, and click **Topology**.

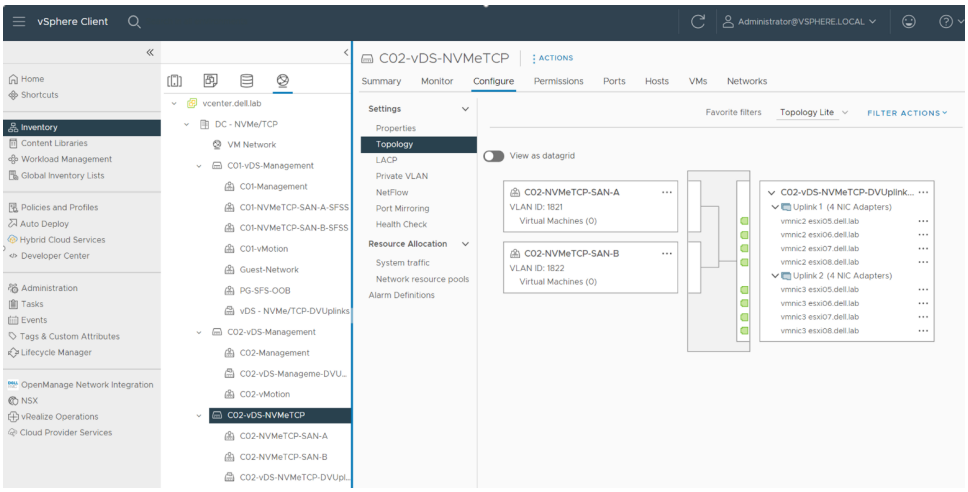


Figure 58. New vDS with two new Port Groups for NVMe/TCP traffic

Create VMkernel ports for NVMe/TCP Storage I/O Traffic

Follow the steps to create VMkernel ports for NVMe/TCP on all hosts connected to the vDS.

The first set of steps provides instructions for port group **C02-NVMeTCP-SAN-A**. The steps are repeated using different IP settings for port group **C02-NVMeTCP-SAN-B**.

1. From the vSphere Client, select **Networking.**
2. Right-click the **C02-NVMeTCP-SAN-A** port group.
3. Select **Add VMkernel Adapters**.

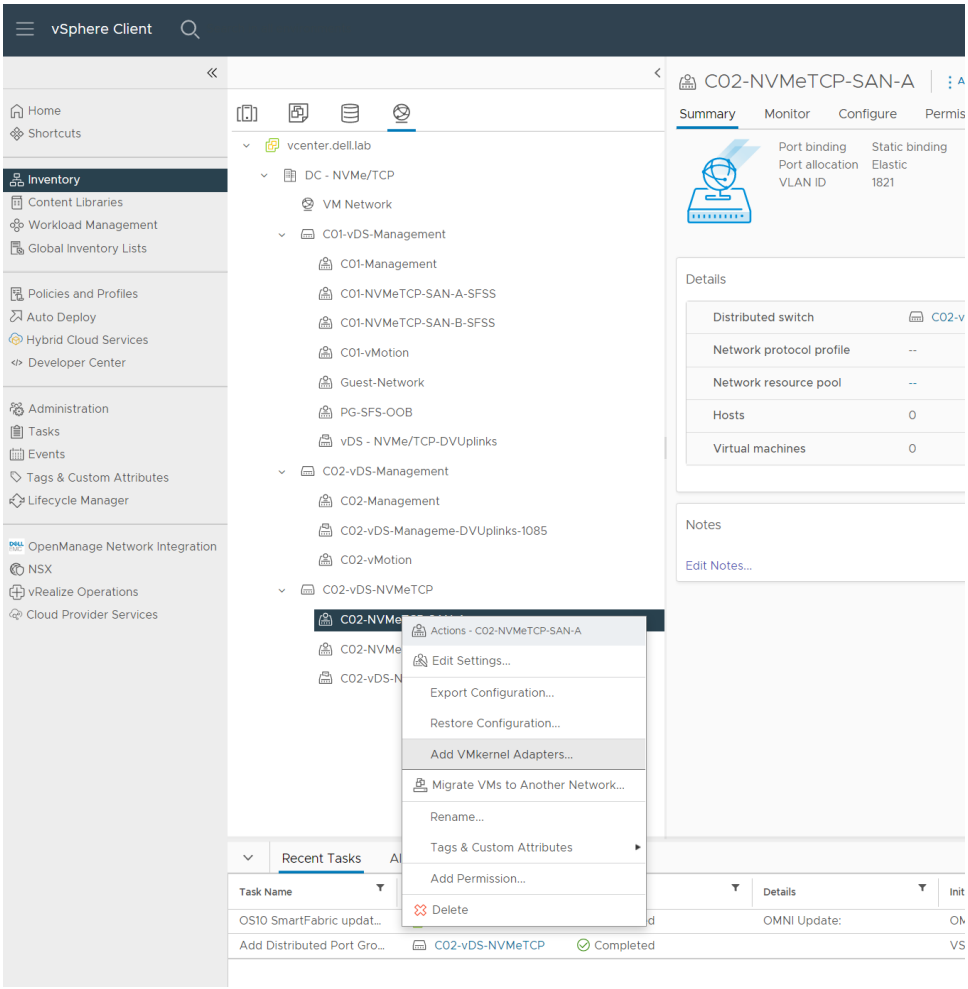


Figure 59. Add VMkernel to Port Group

4. In the **Add VMkernel Adapters** dialog box, select the following options:
   a. On the **Select hosts** page, click **+Attached hosts**.
   b. In the **Select Member Hosts** dialog box, select all the hosts listed.

   NOTE: In this example, hosts **esxi05** through **esxi08** are selected.

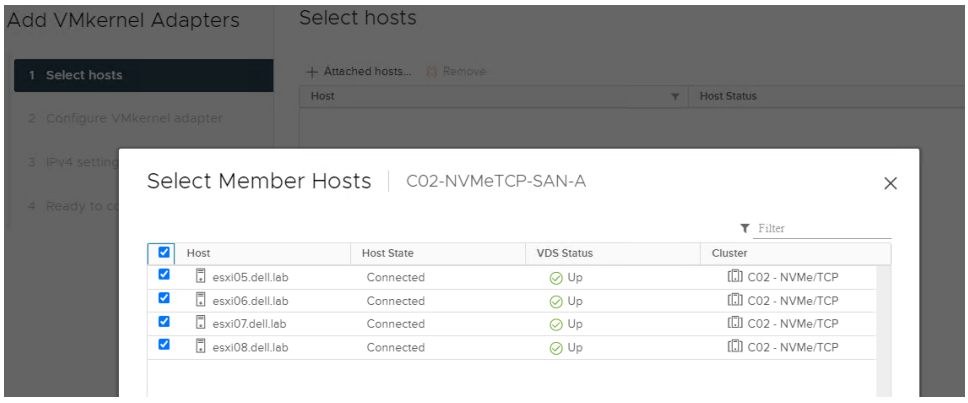


Figure 60. Select host members

   c. Click **OK**.

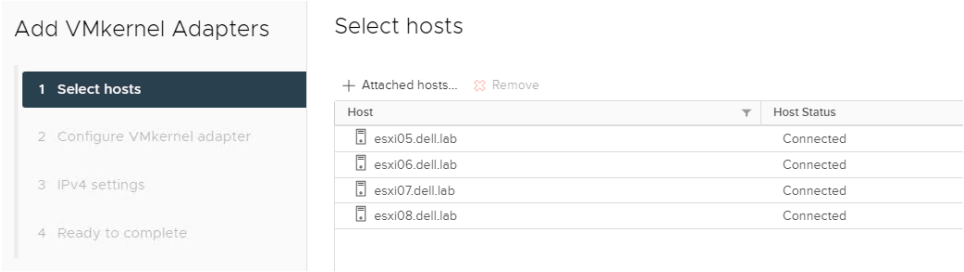


Figure 61. Select hosts

5. Click **Next**.
6. On the **Configure VMkernel adapter** page, set **MTU** to match the network.

   NOTE: In this example, the **MTU** is learned from the switch and is **9000**.
7. From the **Available services** listing, select **NVMe over TCP**.

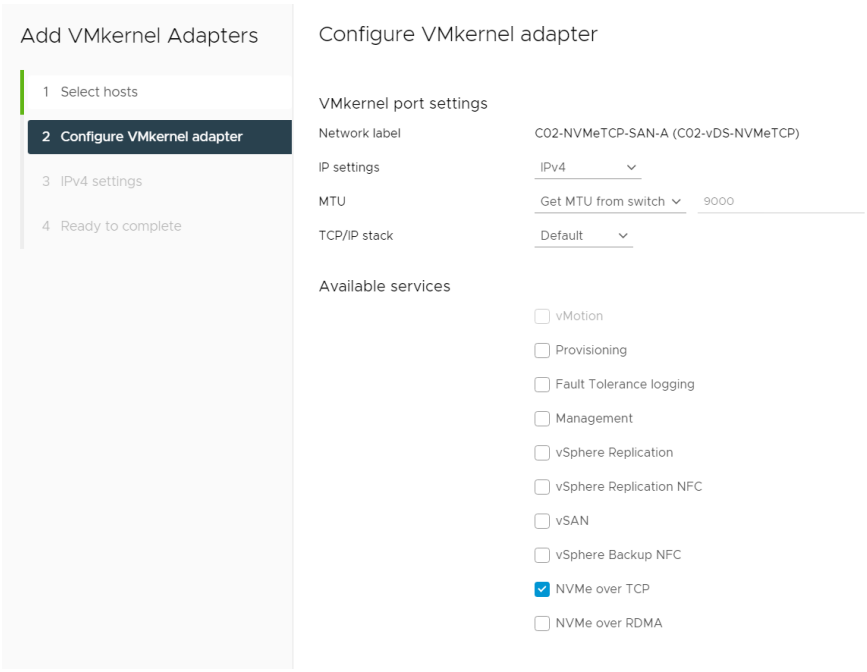


Figure 62. Configure VMkernel adapter

8. Click **Next**.
9. On the IPv4 settings page, select Use static IPv4 settings.
10. Enter the **IP** and **Subnet Mask** for each host.
    a. Use IP addresses from the SAN A NVMe/TCP Storage network. In this example, **172.18.21.105** through **172.18.21.108** are used.
    b. In the **Gateway** section, select **Do not configure** from the drop-down.

       NOTE: If Layer 3 connectivity is required to reach the hosts from SFSS or storage, add a default gateway as follows:

       i. In the **Gateway** section, select the **Configuration type** as **Configure on VMkernel adapters**.

       ii. Enter the **Gateway IP address**.

           NOTE: In this example, gateway 172.18.21.254 is used.

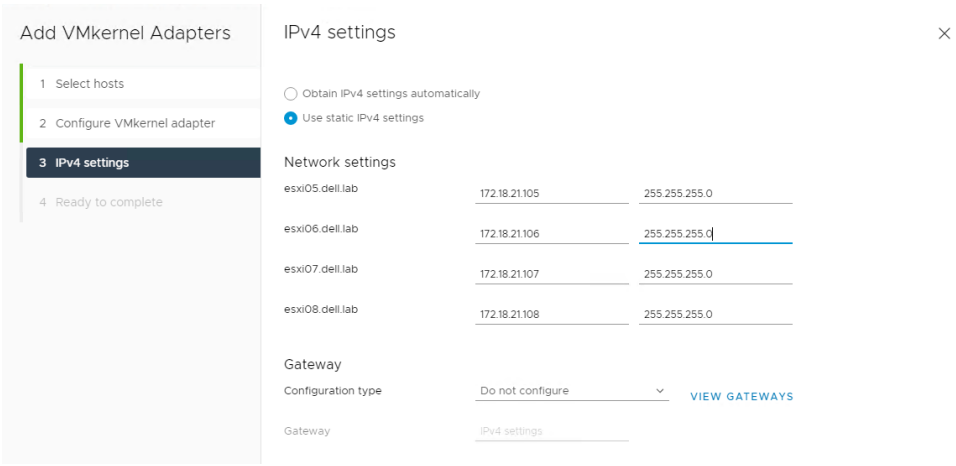


Figure 63. IPv4 settings

11. Click **NEXT**.
12. On the **Ready to complete** page, review the information and click **FINISH**

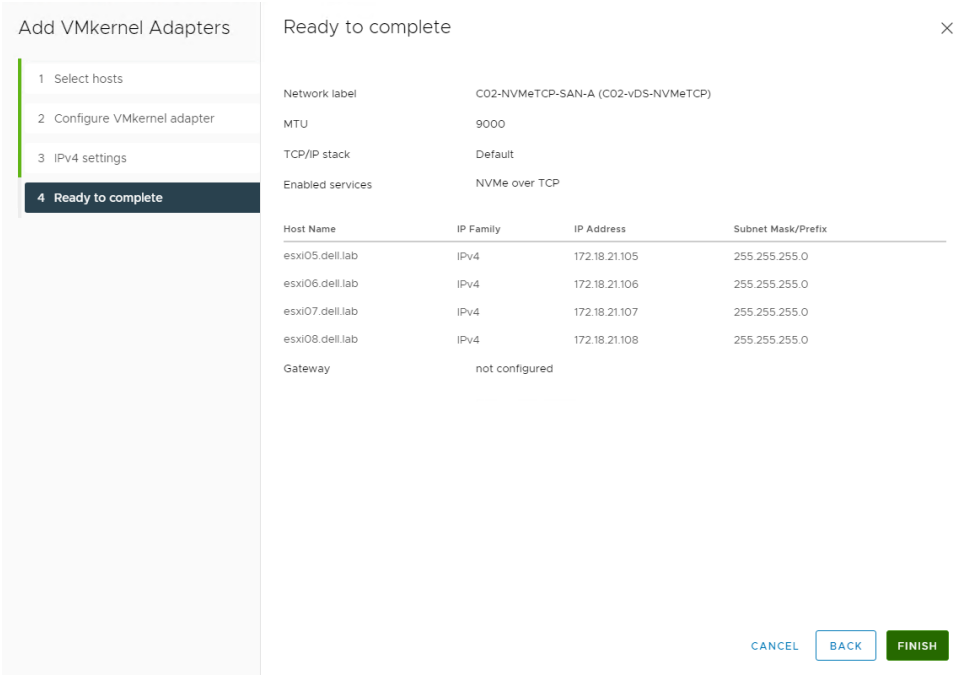


Figure 64. Ready to complete confirmation screen

13. To verify the creation of the VMkernel ports on the hosts, select **C02-vDS–NVMeTCP** > **Configure** > **Topology**.
14. Click to expand the **VMkernel ports** in the **C02-NVMeTCP-SAN-A** port group and view the VMkernel details.

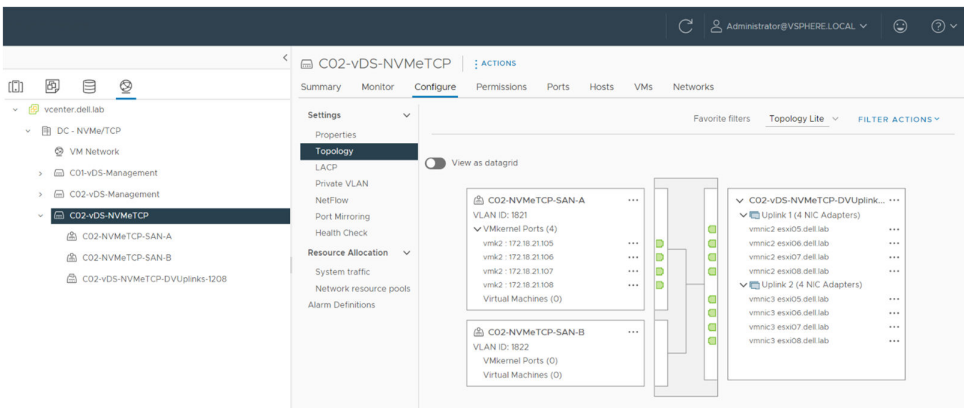


Figure 65. Verifying VMkernel ports for SAN-A

15. To add the VMkernel adapters to **C02-NVMeTCP-SAN-B**, repeat the steps in this section and from vSphere client, select **Networking**.
16. Right-click the **C02-NVMeTCP-SAN-B** port group, and then select **Add VMkernel Adapters**.

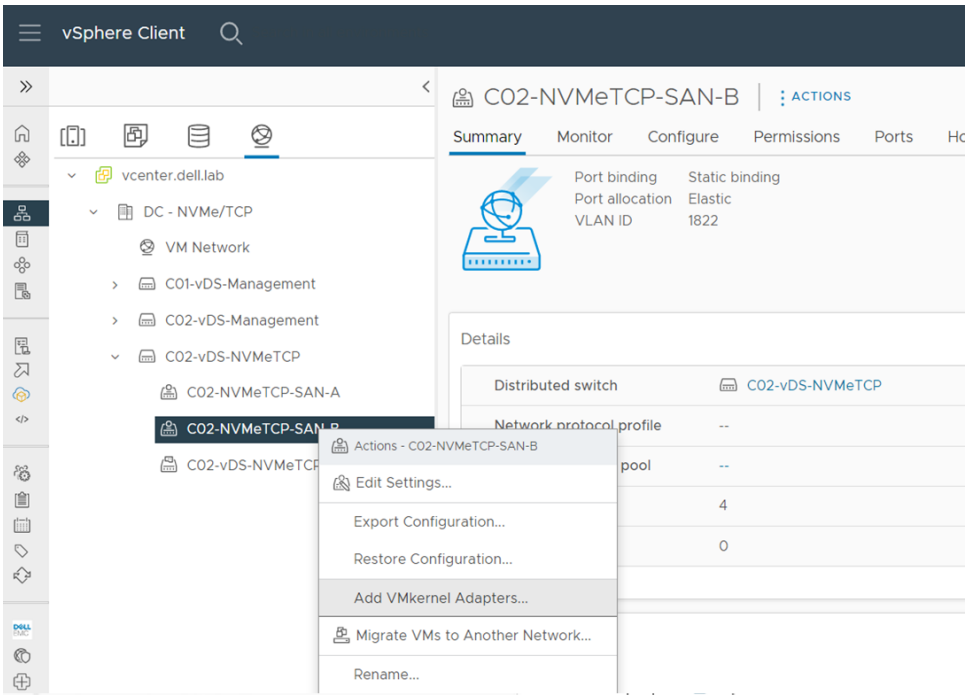


Figure 66. Add VMkernel to Port Group

17. In the **Add VMkernel Adapters** dialog box, select the following options:
    a. On the **Select hosts** page, click **+Attached hosts**.
    b. In the **Select Member Hosts** dialog box, select all the hosts listed.

    NOTE: For this topology, hosts **esxi05** through **esxi08** are selected.

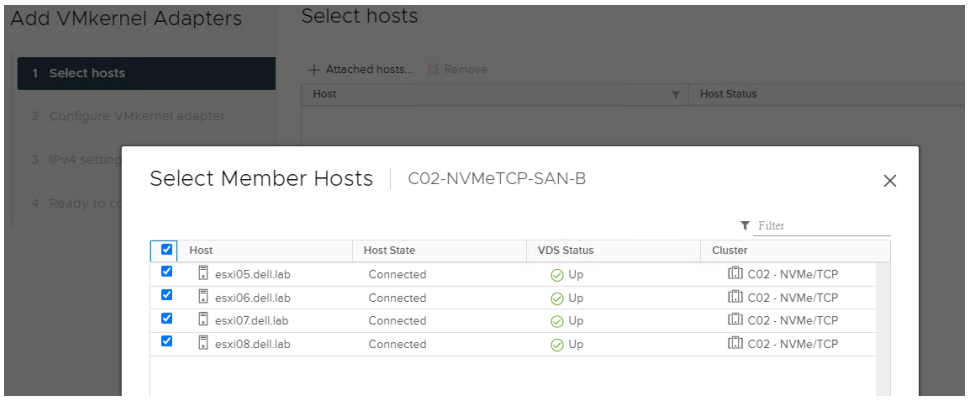


Figure 67. Select Hosts

    c. Click **OK**.

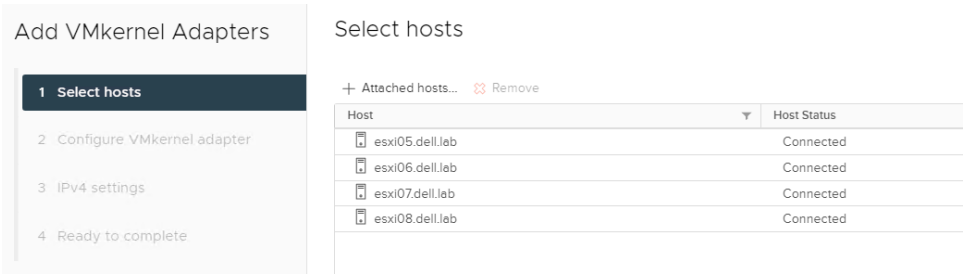


Figure 68. Select hosts for new vmks

18. Click **Next**.

19. Set the **MTU** to match the network. **Note:** In this example, the MTU is learned from the switch and is **9000**.
20. Under **Available services**, select **NVMe over TCP**.

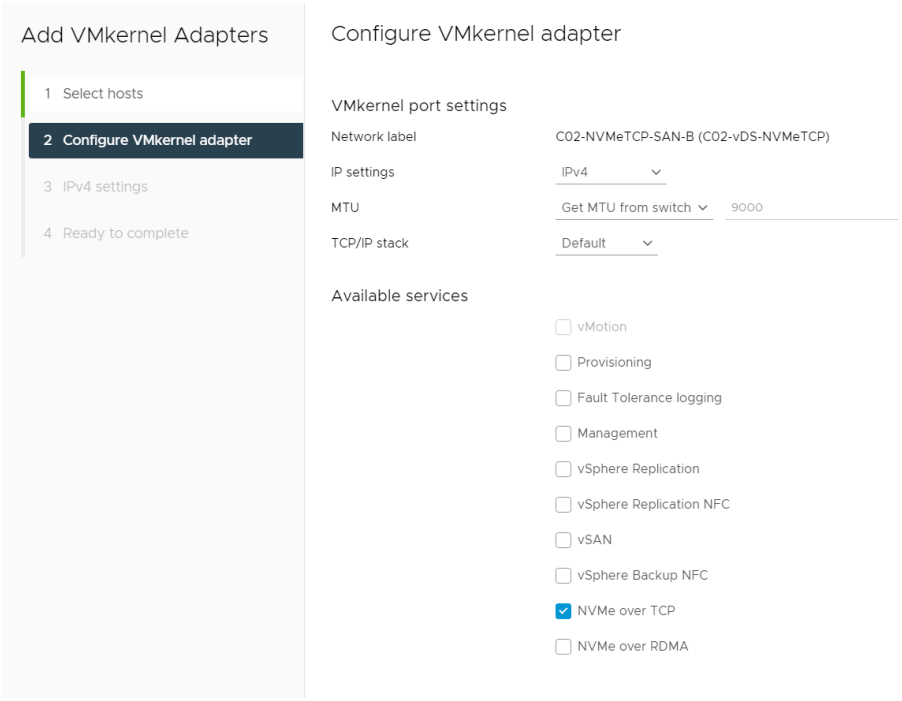


Figure 69. Set MTU and NVMe/TCP on VMkernel adapters

21. Click **Next**.
22. On the **IPv4 settings** page, select **Use static IPv4 settings**.
23. Enter the **IP** and **Subnet Mask** for each host.
    a. Use IP addresses for the NVMe/TCP Storage network planned. In this example, **172.11.22.105** through **172.11.22.108** are used.
    NOTE: The IP address range is in a different subnet than the IP address range that is used for **C02-NVMeTCP-SAN-A**.
    b. In the **Gateway** section, select **Do not configure**.

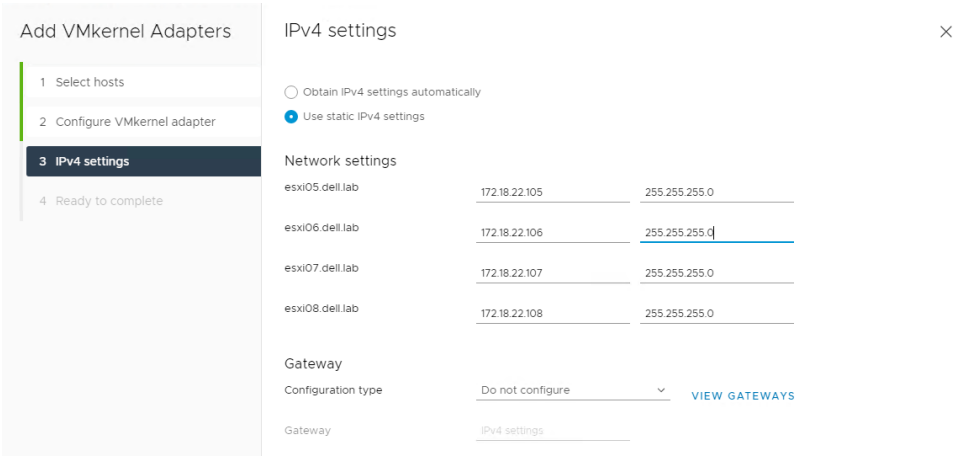


Figure 70. Assign IPs to VMkernel adapters

24. Click **NEXT**.
25. On the **Ready to complete** page, review the information, and then click **FINISH**.

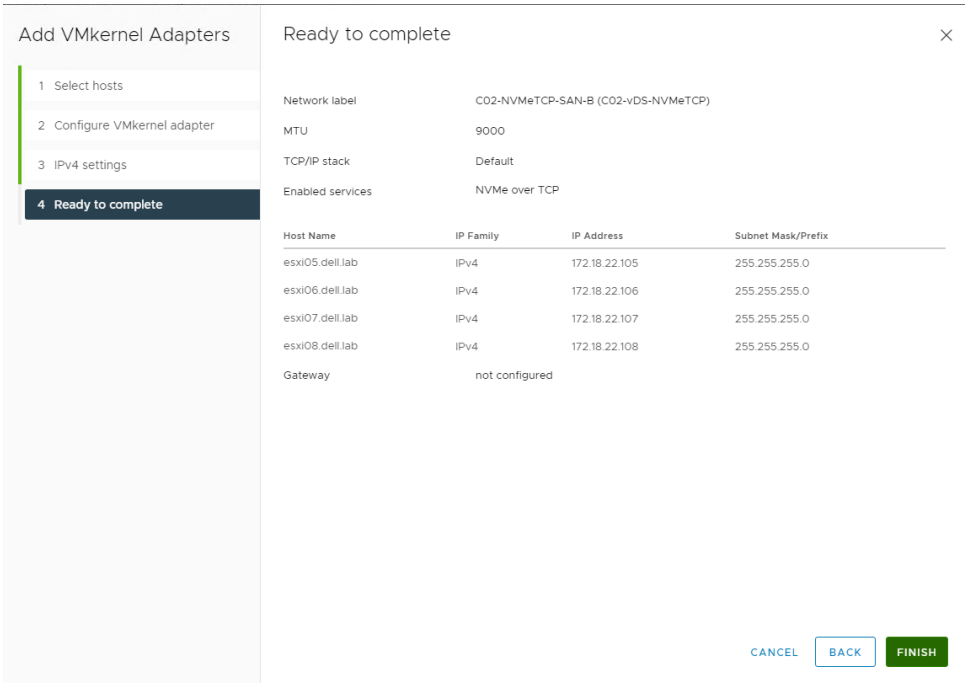


Figure 71. Ready to complete Add VMkernel Adapters

26. Click **C02-vDS-NVMeTCP** > **Configure** > **Topology** to verify that the created VMkernel ports are on the hosts.
27. Click to expand the **VMkernel ports** section in the **C02-NVMeTCP-SAN-B** port group, and view the **VMkernel details**.

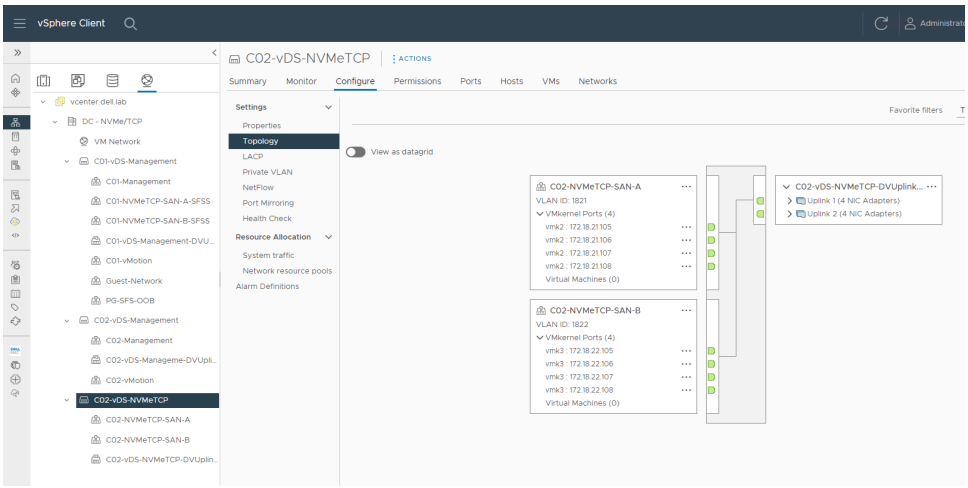


Figure 72. Verifying VMkernel ports for SAN and SAN-B

Create NVMe over TCP storage adapters on each host

To create the storage adapters for NVMe/TCP, perform the following steps.

1. From the vSphere client, select **Hosts and clusters**.
2. Click the **host**. **Note:** In this example, host **esxi05.dell.lab** is selected.
3. Click **Configure** > **Storage Adapters**> **Add Software Adapter**.
4. Select **Add NVMe over TCP adapter**.

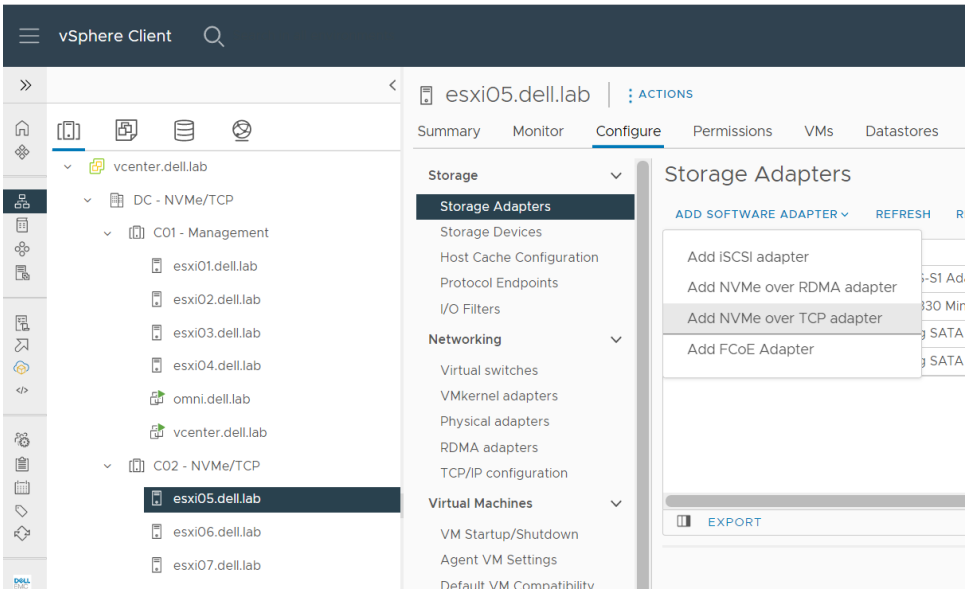


Figure 73. Select Add NVMe/TCP Adapter

5. Select the **Physical Network Adapter** for SAN A**.**

NOTE: In this example, **vmnic2** is selected.

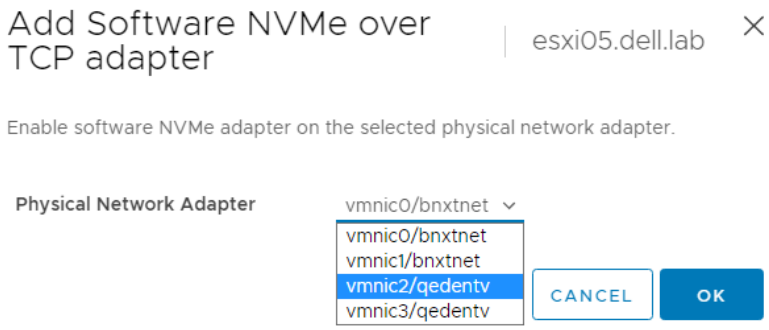


Figure 74. Add software adapter

6. Click **OK.**
7. After a few seconds, verify that the newly created NVMe over TCP software storage adapter, **vmhba64**, was added.

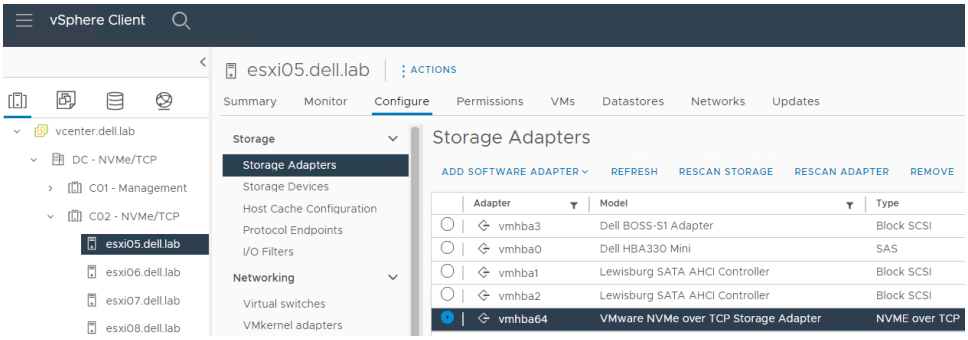


Figure 75. NVMe/TCP storage adapter (vmhba64)

8. Repeat the steps in this section to create a second storage adapter for the host, however, the select the following options for the second uplink:
9. Click **Add Software Adapter**.
10. Select **Add NVMe over TCP adapter**.
11. Select the **Physical Network Adapter** for SAN B.

NOTE: In this example, vmnic3 is selected.

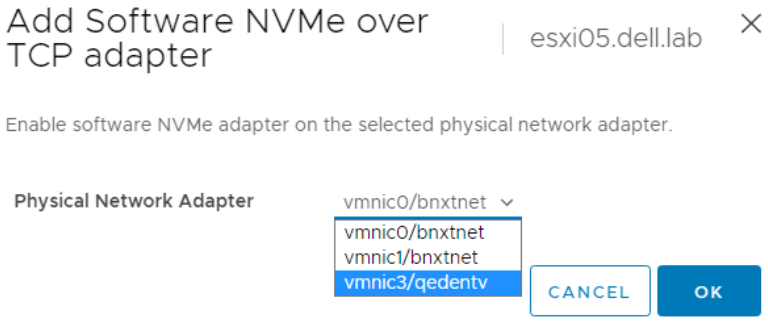


Figure 76. Add a second software adapter

12. Click **OK.**
13. After a few seconds, verify that the second NVMe over TCP software storage adapter, **vmhba65**, was added.

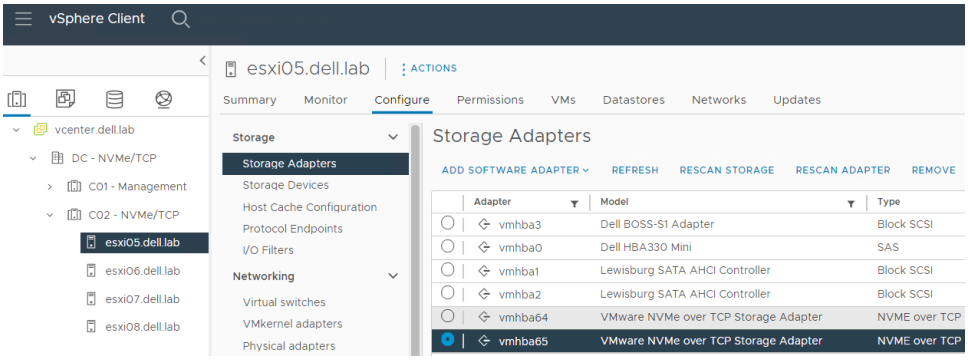


Figure 77. NVMe/TCP storage adapters (vmhba64 and vmhba65)

NOTE: There is a limit of two NVMe/TCP vmhba per host.

14. Repeat the steps above to add two storage adapters on the remaining hosts in the cluster.

NOTE: For the topology in this example, hosts esxi05, esxi06, esxi07, and exsi08 will each have two NVMe/TCP storage adapters (**vmhba64** on physical adapter **vmnic2**, and **vmhba65** on physical adapter **vmnic3**) added.

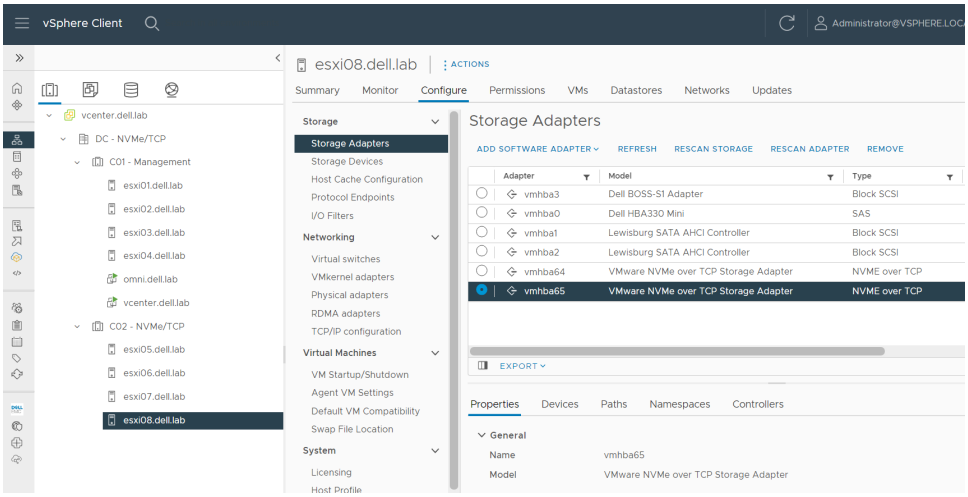


Figure 78. Two storage software adapters for each host

PowerStore Storage Networks

This section demonstrates the creation of NVMe/TCP storage networks in the PowerStore cluster.

Create storage IP networks

The information in this section describes the process of creating two storage IP networks in the PowerStore cluster.

NOTE: This example uses **NVMeTCP-SAN-A** and **NVMeTCP-SAN-B.**

1. From the Dell PowerStore UI, click the **Settings** icon.

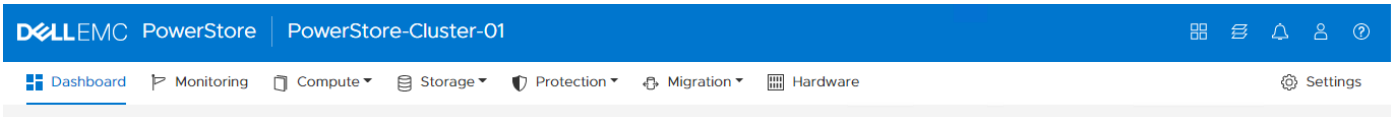


Figure 79. Settings Menu in PowerStore UI

2. Under the **Networking** section, select **Network IPs** > **STORAGE**.

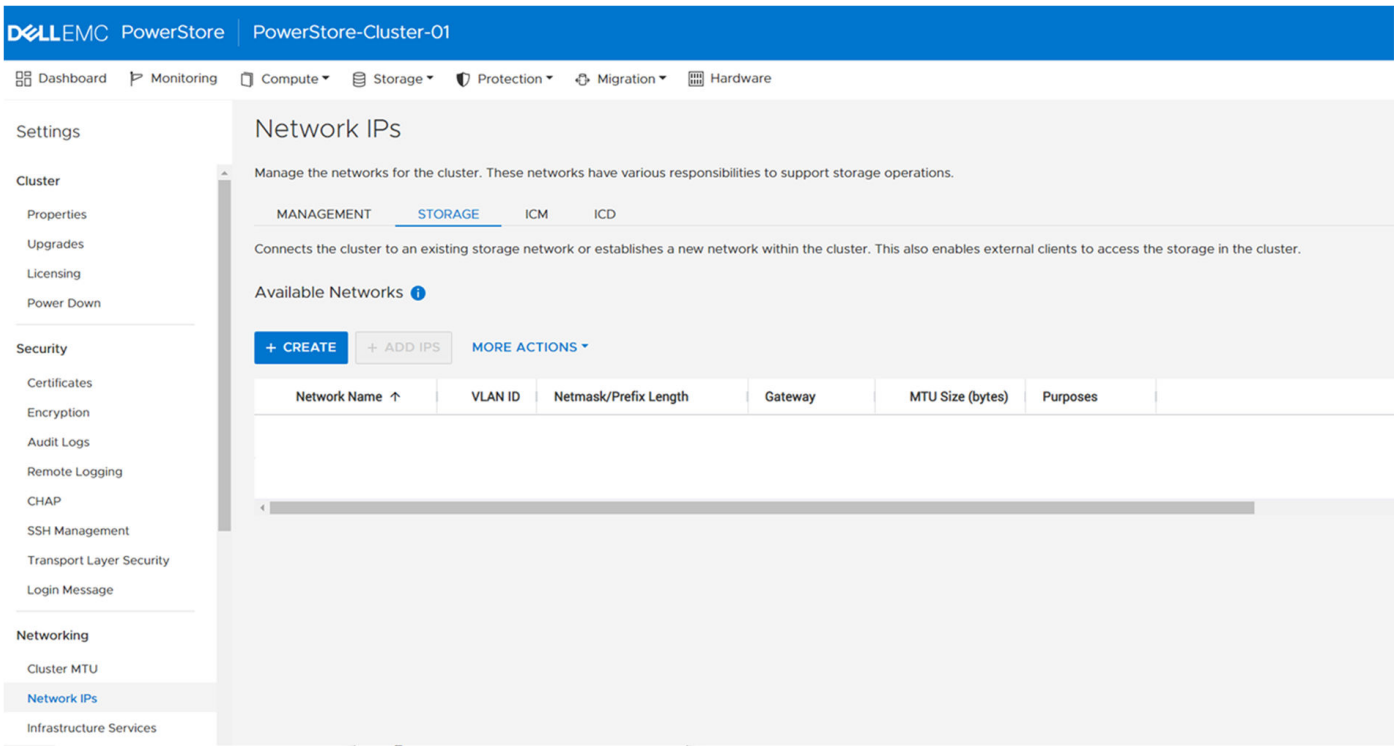


Figure 80. Storage Networks

3. Click **CREATE**. In this example, the following options are selected:
   a. **Network Name:NVMeTCP-SAN-A**
   b. Click to select the **Use VLAN tagging** box
   c. **VLAN ID: 1821**
   d. **Netmask/Prefix Length: 255.255.255.0**
      NOTE: If leveraging Layer 3 routing for NVMe/TCP, enter a Gateway.
   e. Do not enter a **Global Storage Discovery IP**.
   f. From the **Purposes** option, click to clear the check from the **iSCSI** option. **Note:** Verify that **NVMe/TCP** is the only **Purpose** that is selected.
   g. For **Storage Network IPs**, enter **172.18.21.191** and **172.18.21.192**
   h. Set the **Network MTU Size** to match the end-to-end network. This example uses **9000**.

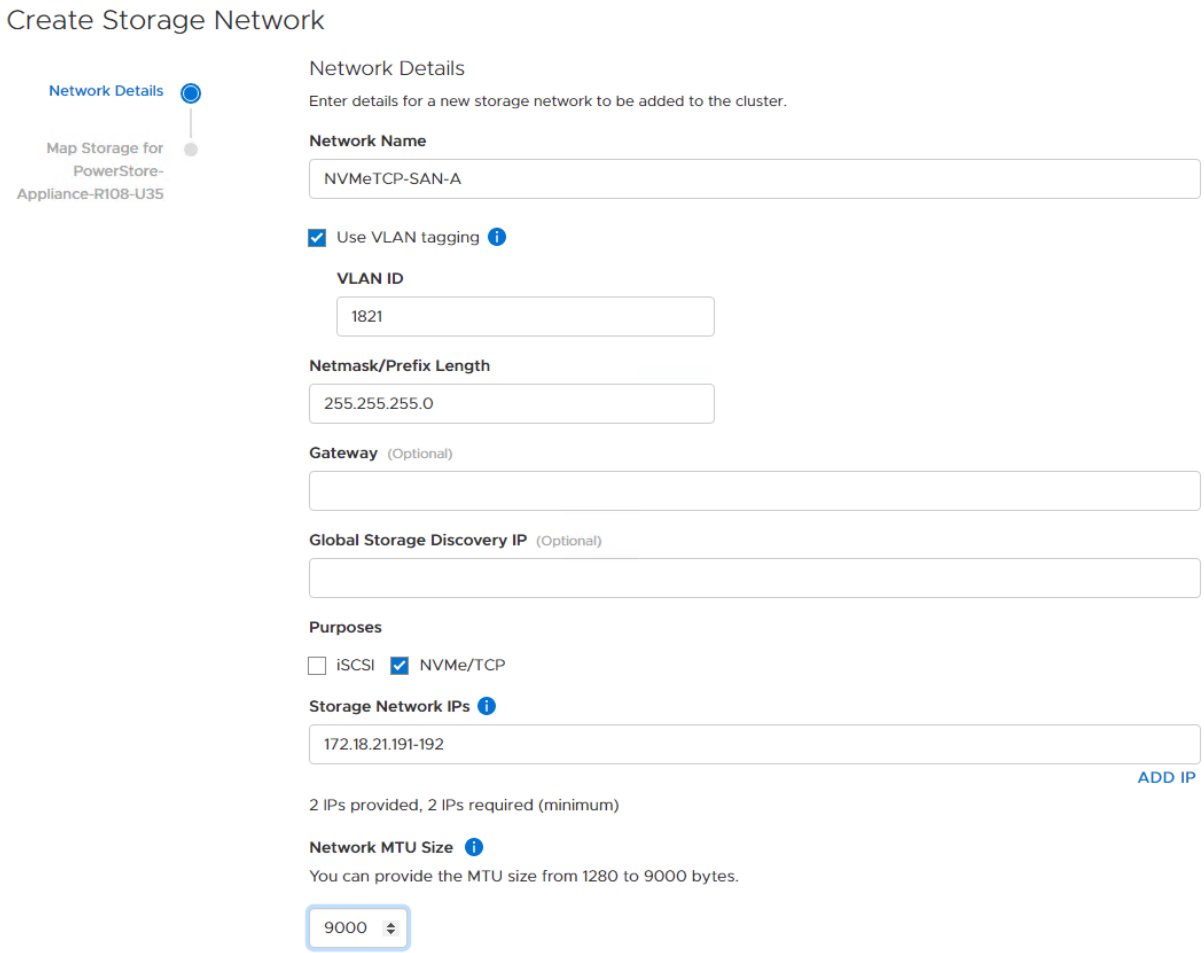


Figure 81. Create Storage Network for SAN A

4. Click **NEXT**.
5. Map Storage for PowerStore-Appliance selecting ports used for NVMe/TCP. In this example, **FEPort0** and **FEPort1** are used.

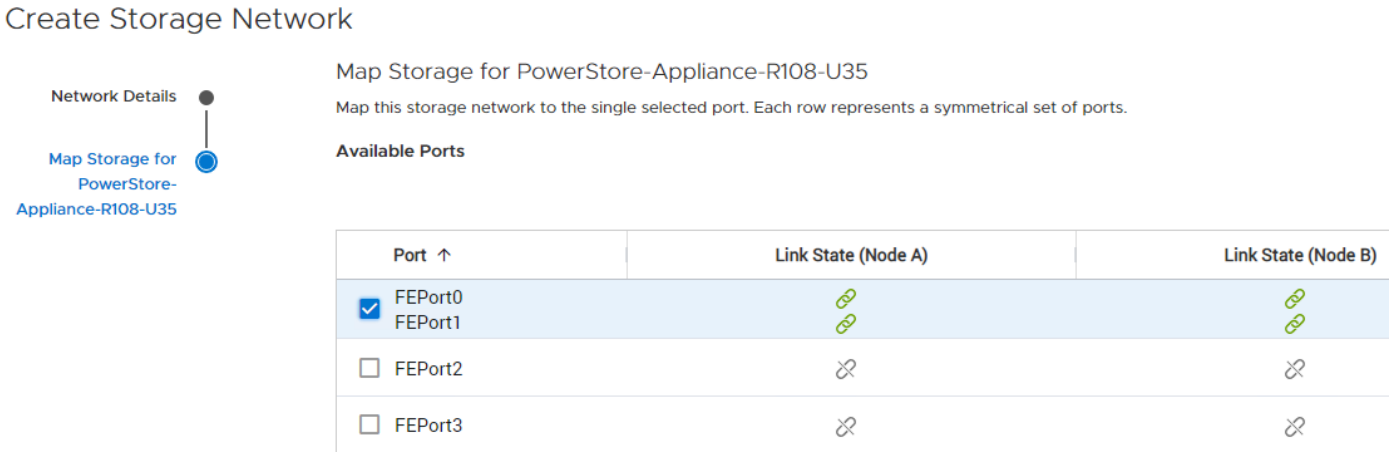


Figure 82. Map ports

NOTE: For air-gapped SAN switches, do not use FEPort0 and FEPort1 as they are in a bond. See the PowerStore Networking Guides page for more information.

6. Click **FINISH**.

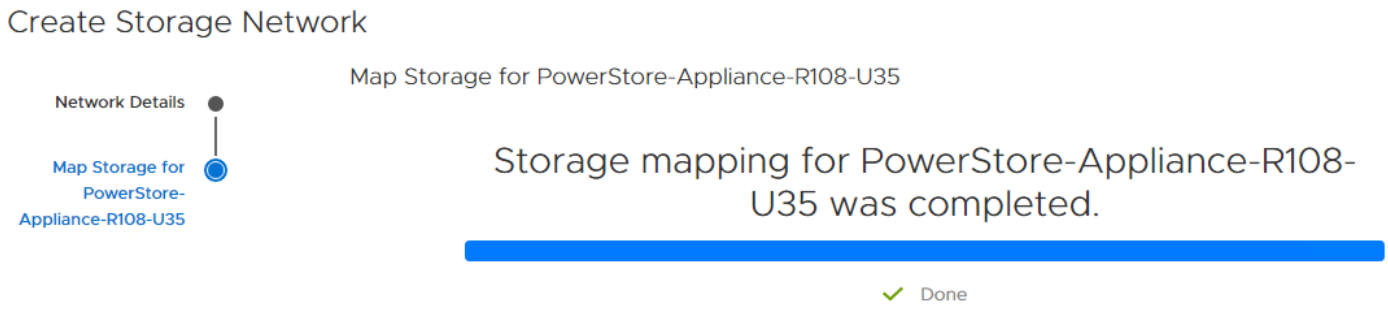


Figure 83. Storage mapping completed successfully

7. Click **Finish** again.

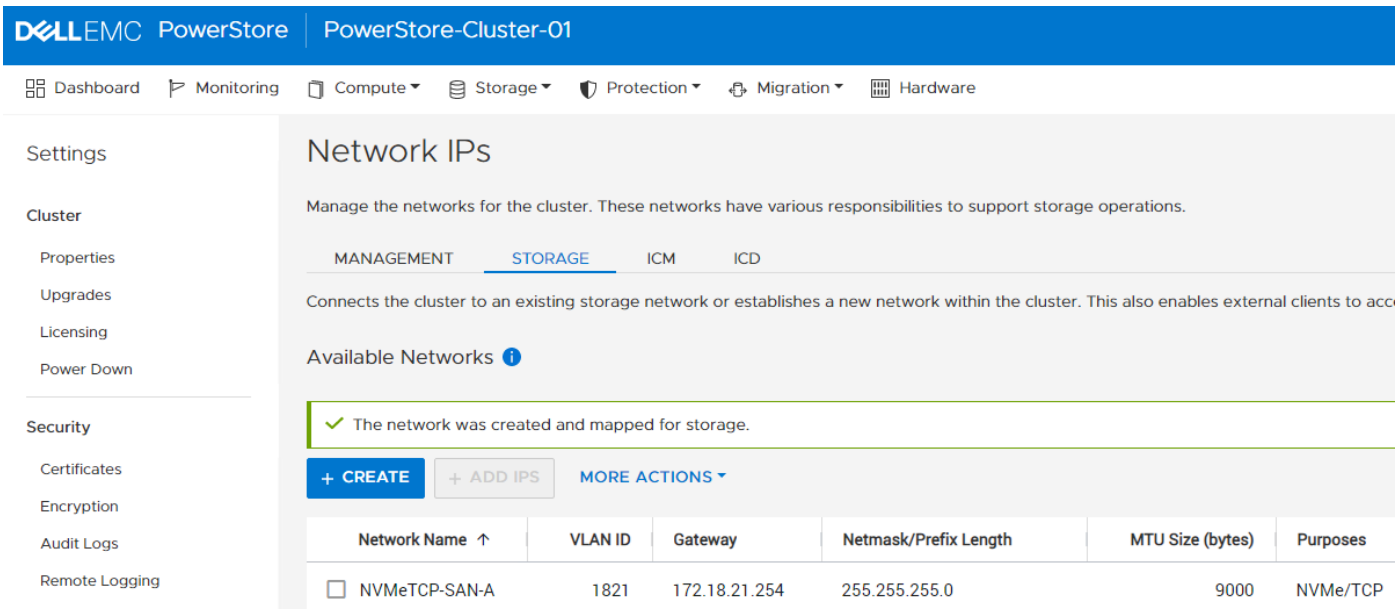


Figure 84. New SAN-A Storage Network added

8. Repeat the steps above to add the second, **NVMeTCP-SAN-B** network, using the following criteria:
   a. **Network Name**: NVMeTCP-SAN-B
   b. **VLAN ID**: 1822
   c. **Netmask/Prefix Length**: 255.255.255.0
      NOTE: If leveraging Layer 3 for NVMe/TCP, enter a Gateway. This example uses 172.18.22.254 for the Layer 2 solution used in this guide.
   d. **Do not** enter a **Global Storage Discovery IP**.
   e. From the **Purposes** option, click to clear the check from the **iSCSI** option. Verify that **NVMe-TCP** is the only **Purpose** that is selected.
   f. **Storage Network IPs**: 172.18.22.191-192
   g. Set the **Network MTU Size** to match the end-to-end network. This example uses **9000**.
9. Click **Next**.

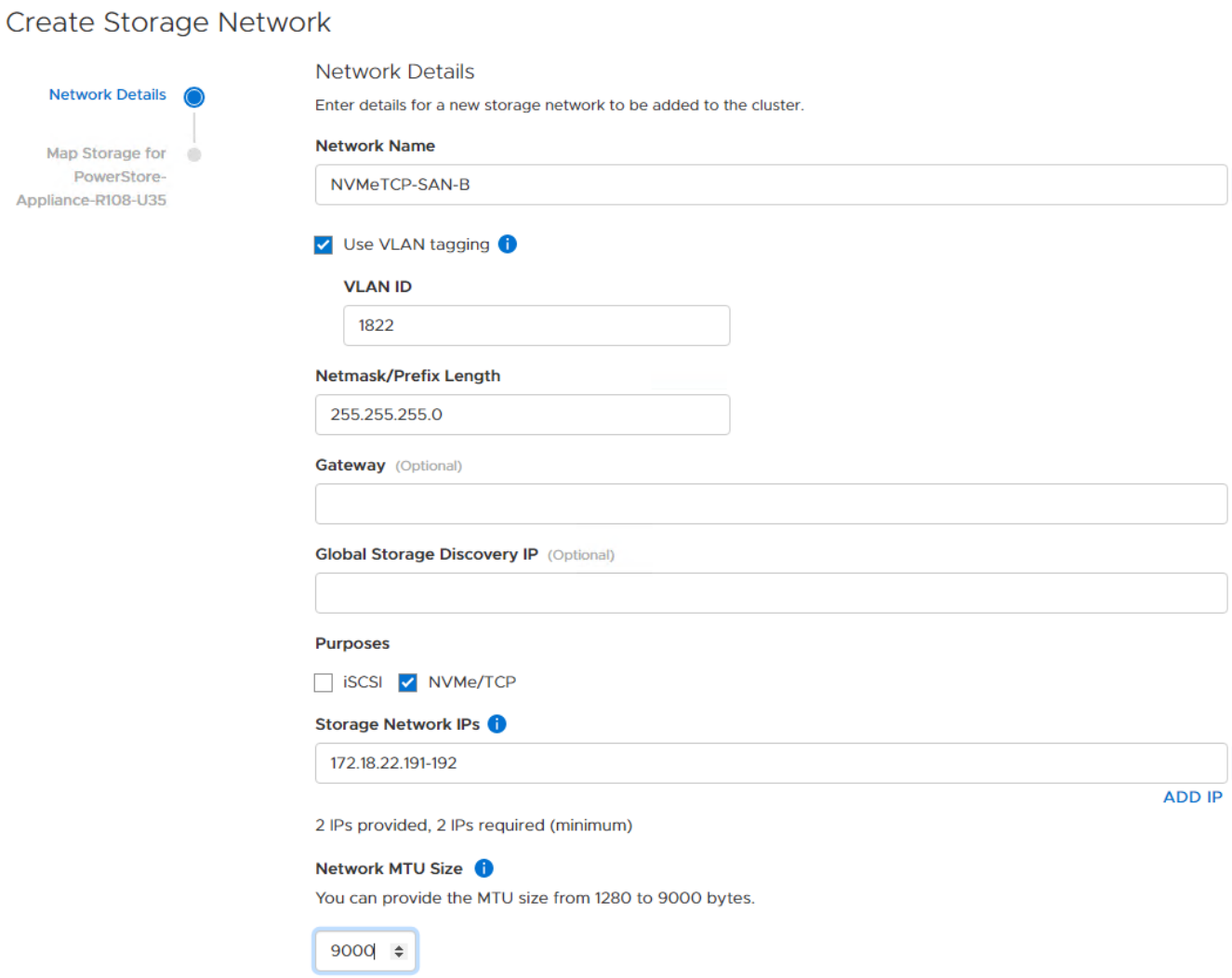


Figure 85. Create Storage Network for SAN B

10. For the **Map Storage for PowerStore-Appliance**, this example uses ports **FEPort0** and **FEPort1**.
11. Click **FINISH**.

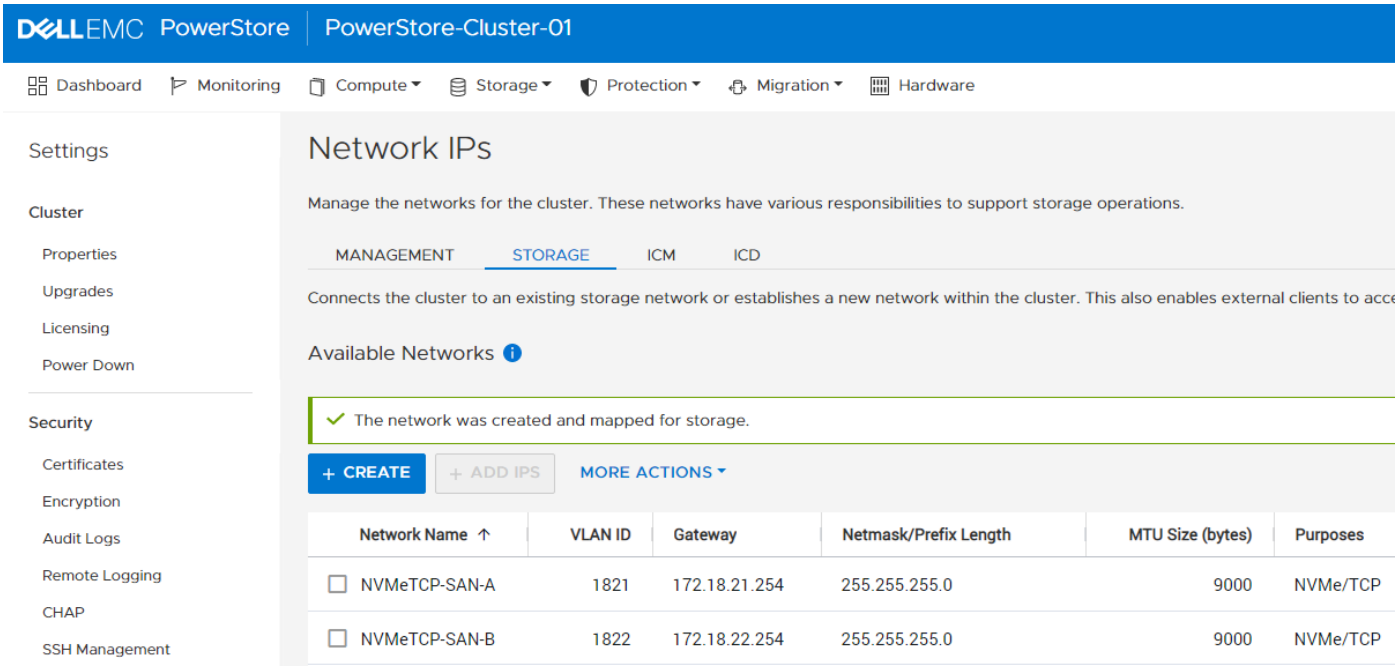


Figure 86. New SAN-B Storage Network added

Deploy SFSS

In this deployment example, SFSS is installed, and NVMe/TCP endpoints are configured.

Steps to deploy SFSS for NVMe/TCP

The information below provides a high-level overview of the deployment of SFSS for NVMe/TCP.

1. Deploy SFSS, configure interfaces, and create the CDC instances.
2. Configure ESXi servers to perform Push registration.
   NOTE: This function will be automated in future VMware vSphere releases.
3. Configure SFSS to perform Pull registration of PowerStore DDC instances.
   NOTE: This function will be automated in future PowerStore releases.
4. Configure the zoning.
5. Create the volume groups and volumes on PowerStore.
6. Add hosts and map to the volume.
7. Create the datastores.

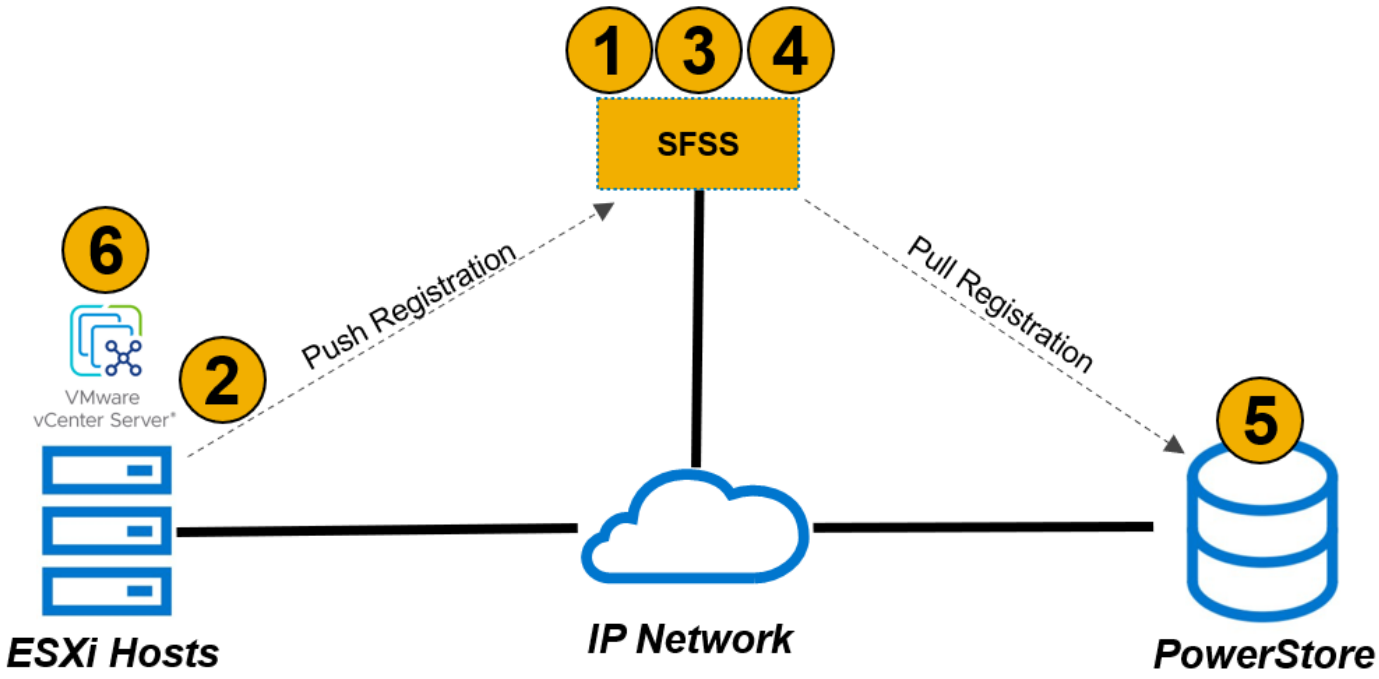


Figure 87. High-level deployment steps with vSphere 7.0U3c and PowerStore 2.1

Download SFSS

1. Identify the SFSS version required using the Networking Solutions Support Matrix.
2. Download the software using the instructions you received in the purchase confirmation email. Alternately, you can also download a trial version of SFSS, you can download it from the Dell Technologies Support Page.

   NOTE: Customers that try SFSS and then purchase the application do not need to download the software again. Simply apply the purchased license to the previously installed software. See the SFSS licenses section for more details.

Deploy SFSS VMware virtual appliance

1. From the vSphere client, select **Hosts and Clusters**, and then right-click and select the **Deploy OVF Template** option.

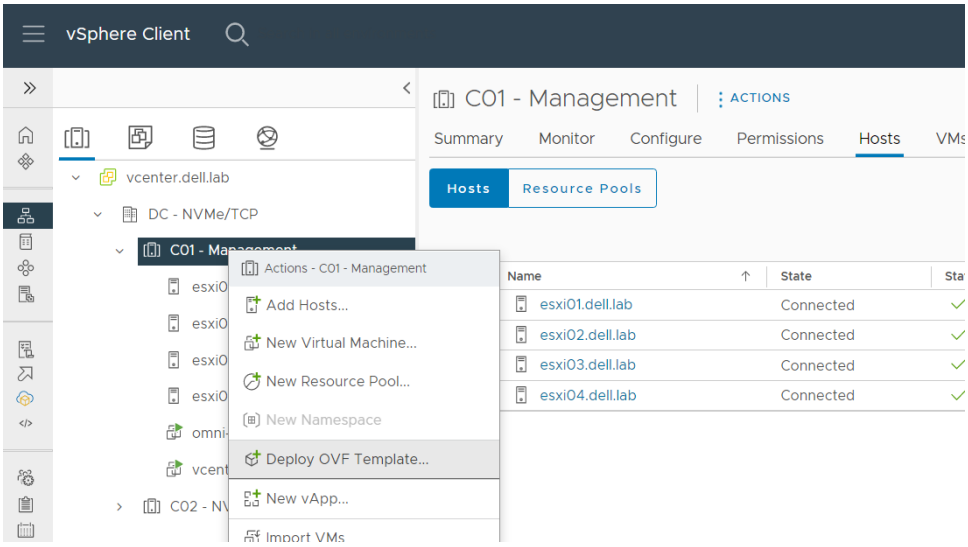


Figure 88. vCenter OVF template deployment

2. On the **Select an OVF template** page, point to the location of the SFSS OVA file and click **NEXT**.

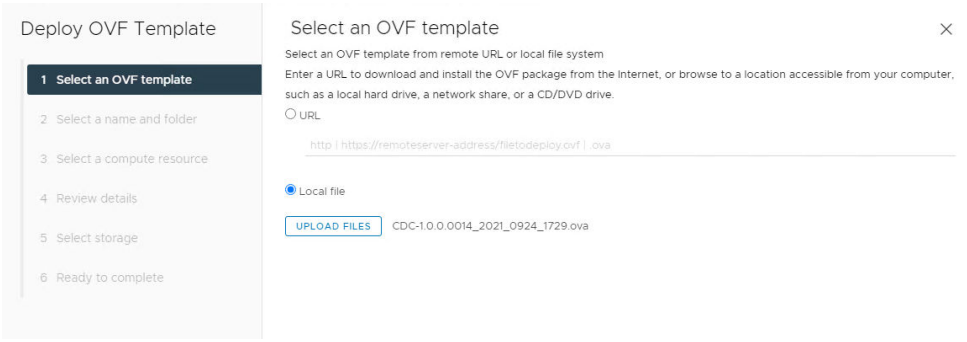


Figure 89. SFSS OVF template installation

3. Select a **name** and **folder** for the VM, then click **NEXT**.

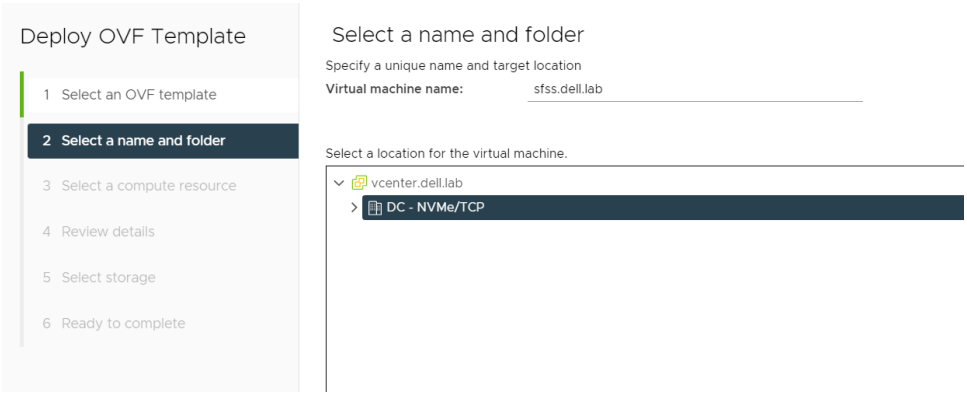


Figure 90. SFSS virtual machine name

4. On the **Select a compute resource** page, select a compute resource.

   NOTE: This example uses **esxi01**.

5. Click **NEXT**.

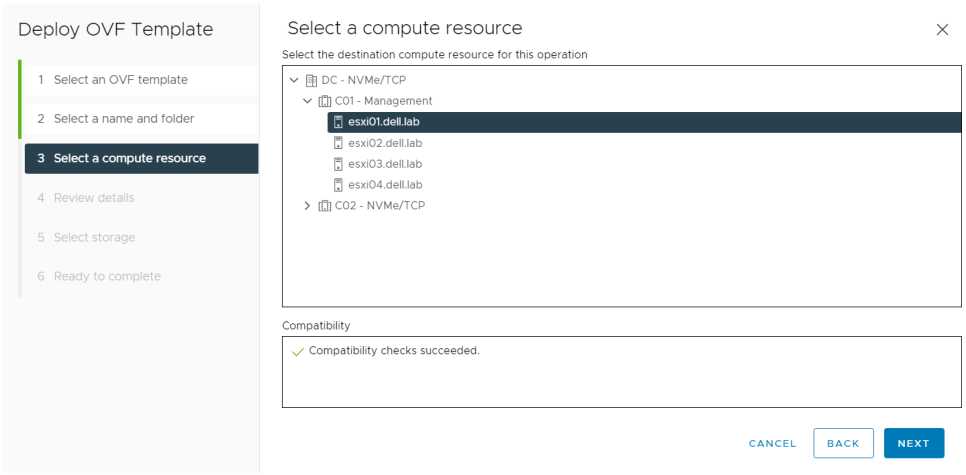


Figure 91. Host selection

6. Click **NEXT** on the **Review details** page.

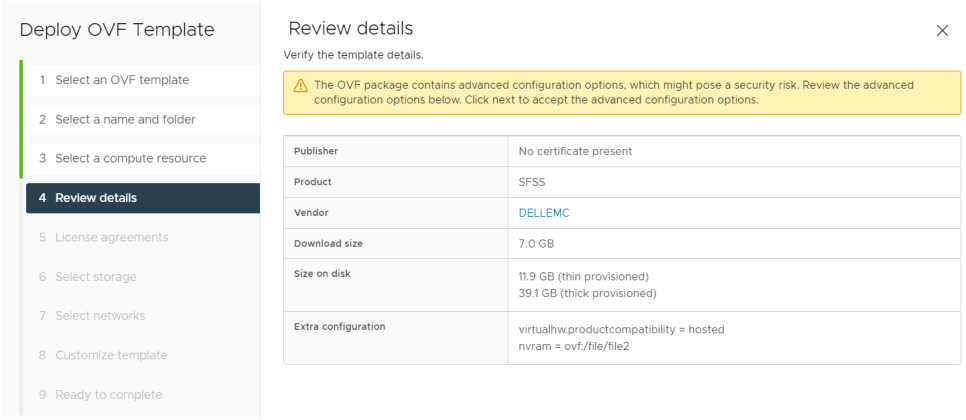


Figure 92. Review details

7. On the **License agreements** page, accept the agreement and click **NEXT**.
8. On the **Select storage** page, first select the datastore, ensuring that **Compatibility checks succeeded** is displayed. Then, change **Select virtual disk format** to **Thin Provision**.

   NOTE: You must select the datastore before selecting the Virtual disk format. If you select the disk format first, you may lose the setting after selecting the datastore.

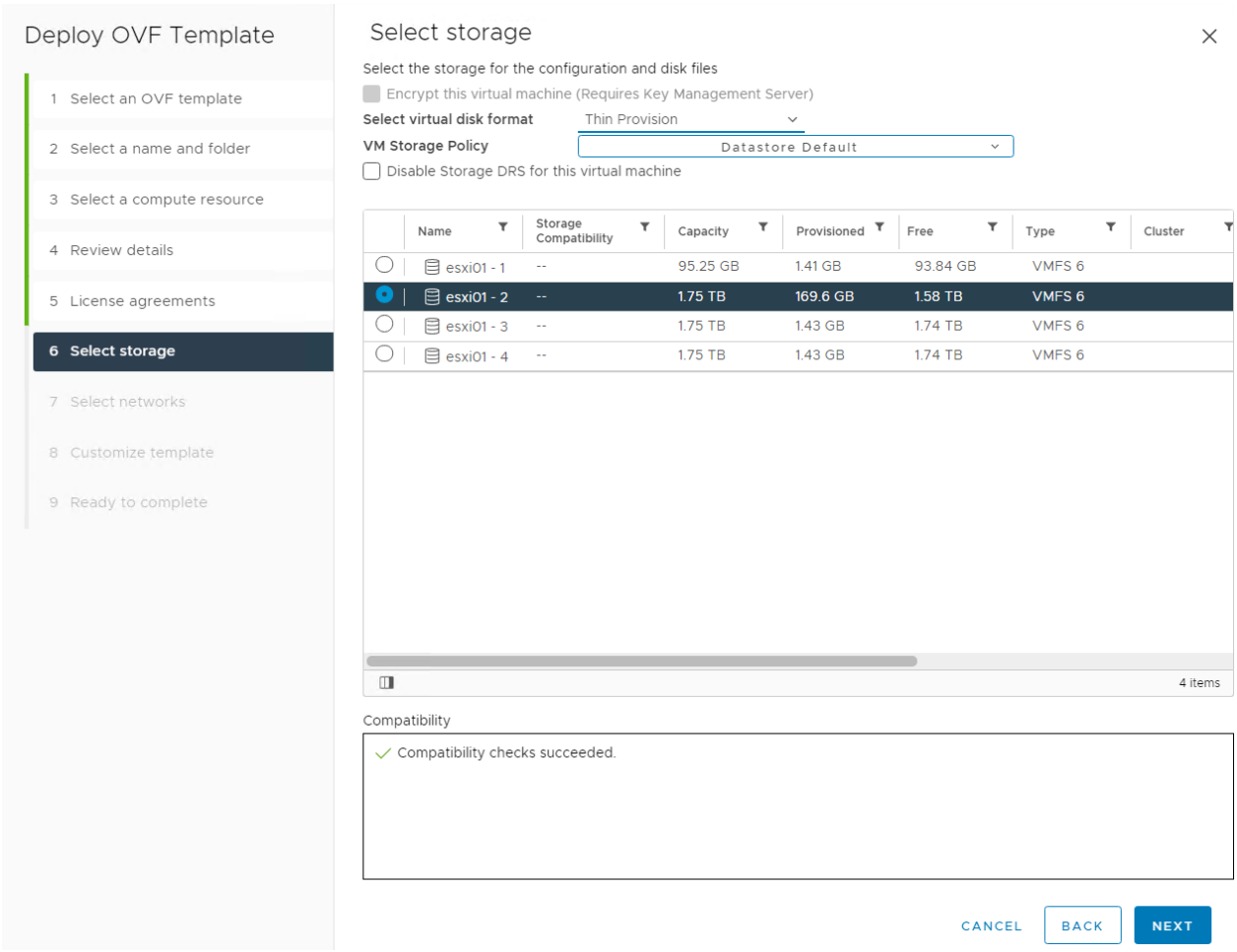


Figure 93. SFSS storage selection

9. Click **NEXT**.
10. On the **Select networks** page, change the three **Destination Networks** to the values as planned in the initial configuration worksheet. In this example, the following Source and Destination networks are used:

Source network	Destination network
VM Network	C01-Management
SAN Network 1	C01-NVMeTCP-SAN-A-SFSS
SAN Network 2	C01-NVMeTCP-SAN-B-SFSS

11. Click **NEXT**.

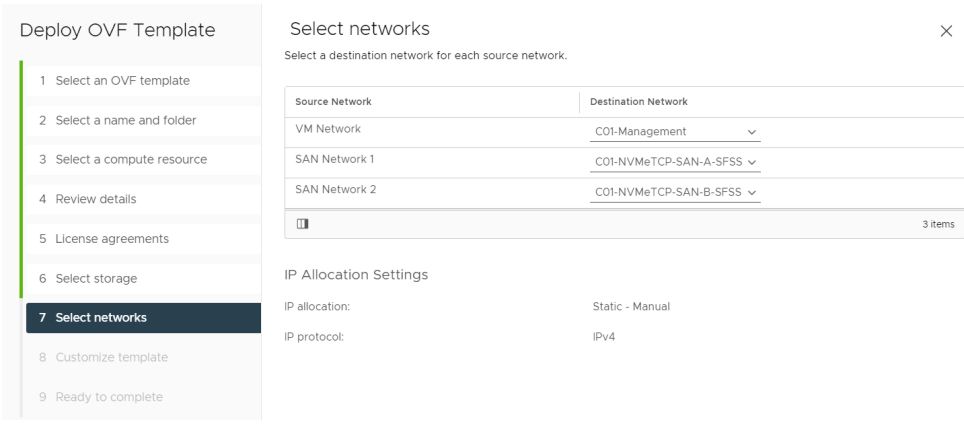


Figure 94. SFSS networks selection

12. In the **Customize template** section, the management interface settings information is provided. Provide the following details to follow the example in this guide:
    a. **Hostname:sfss**
    > **NOTE:** The VM's internal hostname must not contain periods. For this reason, do not use the FQDN in this step as a period will be converted to a dash. For example, **sfss.dell.lab** changes to **sfss-dell-lab**. See the Modify Hostname in SFSS section in this guide for more information.
    b. **IP Address: 172.18.11.57**
    This is the management IP address for SFSS.
    c. **Prefix Length**: **24**
    d. **Gateway**: **172.18.11.254**
    > **NOTE:** If the default subnets assigned to internal networks are already assigned elsewhere, change the default IPv4 Subnet used for internal ipv4 from 172.18.0.0/16 to 172.16.0.0.

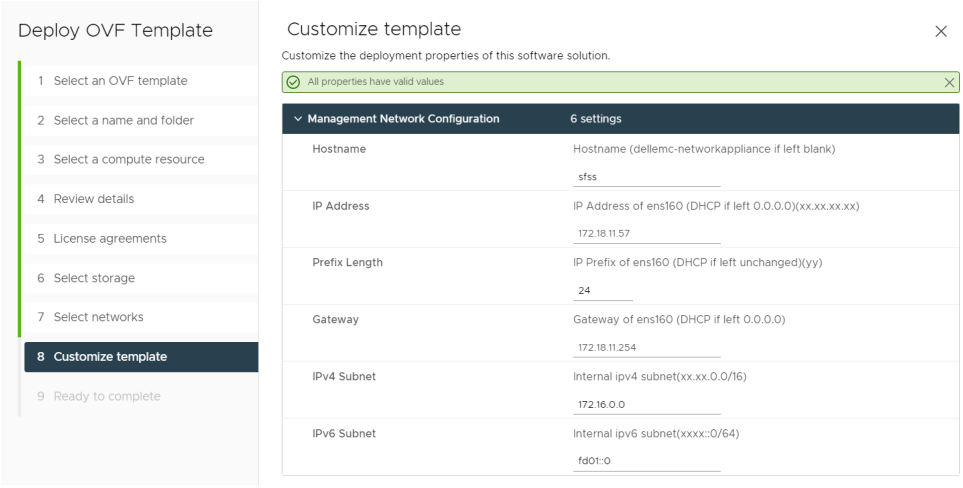


Figure 95. Customize management interface settings

e. Review the settings shown on the **Ready to complete** page and click **FINISH** to deploy the VM.

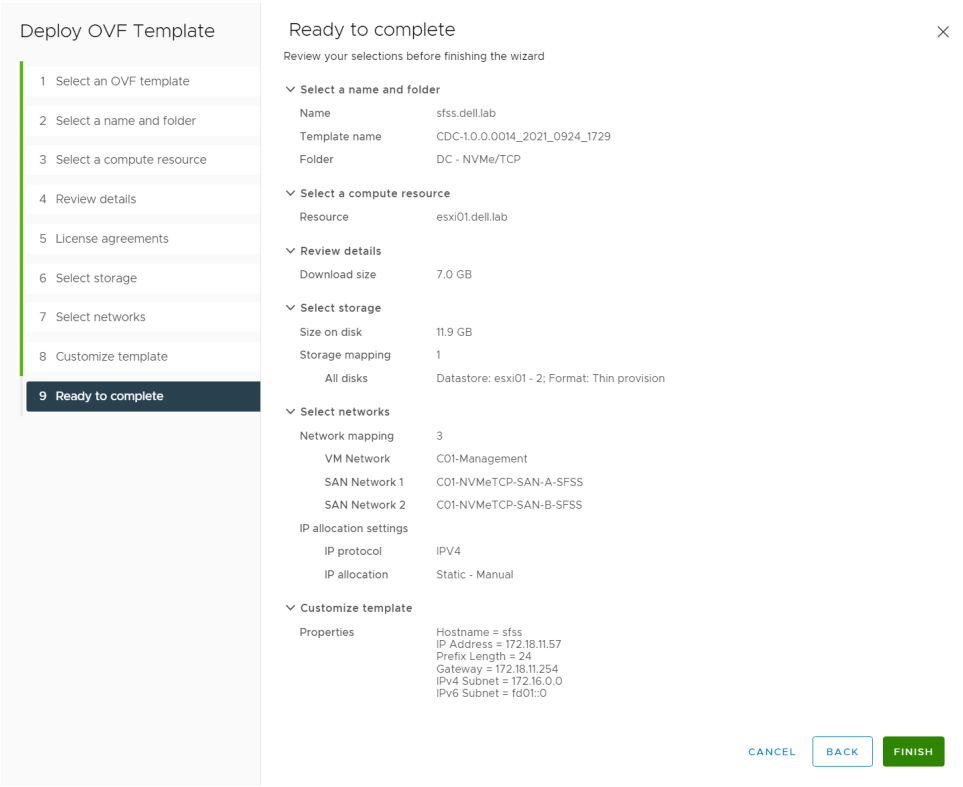


Figure 96. Review and finish the wizard

You can track the progress from the **Recent Tasks** section at the bottom of the vCenter page. The **Import and Deploy tasks** function may take several minutes to complete.

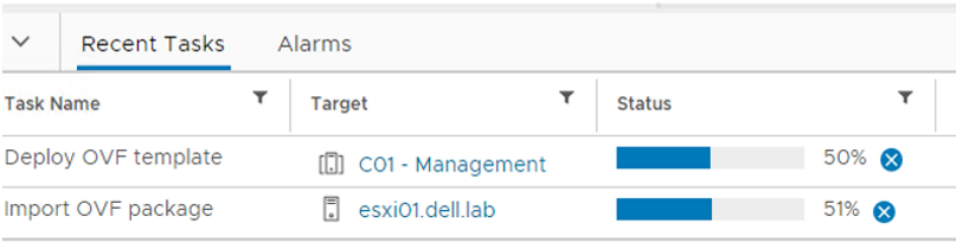


Figure 97. Recent Tasks in progress

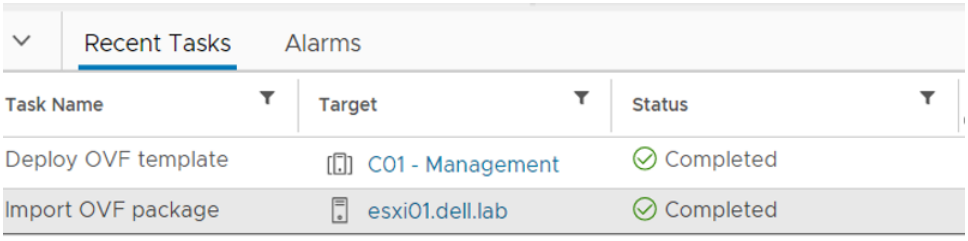


Figure 98. Recent Tasks completed screen

13. Continue to the next section once **Status** is **Completed** on each Task.

NOTE: To adjust the number of interfaces on SFSS, see the Add a network interface to the SFSS vApp and Disable or Remove a network interface on SFSS sections.

Configure SFSS

After completion of the SFSS deployment, perform the steps in this section to configure the following high-level steps:

1. Power on the SFSS vApp.
2. Using the web console, reset the **admin** user password.
3. Use the SSH to log in and verify the infrastructure.
4. Configure the SFSS network interfaces.
5. Enable the CDC Instance.

Power on the SFSS virtual appliance

To power on the SFSS virtual appliance:

From the vSphere Client, right-click the SFSS VM, and select **Power** > **Power On**.

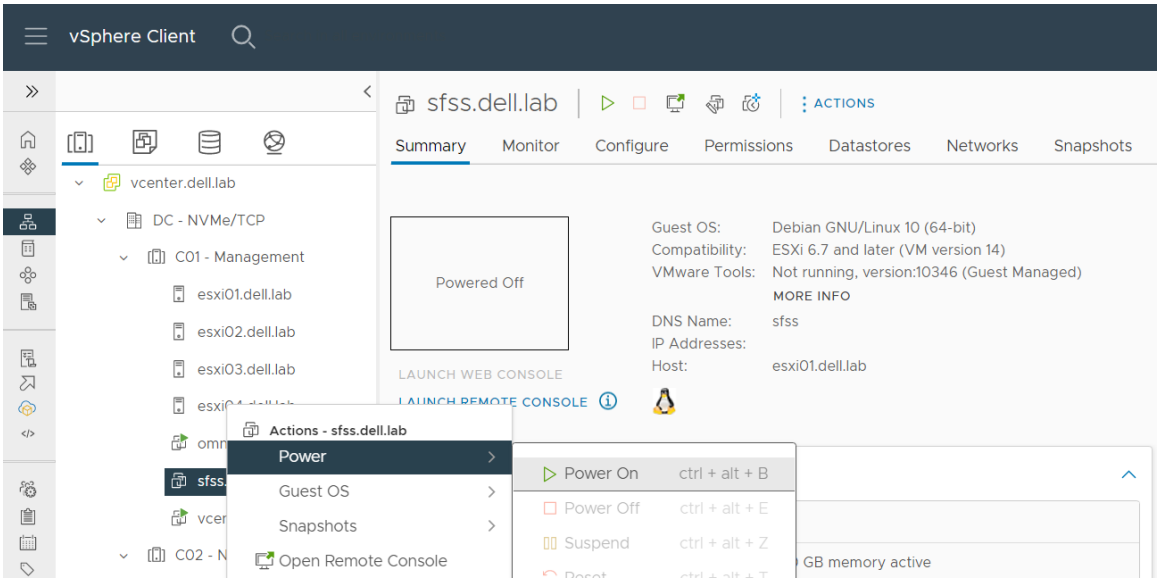


Figure 99. Power on the SFSS virtual appliance

CAUTION: When powering on the VM, the vCenter Summary page for the VM may indicate a newer version of VMware Tools is available. Do not upgrade to a newer version.

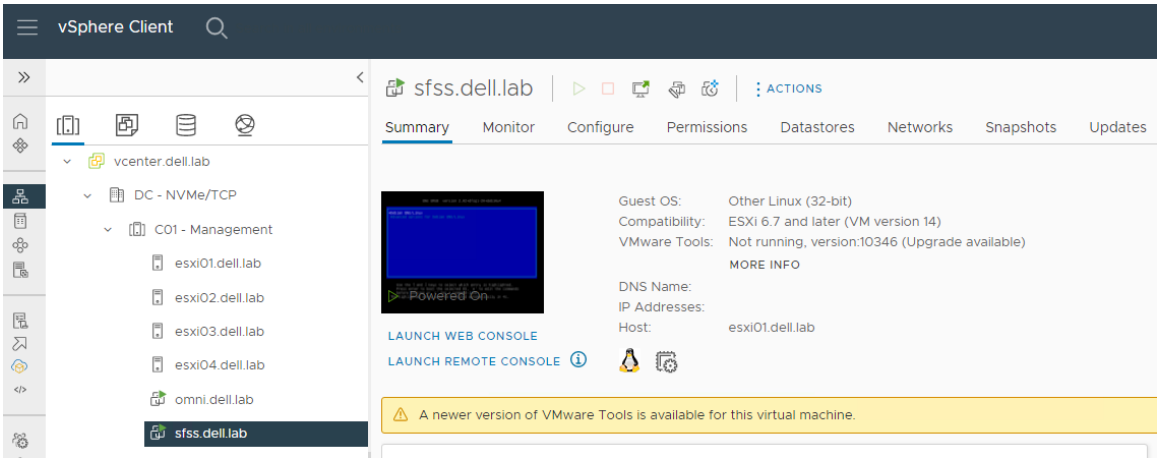


Figure 100. Do not upgrade VMware Tools

Reset admin password

To reset the admin password, perform the following steps:

1. Launch the SFSS VM web console using the **Launch Web Console** button.
2. Authenticate using the default **username** (admin) and the default **password** (admin).
3. In the **New password** line, enter a new admin password, and then retype the new admin password to verify.

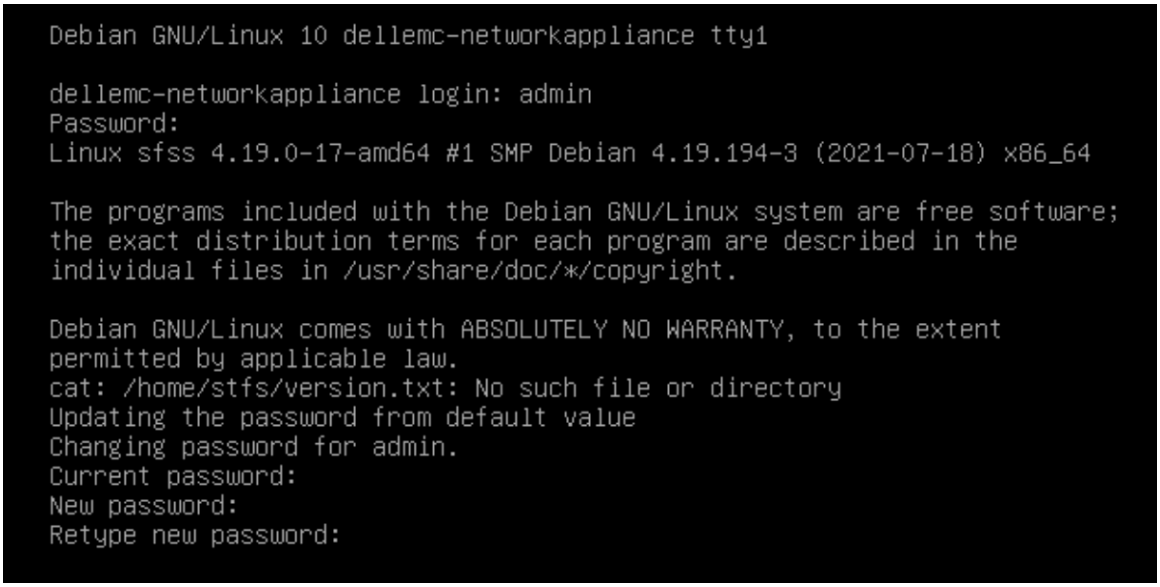


Figure 101. Change default admin password in SFSS

NOTE: The initialization of the services may take a few minutes to complete. If initialization has not completed after 10 minutes, see the Verify the infrastructure section in this guide, or the SmartFabric Storage Software Troubleshooting Guide.

OpenManage Network Integration

NOTE: The OpenManage Network Integration (OMNI) plugin is optional. For more information about OMNI, see the OpenManage Network Integration software section.

When in use, OMNI can connect to SFSS and provide administrators with a single pane of glass infrastructure that manages SFS and SFSS in the vCenter Web Client. You can also use OMNI without SmartFabric Services.

1. From the vCenter client, select **OpenManage Network Integration**.
2. From the **OMNI Home** screen, click the **SFS/SFSS** tab.
3. Click **Create**.

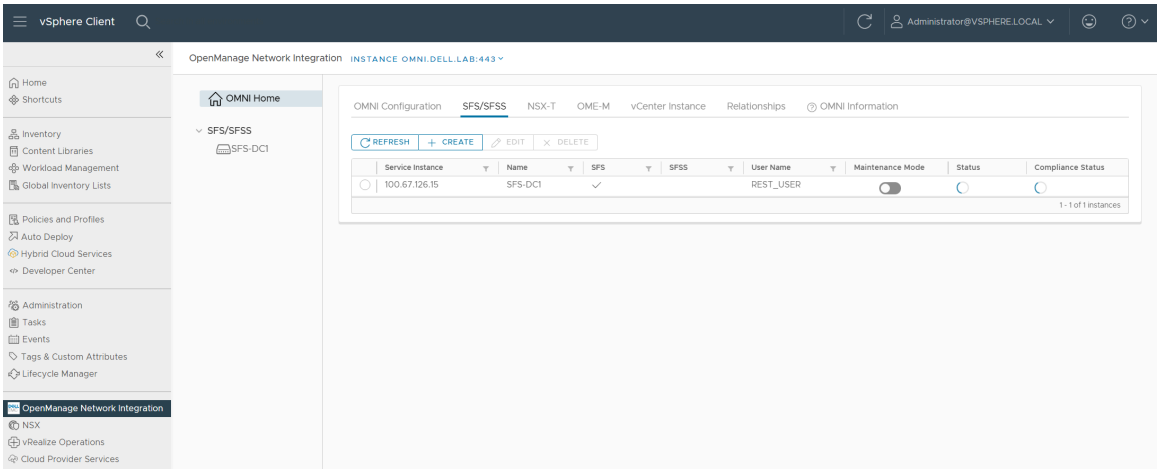


Figure 102. SFS/SFSS configuration within OMNI Home screen

4. Configure the details for the following required fields within the **Add Service Instance** wizard:
   a. **Address:** Management IP address of the SFSS VM
   b. **Name:** Name that will appear in the OMNI UI
   c. **Username**: admin
   d. **Password:** Enter the configured admin password

e. Click to place a check in the **Register for Events** checkbox.
f. Click **ADD**.

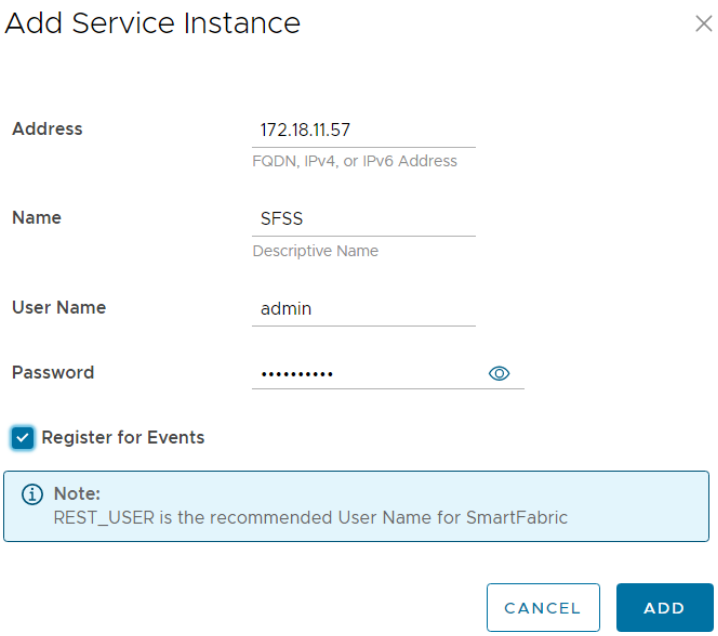


Figure 103. Add SFSS Service Instance

You can now manage SFSS from within vCenter.

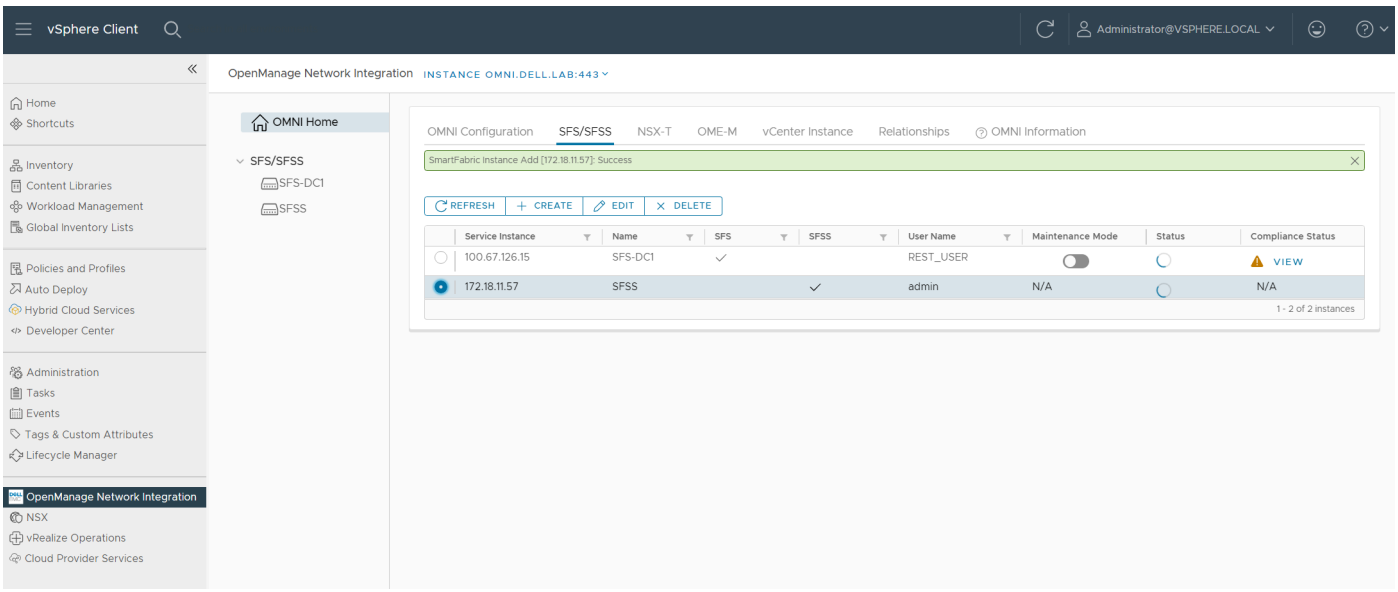


Figure 104. OMNI SFS and SFSS Instances visible in vCenter

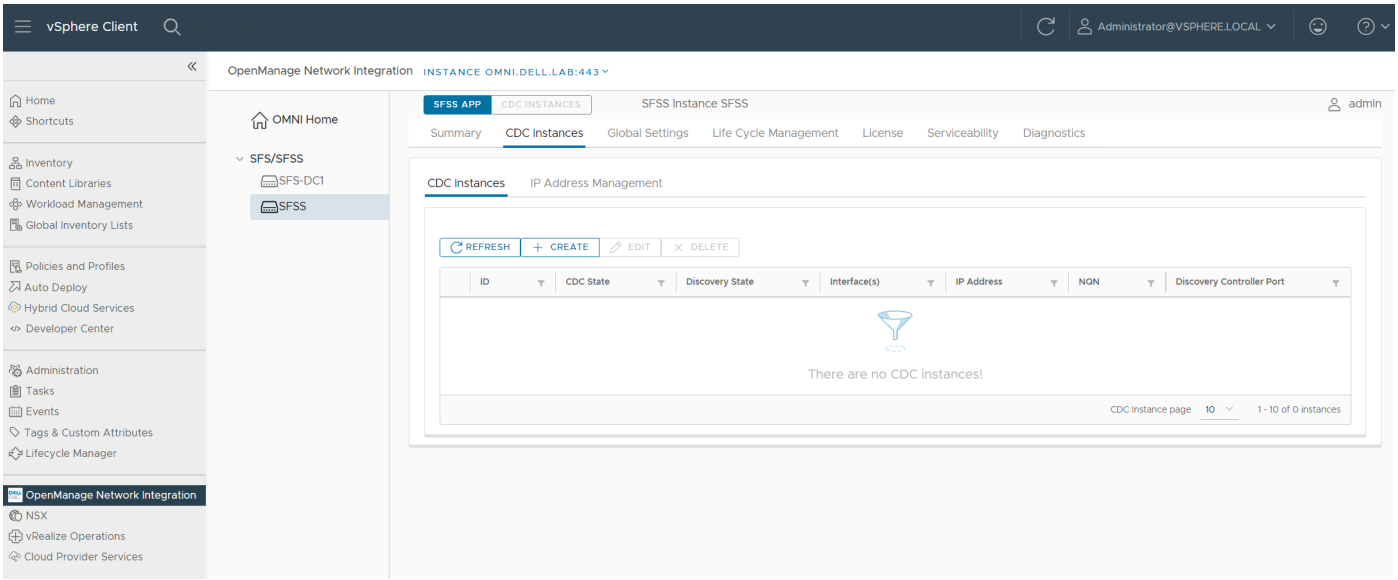


Figure 105. SFSS UI in vCenter

Configure SFSS VM storage network interfaces

In this section, we will configure the Storage network interfaces on the SFSS virtual machine. This interface will communicate with initiators and subsystems.

1. From a browser, open the SFSS using the `https://<SFSS_IP>` address.

   NOTE: This example uses the `https://172.18.11.57` SFSS IP address.

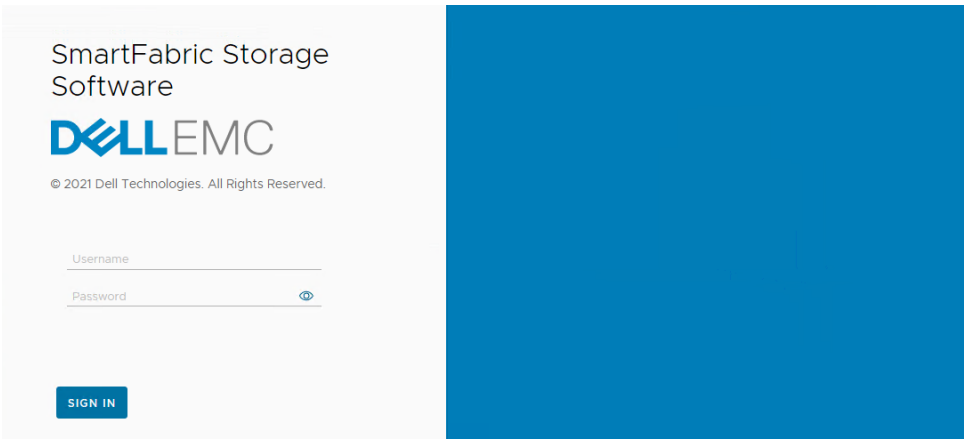


Figure 106. SFSS UI

2. Enter the admin **Username** and **Password** you created when configuring SFSS.

   NOTE: The initial could take several minutes with the **SFSS is almost ready** title screen displayed.

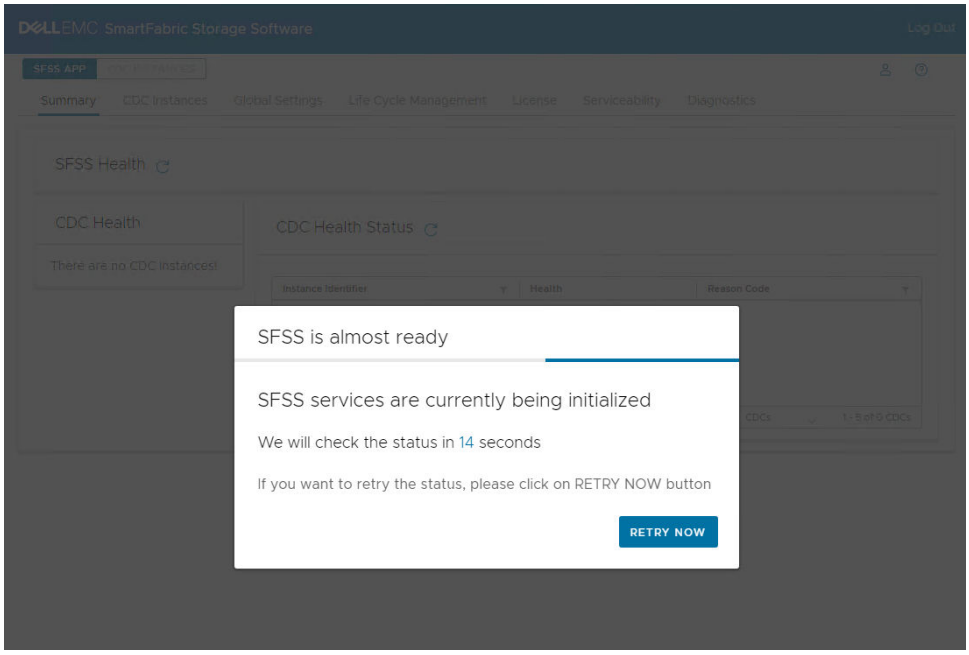


Figure 107. SFSS is almost ready status screen

Upon successful login, the **SFSS Home** page displays.

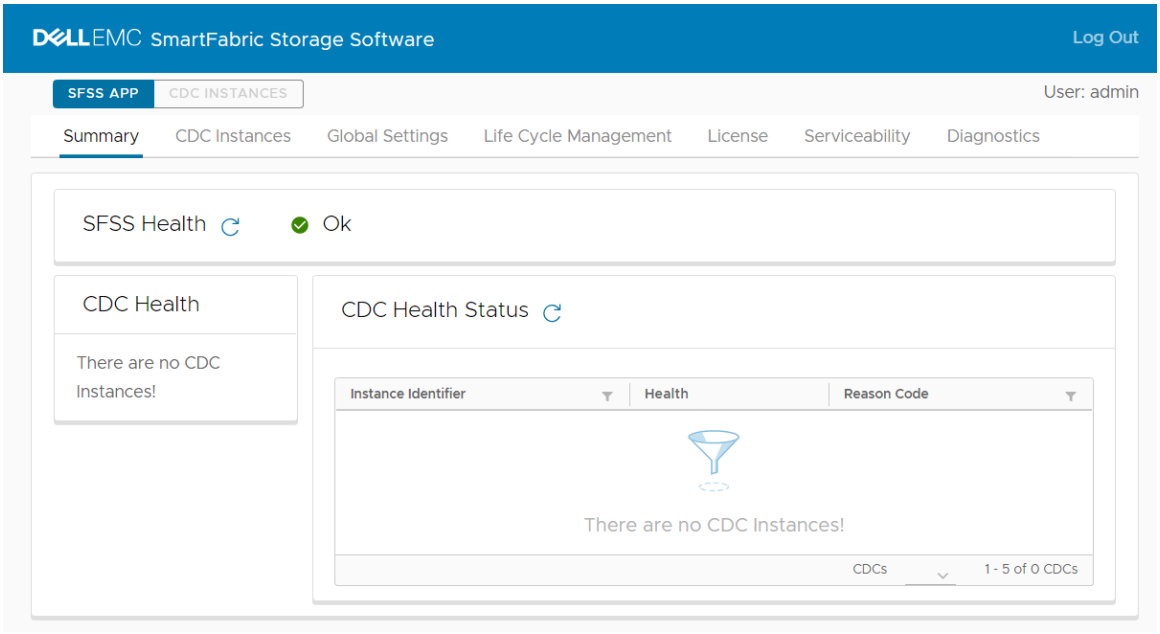


Figure 108. SFSS Home page

NOTE: By default, the **SFSS APP** option is displays at the top of the home page.

The menu options include:

- Summary
- CDC Instances
- Global Settings
- Life Cycle Management
- License
- Serviceability
- Diagnostics

To configure an IP address on the storage network interfaces, perform the following steps:

3. From the **SFSS APP** menu, select **CDC Instances** > **IP Address Management**.
4. For **SAN A**, click to select the **ens192** Interface.

NOTE: Interface ens160 was configured during the OVA deployment.

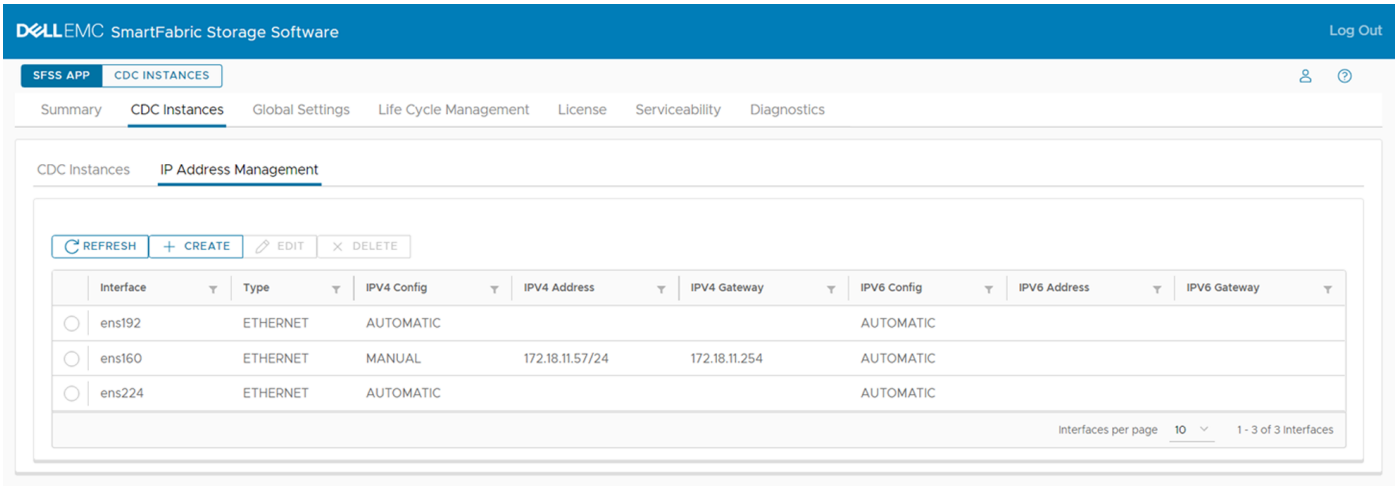


Figure 109. Select ens192 Interface

5. Click the **Edit** button.
6. For **IPV4**, select **Manual**.
7. For the **CDC instance**, assign a unique IP address.

NOTE: This example uses **172.18.21.250** for the instance.

8. For the **Prefix length**, enter **24**.

NOTE: This example is Layer 2 only. If Layer 3 connectivity is required, enter a gateway IP address in the field provided.

NOTE: To avoid an unwanted DHCP IP assignment, change the IP configuration to **Manual** and enter **0.0.0.0** and **32** for IPv4, and **::** and **64** for IPv6.

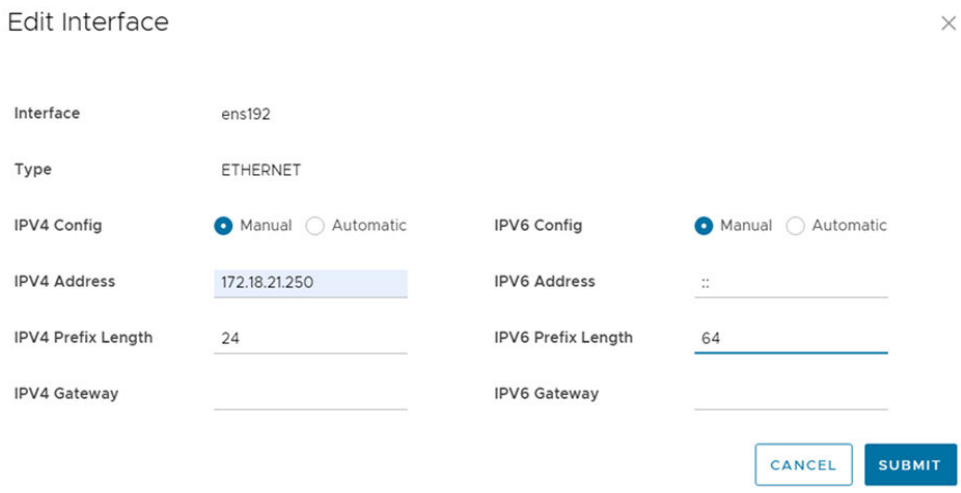


Figure 110. SFSS Interface configuration for SAN A

9. Click the **Submit** button to return to the previous screen.
10. For **SAN B**, click to select the **ens224** Interface.

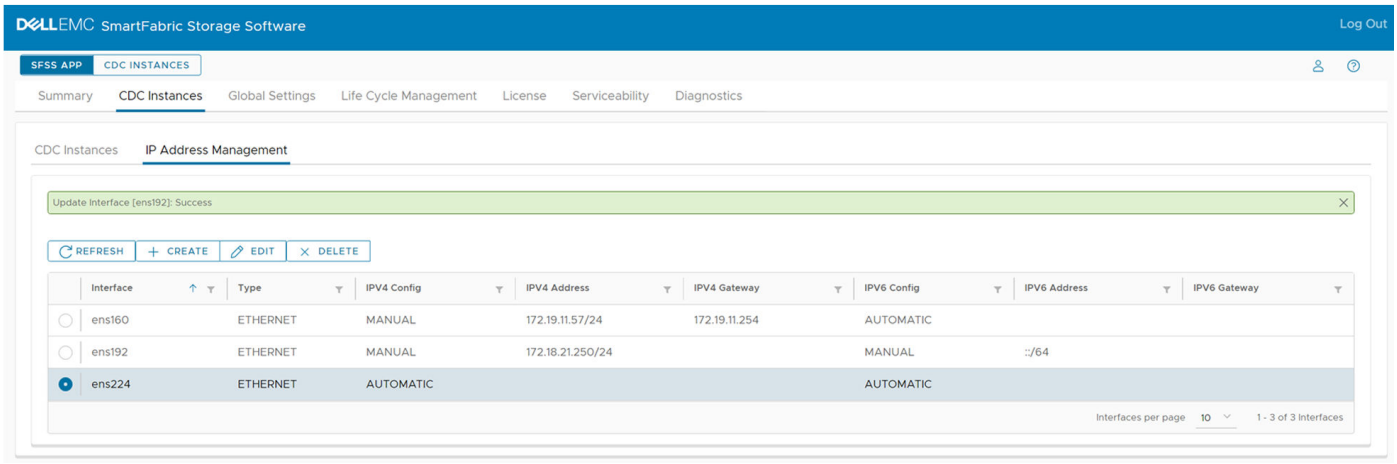


Figure 111. Select ens224 Interface

11. Click the **Edit** button.
12. For IPV4, select **Manual**.
13. For the **CDC instance**, assign a unique IP address.

    NOTE: This example uses **172.18.22.250** for the instance.

14. For the **Prefix length**, enter **24**.

    NOTE: If Layer 3 connectivity is required, assign a gateway address. This example is Layer 2 only.

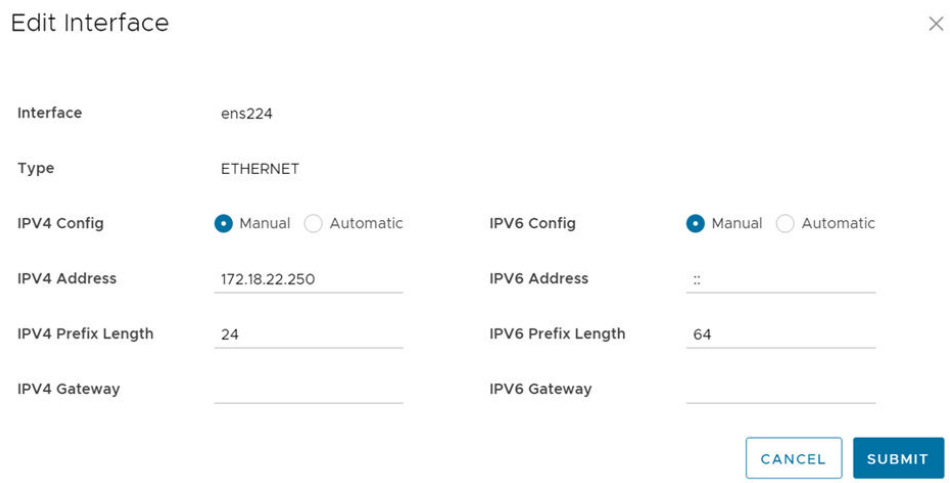


Figure 112. SFSS Interface configuration for SAN B

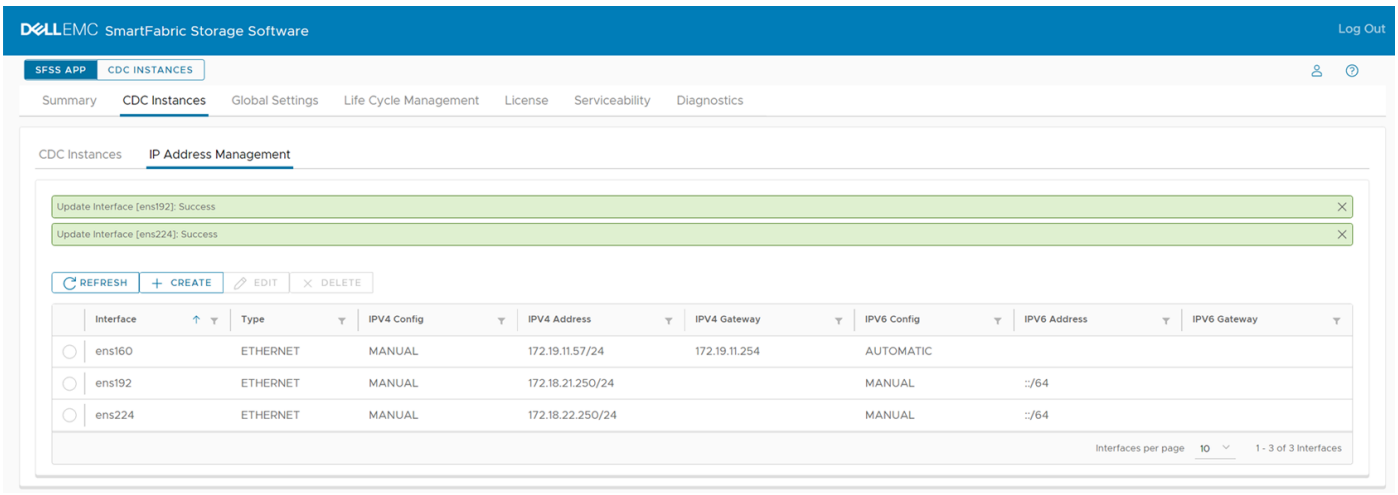


Figure 113. Successful creation of Storage interfaces ens192 and ens224

Configure SFSS MTU

1. In the SFSS UI, click **Global Settings** > **Settings** > **Edit**.

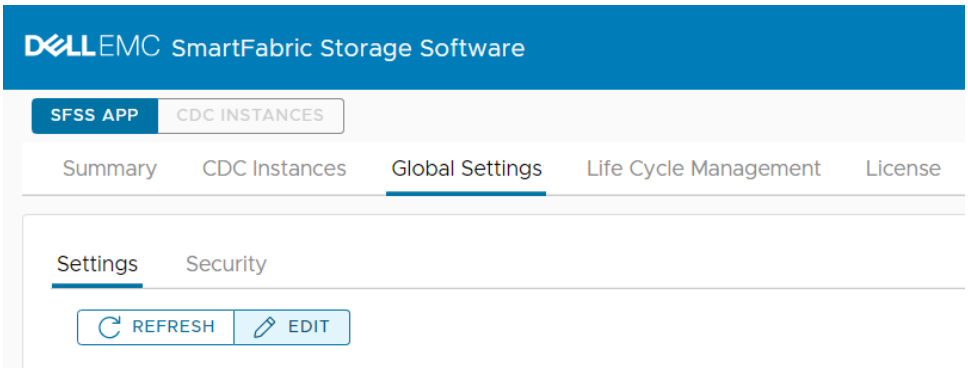


Figure 114. Edit Global Settings

2. Change the MTU to the required value.

NOTE: In this example, the MTU value is set to **9000**.

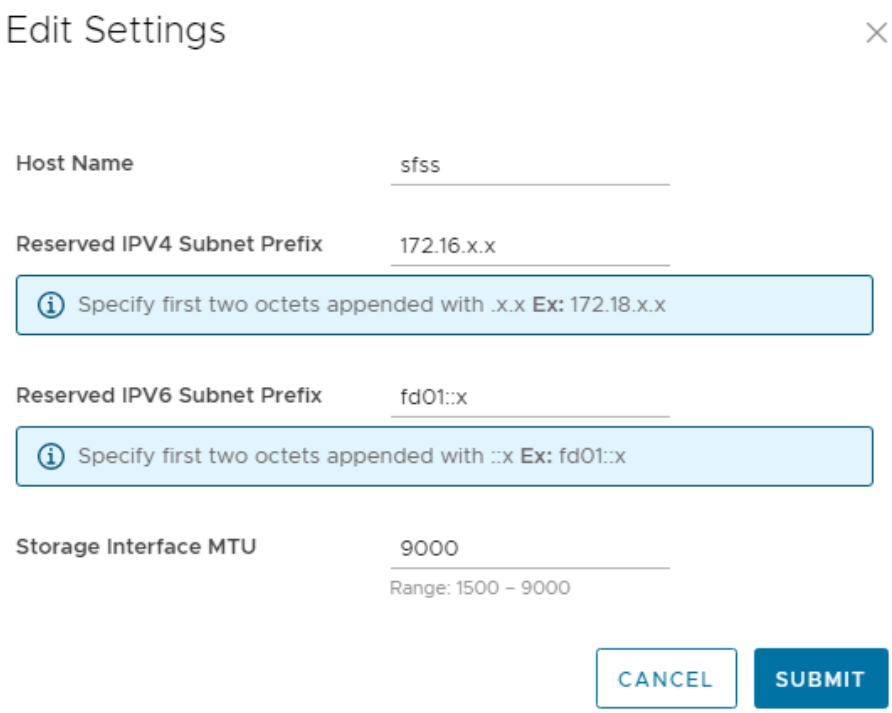


Figure 115. Edit MTU in Global Settings

Verify the network

While this step is optional, it is important to confirm that the network is forwarding traffic as expected, which can prevent issues from occurring in the remaining deployment steps.

To verify the network, you must ping between NVMe/TCP participants.

1. SSH to an ESXi host and ping the SFSS storage network interfaces. In this example, the following commands are used:

```
vmkping -I vmk2 172.18.21.250 -s 9000
vmkping -I vmk3 172.18.22.250 -s 9000
```

```
[root@esxi05:~] vmkping -I vmk2 172.18.21.250 -s 9000
PING 172.18.21.250 (172.18.21.250): 9000 data bytes
9008 bytes from 172.18.21.250: icmp_seq=1 ttl=64 time=0.292 ms
9008 bytes from 172.18.21.250: icmp_seq=2 ttl=64 time=0.249 ms

--- 172.18.21.250 ping statistics ---
3 packets transmitted, 2 packets received, 33.3333% packet loss
round-trip min/avg/max = 0.249/0.270/0.292 ms

[root@esxi05:~] vmkping -I vmk3 172.18.22.250 -s 9000
PING 172.18.22.250 (172.18.22.250): 9000 data bytes
9008 bytes from 172.18.22.250: icmp_seq=1 ttl=64 time=0.288 ms
9008 bytes from 172.18.22.250: icmp_seq=2 ttl=64 time=0.240 ms

--- 172.18.22.250 ping statistics ---
3 packets transmitted, 2 packets received, 33.3333% packet loss
round-trip min/avg/max = 0.240/0.264/0.288 ms
```

Figure 116. Ping from hosts to CDC interfaces

2. Ping from the hosts to the subsystems. In this example, the following commands are used:

```
vmkping -I vmk2 172.18.21.191 -s 9000
vmkping -I vmk2 172.18.21.192 -s 9000
vmkping -I vmk3 172.18.22.191 -s 9000
vmkping -I vmk3 172.18.22.192 -s 9000
```

```
[root@esxi05:~] vmkping -I vmk2 172.18.21.191 -s 9000
PING 172.18.21.191 (172.18.21.191): 9000 data bytes
9008 bytes from 172.18.21.191: icmp_seq=0 ttl=64 time=0.247 ms
9008 bytes from 172.18.21.191: icmp_seq=1 ttl=64 time=0.201 ms
9008 bytes from 172.18.21.191: icmp_seq=2 ttl=64 time=0.188 ms

--- 172.18.21.191 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.188/0.212/0.247 ms

[root@esxi05:~] vmkping -I vmk2 172.18.21.192 -s 9000
PING 172.18.21.192 (172.18.21.192): 9000 data bytes
9008 bytes from 172.18.21.192: icmp_seq=0 ttl=64 time=0.213 ms
9008 bytes from 172.18.21.192: icmp_seq=1 ttl=64 time=0.188 ms
9008 bytes from 172.18.21.192: icmp_seq=2 ttl=64 time=0.195 ms

--- 172.18.21.192 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.188/0.199/0.213 ms

[root@esxi05:~] vmkping -I vmk3 172.18.22.191 -s 9000
PING 172.18.22.191 (172.18.22.191): 9000 data bytes
9008 bytes from 172.18.22.191: icmp_seq=0 ttl=64 time=0.237 ms
9008 bytes from 172.18.22.191: icmp_seq=1 ttl=64 time=0.180 ms
9008 bytes from 172.18.22.191: icmp_seq=2 ttl=64 time=0.196 ms

--- 172.18.22.191 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.180/0.204/0.237 ms

[root@esxi05:~] vmkping -I vmk3 172.18.22.192 -s 9000
PING 172.18.22.192 (172.18.22.192): 9000 data bytes
9008 bytes from 172.18.22.192: icmp_seq=0 ttl=64 time=0.235 ms
9008 bytes from 172.18.22.192: icmp_seq=1 ttl=64 time=0.187 ms
9008 bytes from 172.18.22.192: icmp_seq=2 ttl=64 time=0.182 ms

--- 172.18.22.192 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.182/0.201/0.235 ms
```

Figure 117. Ping from host to subsystems

3. SSH to the SFSS Management IP address.
4. Enter **2** to **Debug**.
5. Enter **shell** in the field provided.

```
################################################################################
    Welcome to Dell EMC Smart Fabric Storage Software (SFSS) management
################################################################################

    Menu
------------------------------------------------------
1.  Show version
2.  Debug
3.  Password/SSL configuration menu
4.  Show EULA
5.  Interface configuration menu
6.  Reboot
7.  Logout

Enter selection [ 1 - 7 ] : 2
Enter Module name (app-alerts, app-redis, app-rest, cdcproxy, centralnz, discovery, license, redis-d
eployment, syslogng, shell): shell
Linux Shell Mode
root@sfss:/home/stfs# _
```

Figure 118. Enter SFSS shell

6. Ping from SFSS CDC interfaces to the subsystems. In this example, the following commands are used:

```
ping -I ens192 172.18.21.191 -s 9000
ping -I ens192 172.18.21.192 -s 9000
ping -I ens224 172.18.22.191 -s 9000
ping -I ens224 172.18.22.192 -s 9000
```

```
root@sfss:/home/stfs# ping -I ens192 172.18.21.191 -s 9000
PING 172.18.21.191 (172.18.21.191) from 172.18.21.250 ens192: 9000(9028) bytes of data.
9008 bytes from 172.18.21.191: icmp_seq=1 ttl=64 time=0.194 ms
9008 bytes from 172.18.21.191: icmp_seq=2 ttl=64 time=0.212 ms
^C
--- 172.18.21.191 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 14ms
rtt min/avg/max/mdev = 0.194/0.203/0.212/0.009 ms
root@sfss:/home/stfs# ping -I ens192 172.18.21.192 -s 9000
PING 172.18.21.192 (172.18.21.192) from 172.18.21.250 ens192: 9000(9028) bytes of data.
9008 bytes from 172.18.21.192: icmp_seq=1 ttl=64 time=0.216 ms
9008 bytes from 172.18.21.192: icmp_seq=2 ttl=64 time=0.182 ms
^C
--- 172.18.21.192 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 30ms
rtt min/avg/max/mdev = 0.182/0.199/0.216/0.017 ms
root@sfss:/home/stfs# ping -I ens224 172.18.22.191 -s 9000
PING 172.18.22.191 (172.18.22.191) from 172.18.22.250 ens224: 9000(9028) bytes of data.
9008 bytes from 172.18.22.191: icmp_seq=1 ttl=64 time=0.203 ms
9008 bytes from 172.18.22.191: icmp_seq=2 ttl=64 time=0.187 ms
^C
--- 172.18.22.191 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 15ms
rtt min/avg/max/mdev = 0.187/0.195/0.203/0.008 ms
root@sfss:/home/stfs# ping -I ens224 172.18.22.192 -s 9000
PING 172.18.22.192 (172.18.22.192) from 172.18.22.250 ens224: 9000(9028) bytes of data.
9008 bytes from 172.18.22.192: icmp_seq=1 ttl=64 time=0.195 ms
9008 bytes from 172.18.22.192: icmp_seq=2 ttl=64 time=0.198 ms
^C
--- 172.18.22.192 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 23ms
rtt min/avg/max/mdev = 0.195/0.196/0.198/0.014 ms
root@sfss:/home/stfs#
```

Figure 119. Ping from SFSS to subsystems

Create the CDC instances

Create two CDC Instances using the SFSS Web UI. In this example.

- **CDC Instance 1** is used for **SAN A** (using interface **ens192**)
- **CDC Instance 2** is used for **SAN B** (using interface **ens224**)

1. From the SFSS **Home** page, select **SFSS APP** > **CDC Instances** > **CDC Instances**.

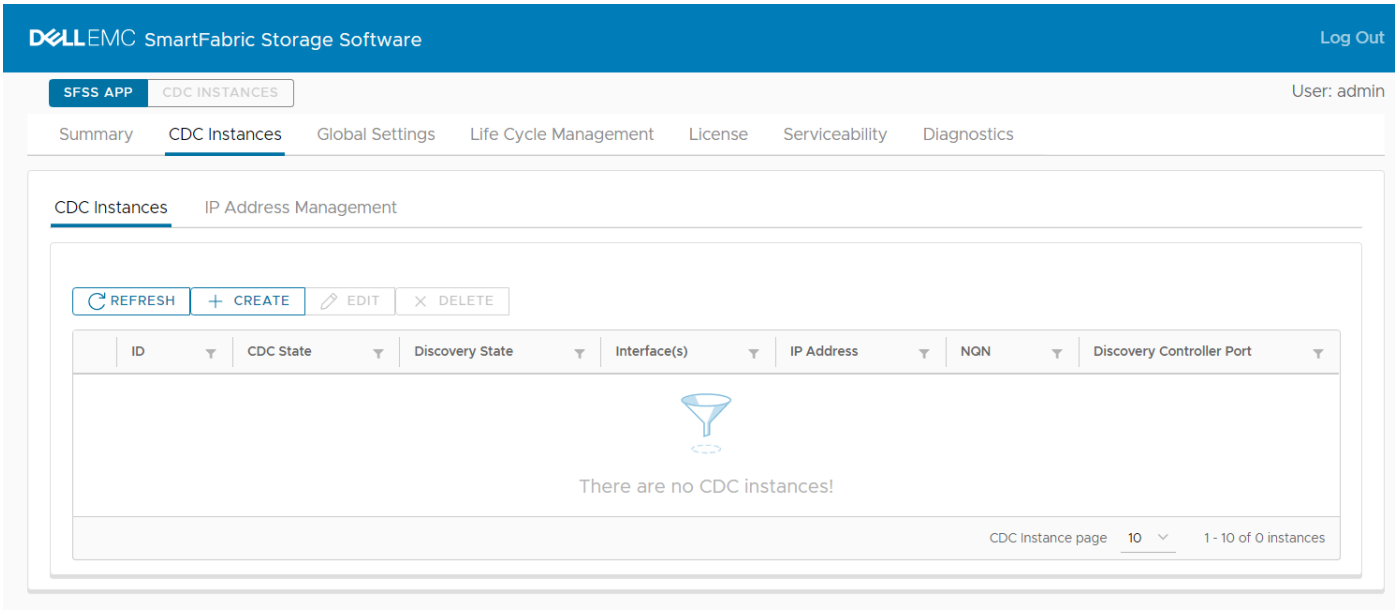


Figure 120. SFSS CDC Instances View

2. Click the **+Create** button.
3. For the first **CDC Instance ID**, enter **1**.
4. Select the interface created for NVMe/TCP SAN-A control traffic.

NOTE: This example uses **ens192**. The **Discovery State** and **CDC State** are **enabled**.

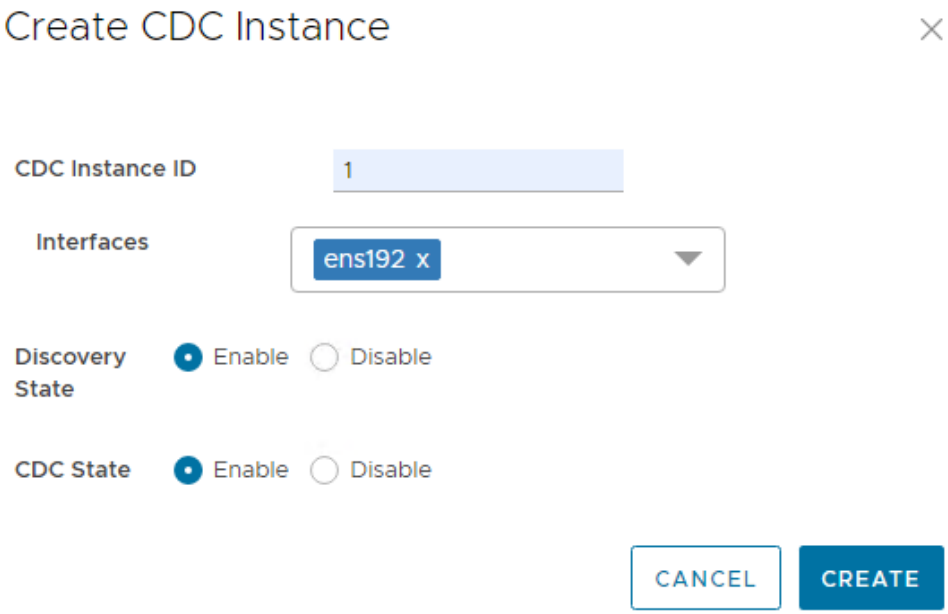


Figure 121. Create CDC Instance 1

5. Click the **+Create** button.

NOTE: Verify that the new CDC Instance displays in the list.

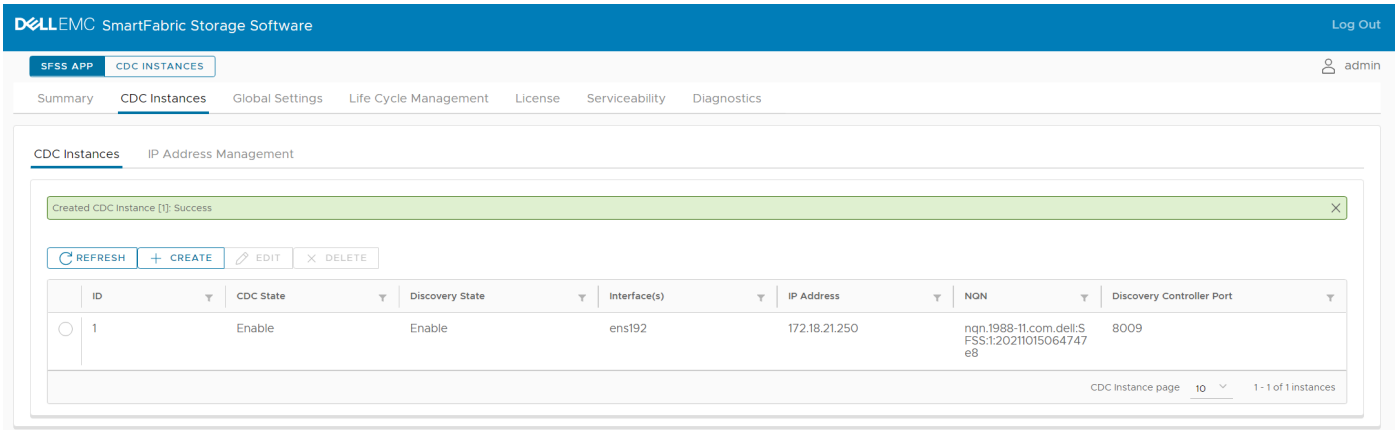


Figure 122. New CDC Instance

6. Click the **+Create** button again.
7. For the second **CDC Instance ID**, enter **2.**
8. Select the interface created for NVMe/TCP SAN-B control traffic.

   NOTE: This example uses **ens224**. The **Discovery State** and **CDC State** are **enabled**.

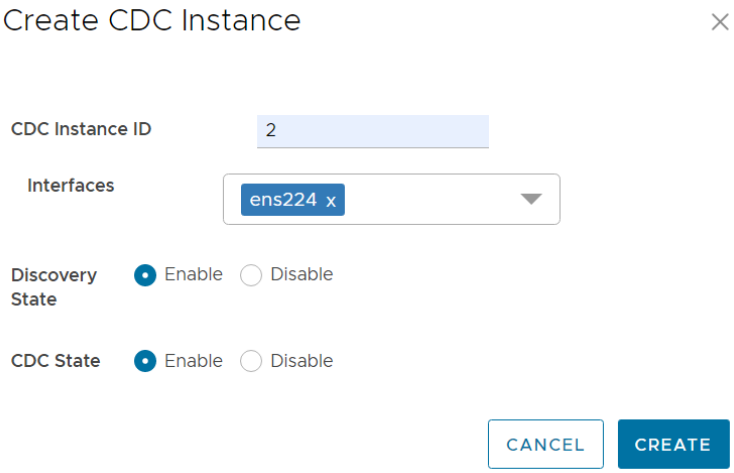


Figure 123. Create CDC Instance 2

9. From the **CDC Instances** section, click **+Create**.

   NOTE: Verify that the new CDC Instance displays in the list.

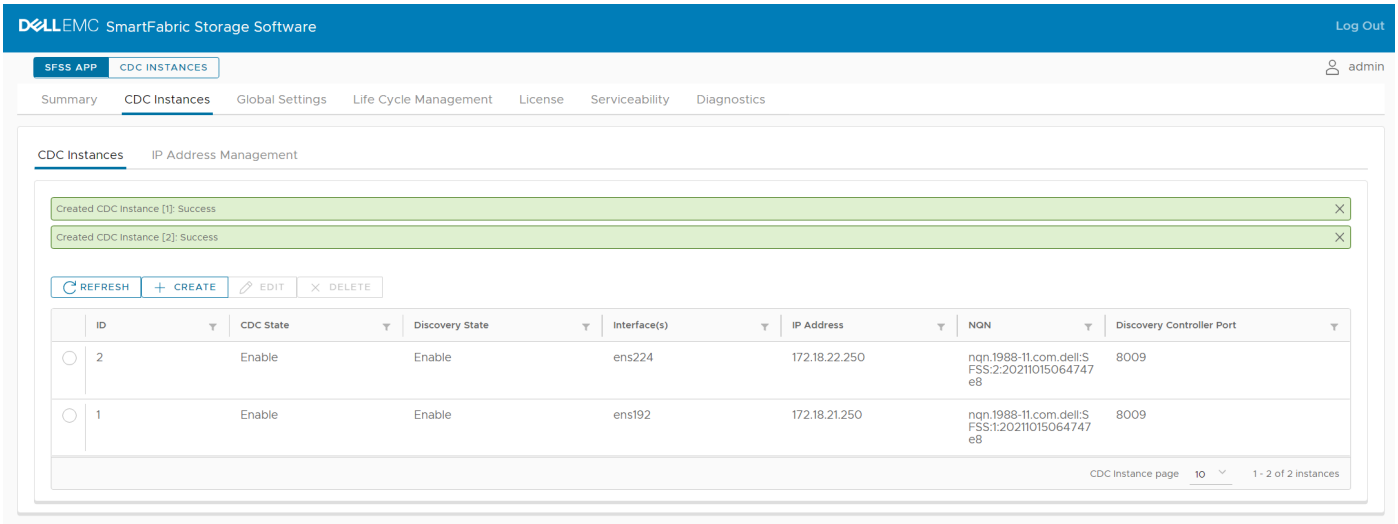


Figure 124. Two CDCs created

NOTE: For information on the installation of a license, see the SFSS Licenses section.

Register SFSS in ESXi hosts

In this step, the hosts perform another pull registration to get the details of the PowerStore DDCs from the SFSS CDC.

NOTE: In a future VMware vSphere release, this step is automated. Repeat the steps in this section for each ESXi host. Alternatively, this step can be done using the CLI. For more information, see the Register SFSS in the ESXi hosts using CLI

To add the controller to the storage adapters, follow the steps below:

1. Log in to the vSphere web client.
2. Select **Hosts and clusters**.
3. Click to select the **host**. In this example, host **esxi05** is selected.
4. Click **Configure** > **Storage** > **Storage Adapters**.
5. Click to select the **vmhba64** adapter.
   NOTE: This is a VMware NVMe over TCP Storage Adapter model.
6. Select **Controllers** > **ADD CONTROLLER**.

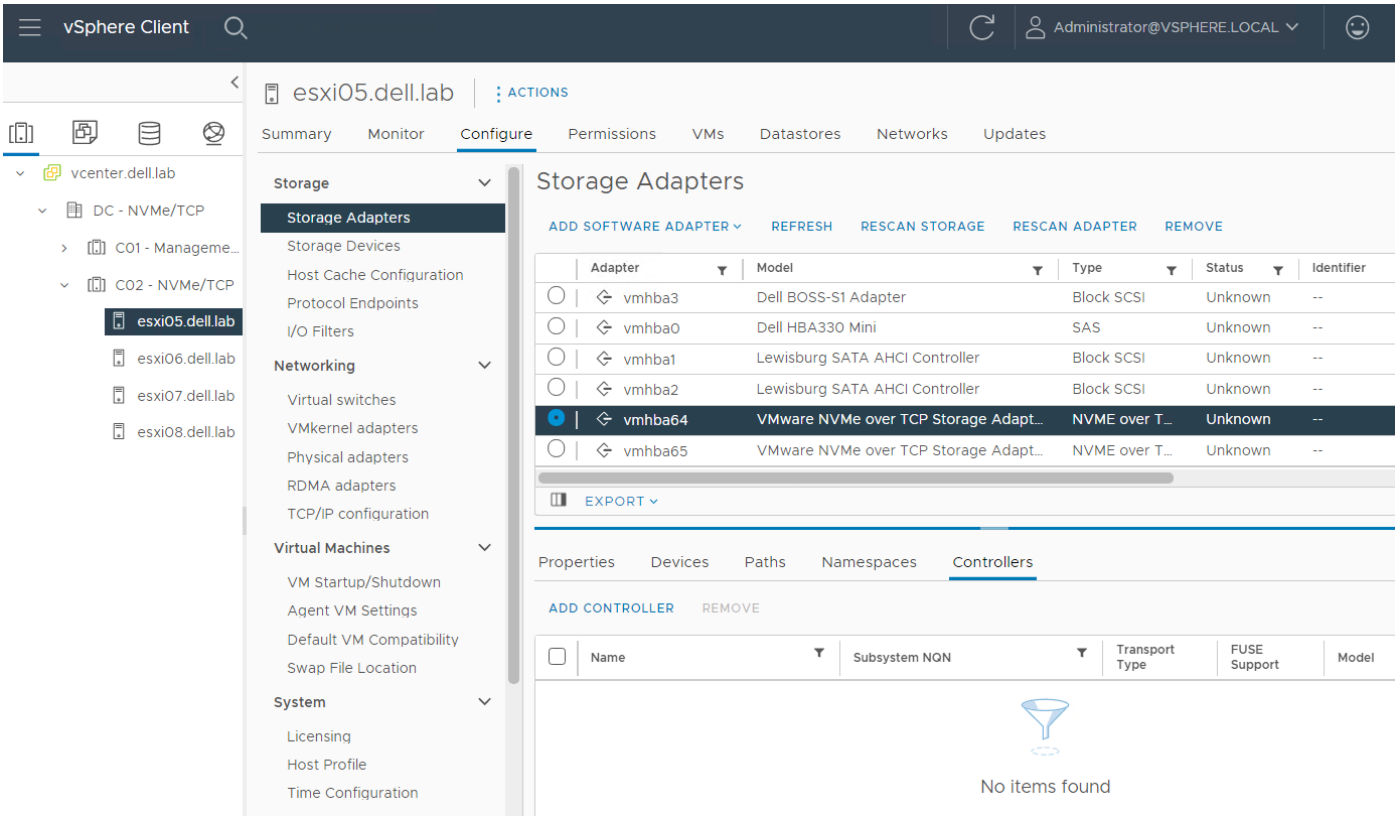


Figure 125. Storage Adapters screen

7. In the **Automatically** tab, enter the follow details:
   a. In the **IP** field, enter the CDC instance IP address.
      NOTE: This example uses IP address **172.18.21.250**.
   b. Click to place a check in the **Root discovery controller** box.
      NOTE: This refers to the SFSS vApp.
   c. In the **Port Number** field, enter the port number. This example uses **8009**.
   d. Leave the **Digest parameter** options in the default, cleared state.
   e. Click the **DISCOVER CONTROLLERS** button.

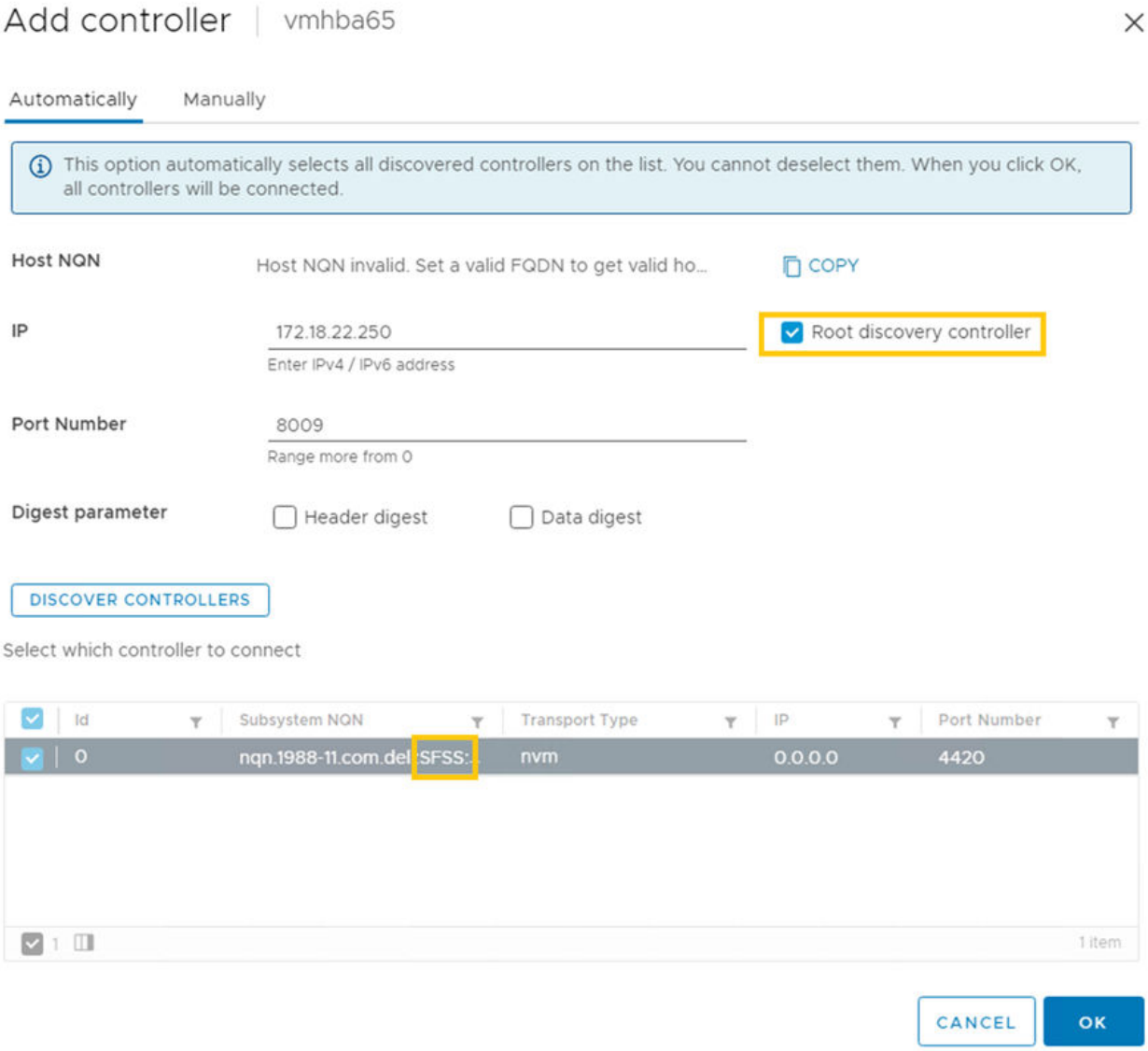


Figure 126. Add controllers

NOTE: The subsystem NQN is that of SFSS rather than that of a storage subsystem.

f. Click **OK**.

g. Repeat this step for the SAN B vmhba.

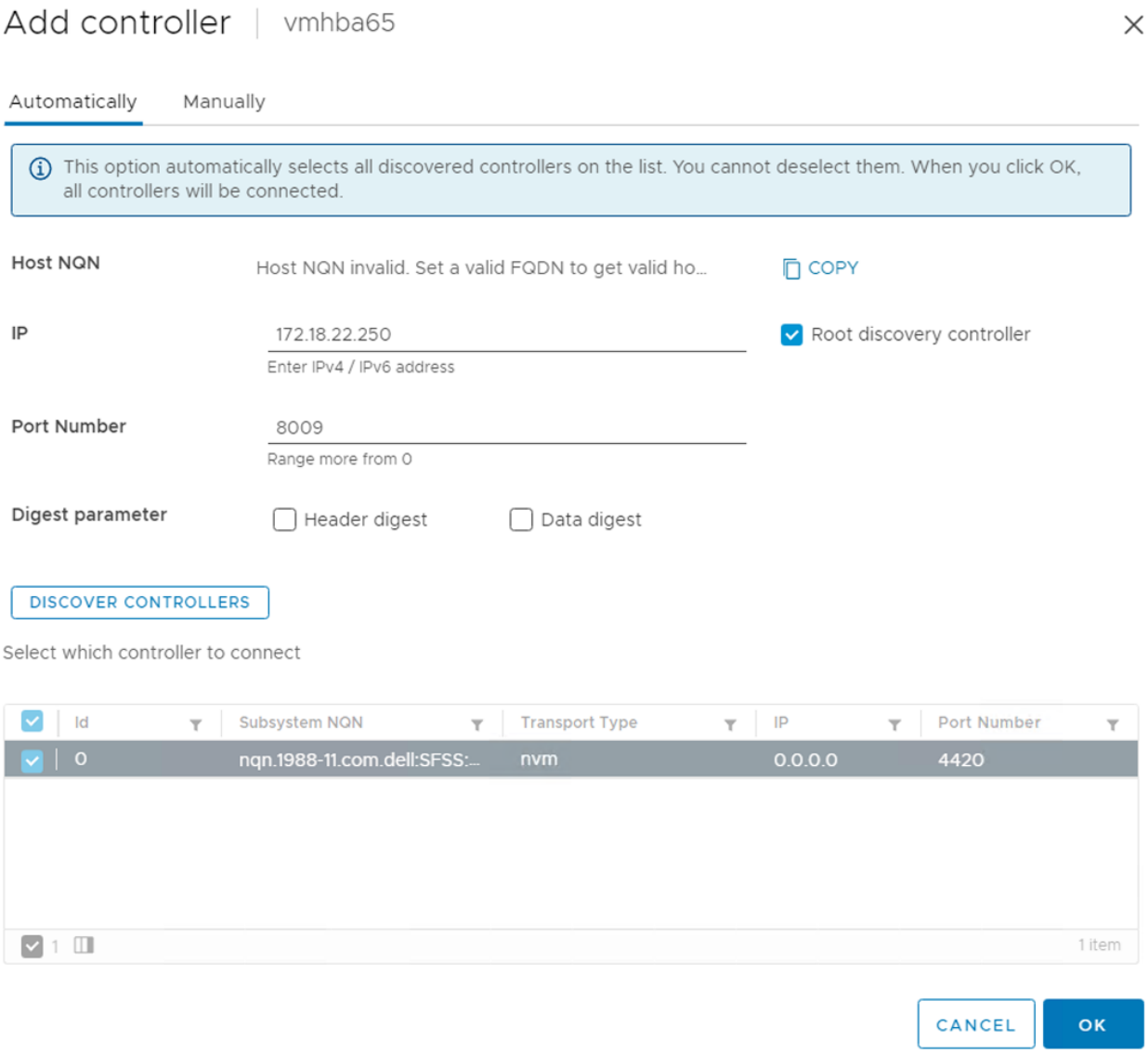


Figure 127. Add Controller to Software Adapter

8. Repeat the above steps for each NVMe/TCP storage adapter on each host participating in IP SAN.

   NOTE: The **ADD CONTROLLER** fields for each host will show **No items found**. The message changes after the configuration is completed later in the process.

9. To verify all hosts are registered with each CDC:
   a. Log in to the SFSS.
   b. Click **CDC INSTANCES** and select **1** from the drop-down menu.
   c. Click **Endpoints** > **Host** to see the list of hosts registered with **CDC 1**.

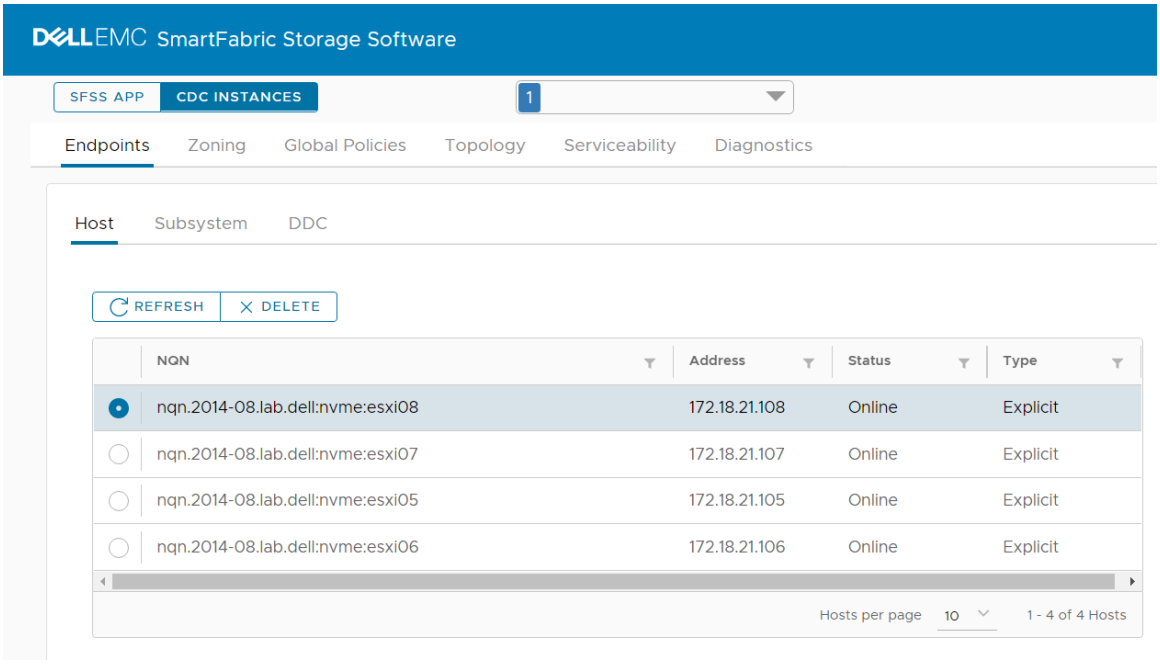


Figure 128. Hosts appear CDC Instance 1

d. Select **2** from the drop-down menu to see the same list of hosts registered with **CDC 2**. In this listing, the hosts have IP addresses in the SAN B **172.18.22.xxx** network.

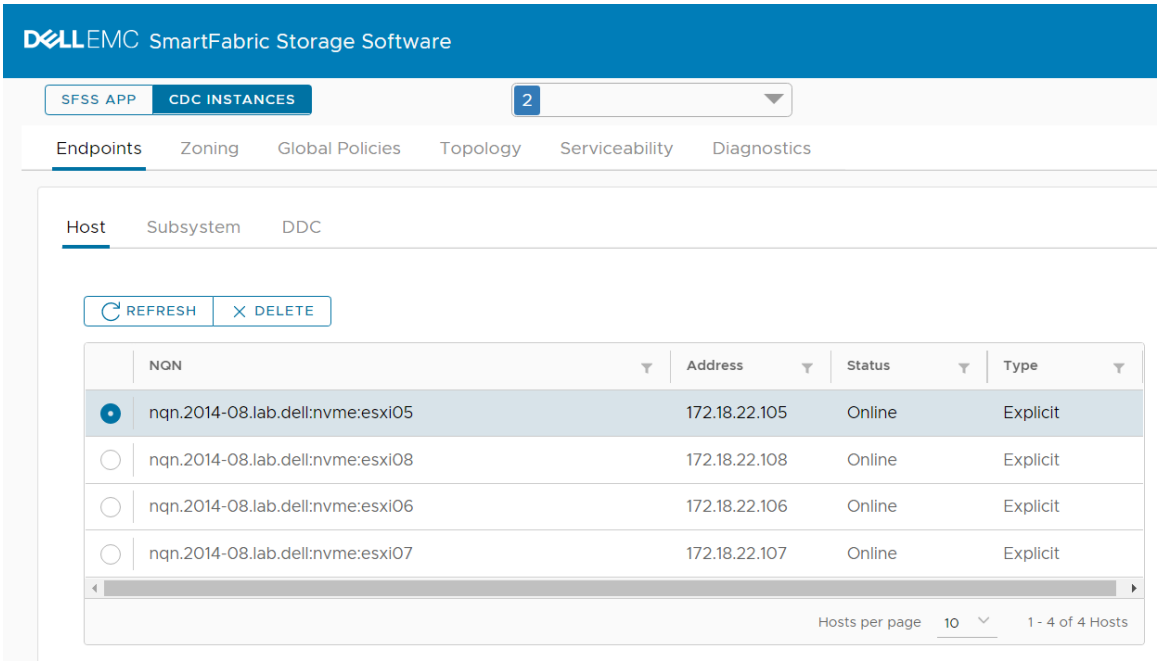


Figure 129. Hosts appear CDC Instance 2

Register PowerStore in SFSS

NOTE: In a future PowerStoreOS release, this step is automated.

This section provides the instructions to register the PowerStore Direct Discovery Controllers (DDC) in SFSS. DDCs are created when the Storage IPs are initialized. There are four DDCs in this example:

- Two for **SAN-A** (one for each PowerStore node)
- Two for **SAN-B** (one for each PowerStore node)

The following provides the information you need to complete the registration process. The steps that follow use the first row of information in the **DDC registration information** table to guide you through the addition of the first DDC. Use the remaining rows of information to complete the process of adding all four DDCs.

Table 23. DDC registration information

CDC Instance	SAN	PowerStore controller	Address	Port ID
1	SAN-A	Node-A	172.18.21.191	8009
		Node-B	172.18.21.192	
2	SAN-B	Node-A	172.18.22.191	
		Node-B	172.18.22.192	

This section demonstrates the pull registration of PowerStore DDCs in SFSS. SAN A Endpoints are registered in CDC Instance 1, and SAN B Endpoints are registered in CDC Instance 2.

1. Log in to SFSS.
2. Select CDC instance **1** using the drop-down menu.
3. Select **CDC INSTANCES** > **Endpoints** > **DDC**.

   NOTE: Verify that you are in the correct CDC instance.

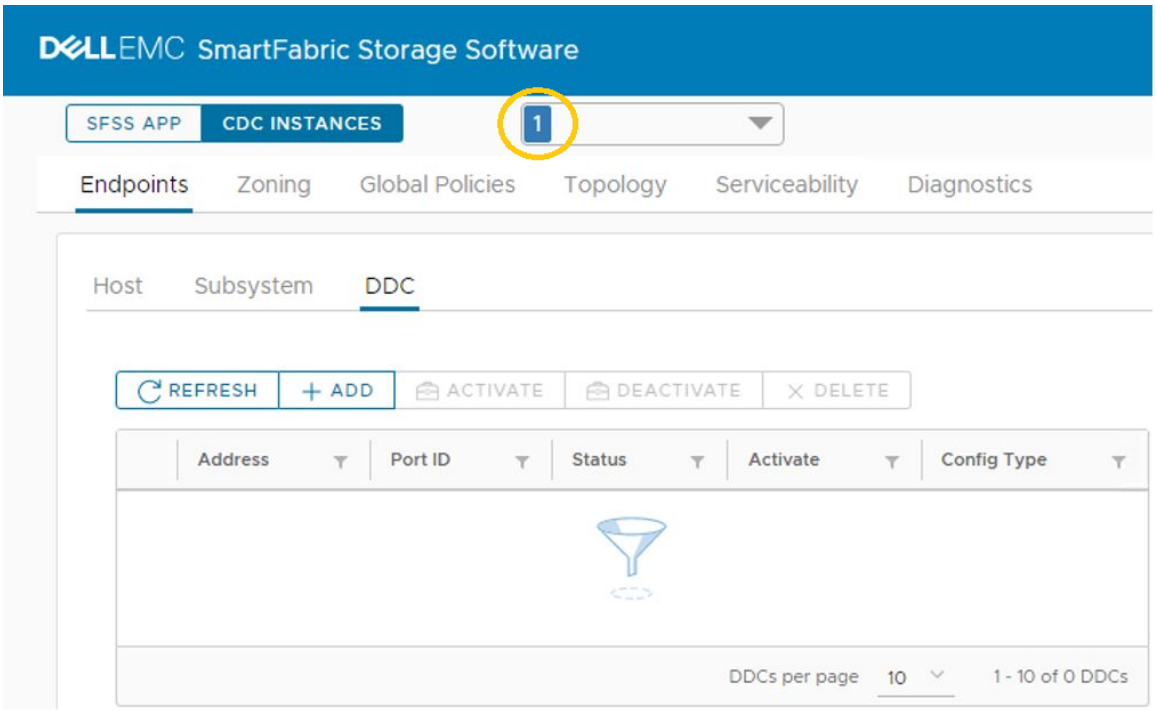


Figure 130. DDC View in CDC 1

4. Click **ADD**.
   The **Add a Static DDC** dialog box opens.
5. In the **Address** field, enter the first IP in the new **SAN-A** storage network on the storage array. **Note:** This example uses **172.18.21.191**.
6. In the **Port** field, enter **8009** as the default value.
7. Click to switch the **Activate** option to the **on** position.

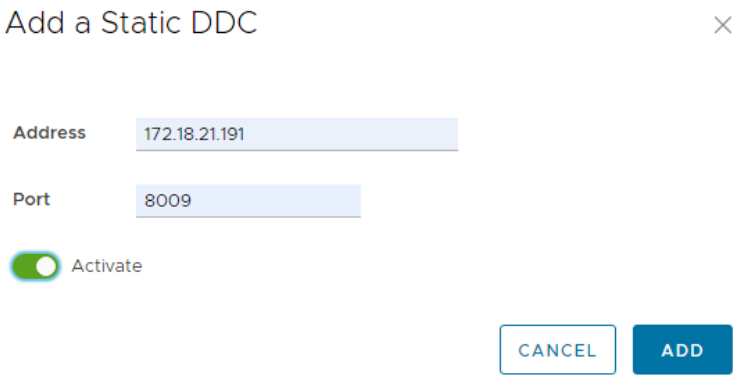


Figure 131. Add DDC

8. Click **ADD**.
   The message for adding the DDC successfully displays.

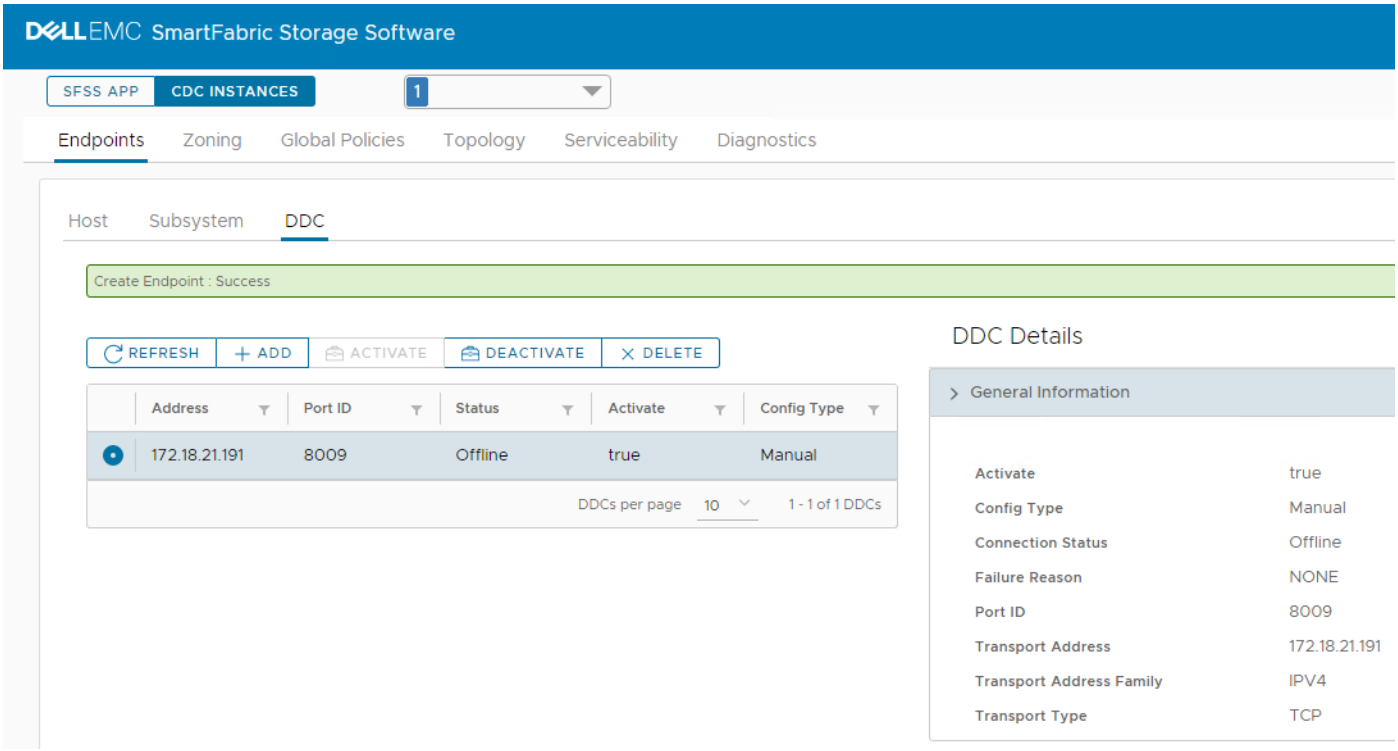


Figure 132. First PowerStore DDC successfully added

9. Click the **REFRESH** button in the **DDC** tab.
   The **Status** changes to **Online**

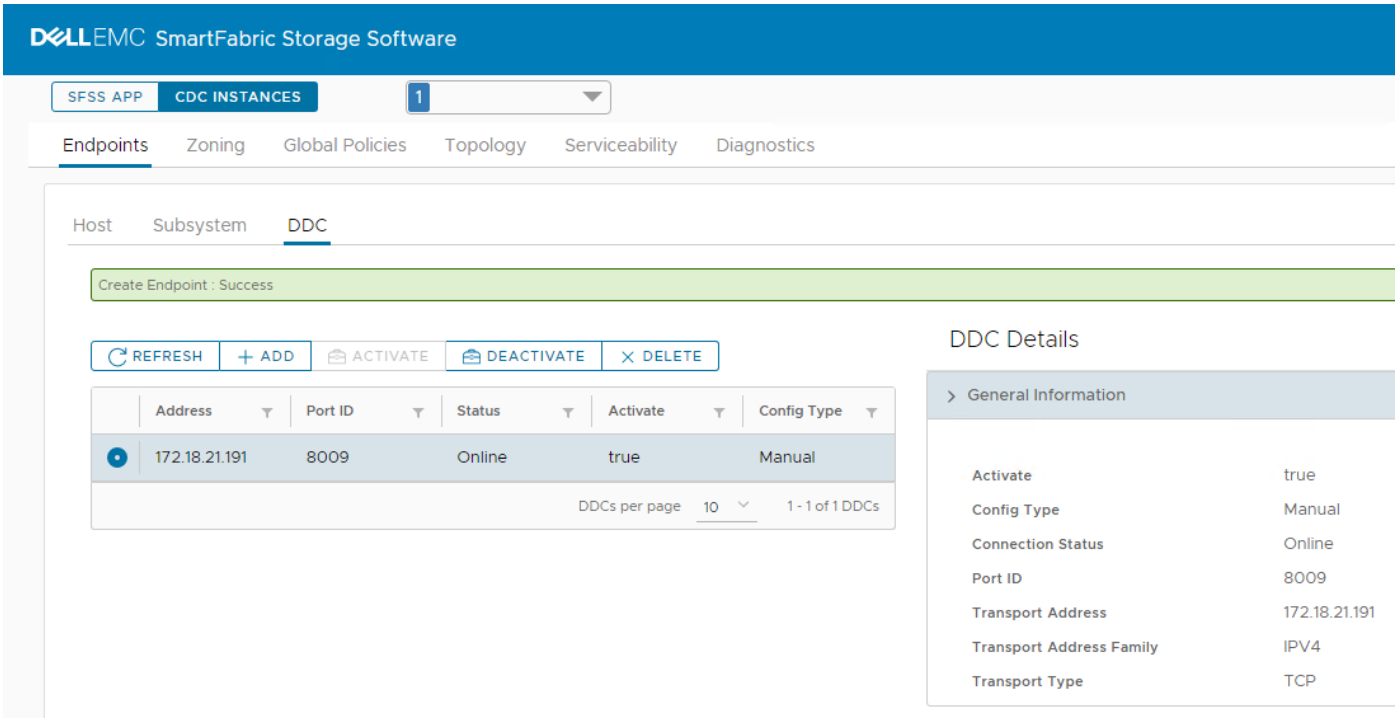


Figure 133. DDC connection status

10. Repeat the steps in this section to add the remaining DDCs. In this example, three more DDCs are added.
11. Verify that the DDCs are registered. In this example, two are listed in **Instance 1**, and two are listed in **Instance 2**.

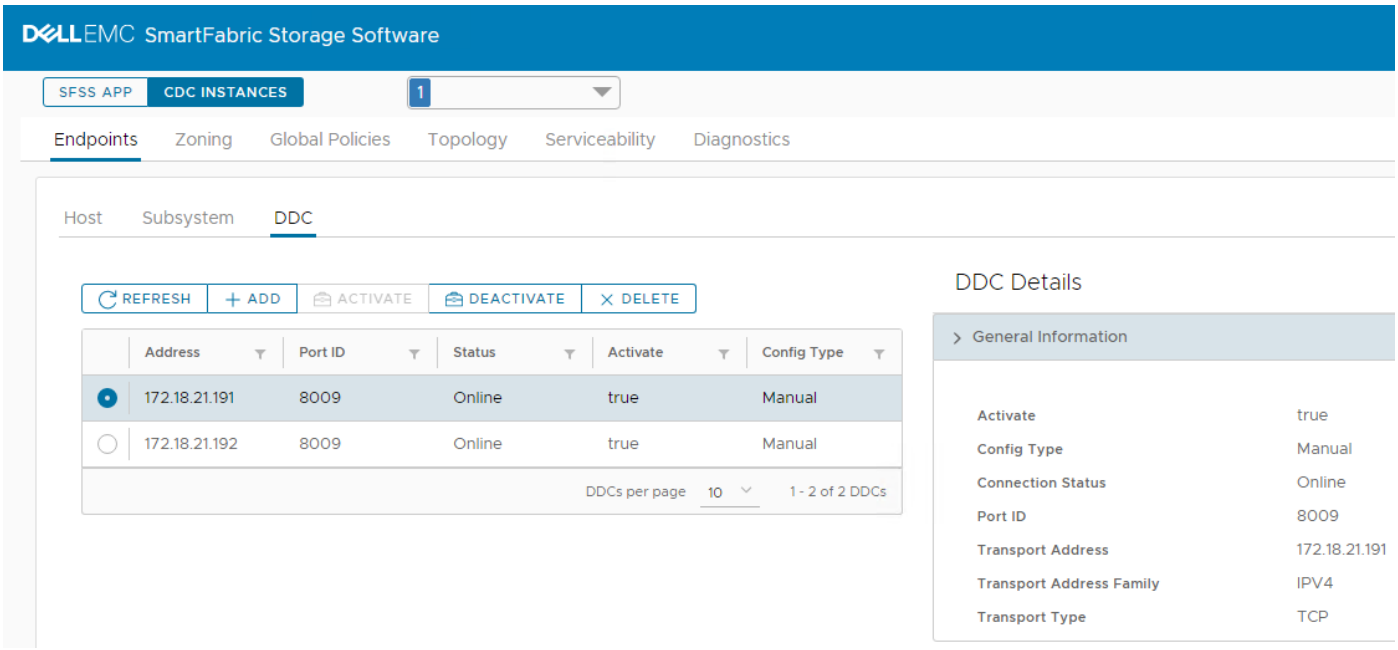


Figure 134. PowerStore DDCs registered on Instance 1

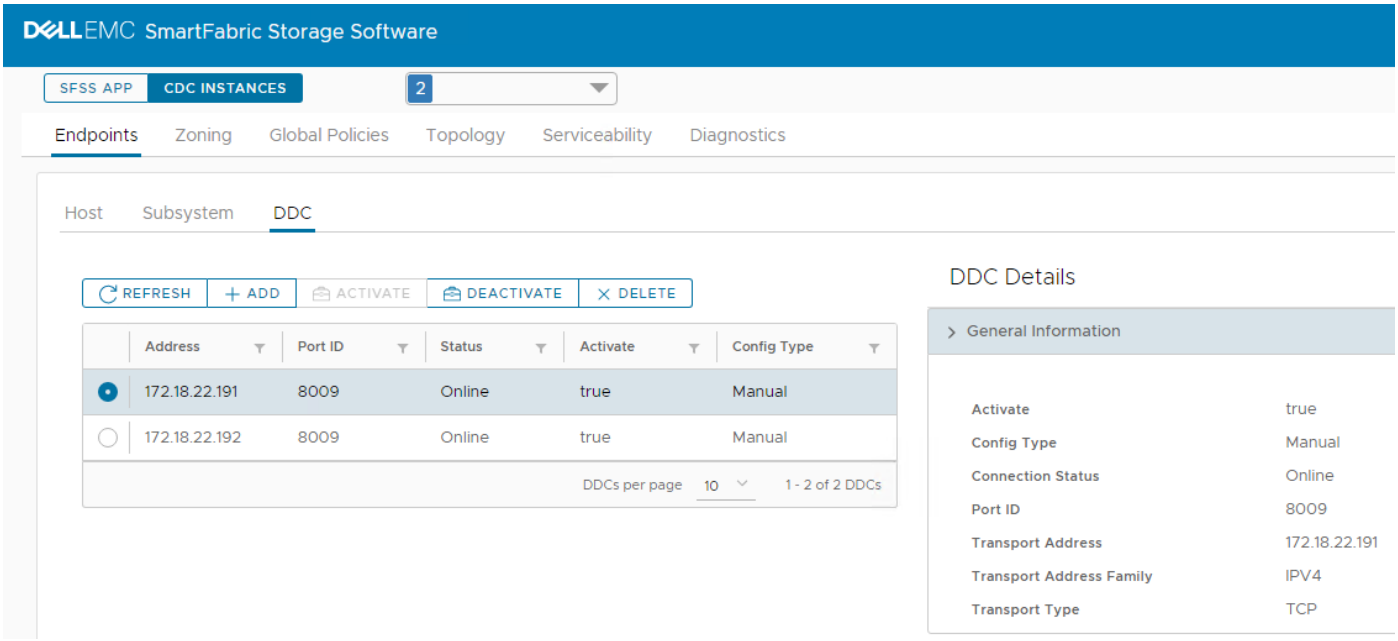


Figure 135. PowerStore DDCs registered on Instance 2

12. In the **Endpoints** section, select **Subsystem**. The Subsystem section shows the relevant details.

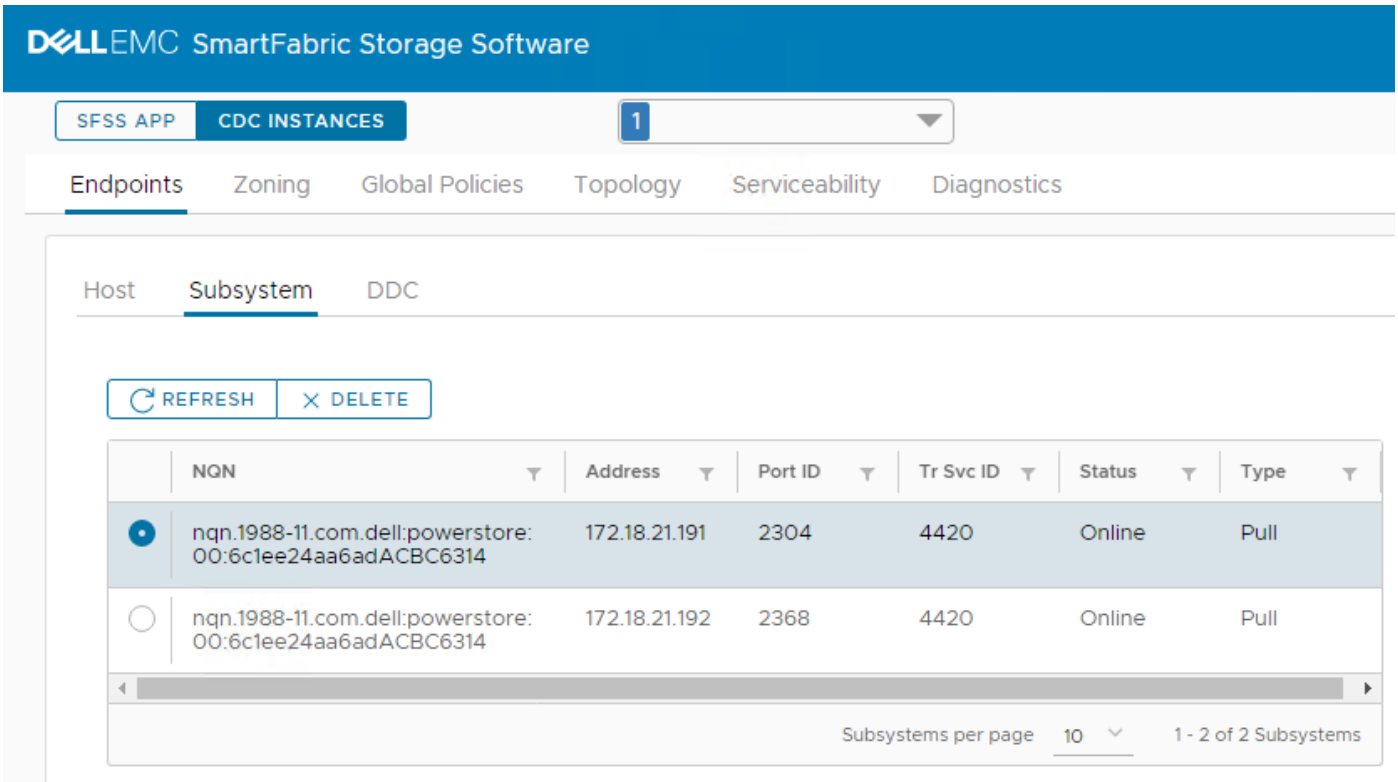


Figure 136. Verify Subsystems are registered on Instance 1

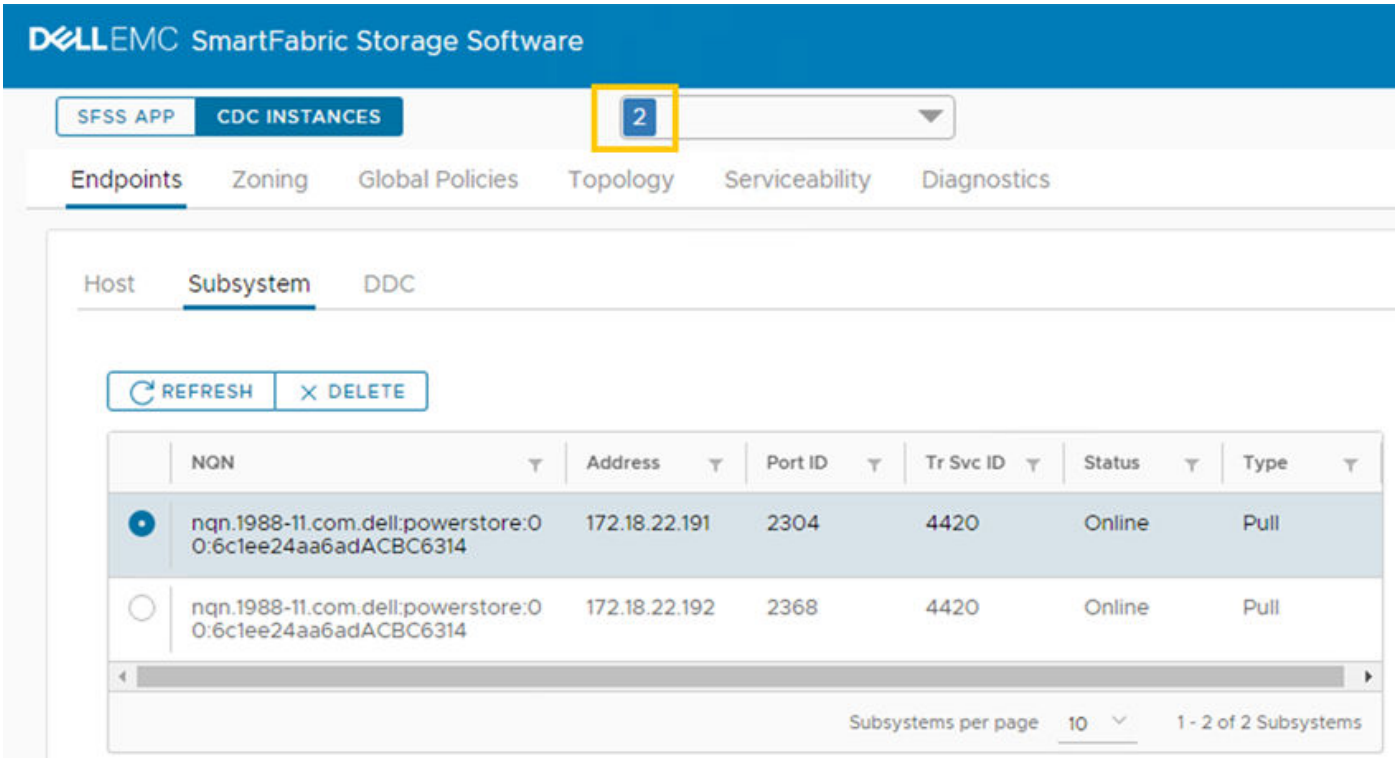


Figure 137. Verify Subsystems are registered on Instance 2

NOTE: If the output is not as expected, see the SmartFabric Storage Software Troubleshooting Guide for assistance.

Configure Zoning in SFSS

To control access, SFSS allows the ability to soft-zone subsystems and hosts. In this example, the SAN A zone will contain all Endpoints in the 172.18.21.0/24 network, and SAN B will contain all Endpoints in the 172.18.22.0/24 network.

NOTE: Before zoning, hosts are denied access to all subsystems by default.

The high-level steps are as follows:

- Create Zone Group
- Create Zone
- Add Members
- Activate zoning
- Verify

Create Zone Group and Zone

The steps below explain how to create a zone for Endpoints in SAN A. In this example, Zone **Z-NVMe-SAN-A** is in Zone Group **ZG-NVMe-SAN-A** in CDC Instance **1**.

NVMe IP SANs do not require single initiator or single target zoning. Similar to Cisco SmartZoning or Broadcom Peer Zoning, SFSS zones contain groups of host ports and the storage ports they access. The figure below shows four host ports accessing the same two storage ports. As a result, it is logical to put these hosts and storage ports in the same zone.

To avoid wasting system resources on both the host and the storage subsystem, only zone host interfaces to a limited number of storage ports. Each host interface will access two PowerStore interfaces - one on Node A, and one on Node B.

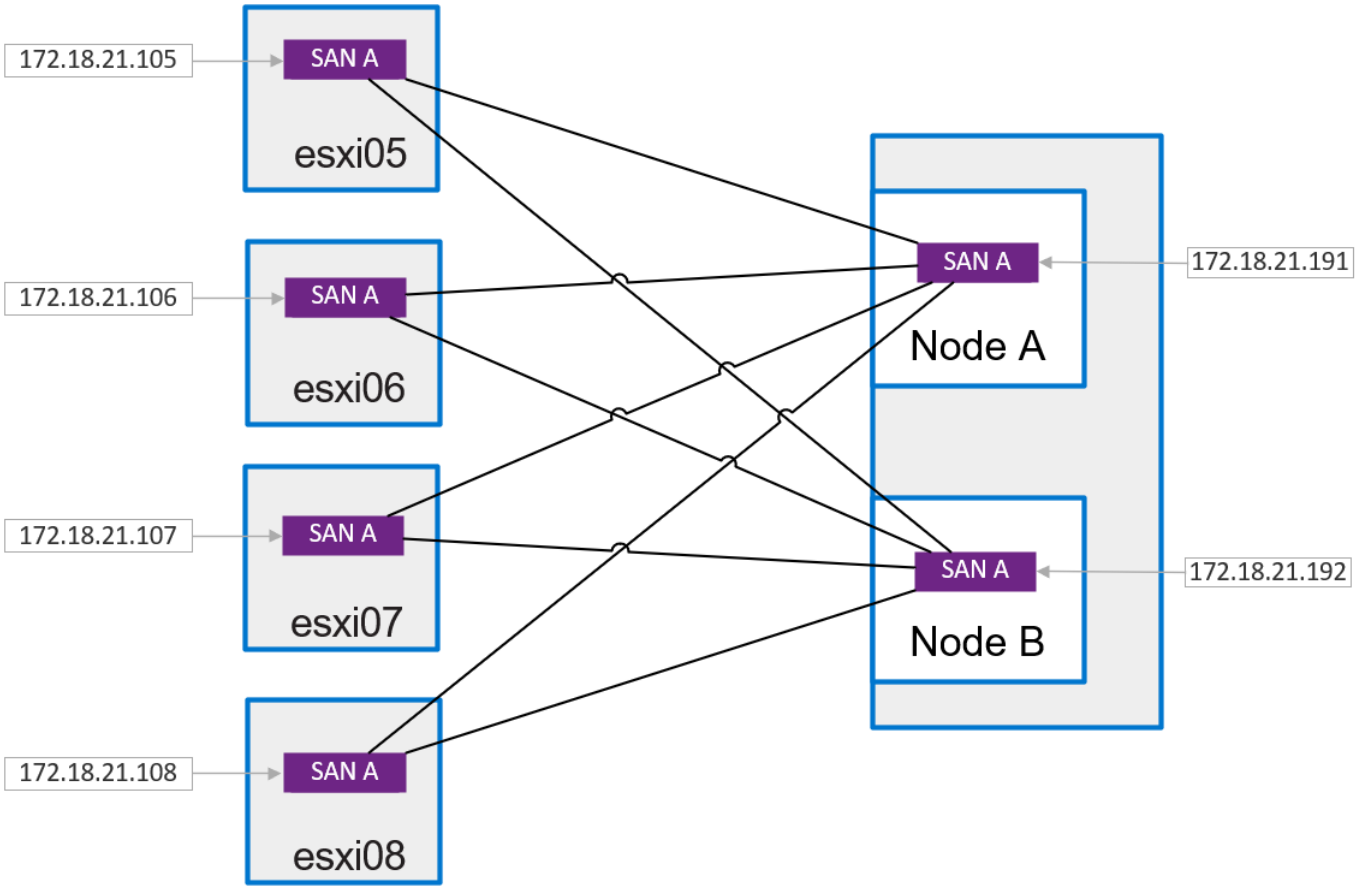


Figure 138. Zone A - Z-NVMe-SAN-A

To create a Zone Group:

1. From the SFSS **Home** page, click **CDC INSTANCES**, and select **1** from the drop-down menu.
2. Click **Zoning**.

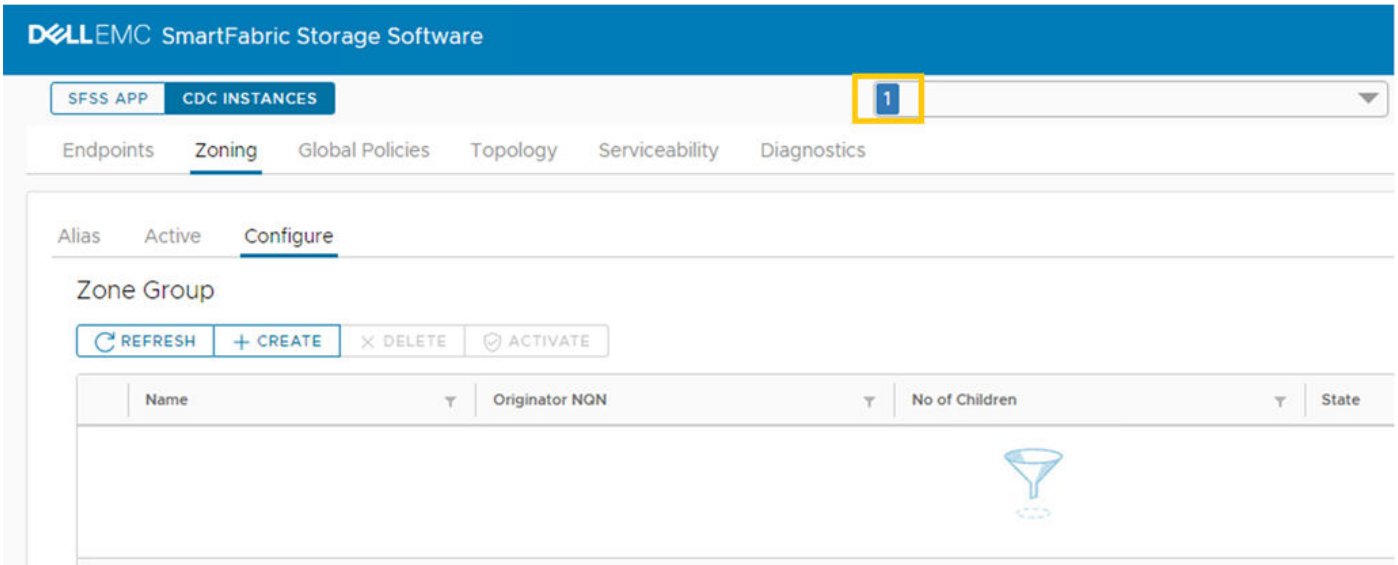


Figure 139. Zoning

3. Click **Configure** > **CREATE**.
4. In the **Create Zone Group** window, provide a name for the zone group.

NOTE: This example uses **ZG-NVMe-SAN-A**.

5. Click **SUBMIT**.

Figure 140. Create Zone Group

The newly created zone group displays.

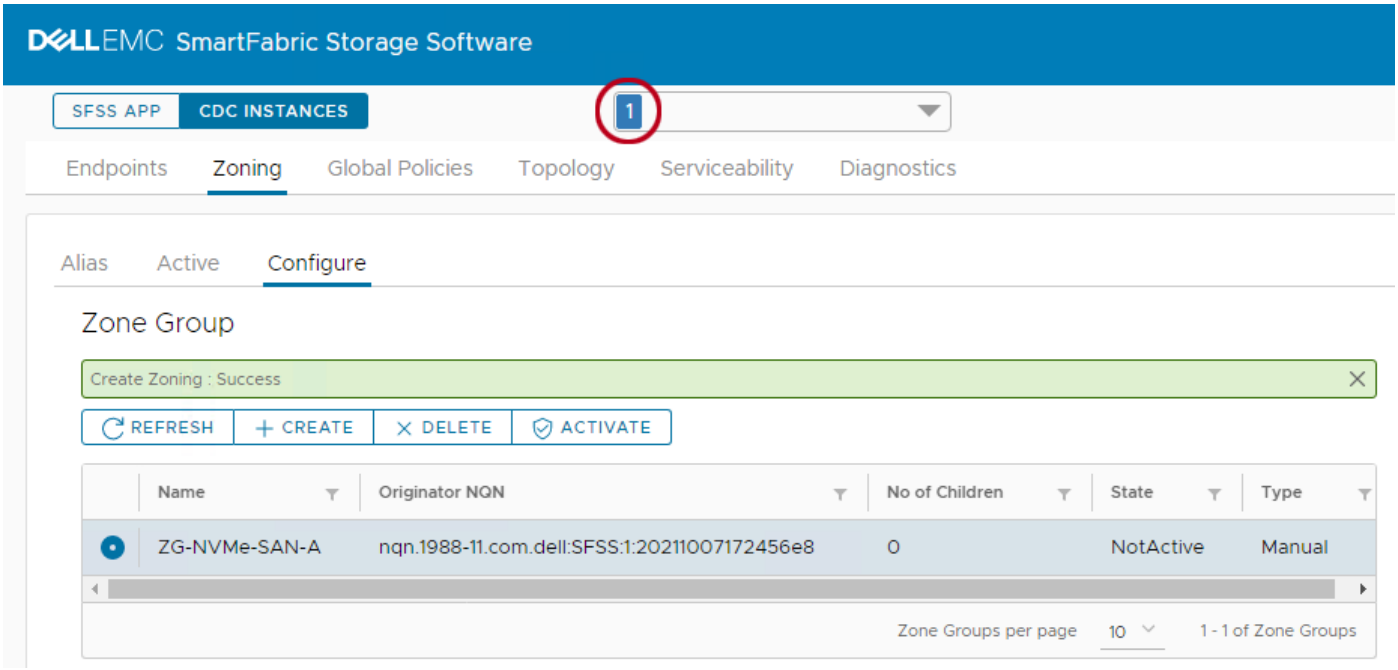


Figure 141. Created zone group

Create Zone and add members

To create the Zone and add members, perform the following steps:

1. Click to select the radio button next to the zone group name.

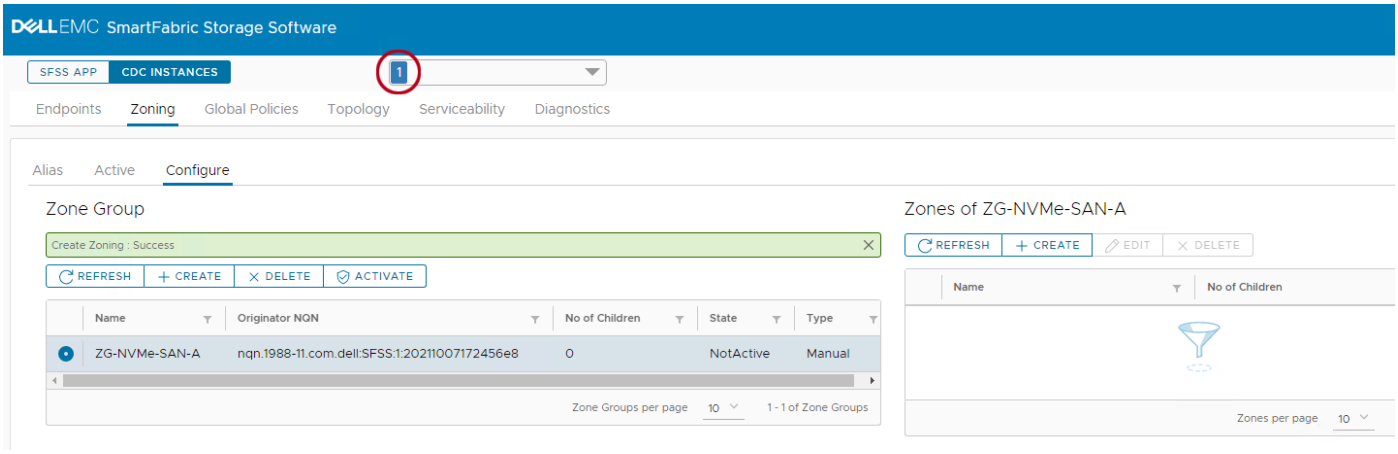


Figure 142. Select zone group

2. From **Zones** under **ZG-NVMe-SAN-A**, click the **+ CREATE** button.
3. In the **Zone Name** field, enter a zone name. This example uses **Z-NVMe-SAN-A** for the zone name.

Figure 143. Create Zone screen

4. Click **SUBMIT**.
   The new zone displays under the **Zones** of **ZG-NVMe-SAN-A**.

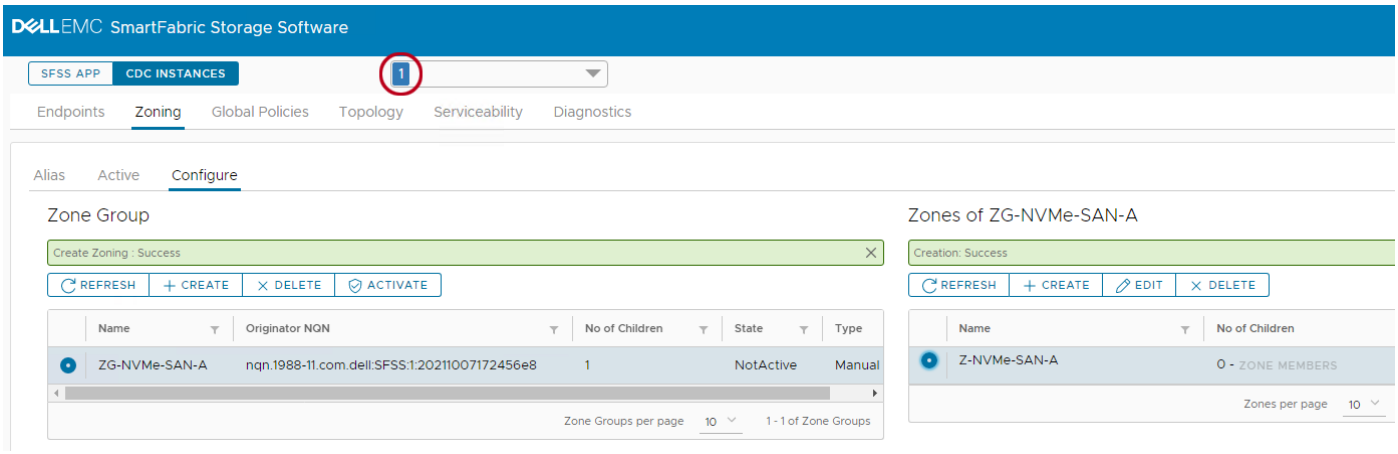


Figure 144. Zone created for Zone Group

5. Click to select radio button next to the wanted zone.
6. Click the **EDIT** button.
7. In the **Available Endpoints** section, select **FullQualifiedName** from the drop-down. This option provides more information about the hosts listed. The default type selected is **Host**.
8. Select all the SAN A host Endpoints.

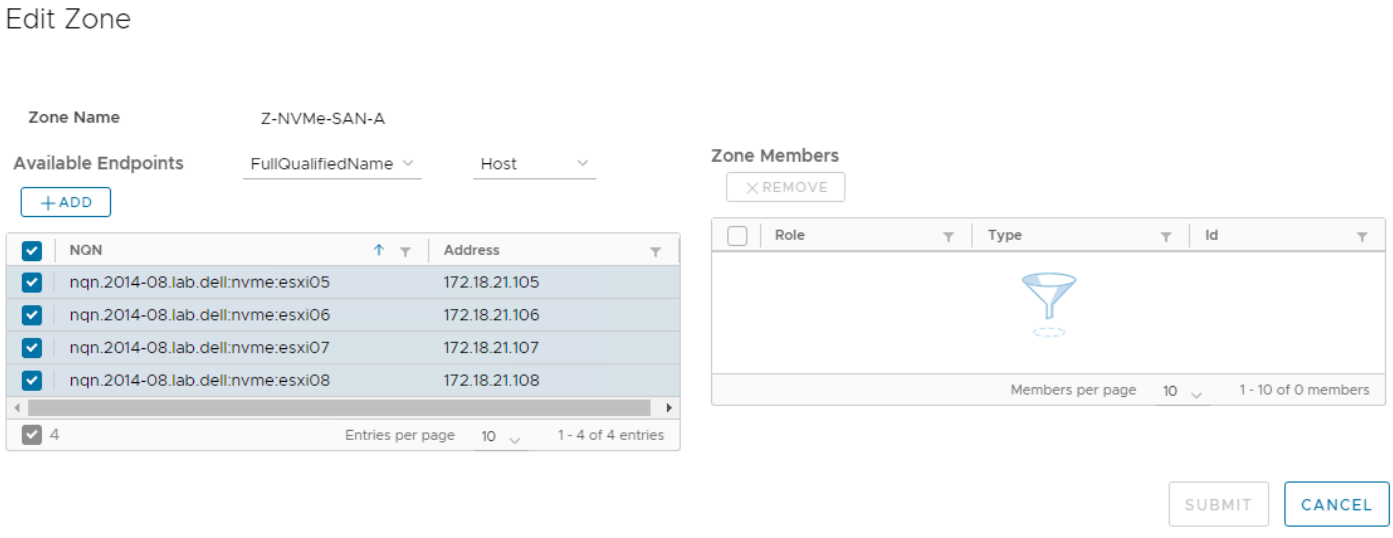


Figure 145. Add hosts to zone

9. Click **+ADD**. All the selected hosts are shown in the zone members list.

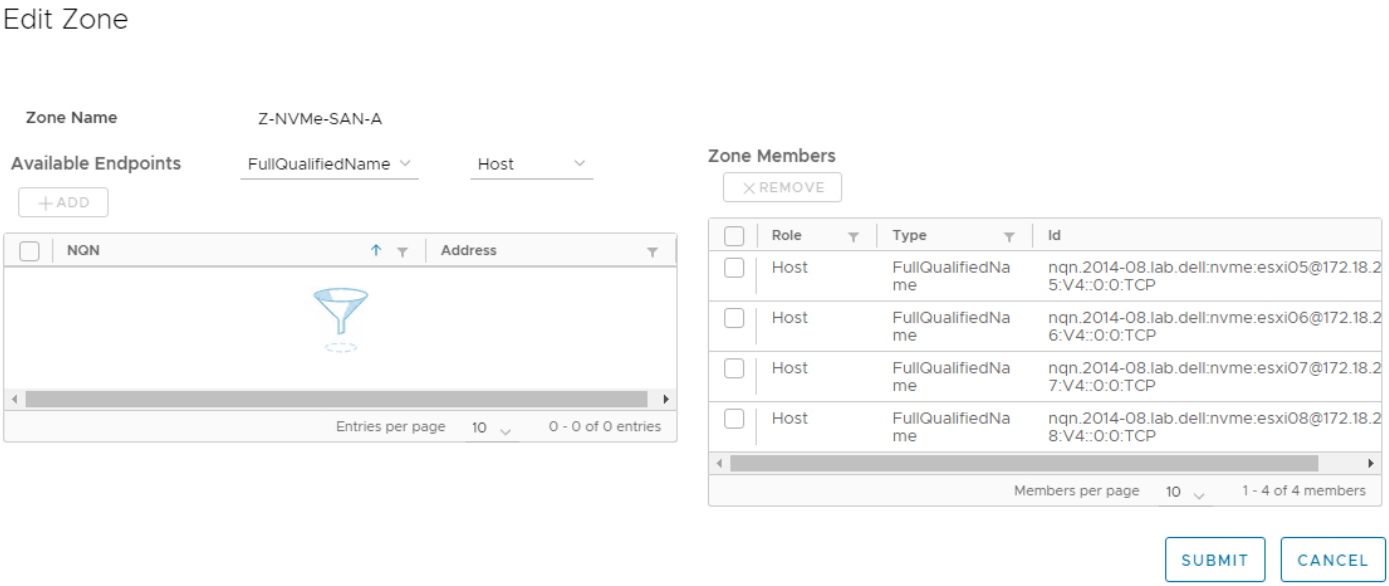


Figure 146. Add hosts to zone

10. With **Available Endpoints** set to **FullQualifiedName**, change the type to **Subsystem**.
11. Click to select the Subsystems that you want to include in the zone. In this example, both subsystems for SAN-A (network 172.18.21.0/24) are selected.

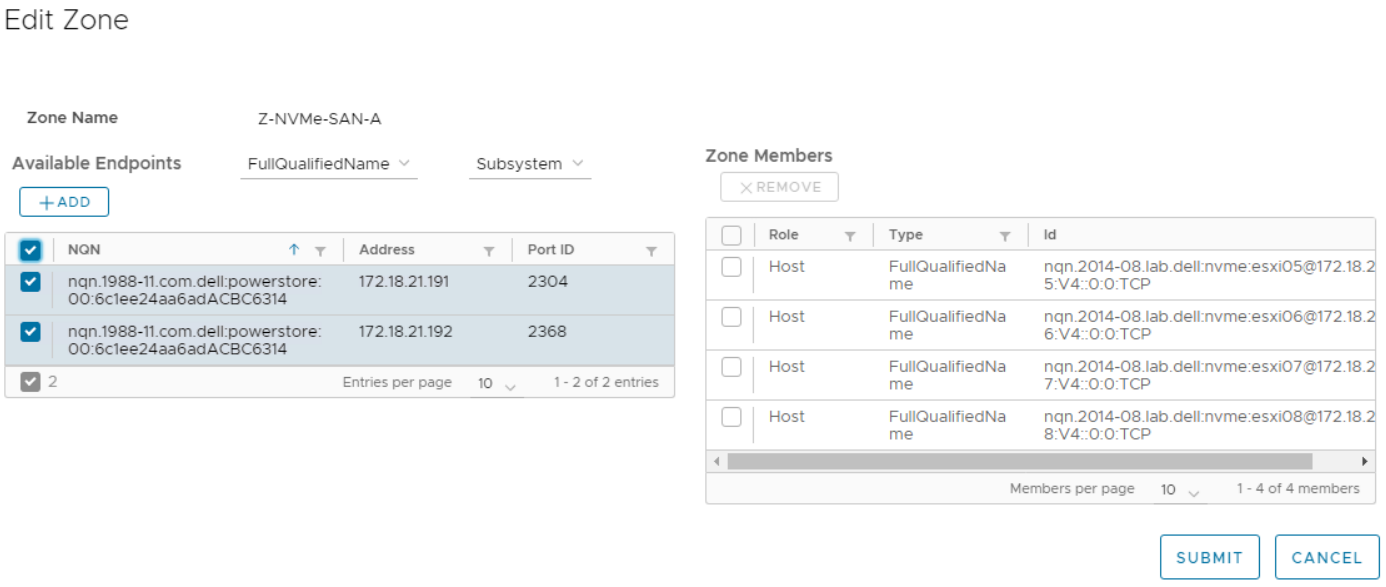


Figure 147. Add subsystems to zone

12. Click **ADD**.
    The hosts and subsystems display in the zone members list.

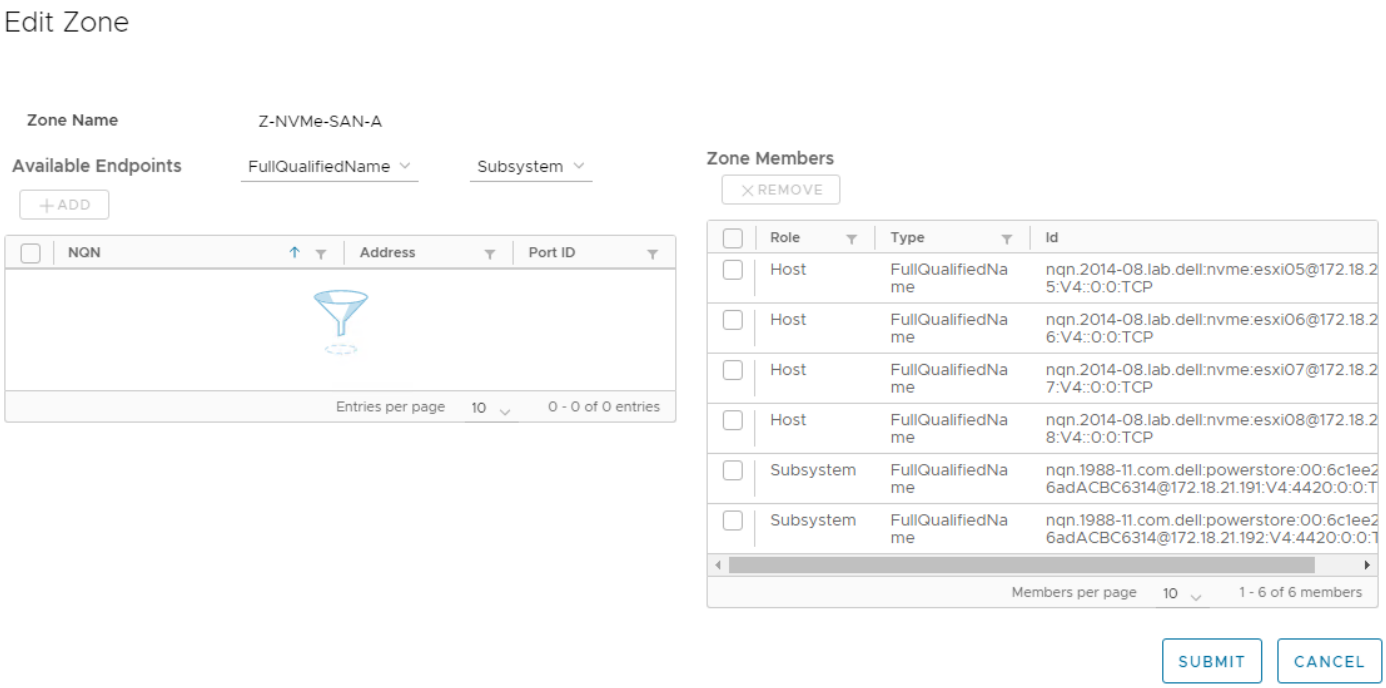


Figure 148. View Zone members

13. Click **SUBMIT**.
    The **Success** message displays, and the state of the zone group is **NotActive**.

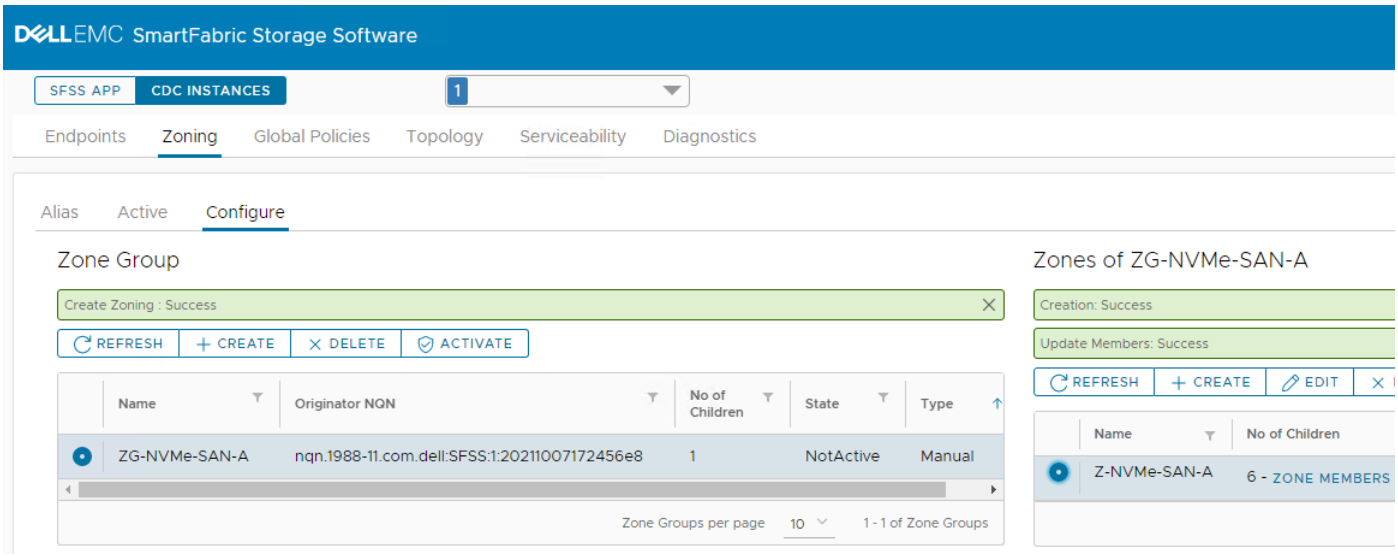


Figure 149. Zones in Instance 1

Activate Zone Group

This section lists the steps needed to activate a Zone Group.

1. Select the **Instance**. In this example, **Instance 1** is selected.
2. Click to select the radio button next to the zone group. This example uses **ZG-NVMe-SAN-A**.
3. Click **ACTIVATE**.

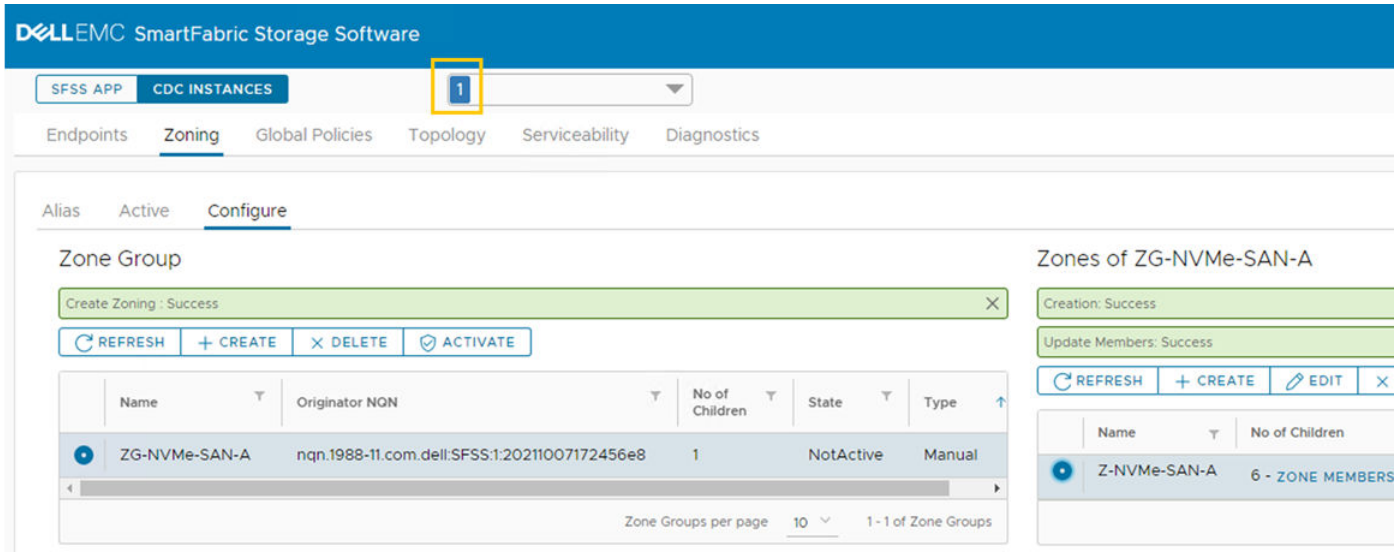


Figure 150. Select zone group

4. In the dialog box that opens, click **ACTIVATE**.

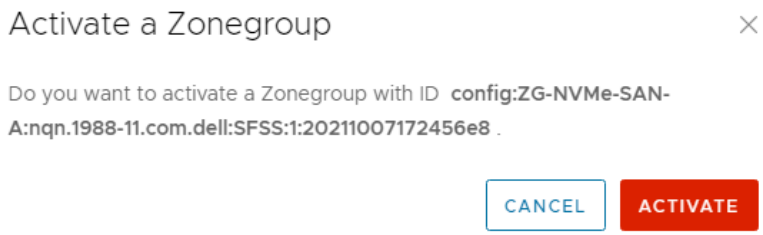


Figure 151. Activate a Zonegroup screen

The **Success** message displays, and the **Status** changes to **Active**.

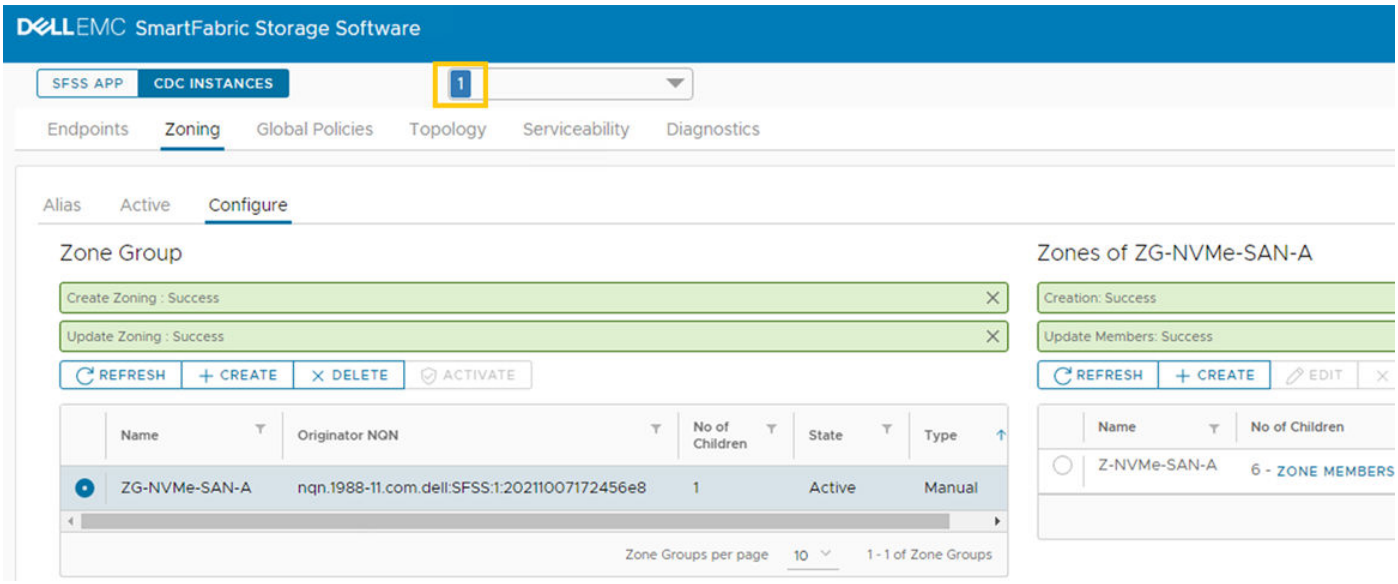


Figure 152. Active Zone Group

The **State** of the zone group shows as **Active**.

NOTE: Any future changes to zoning will require the Zone Group to be reactivated.

Verify host zoning

To verify that zoning is configured, and to verify the host access to subsystems after zoning, perform the following steps:

1. Click **CDC INSTANCES** > **Endpoints**.
2. Select a host that was added as a zone member.
3. Expand the **Allowed Subsystems** listing in the right panel.

   NOTE: Both Subsystems registered are accessible.

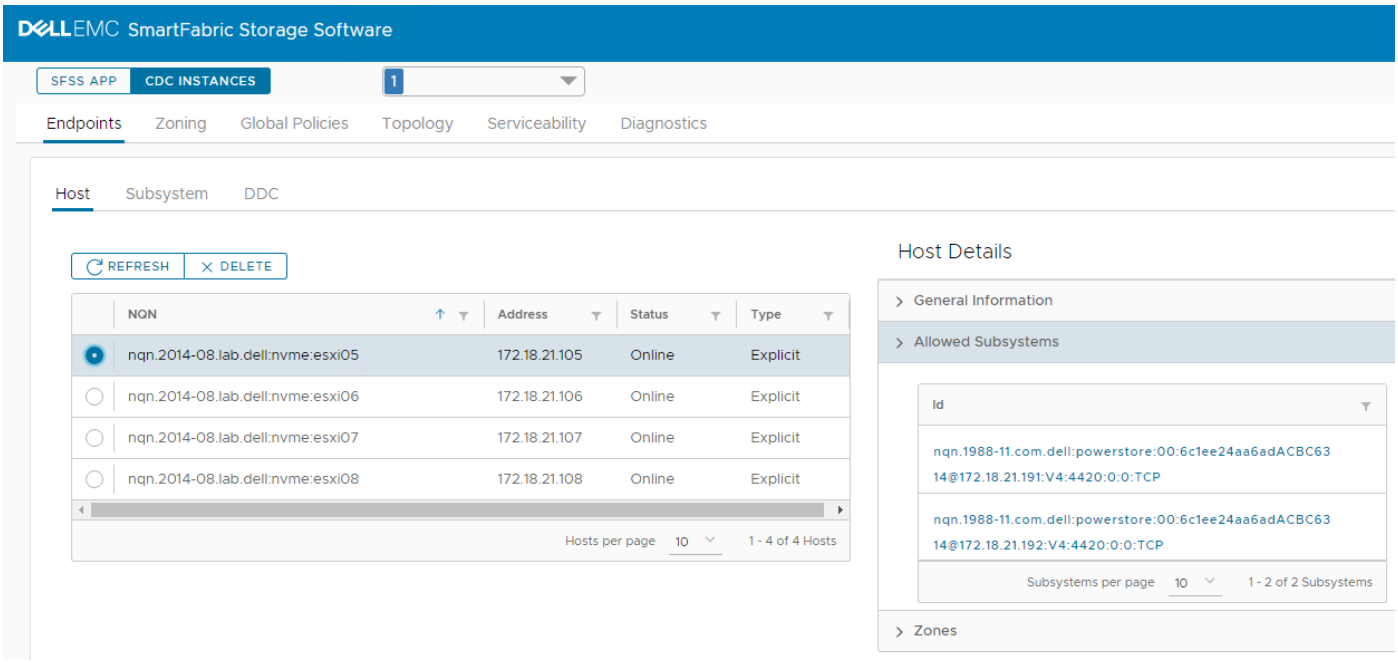


Figure 153. Verify allowed Subsystem

4. Click the NQN of a subsystem in the **Allowed Subsystems** list for more information regarding that Subsystem.

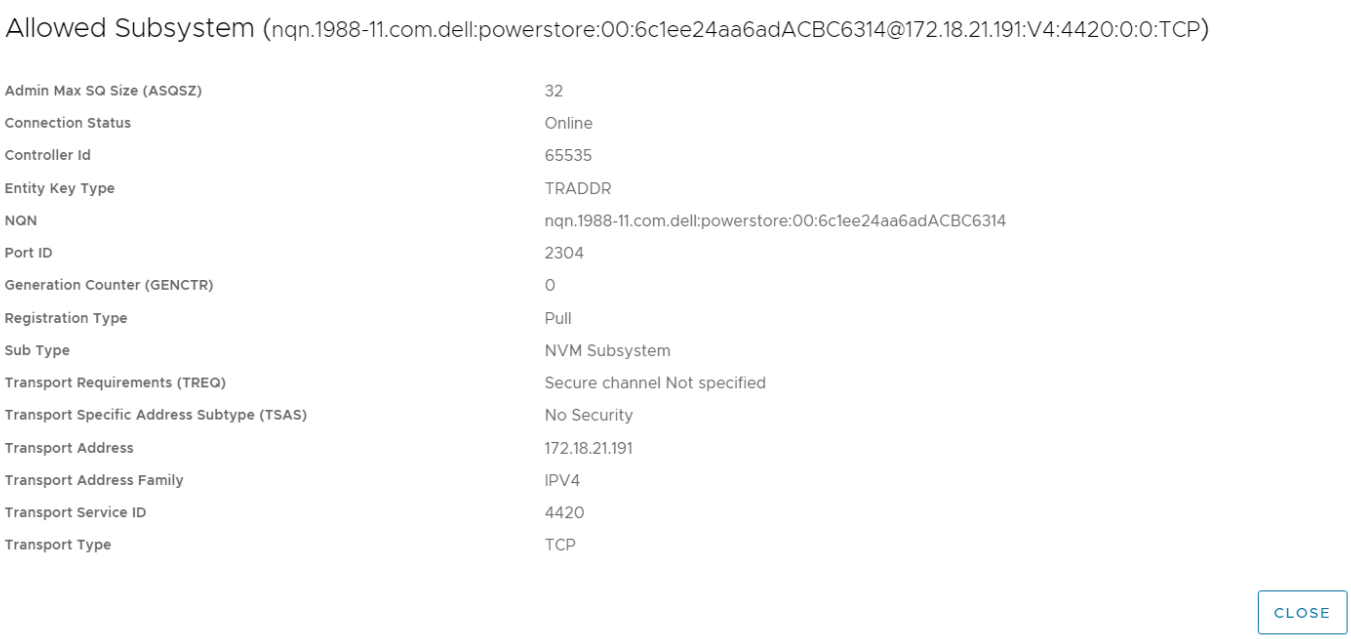


Figure 154. Allowed Subsystem confirmation screen

5. Click **CLOSE** to exit.
6. Expand the **Zones** section in the right navigation pane. The zone membership displays.

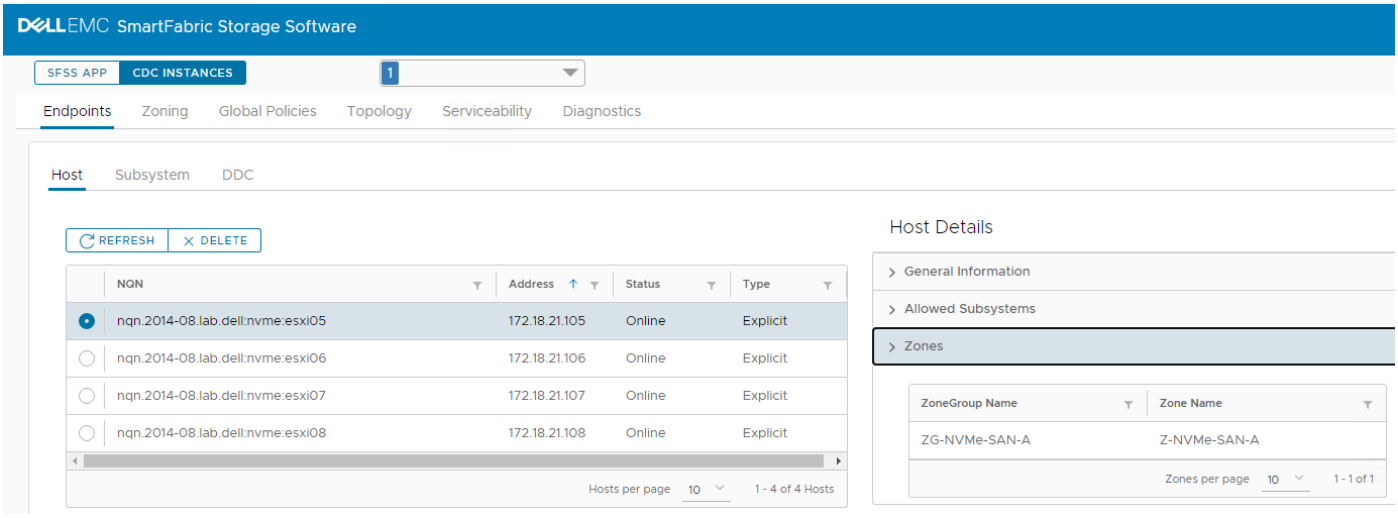


Figure 155. Host Zone membership

NOTE: If a host is selected that is not a zone member, **Allowed Subsystems** and **Zones** will not show in the **Host Details** pane.

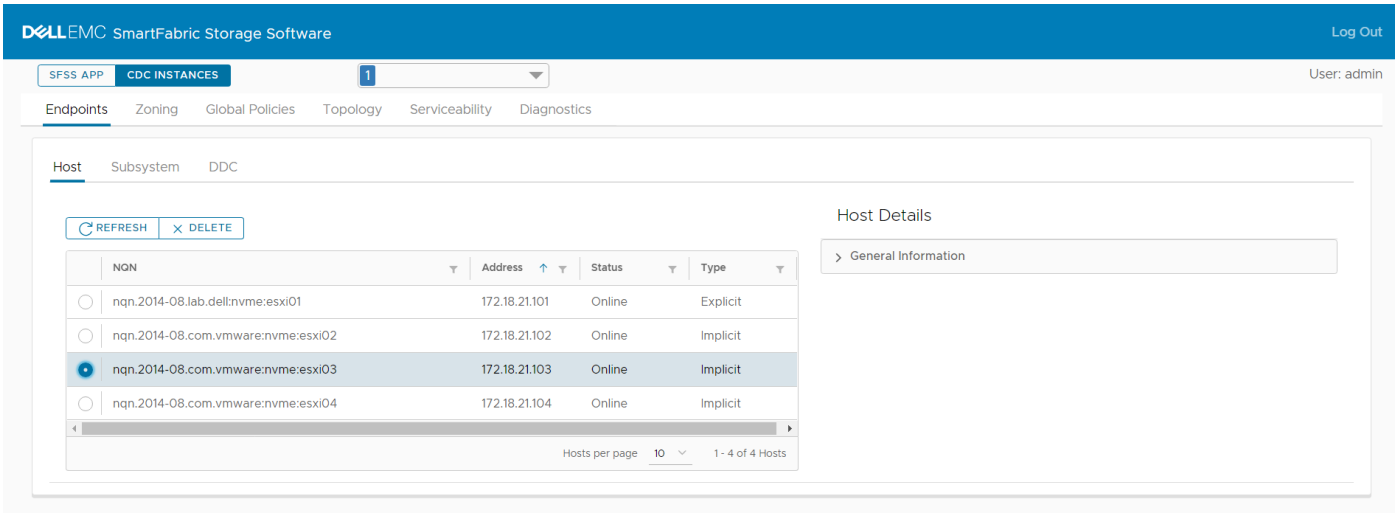


Figure 156. Example of a host that is not zoned

Repeat zoning configuration for SAN B

The following steps detail the steps in creating a zone for Endpoints in SAN A. In this example, Zone **Z-NVMe-SAN-A** is in Zone Group **ZG-NVMe-SAN-A** in CDC Instance **2**.

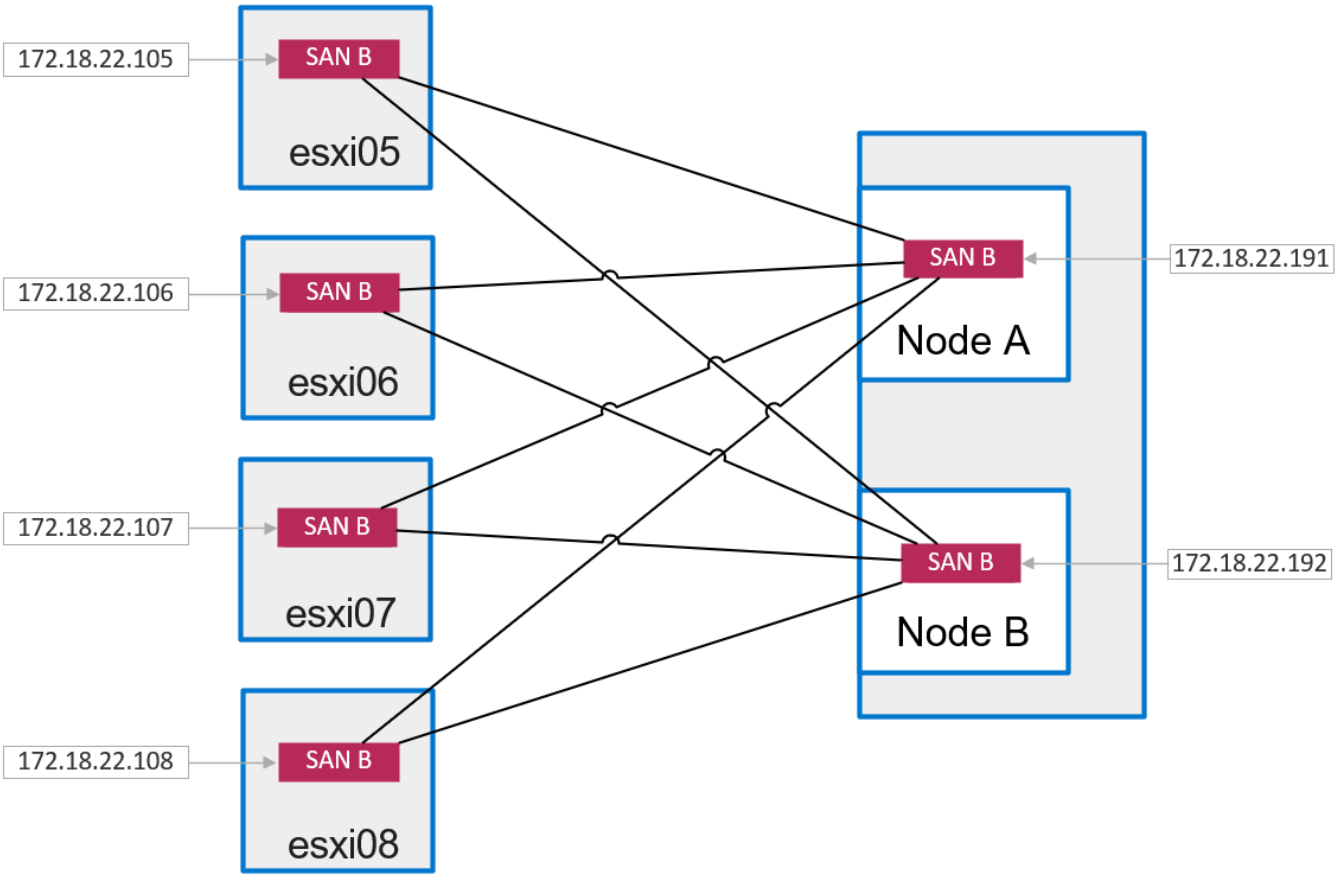


Figure 157. Zone B - Z-NVMe-SAN-B

1. Repeat the steps to create additional Zone Groups. For this example, in **CDC Instance 2,** Zone Group **ZG-NVMe-SAN-B** was created by following the steps. Once complete, the **Zone Group** for **Instance 2** displays.

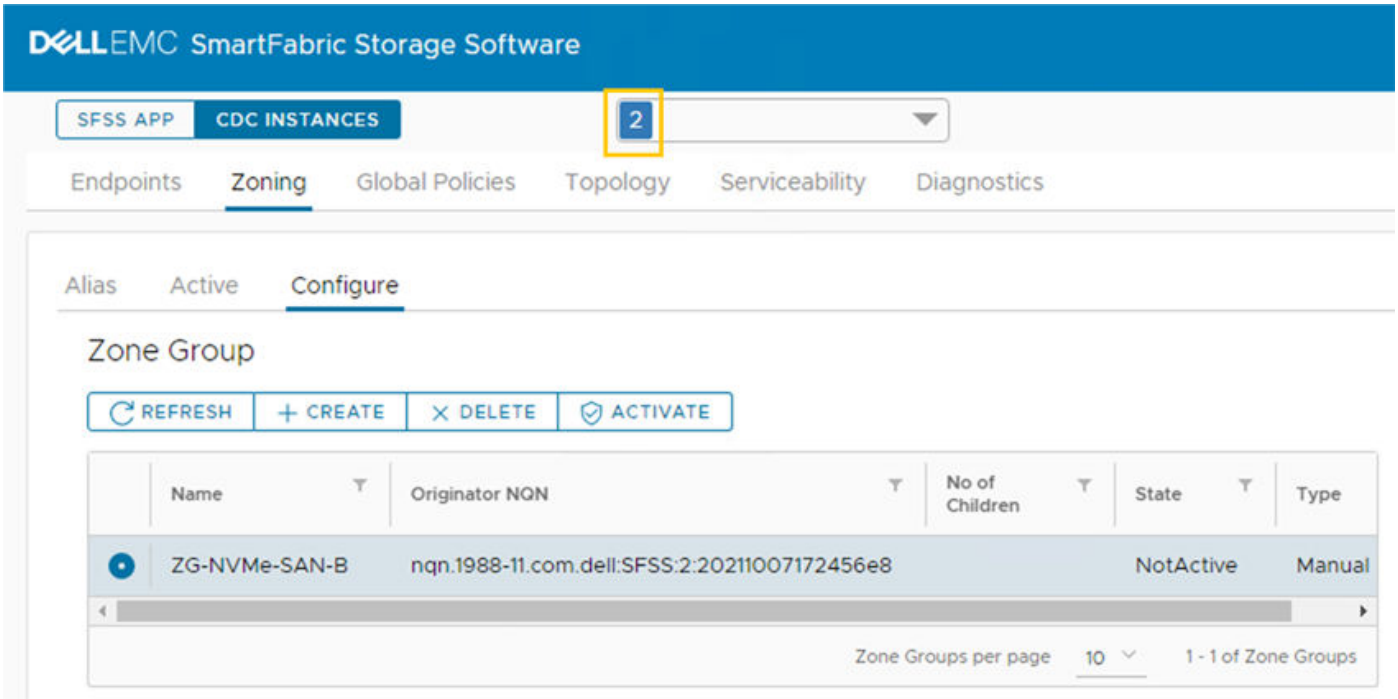


Figure 158. CDC Instances Zoning Configuration screen

2. Repeat the steps to create additional Zones. In this example, another Zone is created for SAN-B (network 172.18.22.0) using the following details:
   a. Select **CDC Instance 2**.
   b. Select the **ZG-NVMe-SAN-B** radio button.
   c. Under **Zones** of **ZG-NVMe-SAN-B**, click **CREATE**.
   d. Provide the zone name **Z-NVMe-SAN-B**.
   e. Click **SUBMIT**. The new zone displays under the **Zones** of **ZG-NVMe-SAN-B**.
   f. Click the radio button next to the new zone.
   g. Click **EDIT**.
   h. From the drop-down menu, select **FullQualifiedName**.
   i. Select all SAN B hosts.
   j. Click **+ADD**. All the selected hosts are added to the zone members list.
   k. Change the **Type** to **Subsystem**.
   l. Select both subsystems for SAN-B (network 172.18.22.0).
   m. Click **ADD**. The hosts and subsystems display in the zone members list.
   n. Click **SUBMIT**.

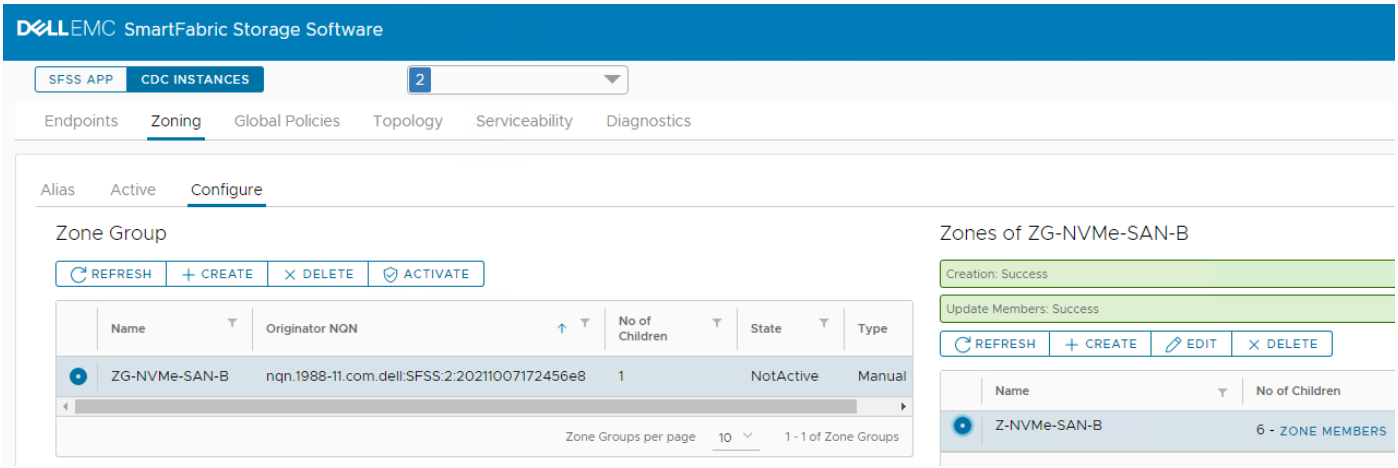


Figure 159. Zone Group and Zone with members created in CDC Instance 2

3. Click the radio button next to **ZG-NVMe-SAN-B,** click **Activate,** and click **Activate** again.

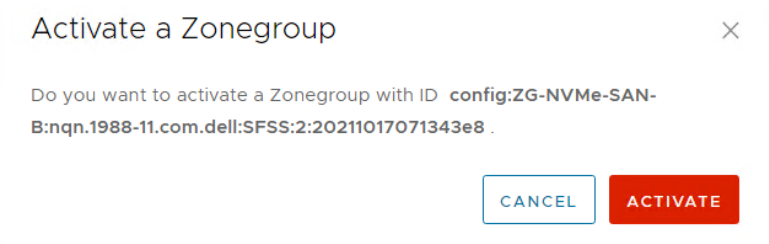


Figure 160. Activate SAN B Zone

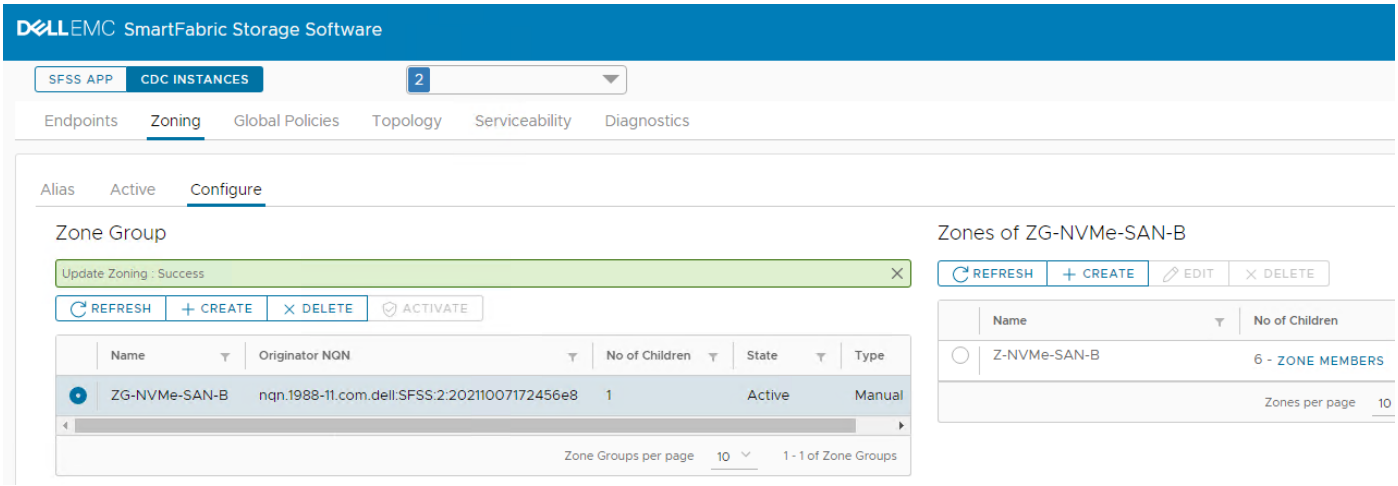


Figure 161. Zone B Activated

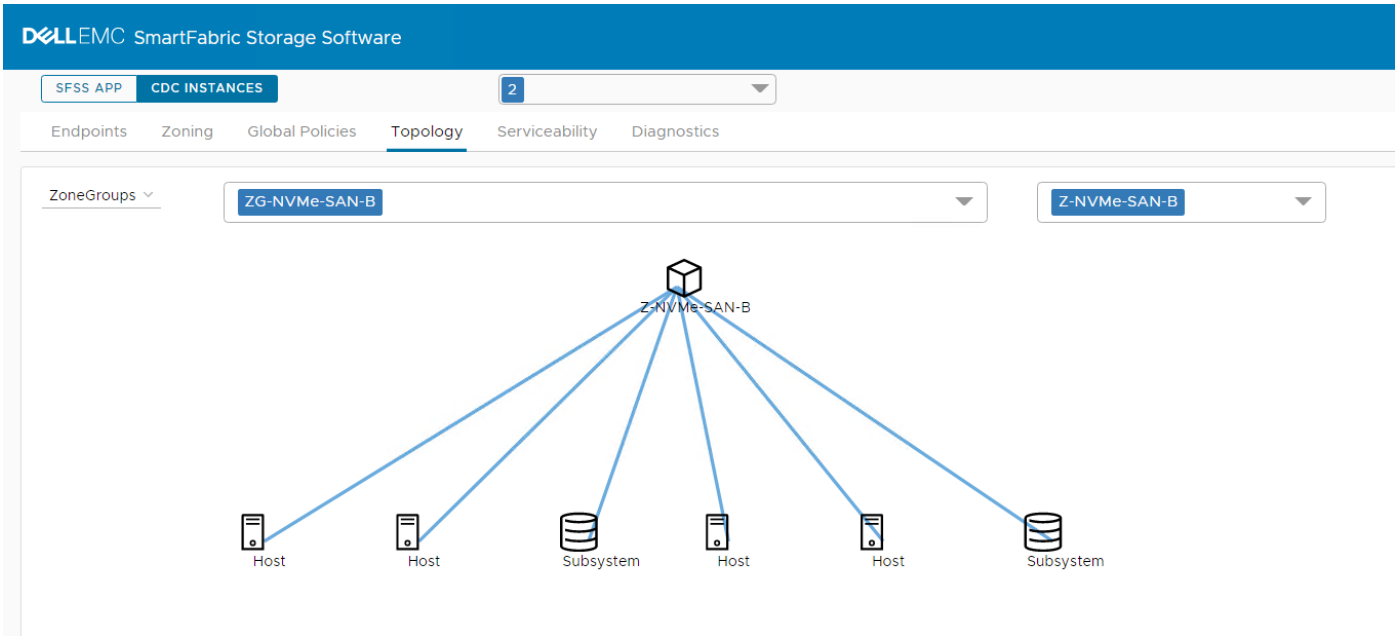


Figure 162. Zone B Topology

Establish NVMe/TCP between Endpoints

The steps provided in this section help in establishing NVMe/TCP between Endpoints.

Add zoned hosts to PowerStore

1. Log in to the **PowerStore Manager**.
2. Click the **Compute** drop-down and select **Hosts and Host Groups**.

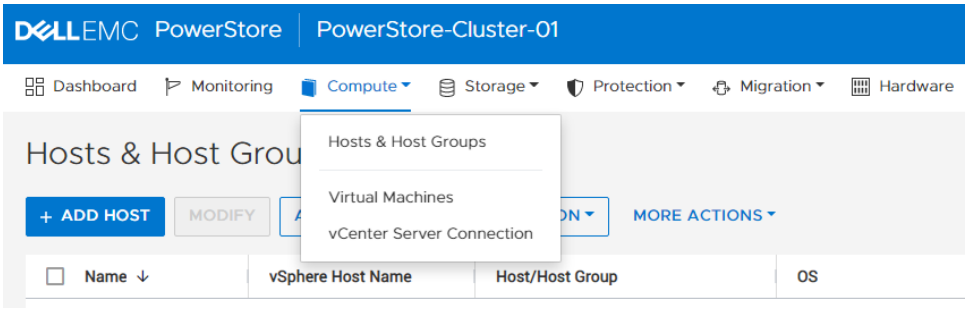


Figure 163. Add host

3. Click **ADD HOST**.
4. In the field provided, enter a **Host Friendly Name** for the host. In this example, the first initiator is **esxi05**.
5. Using the drop-down menu, select the operating system.

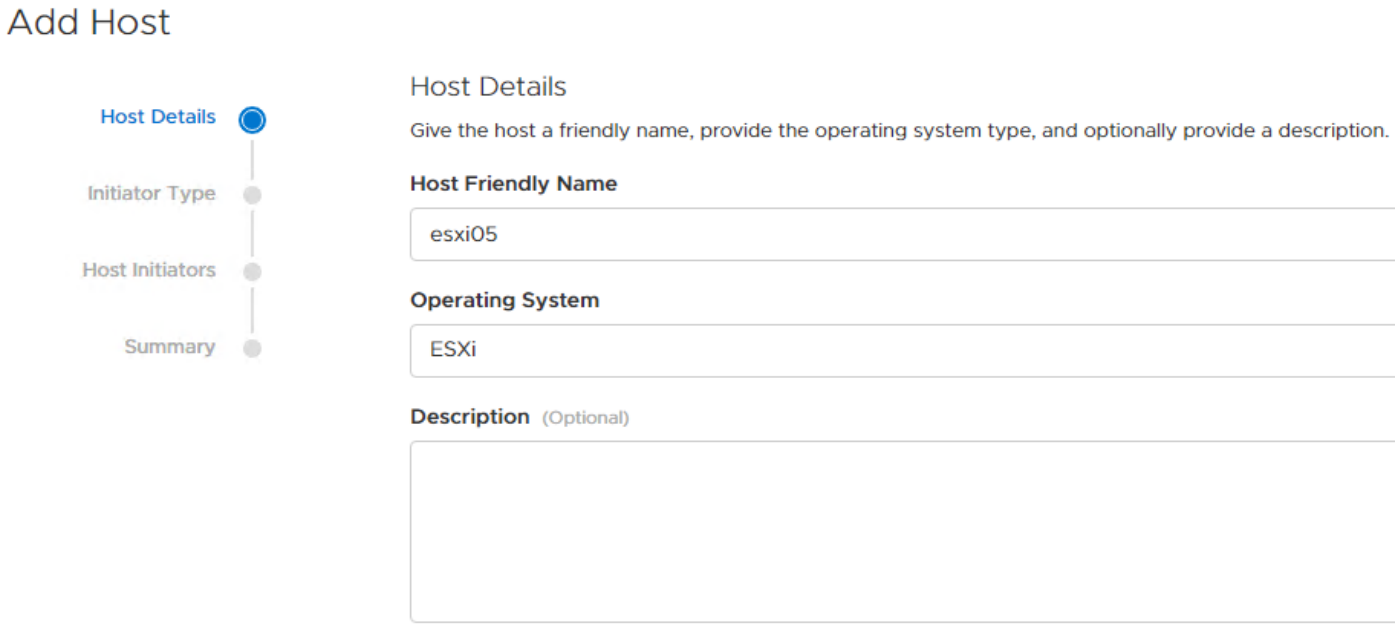


Figure 164. Add Host Details screen

6. Click **NEXT**.
7. Select the **Protocol Type** as NVMe and then click **NEXT**. The initiators are automatically discovered.

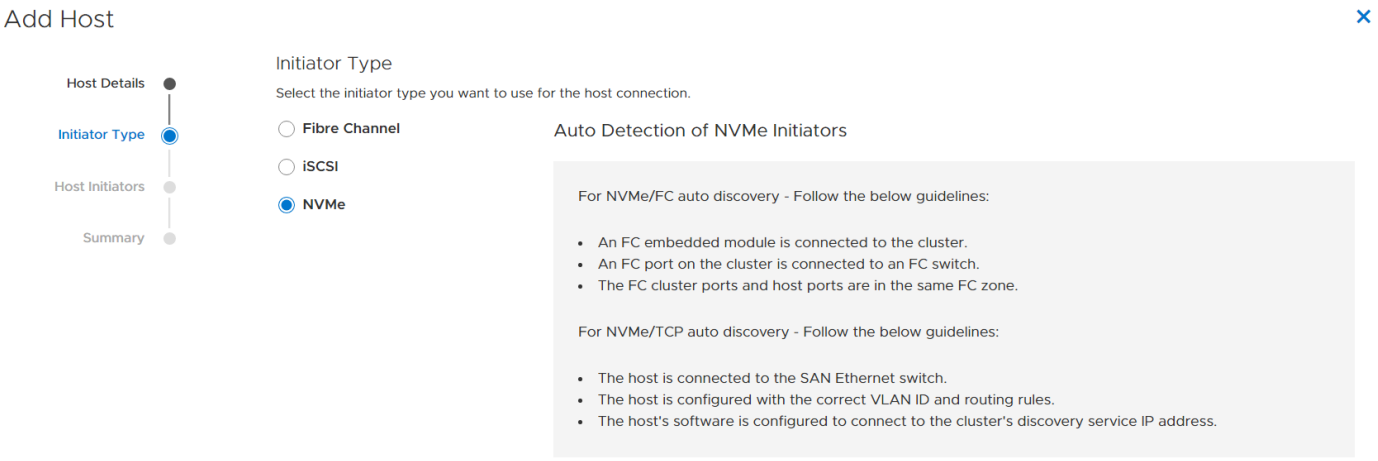


Figure 165. Select protocol type as NVMe

8. Select the initiator for the new host. In this example, **esxi05 only** is used.

NOTE: Add one initiator per host instance. In this example, the host initiators for hosts esxi05 through esxi08 are listed since the controllers were added to the NVMe/TCP storage adapters on the ESXi host esxi05 through esxi08 and were automatically discovered.

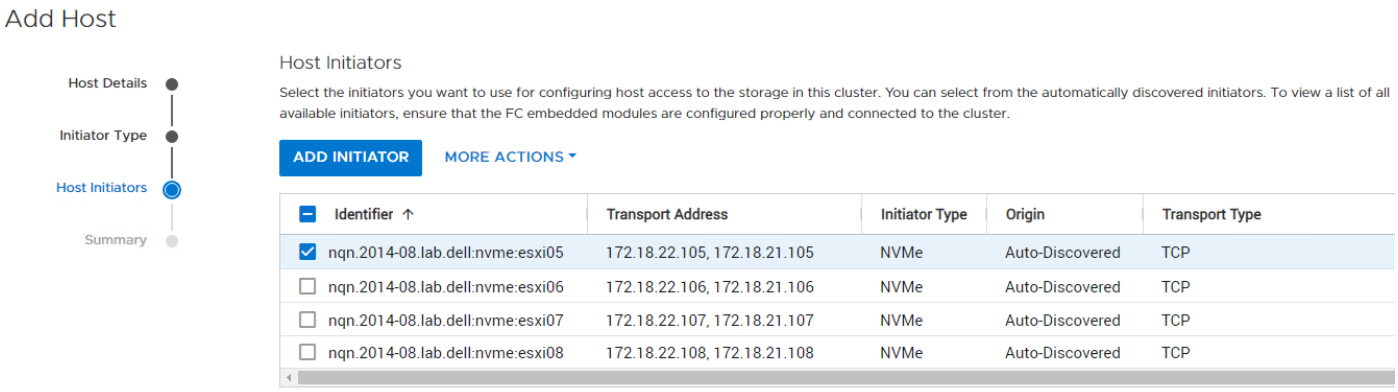


Figure 166. Add host initiator

9. Review the host details and click the **ADD HOST** button.

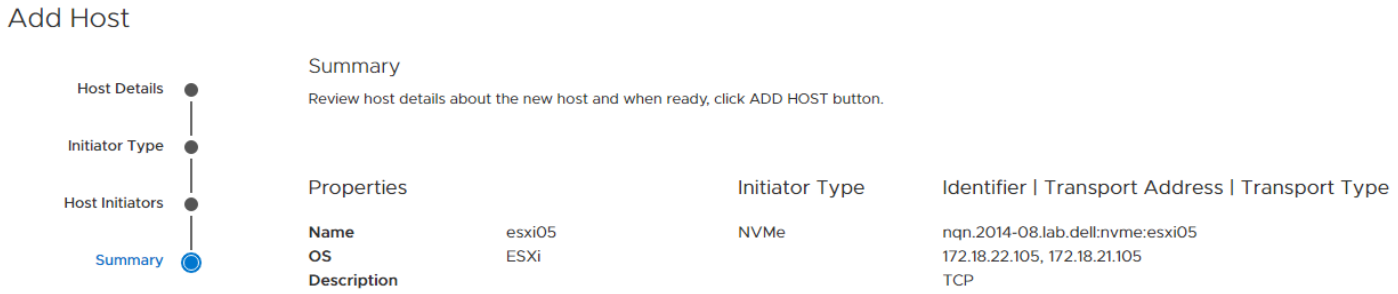


Figure 167. Review Host Details and add host

NOTE: Both of the host NVMe/TCP IP addresses are listed as the host can access storage using SAN A and SAN B.

10. Observe the host in **Hosts & Host Groups**.

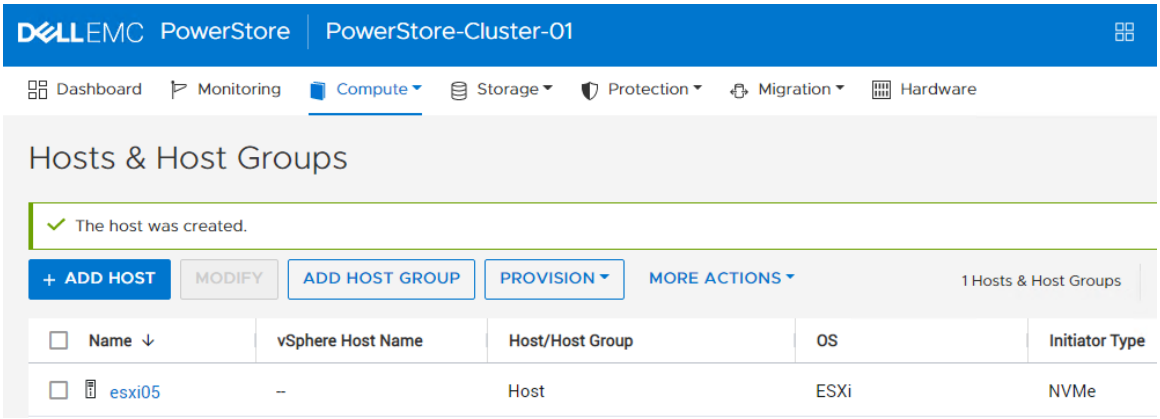


Figure 168. Host & Host Groups screen

11. Repeat the steps in this section to add more hosts. In this example, **esxi06, esxi07,** and **esxi08** are added. The following image shows all four hosts.

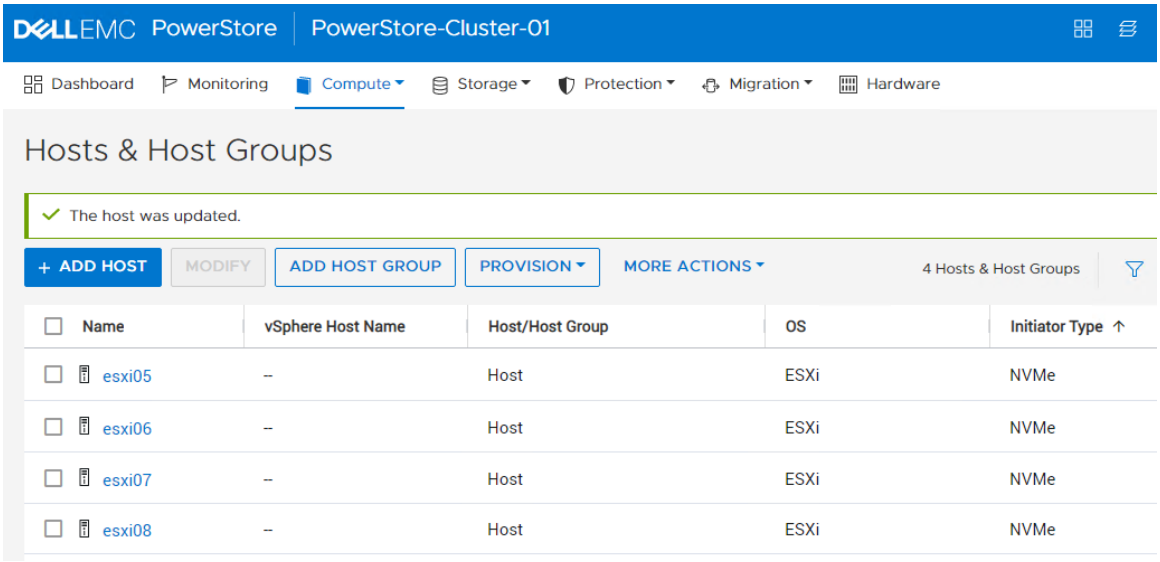


Figure 169. Hosts & Host Groups added in PowerStore

Verify Storage Adapter Controllers in vSphere

Hosts NVMe/TCP storage adapters, or vmhba, are now able to access the direct discovery controllers in PowerStore. Verify this using the following steps.

1. Log in to vSphere.
2. Select a host. For this example, **esxi05** is selected.
3. Click **Configure** > **Storage** > **Storage Adapters**.
4. Click the radio button next to the vmhba adapter. In this example, **vmhba64** is selected.
5. Select **Controllers**. **Note**: Click **REFRESH** to see the controllers if they are not initially listed.

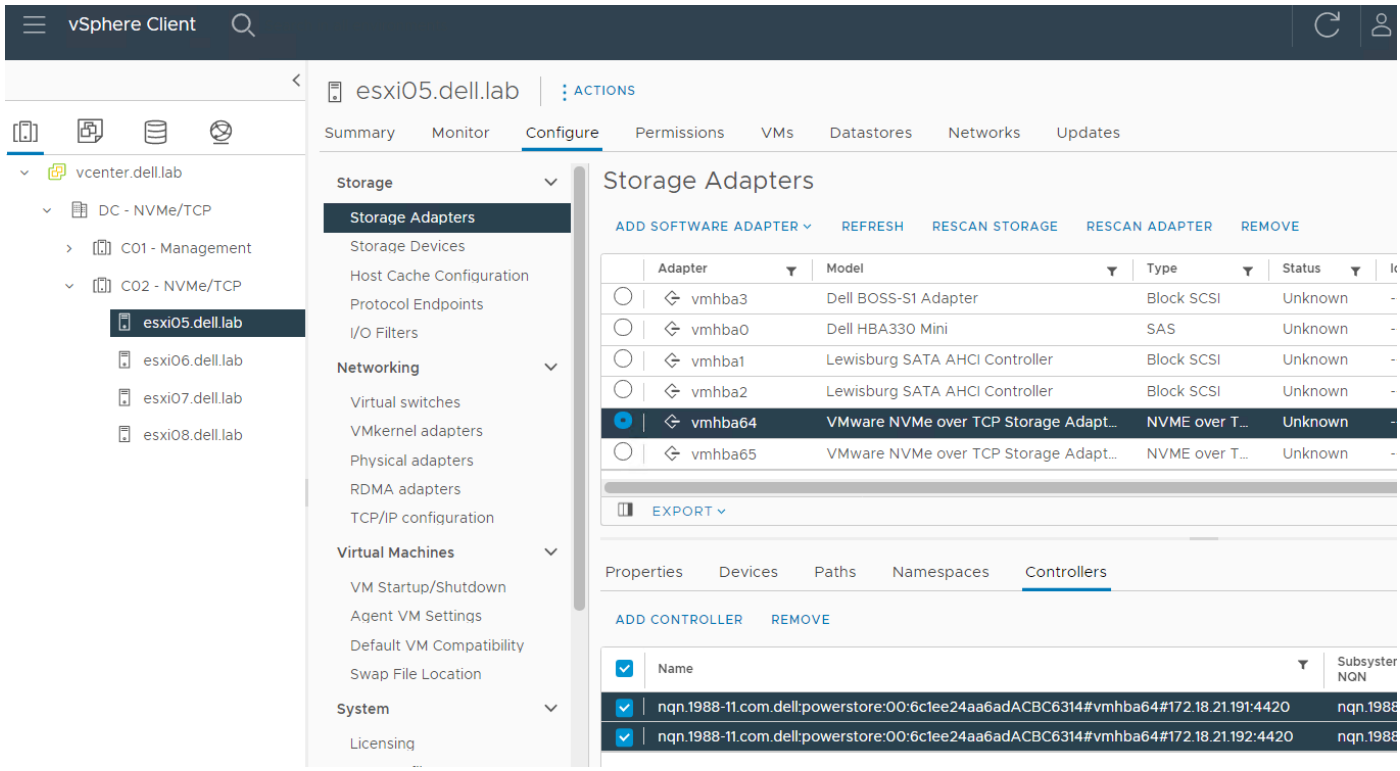


Figure 170. Controllers added for vmhba64

6. Click the radio button beside the **vmhba65** adapter.

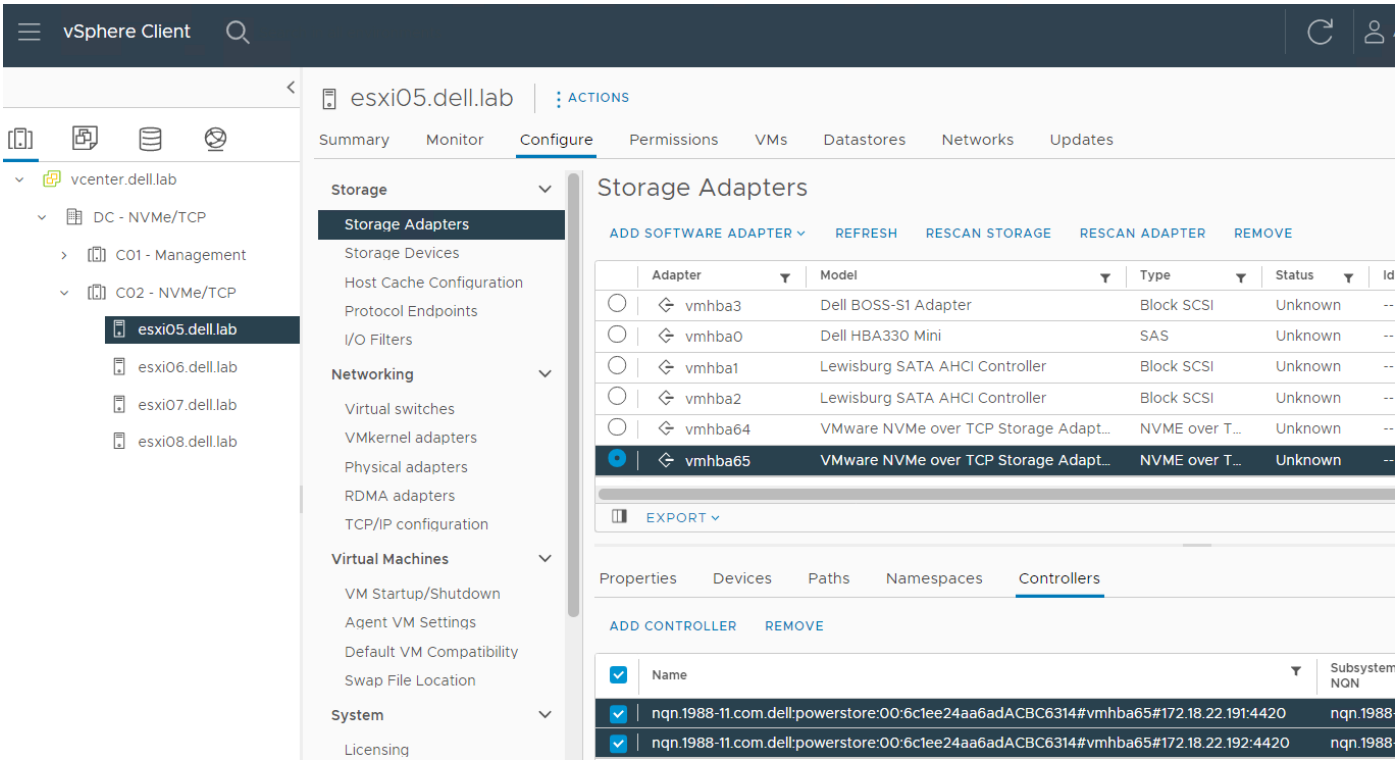


Figure 171. Controllers added for vmhba65

7. Repeat the steps in this section to verify the remaining vmhba adapters for the remaining hosts. For this example, click each remaining host (esxi06, esxi07, and esxi08) and verify controllers for vmhba64 and vmhba65.

Create volume groups in PowerStore

To create the volume groups in PowerStore, perform the following steps:

1. Log in to **PowerStore Manager**.
2. Click **Storage** > **Volume Groups**.

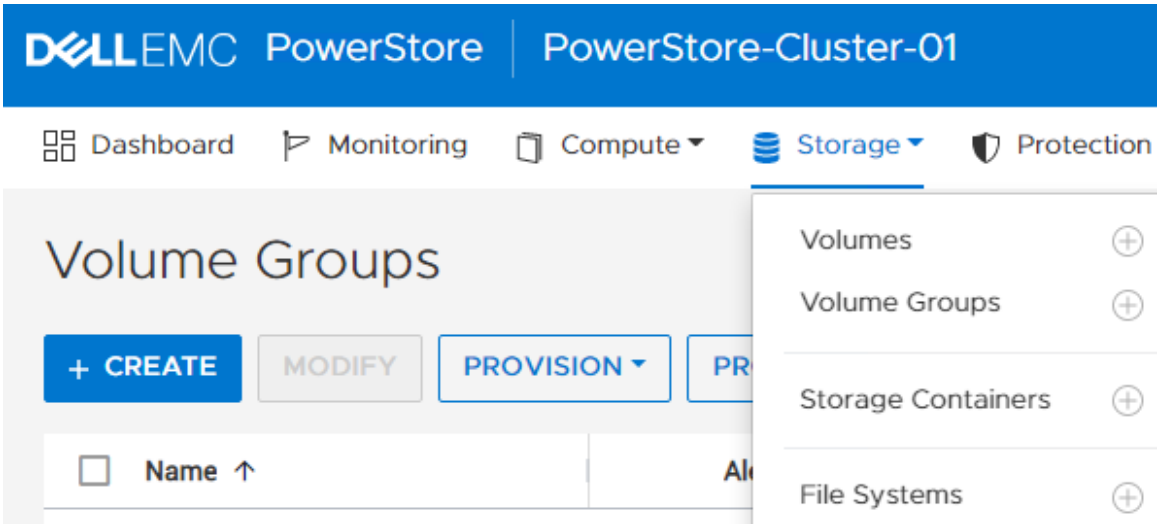


Figure 172. Volume Groups selection screen

3. Click **CREATE**.
4. In the **Name** field, provide a name for the volume group. This example uses **VG1-NVMe**.

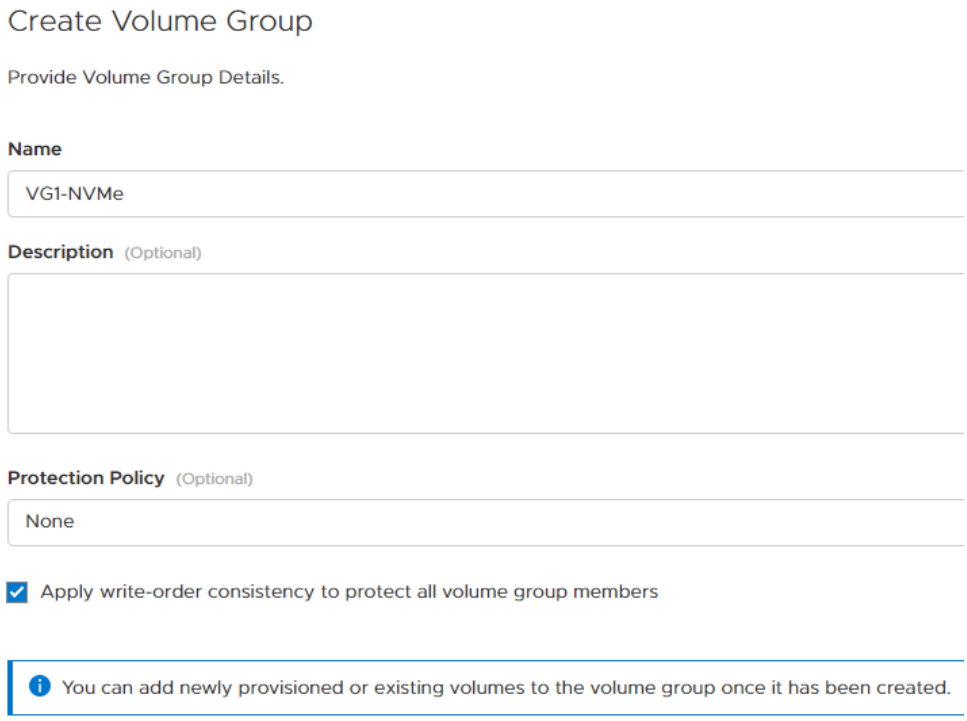


Figure 173. Provide Volume Group details

5. Click **CREATE**.

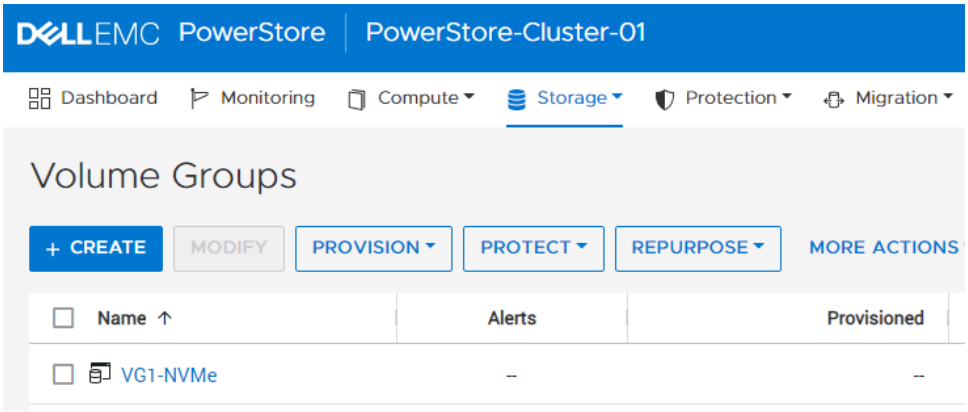


Figure 174. Created Volume Groups

Create volume

To create the volume, perform the following steps:

1. Click **Storage** > **Volumes** > **CREATE**.

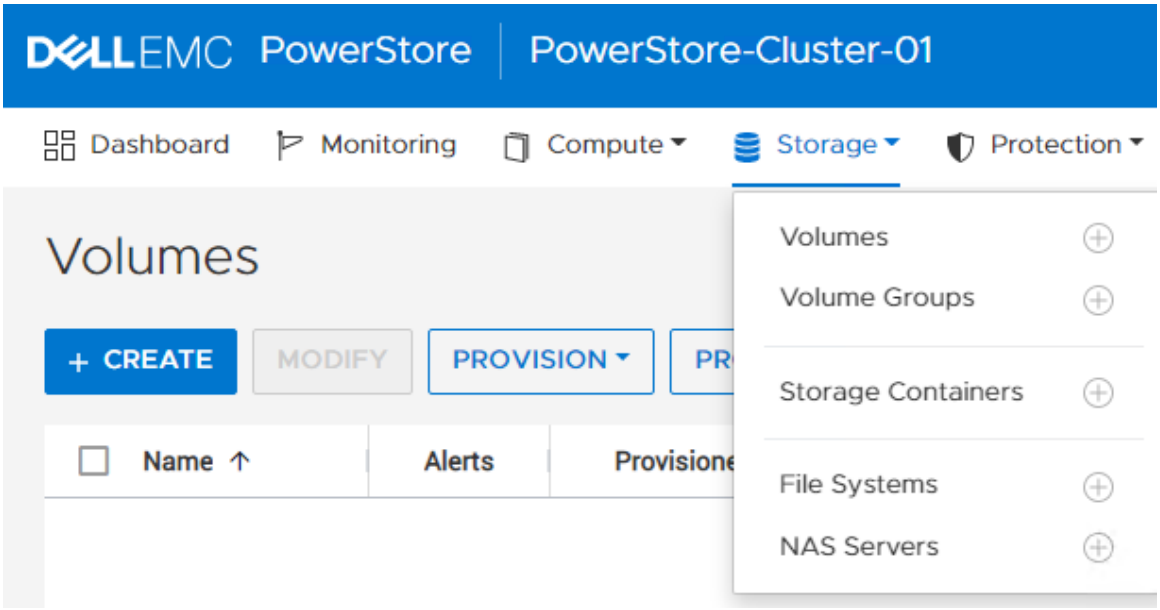


Figure 175. Create Volume

2. Provide a **Name.** This example uses **V1-NVMe**.
3. Select a **Category** and **Application**, as applicable. In this example, **Other** is selected.
4. Provide **Quantity** and **Size.** In this example, Quantity is **1,** and Size is **500 GB.**
5. Under **Additional properties,** for the **Associated Volume Group,** click **SELECT**.
6. Choose the **Volume Group** that was created.
7. Click **SELECT.**

NOTE: Other settings are left at their defaults.

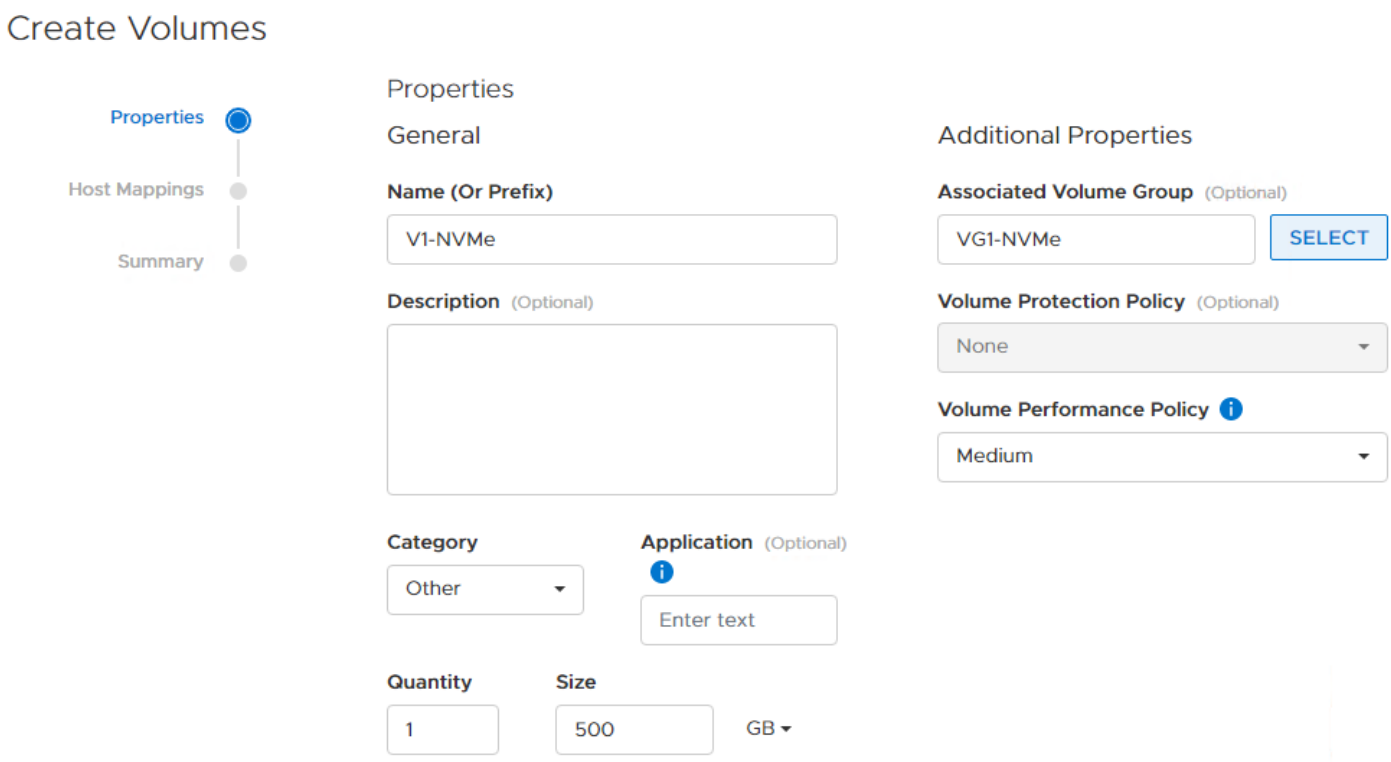


Figure 176. Create Volumes Properties screen

8. Click **NEXT**.
9. For the **Host Mappings**, select the **NVMe** radio button. Hosts are populated.

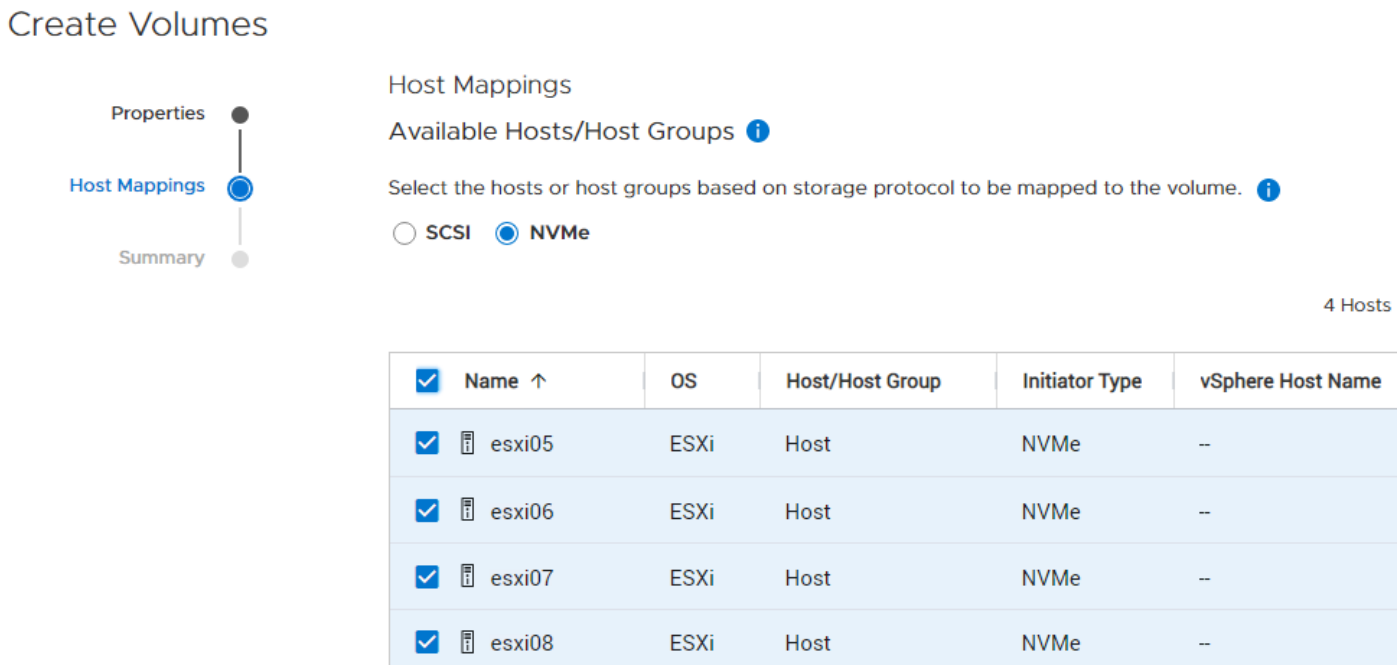


Figure 177. Select NVMe in Host Mappings

10. Click **NEXT**.
11. Review the selections and then click **CREATE**.

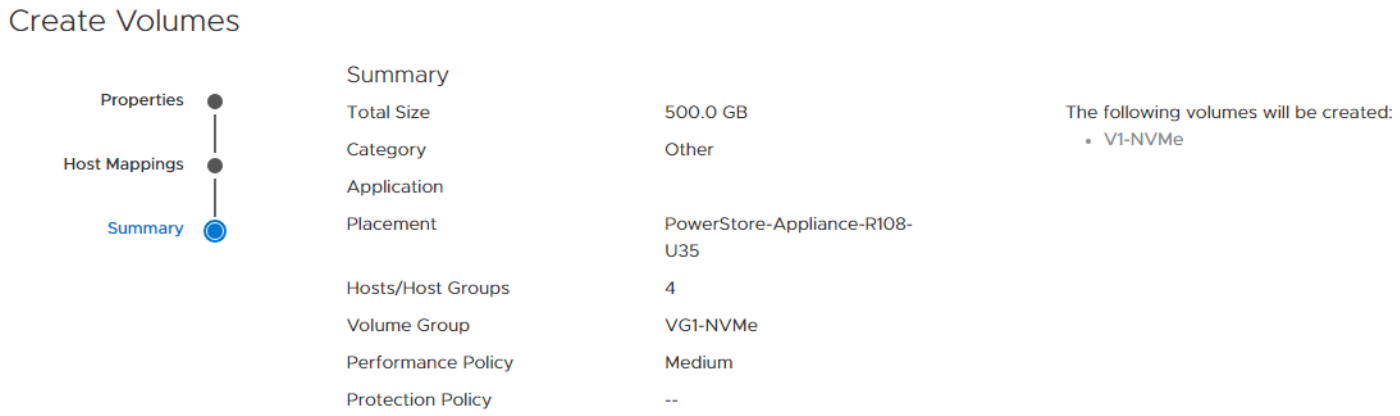


Figure 178. Review summary

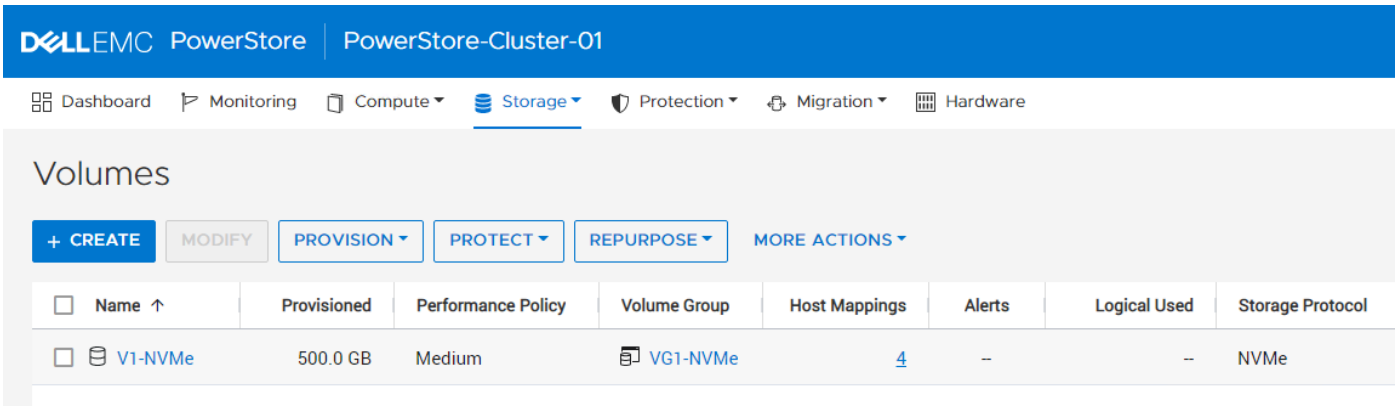


Figure 179. Created Volume

Create datastore for ESXi host

1. From the vSphere client, right-click the NVMe/TCP cluster.
2. Select **Storage** > **New Datastore**.

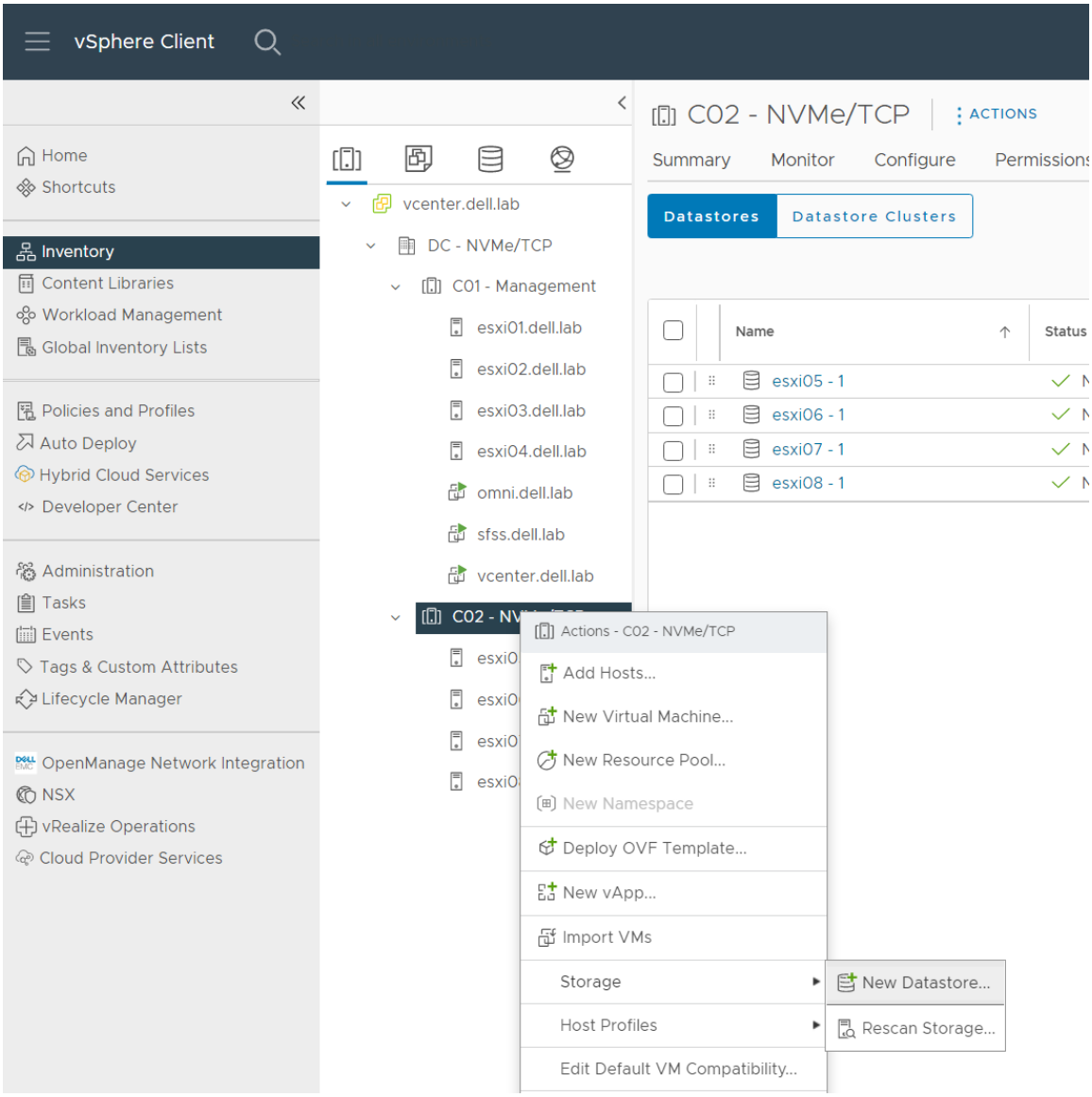


Figure 180. Select New Datastore

3. Select the datastore type. In this example, **VMFS** is selected.
4. Click **NEXT**.

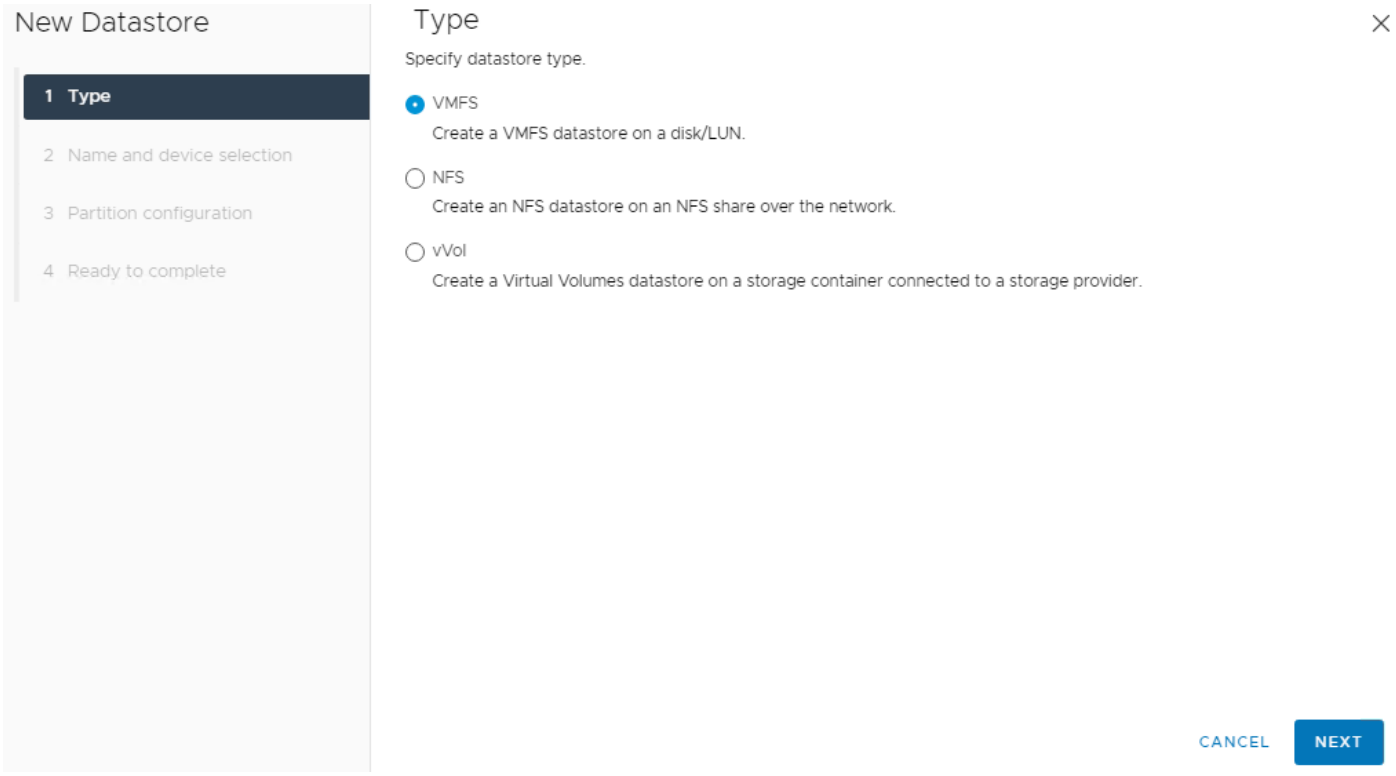


Figure 181. Specify datastore type

5. Provide a **name** and select the **LUN** for provisioning the datastore. In this example, the **NVMe TCP Disk** on PowerStore is selected.
6. Select a host to view accessible LUNs. In this example, **esxi05** is selected.

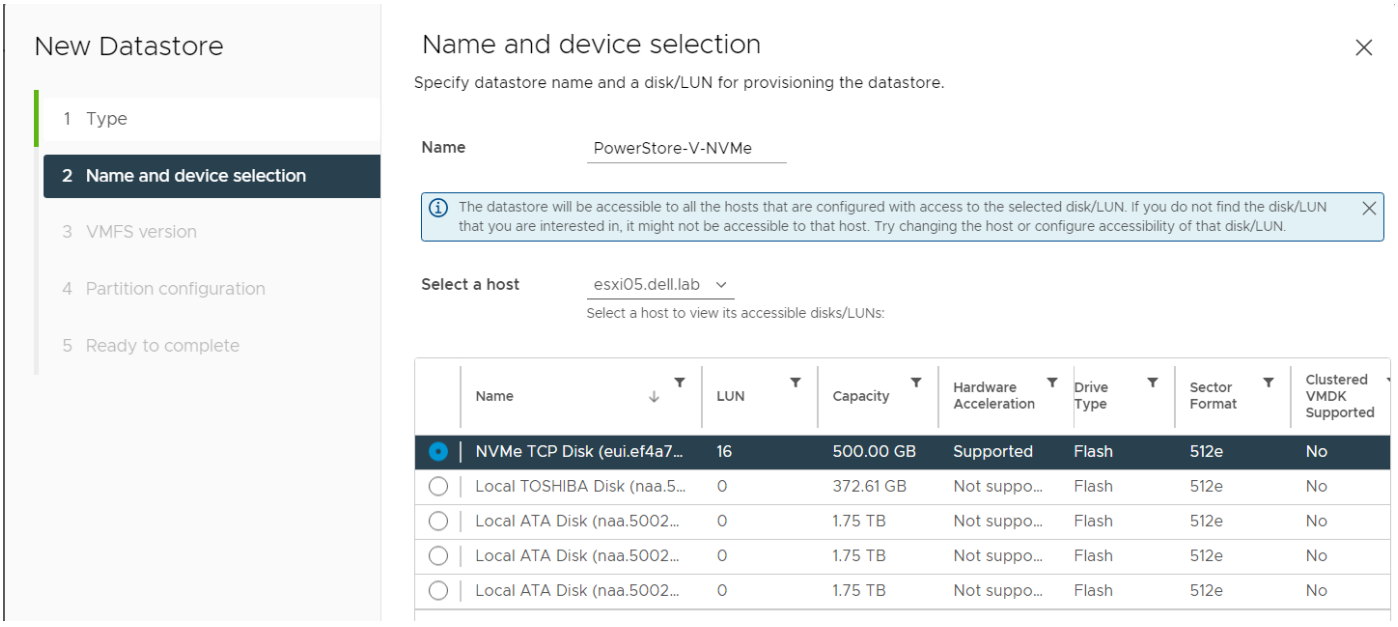


Figure 182. Select LUN

7. Click **NEXT**.
8. Specify the **VMFS** version for the datastore and then click **NEXT**.

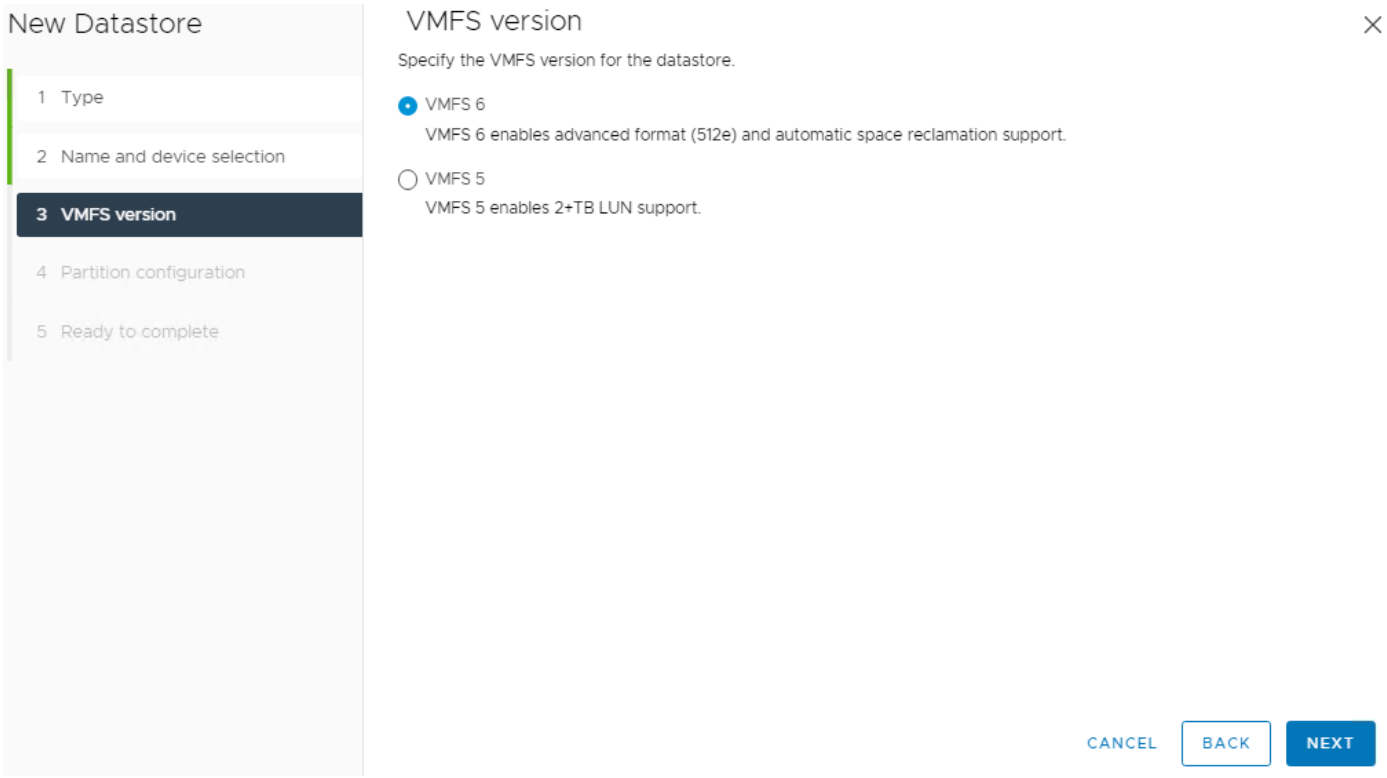


Figure 183. Select VMFS version

9. Review the disk layout and specify partition configuration details. In this example, the datastore size is specified as **500 GB**.

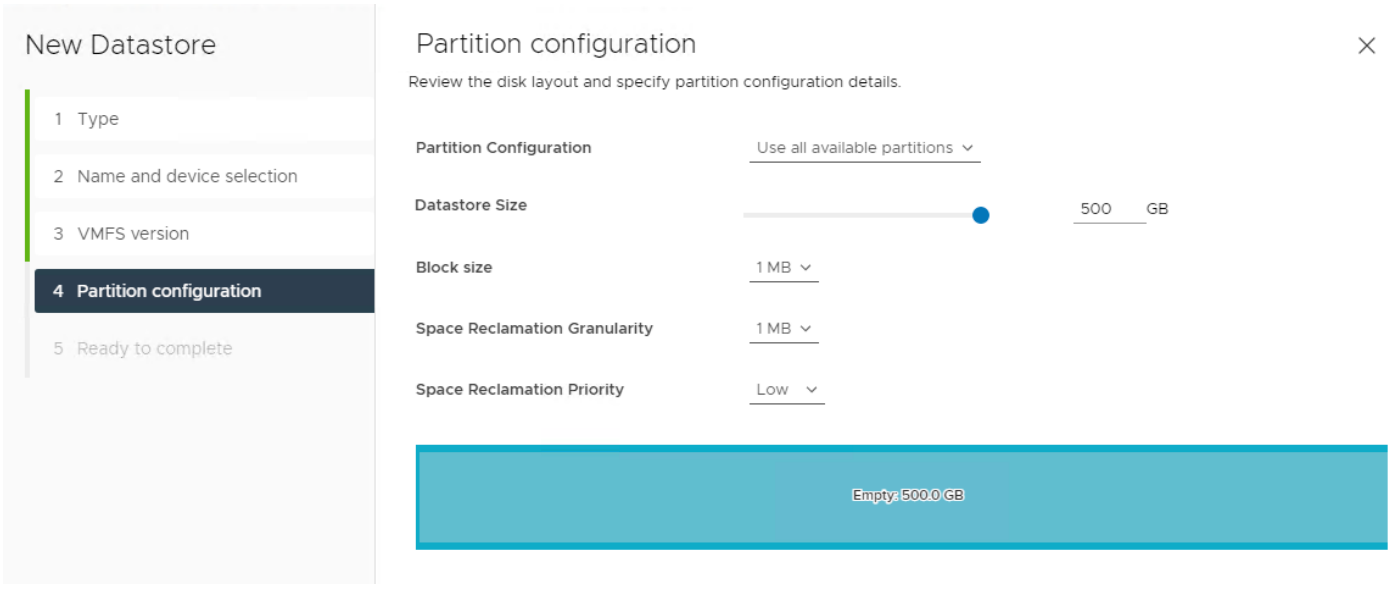


Figure 184. Provide partition configuration details

10. Click **NEXT**.
11. Review the settings and click **FINISH**.

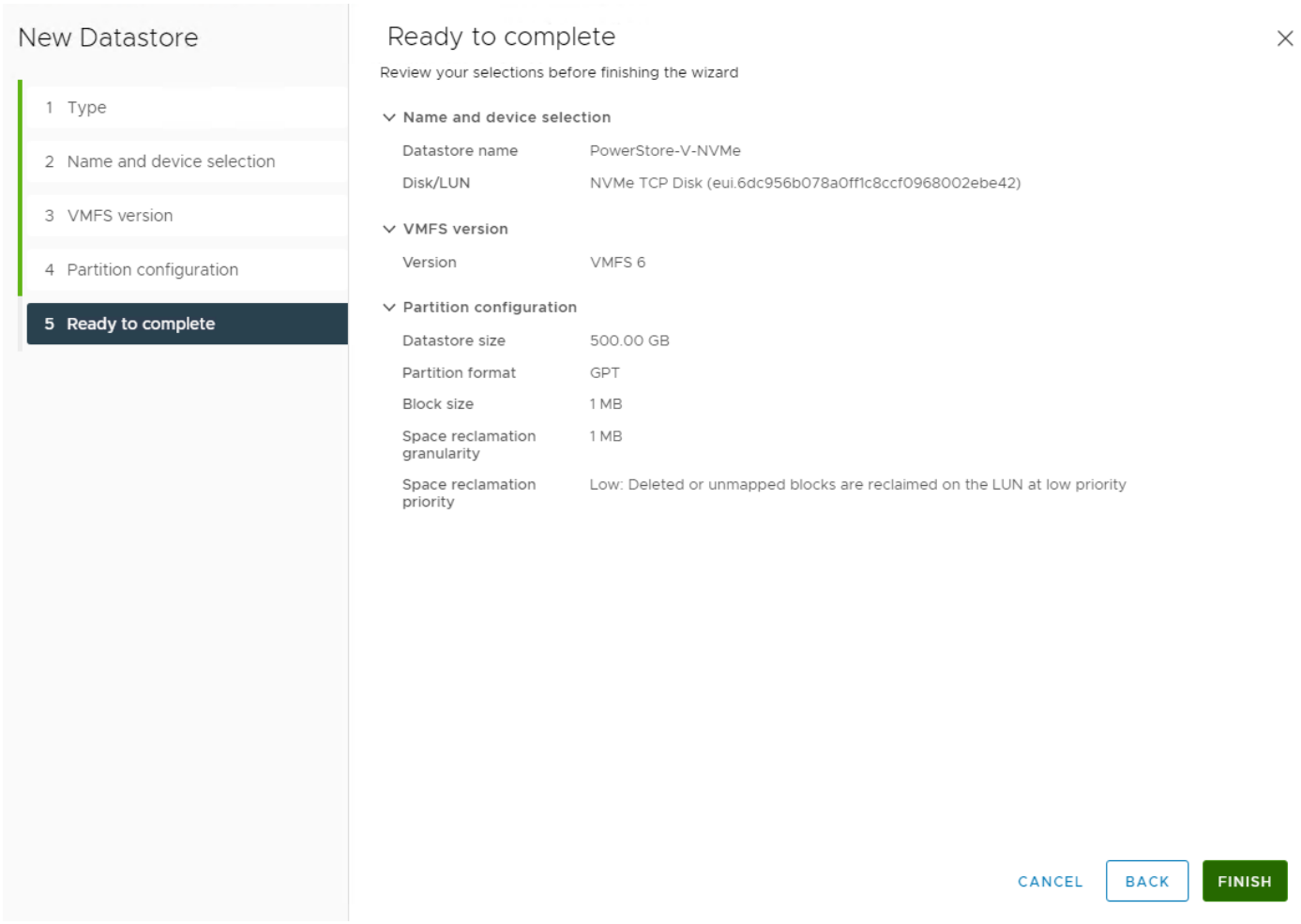


Figure 185. Review settings

12. Verify the datastore that was newly created. From **Inventory**, click **Datastores** and select the new datastore. In this example **PowerStore-V-NVMe** is selected.
13. Click the **Configure** tab, and select **Connectivity and Multipathing**.

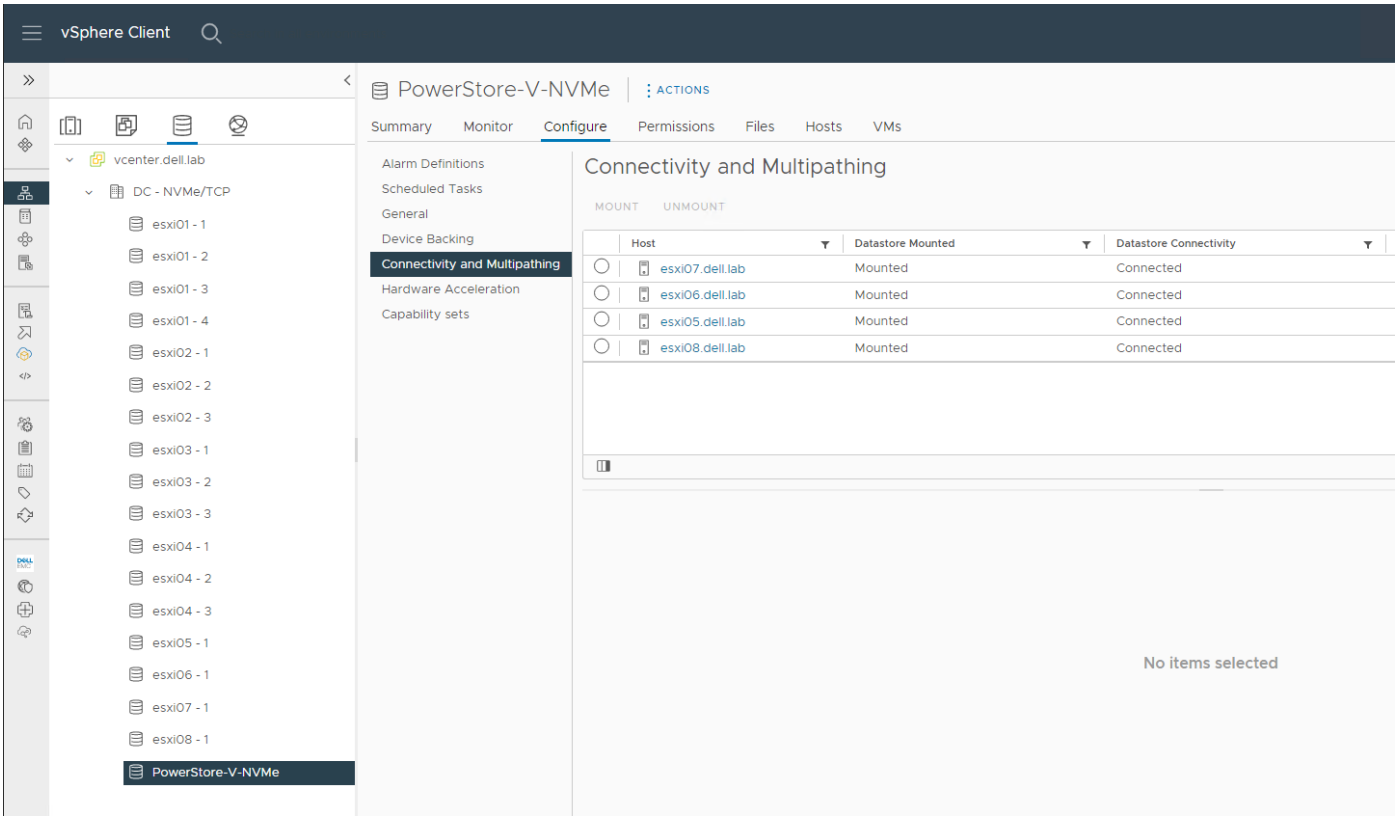


Figure 186. Verify created datastore

14. Right-click the host and click **Storage Adapters** if some of the hosts are not listed.
15. To verify that the new shared storage is accessible to other hosts in the cluster, select the host, go to **Storage Adapters,** and click **REFRESH**.

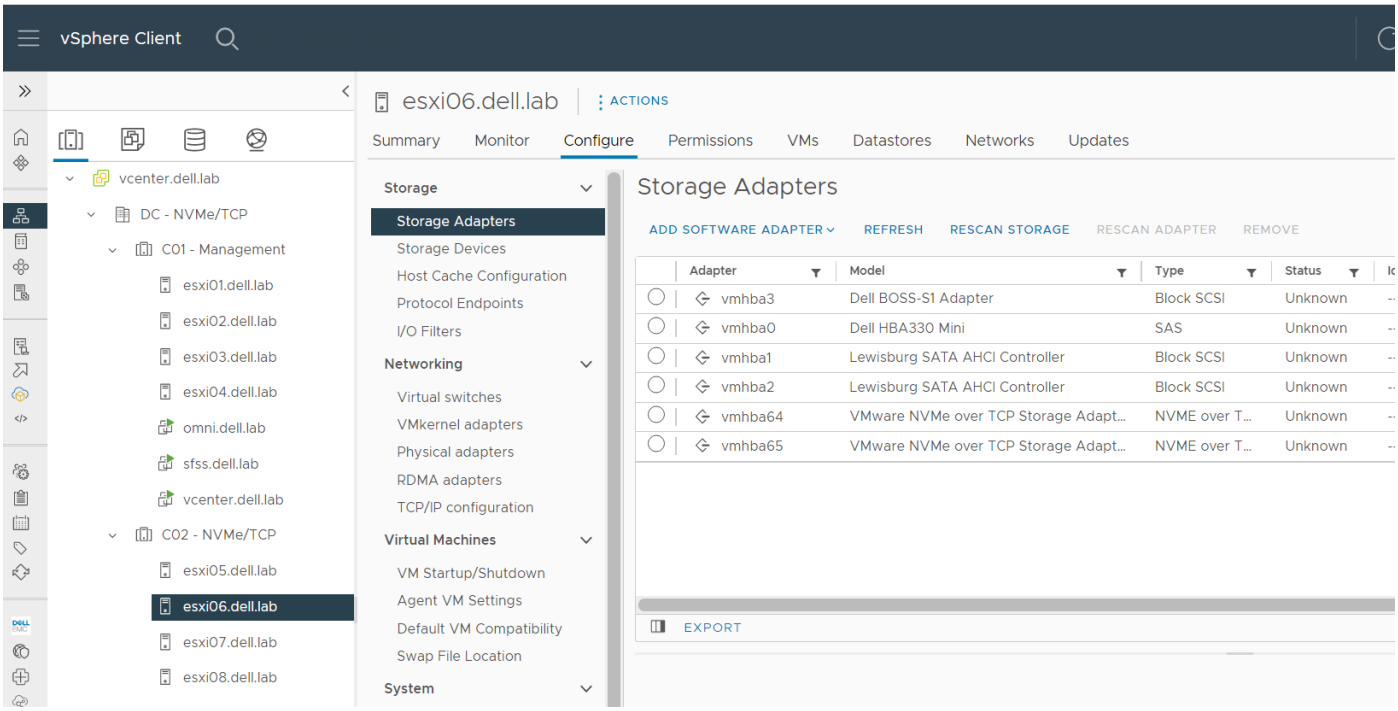


Figure 187. Refresh storage adapter

NVMe/TCP Storage is now ready for use by all hosts in the cluster.

A

Hardware and Software Used in this Guide

This section briefly describes the hardware used to validate the deployment examples in this Guide. Appendix B contains a detailed listing of hardware and software versions used.

PowerSwitch systems

Table 24. Switches and operating systems

Quantity	Item	Operating system version
2	PowerSwitch N3248TE-ON management switches	10.5.2.3
2	PowerSwitch S4148F-ON external switches	10.5.2.3
2	PowerSwitch S5232F-ON spine switches	10.5.2.3
4	PowerSwitch S5248F-ON leaf switches	10.5.2.3

Dell PowerSwitch N3248TE-ON

The Dell PowerSwitch N3248TE-ON is a 1U switch with 48x 1 GbE BASE-T ports, and 4x 10 GbE SFP+ ports.

Figure 188. Dell PowerSwitch N3248TE-ON

Dell PowerSwitch S4148F-ON

The Dell PowerSwitch S4148F-ON is a 1U multilayer switch with 48x 10 GbE and 4x 100 GbE ports.

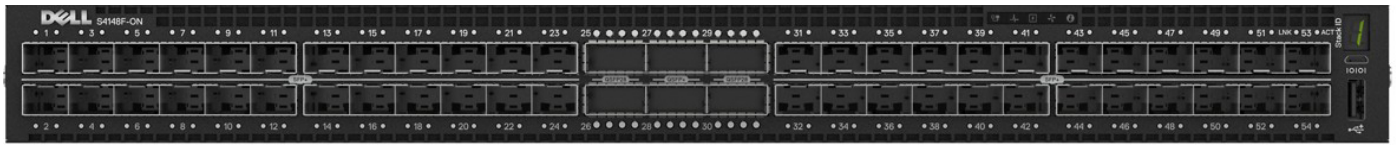


Figure 189. PowerSwitch S4148F-ON

Dell PowerSwitch S5232F-ON

The Dell PowerSwitch S5232F-ON is a 1U, multilayer switch with 32x 100 GbE QSFP28 ports and 2x 10 GbE SFP+ ports.

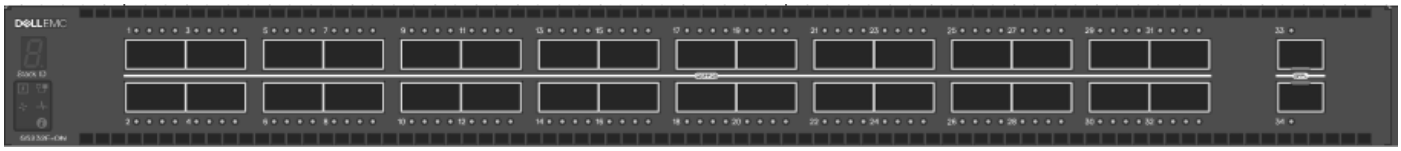


Figure 190. Dell PowerSwitch S5232F-ON

Dell PowerSwitch S5248F-ON

Dell PowerSwitch S5248F-ON is a 1-Rack Unit (1U), multilayer switch with 48x 25 GbE SFP28 ports, 4x 100 GbE QSFP28 ports, and 2x 200 GbE QFSP28-DD ports.

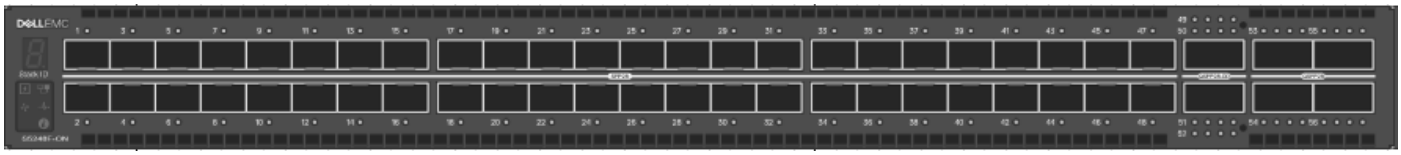


Figure 191. Dell PowerSwitch S5248F-ON

PowerEdge servers for ESXi

PowerEdge servers provide the highest performance for a diverse set of workloads from the edge, to the cloud, to the core. PowerEdge servers and VMware provide industry-leading solutions for a modern data center including servers, virtualization, HCI, storage, networking, and cloud. PowerEdge delivers lower TCO, scalable architectures, intelligent automation and management, and multilayer security when paired with the industry leader in enterprise virtualization and HCI software.

Table 25. Server hardware

Quantity	Item	Version
4	PowerEdge R640	-
	BIOS	2.5.5
	iDRAC	2.70.70.70
	Broadcom NIC	21.80.16.95

Dell PowerEdge R640

PowerEdge servers and VMware provide industry-leading solutions for a modern data center including servers, virtualization, HCI, storage, networking, and cloud. PowerEdge delivers lower TCO, scalable architectures, intelligent automation and management, and multilayer security when paired with the industry leader in enterprise virtualization and HCI software.

Figure 192. Dell PowerEdge R640 server - front view

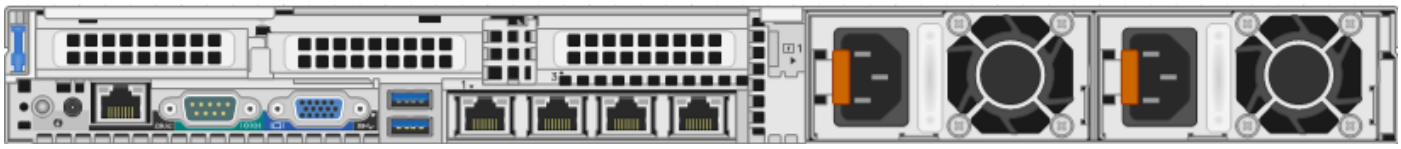


Figure 193. Dell PowerEdge R640 server - rear view

PowerStore storage

PowerStore provides our customers with data centric, intelligent, and adaptable infrastructure that supports both traditional and modern workloads. PowerStore is designed to support any workload by delivering unified storage (physical or virtual, file-based, or container-based) in a performance optimized appliance that can scale up and out when demands increase. Driving automation and operational efficiency across the management environment is a top priority for organizations seeking to free up resources and reduce staffing requirements for IT specialists who are difficult to hire and retain. PowerStore enables autonomous,

consistent operations with programmable infrastructure that enables automation and DevOps by streamlining development environments and automating end-to-end workflows.

PowerStore 5000T

The PowerStore 5000T is a 2U storage array with 4 x 25/10/1 GbE optical or 4 x 10/1 GbE BASE-T ports, and supports 4 x 32 Gb FC, 4 x 25/10/1 GbE optical, and 4 x 10/1 GbE BASE-T I/O modules.

Figure 194. PowerStore 5000T front view

Figure 195. PowerStore 5000T I/O view

VMware

Table 26. VMware software

Item	Version
VMware ESXi	7.0U3c
VMware vCenter Server Appliance	7.0U3c

SFSS software

Table 27. SFSS software

Item	Version
SFSS	1.0.0

OMNI software

Table 28. OMNI software

Item	Version
OMNI	3.0.0

B

Additional Configuration and Settings Information

ESXi CLI commands for NVMe/TCP

The following table details the optional commands you can run on the ESXi shell to enable the host for NVMe/TCP and register with the SFSS storage instance. The following tasks can be completed in the UI.

Table 29. ESXi CLI commands for NVMe/TCP

Function	Commands

Enable NVMe/TCP feature on the ESXi node	`feature-state-util -f`
	`feature-state-util -e nvme_stfs`
	`feature-state-util -e nvmetcp`
	After enabling NVME/TCP features, reboot the ESXi node

Add a virtual standard switch. In this example, a vSS named **vs1** is created.	`esxcfg-vswitch -a vs1`
Add a port group. In this example, a portgroup named **PG-NVMe-TCP** is created.	`esxcfg-vswitch -A PG-NVMe-TCP vs1C`
Configure VLAN for the port group. In this example, **VLAN 1821** is used for port group **PG-NVMe-TCP**.	`esxcfg-vswitch -v 1821 -p PG-NVMe-TCP vs1`
Add uplinks to the switch. In this example, vmnic4 and vmnic5 are added.	`esxcfg-vswitch -L vmnic4 vs1` `esxcfg-vswitch -L vmnic5 vs1`
Assign an IP for the VMkernel.	`esxcfg-vmknic -a -i 172.18.21.101 -n 255.255.255.0 -p PG - NVMe-TCP`
Enable VMkernel for NVMe/TCP.	`esxcli network ip interface tag add -i vmk1 -t NVMeTCP`
Enable NVMe/TCP on the NIC and create the NVMe storage adapters.	`esxcli nvme fabrics enable -p TCP -d vmnic64` `esxcli nvme fabrics enable -p TCP -d vmnic65`
Validate the NVMe adapters created.	`esxcli nvme adapter list`

OpenManage Network Integration

OpenManage Network Integration (OMNI) enables configuration and management of Dell PowerSwitch systems running Dell SmartFabric OS10 within VMware vCenter. With OMNI, networks created in vCenter are automatically configured in the fabric.

The following tasks are done in the OMNI plugin in vCenter:

- View the leaf-spine topology
- View switch status
- Configure server-facing interfaces and port channels
- Configure uplinks to external networks
- Create networks
- Configure routing
- Upgrade SmartFabric OS10

Use CLI to register SFSS in ESXi hosts

In this step, the hosts register with the CDCs in SFSS. Hosts esxi05, exsi06, esxi07, and esxi08 are the initiators in this example.

NOTE: In a future VMware vSphere release, this step is automated. Repeat the steps in this section for each ESXi host.

For the initial registration with SFSS using the CLI, perform the following steps:

1. Using the **root** credentials, SSH to each host.
2. Run the `esxcli nvme fabrics discover -a vmhba[id] -i [CDC IP] -p 8009 -c -r` commands on each host to register each NVMe/TCP vmhba in the cluster. In this example, the following commands are run:

```
esxcli nvme fabrics discover -a vmhba64 -i 172.18.21.250 -p 8009 -c -r
esxcli nvme fabrics discover -a vmhba65 -i 172.18.22.250 -p 8009 -c -r
```

```
[root@esxi05:~] esxcli nvme fabrics discover -a vmhba64 -i 172.18.21.250 -p 8009 -c -r
Transport Type  Address Family  Subsystem Type  Controller ID  Admin Queue Max Size  Transport Address  Transport Service ID  Subsystem NQN                                        Connected
--------------  --------------  --------------  -------------  --------------------  -----------------  --------------------  ---------------------------------------------  ---------
TCP             IPv4            NVM                         0                     0  0.0.0.0            4420                  nqn.1988-11.com.dell:SFSS:1:20211126144255e8       false
[root@esxi05:~] esxcli nvme fabrics discover -a vmhba65 -i 172.18.22.250 -p 8009 -c -r
Transport Type  Address Family  Subsystem Type  Controller ID  Admin Queue Max Size  Transport Address  Transport Service ID  Subsystem NQN                                        Connected
--------------  --------------  --------------  -------------  --------------------  -----------------  --------------------  ---------------------------------------------  ---------
TCP             IPv4            NVM                         0                     0  0.0.0.0            4420                  nqn.1988-11.com.dell:SFSS:2:20211126144255e8       false
```

```
[root@esxi05:~] esxcli nvme fabrics discover -a vmhba64 -i 172.18.21.250 -p 8009 -c -r
Transport Type  Address Family  Subsystem Type  Controller ID  Admin Queue Max Size  Transport Address  Transport Service ID  Subsystem NQN                                        Connected
--------------  --------------  --------------  -------------  --------------------  -----------------  --------------------  ---------------------------------------------  ---------
TCP             IPv4            NVM                         0                     0  0.0.0.0            4420                  nqn.1988-11.com.dell:SFSS:1:20211126144255e8       false
[root@esxi05:~] esxcli nvme fabrics discover -a vmhba65 -i 172.18.22.250 -p 8009 -c -r
Transport Type  Address Family  Subsystem Type  Controller ID  Admin Queue Max Size  Transport Address  Transport Service ID  Subsystem NQN                                        Connected
--------------  --------------  --------------  -------------  --------------------  -----------------  --------------------  ---------------------------------------------  ---------
TCP             IPv4            NVM                         0                     0  0.0.0.0            4420                  nqn.1988-11.com.dell:SFSS:2:20211126144255e8       false
```

```
[root@esxi05:~] esxcli nvme fabrics discover -a vmhba64 -i 172.18.21.250 -p 8009 -c -r
Transport Type  Address Family  Subsystem Type  Controller ID  Admin Queue Max Size  Transport Address  Transport Service ID  Subsystem NQN                                        Connected
--------------  --------------  --------------  -------------  --------------------  -----------------  --------------------  ---------------------------------------------  ---------
TCP             IPv4            NVM                         0                     0  0.0.0.0            4420                  nqn.1988-11.com.dell:SFSS:1:20211126144255e8       false
[root@esxi05:~] esxcli nvme fabrics discover -a vmhba65 -i 172.18.22.250 -p 8009 -c -r
Transport Type  Address Family  Subsystem Type  Controller ID  Admin Queue Max Size  Transport Address  Transport Service ID  Subsystem NQN                                        Connected
--------------  --------------  --------------  -------------  --------------------  -----------------  --------------------  ---------------------------------------------  ---------
TCP             IPv4            NVM                         0                     0  0.0.0.0            4420                  nqn.1988-11.com.dell:SFSS:2:20211126144255e8       false
```

```
[root@esxi05:~] esxcli nvme fabrics discover -a vmhba64 -i 172.18.21.250 -p 8009 -c -r
Transport Type  Address Family  Subsystem Type  Controller ID  Admin Queue Max Size  Transport Address  Transport Service ID  Subsystem NQN                                        Connected
--------------  --------------  --------------  -------------  --------------------  -----------------  --------------------  ---------------------------------------------  ---------
TCP             IPv4            NVM                         0                     0  0.0.0.0            4420                  nqn.1988-11.com.dell:SFSS:1:20211126144255e8       false
[root@esxi05:~] esxcli nvme fabrics discover -a vmhba65 -i 172.18.22.250 -p 8009 -c -r
Transport Type  Address Family  Subsystem Type  Controller ID  Admin Queue Max Size  Transport Address  Transport Service ID  Subsystem NQN                                        Connected
--------------  --------------  --------------  -------------  --------------------  -----------------  --------------------  ---------------------------------------------  ---------
TCP             IPv4            NVM                         0                     0  0.0.0.0            4420                  nqn.1988-11.com.dell:SFSS:2:20211126144255e8       false
```

The prompt returns without any message or error.

NOTE: There are no controllers listed in vSphere because the CDC in SFSS only returns Storage DDCs. These controllers are not visible until zoning is complete.

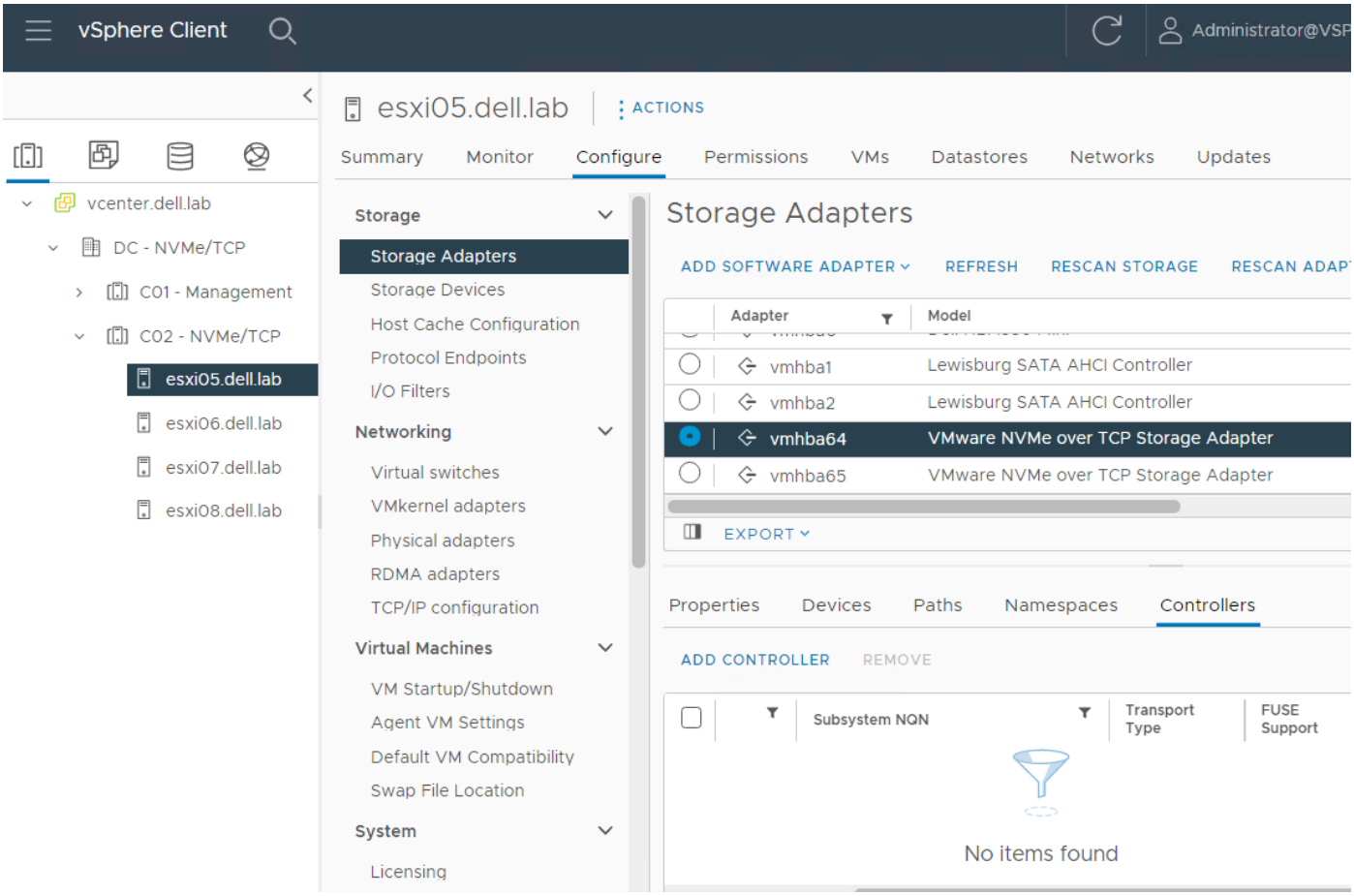


Figure 196. vSphere showing no controllers listed

3. To verify the hosts are registered with each CDC:
   a. Log in to the SFSS.
   b. Click **CDC INSTANCES** and select **1** from the drop-down menu.
   c. Click **Endpoints** > **Host** to see the list of hosts registered with **CDC 1**.

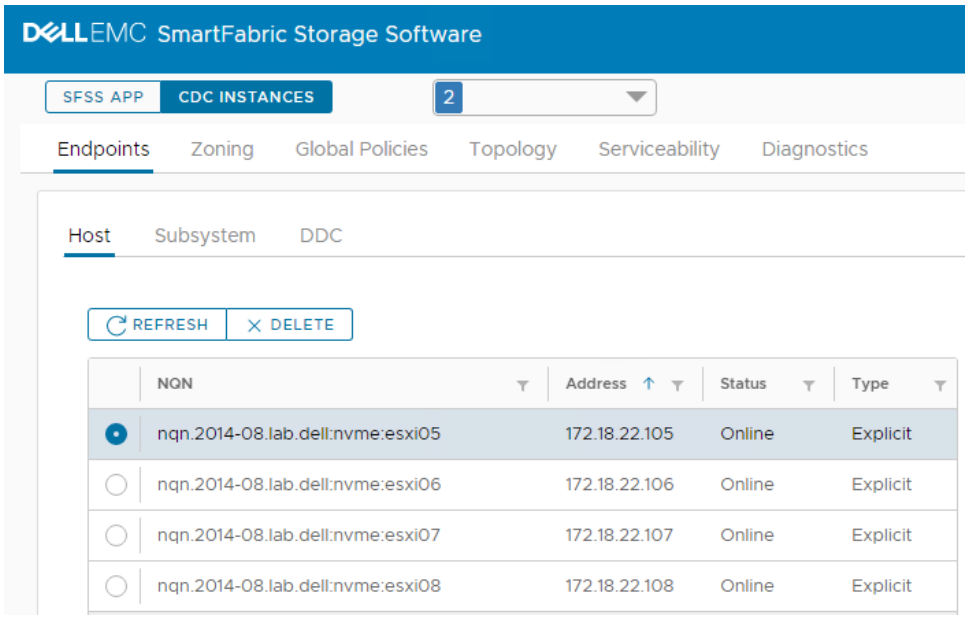


Figure 197. Hosts appear in CDC Instance 1

   d. From the drop-down menu, select **2** to see the same list of hosts registered with **CDC 2**. In this listing, the hosts have IP addresses in the SAN B **172.18.22.xxx** network.

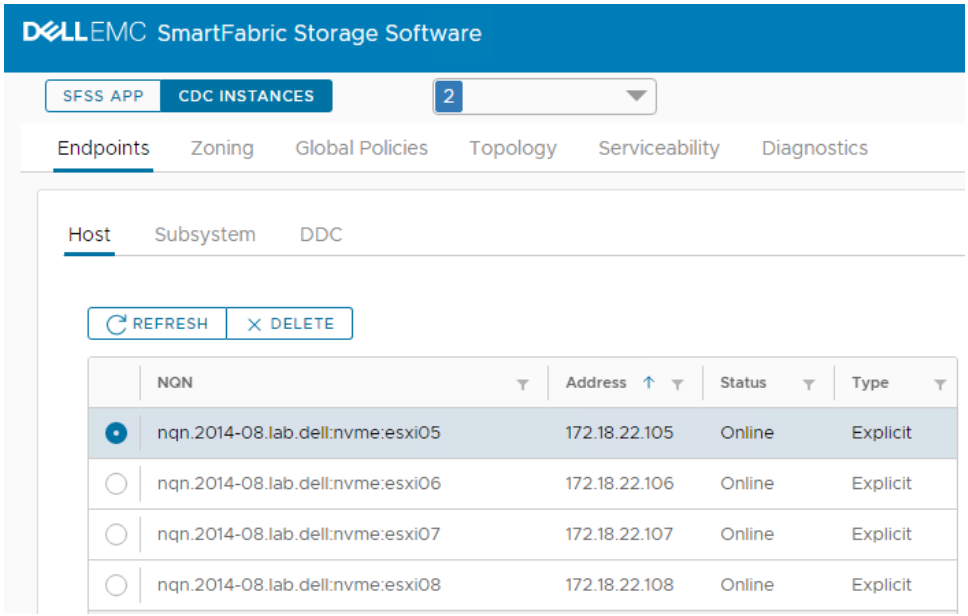


Figure 198. Hosts appear CDC Instance 2

Sample initial configuration worksheet for dual SFSS

Table 30. Sample initial configuration worksheet for dual SFSS

SFSS configuration item	Value for SAN A	Value for SAN B
Hostname	sfss-san-a	sfss-san-b
Default Username	admin	admin
Default Password	admin	admin
Management Interface IP	172.18.11.57	172.18.11.58
Management Mask/Prefix	24	24
Management Gateway	172.18.11.254	172.18.11.254
Associated CDC Instance(s)	1	2
Storage interface MTU	9000	9000
IPv4 Internal Network	172.18.0.0/16	172.17.0.0/16
IPv6 Internal Network	fd01::0/64	fe02::0/64

SFSS Licenses

SFSS licenses are tied to a unique device ID that is generated at the time of SFSS VM creation. SFSS supports two types of licenses: Base perpetual and Expansion.

- Base Perpetual—There are two types:
  - Enterprise license—A perpetual license that supports 48 endpoints.
  - Partner license—(For demonstration purposes only) A perpetual license that supports 10 endpoints. This license cannot be expanded to include additional endpoints.
- Expansion license—A perpetual license that incrementally supports additional endpoints.

Endpoints include NVMe hosts and NVM subsystems that register their information with CDC. The endpoint count is calculated by adding the total number of host NQNs (or IP addresses) and subsystem NQNs (or IP addresses) that are registered with all the CDC instances in an SFSS deployment.

When you use SFSS for the first time, the system supports up to a maximum of 2048 endpoints for a trial period of up to 90 days. Before the trial period expires, you must obtain and install an Enterprise Base license (and optionally Expansion licenses depending on the endpoint count in your deployment). The endpoint count includes the total number of hosts and subsystems in your deployment.

The system sends periodic notifications to warn you about the trial period expiry. You receive a notification:

- One month before the date of expiry
- One week before the date of expiry
- One day before the date of expiry

You can install and run SFSS without a license during a 90-day trial period from the Dell Technologies Support Page. You must sign in to download the software.

NOTE: If you have not installed perpetual licenses and the trial period expires, SFSS does not accept any new endpoint registration requests. Ensure that you obtain the necessary licenses and install them in SFSS before the trial period expires. Use the SFSS web UI to manage the licenses.

Related information

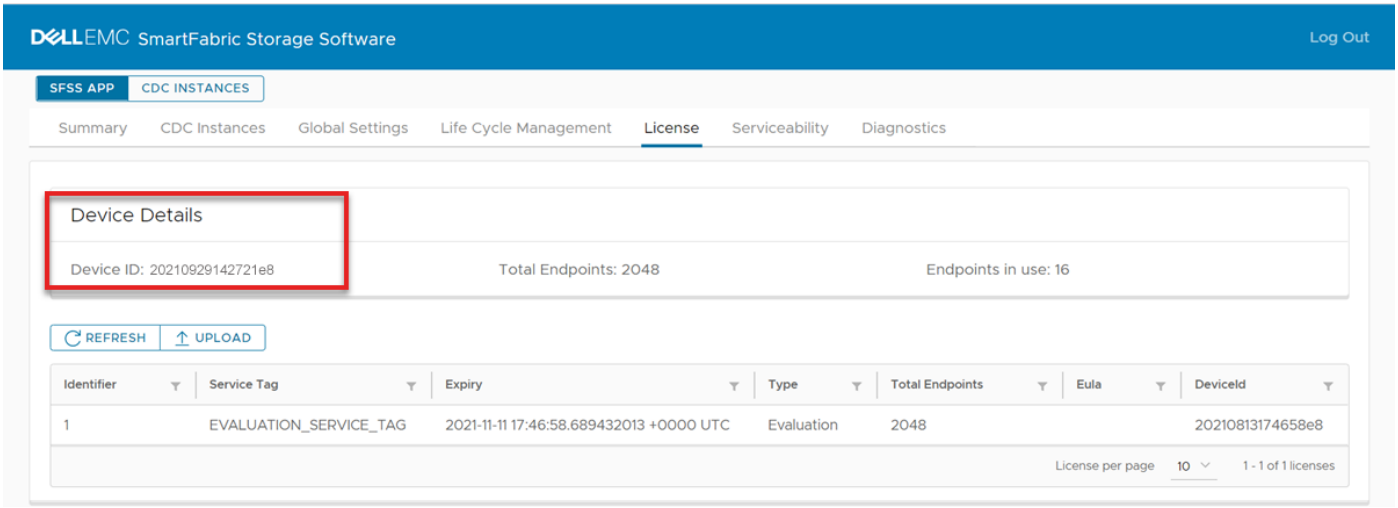
Obtain licenses

Obtain licenses

Log in to DDL and generate the SFSS license keys.

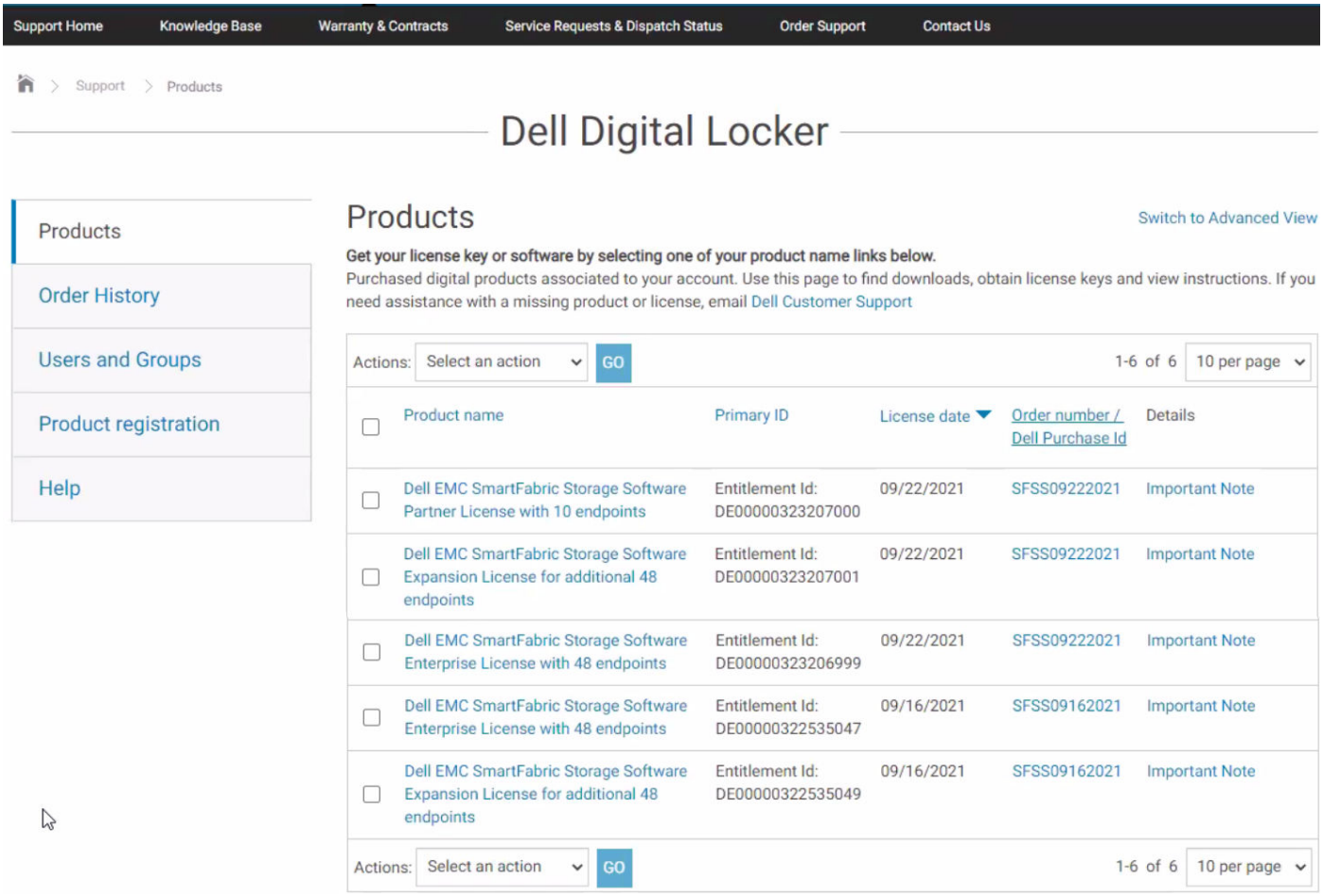
Before you begin

Log in to the SFSS web UI and go to **SFSS App > License**. The **Device Details** page appears. Make a note of the **Device ID**.



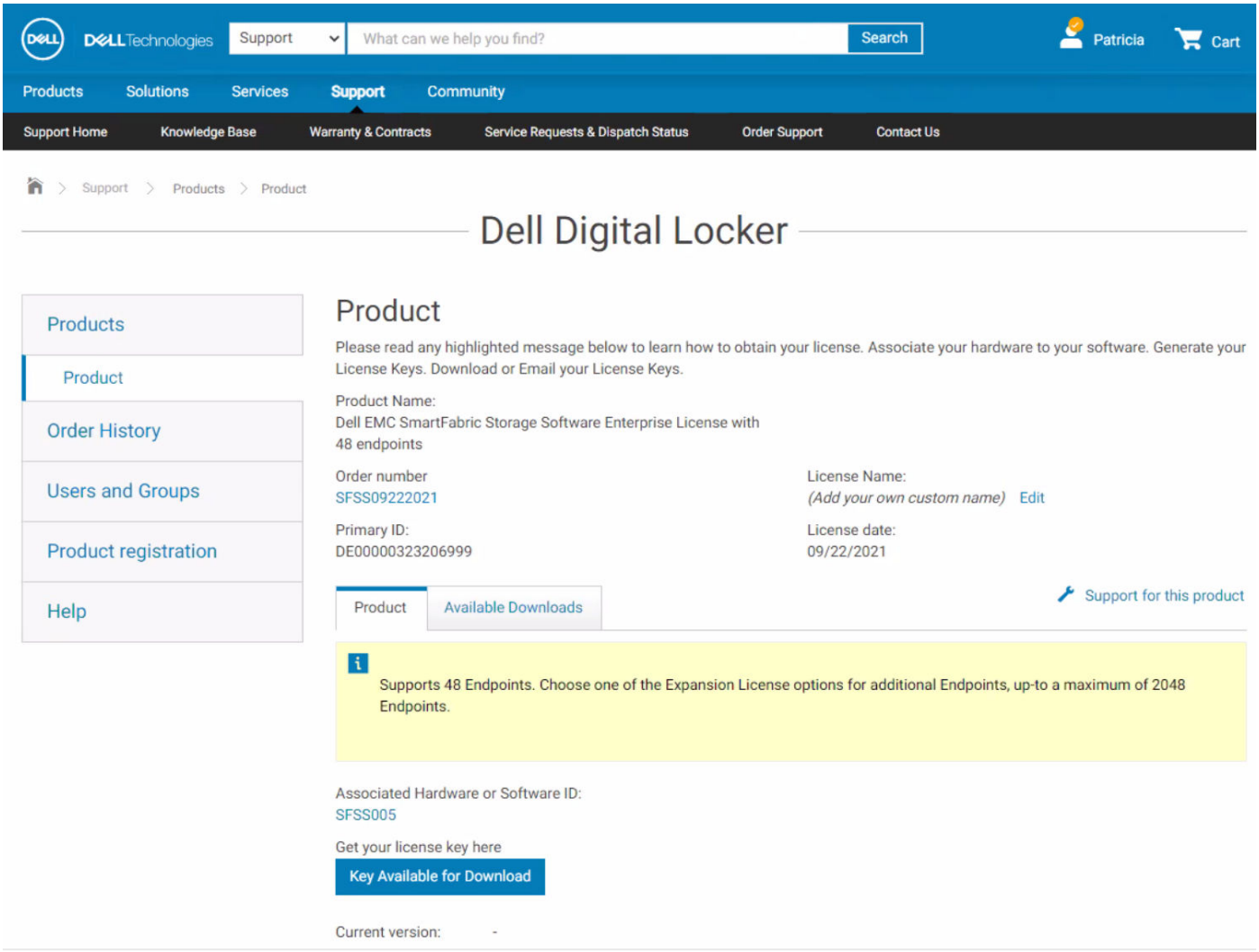
To obtain a perpetual license:

1. Log in to the Dell Digital Locker (DDL) using your account credentials.
2. Locate the product name with the entitlement ID (Primary ID).

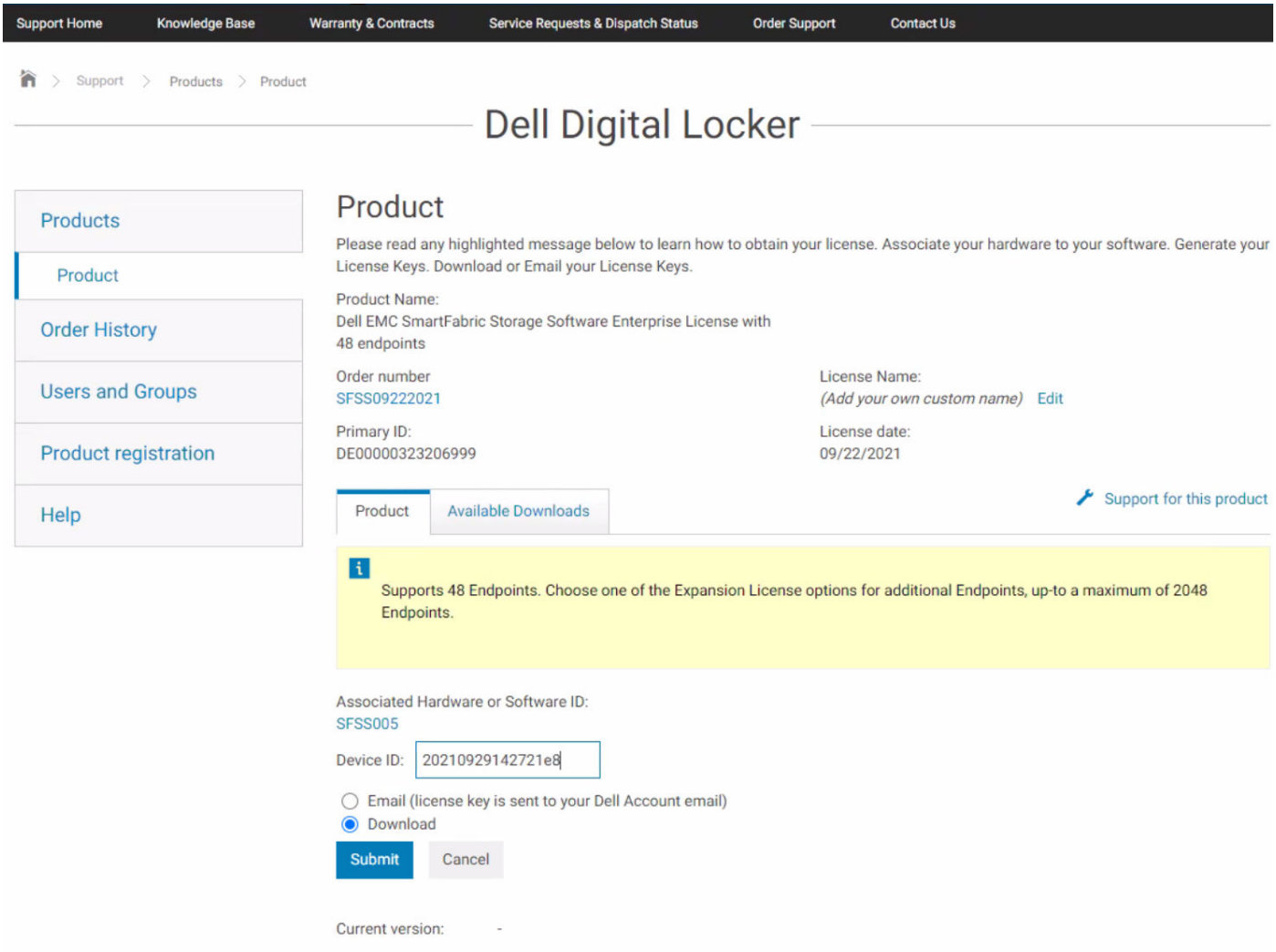


The product is listed.

3. Select the product. The Order Number, Primary ID, and Software Service Tag (Associated Hardware or Software ID) are displayed.



4. Click **Key Available for Download**.
5. Enter the device ID.



6. Click **Download** to download the license file.

   You can alternatively choose to receive the license file in your Dell Account email.

7. Click **Submit** to download the license file to the **Downloads** folder in your system.

Modify hostname in SFSS

To modify the hostname in SFSS, perform the following steps:

1. Log in to the SFSS web UI
2. Click **SFSS App** > **Global Settings** > **Edit**.

   CAUTION: Verify that the VM internal hostname does not contain a period (.). The FQDN in this step replaces the periods with dashes. For example, sfss.dell.lab is replaced with sfss-dell-lab.

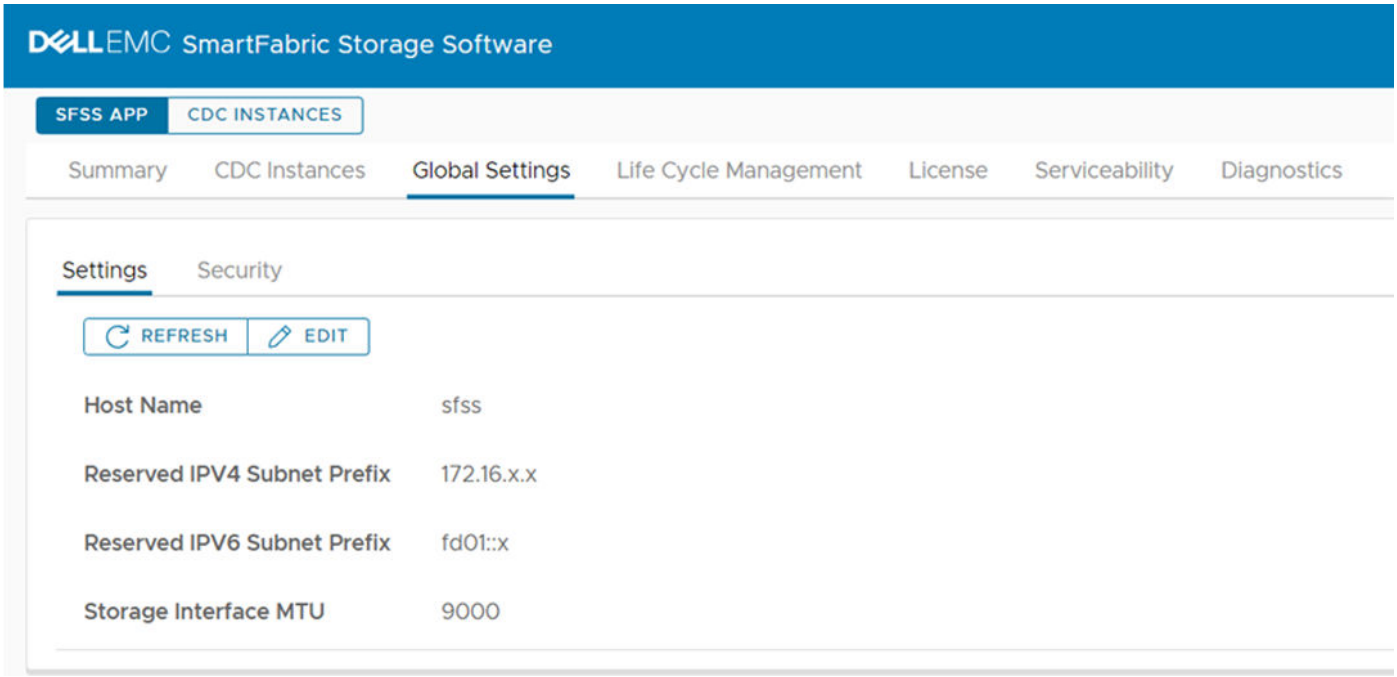


Figure 199. SFSS Global Settings

3. Edit the name and click **Submit**.

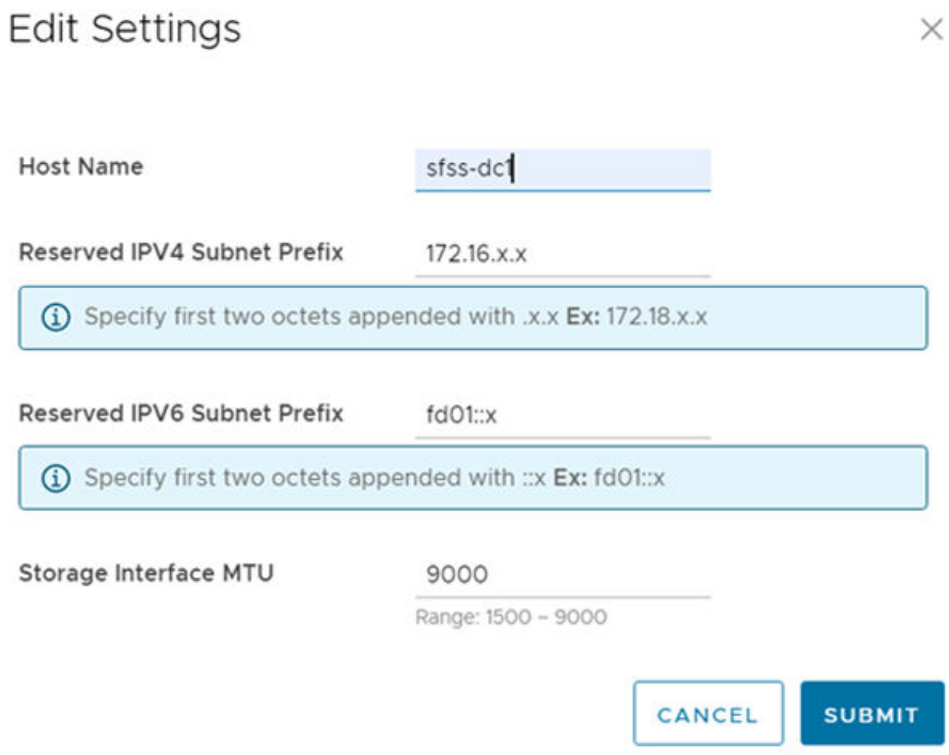


Figure 200. Edit the internal Host Name

4. Click the checkbox to accept the **Warning** to reboot the VM.

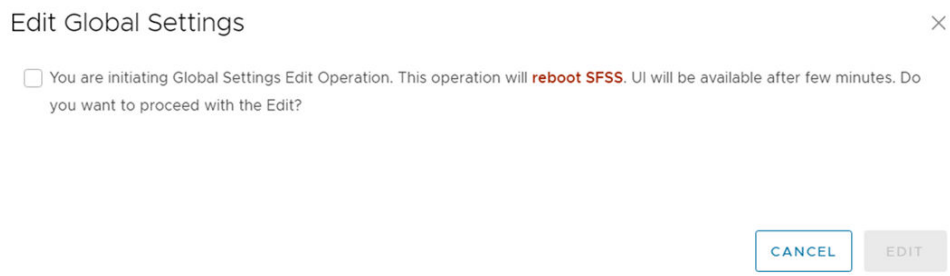


Figure 201. Edit Global Settings Warning

The SFSS VM reboots.

5. To rename the VM in vCenter, right-click the **SFSS VM** and select **Rename**.

Figure 202. Rename the SFSS VMware vApp

Add a network interface to SFSS vApp

Changes to SFSS VM's Network Adapters require a reboot. Ideally changes are made **before** powering on the SFSS vApp for the first time.

Additional interfaces can be created by adding network adapters to the VM, or by creating virtual interfaces within SFSS. Virtual interfaces act like subinterfaces which divide the interface into different VLANs.

To add an SFSS VM interface, perform the following steps:

1. Right-click the SFSS vApp and select **Edit Settings**.

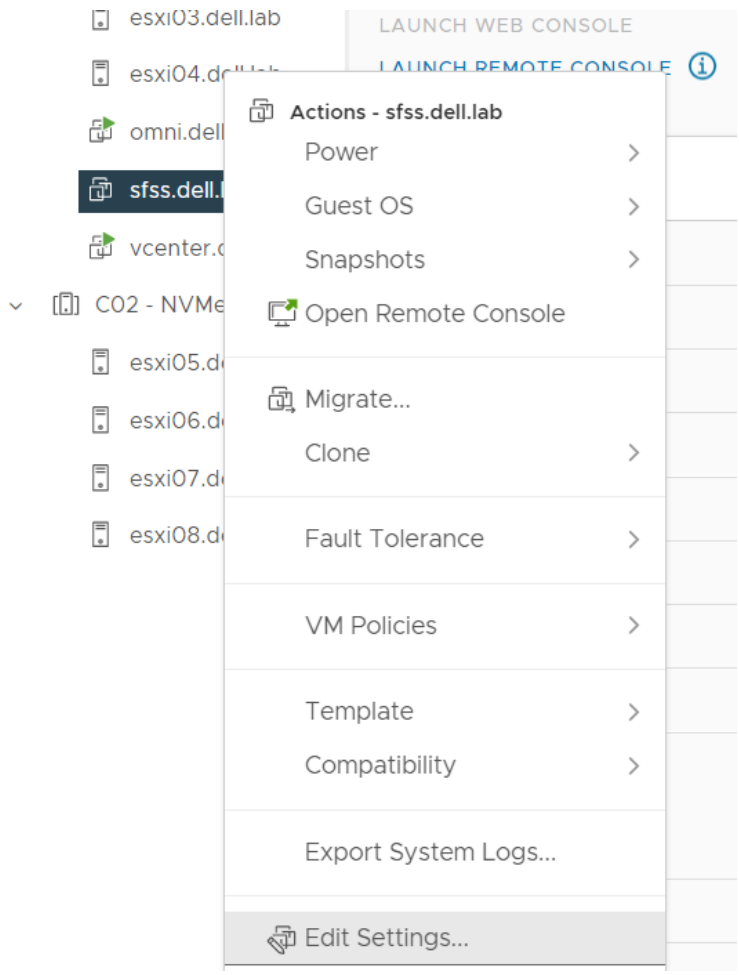


Figure 203. SFSS vApp Edit Settings option

2. Click **Add New Device** drop-down and select **Network Adapter**.

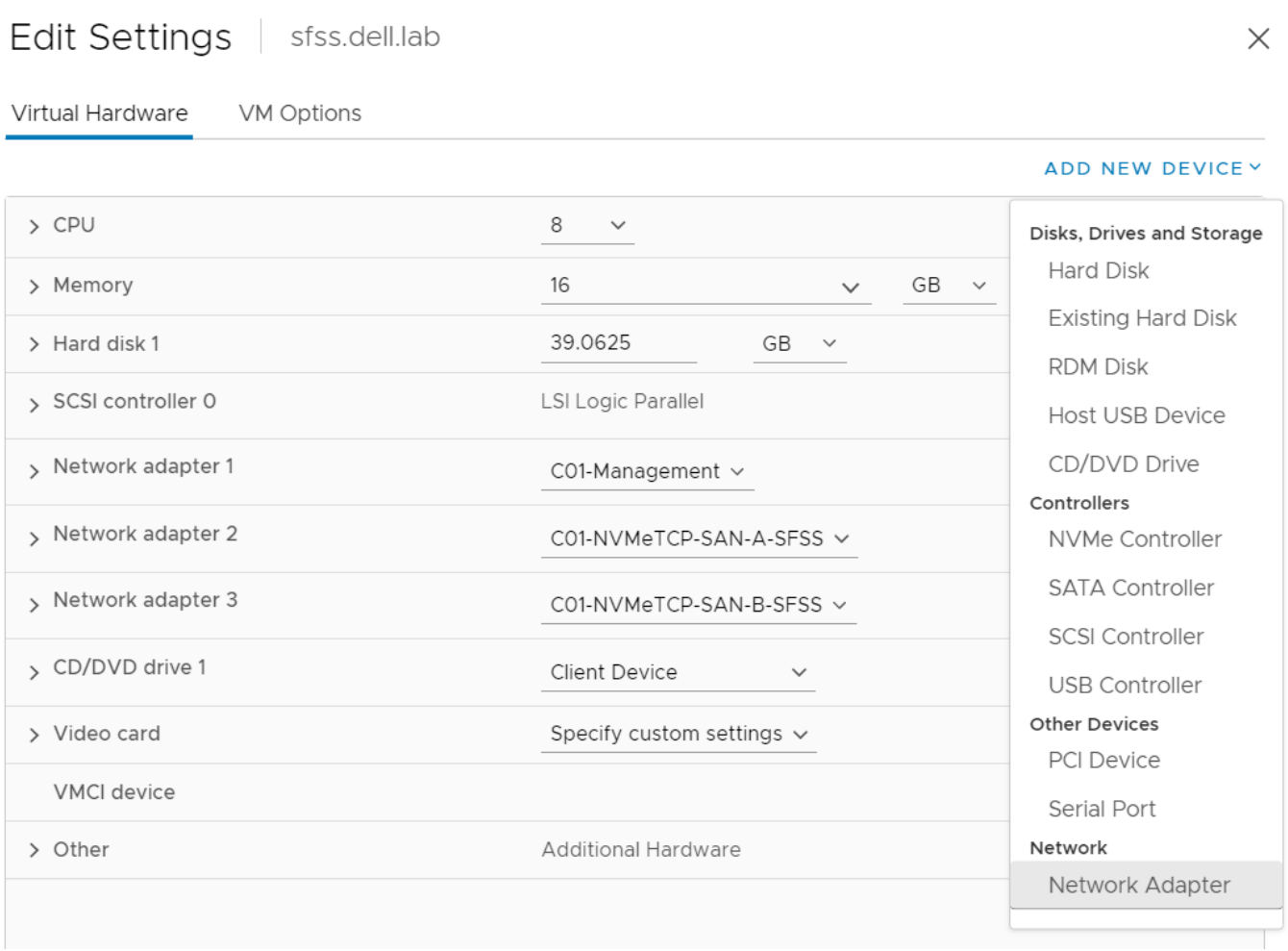


Figure 204. Add new network adapter screen

3. From the **New Network** listing, click the **Port Group** drop-down and select **Browse**.

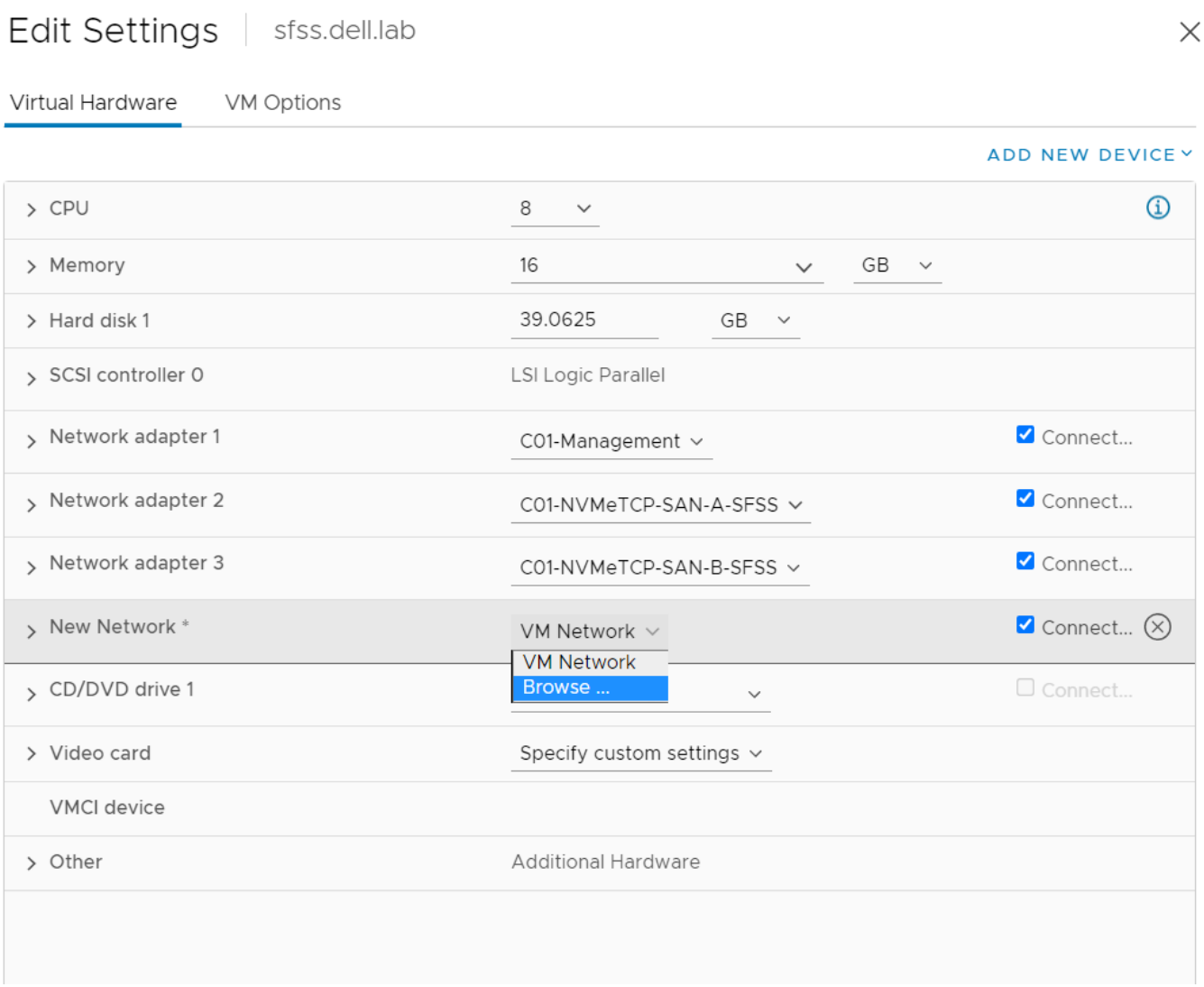


Figure 205. New Network drop-down

4. Select the **Port Group** for the additional interface.

   NOTE: In this example **Guest-Network** is used for demonstration purposes only. It is not required for this deployment and will be removed.

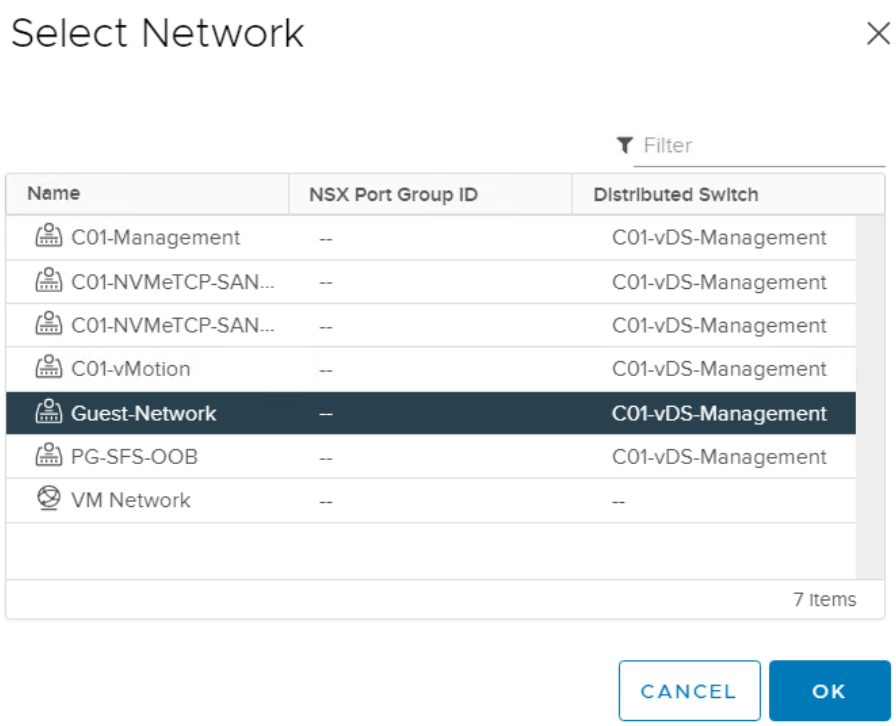


Figure 206. Guest-Network listing

5. Click **OK**.
6. Change the **Adapter Type** to **E1000**.

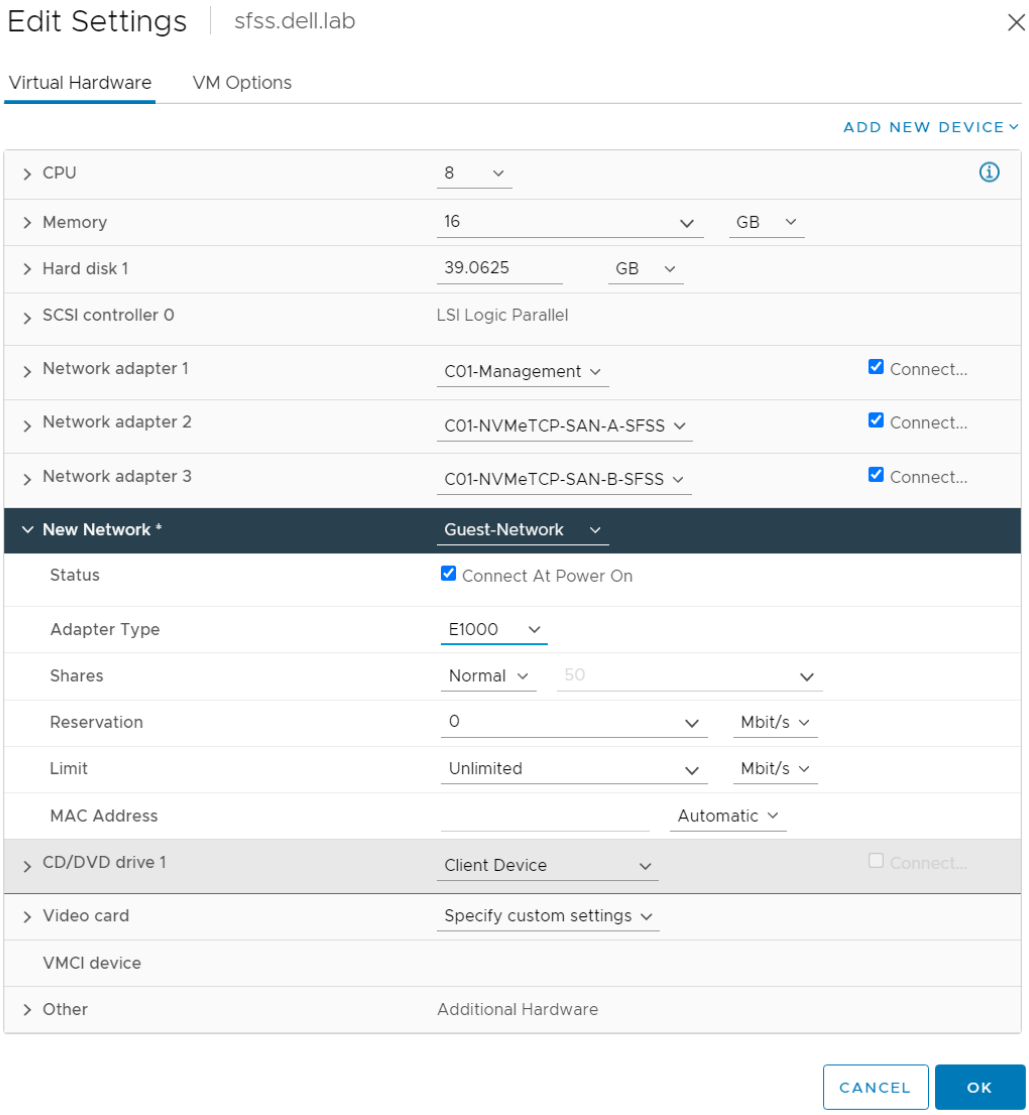


Figure 207. New Network adapter listing

7. Click **OK**.
8. From the **Recent Tasks** section, view the status of the task.

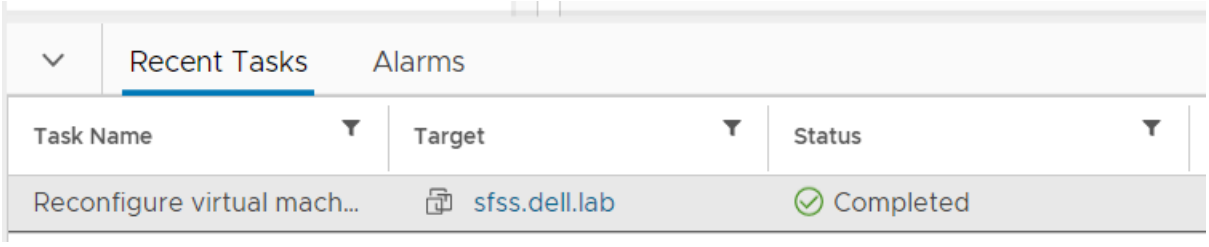


Figure 208. Recent Tasks status listings

NOTE: As a best practice, only configure one interface per CDC. However, the topology figure below shows the use of two interfaces in a single CDC, the hosts and subsystems are in different subnets where SFSS has Layer 2 access to the hosts and subsystems.

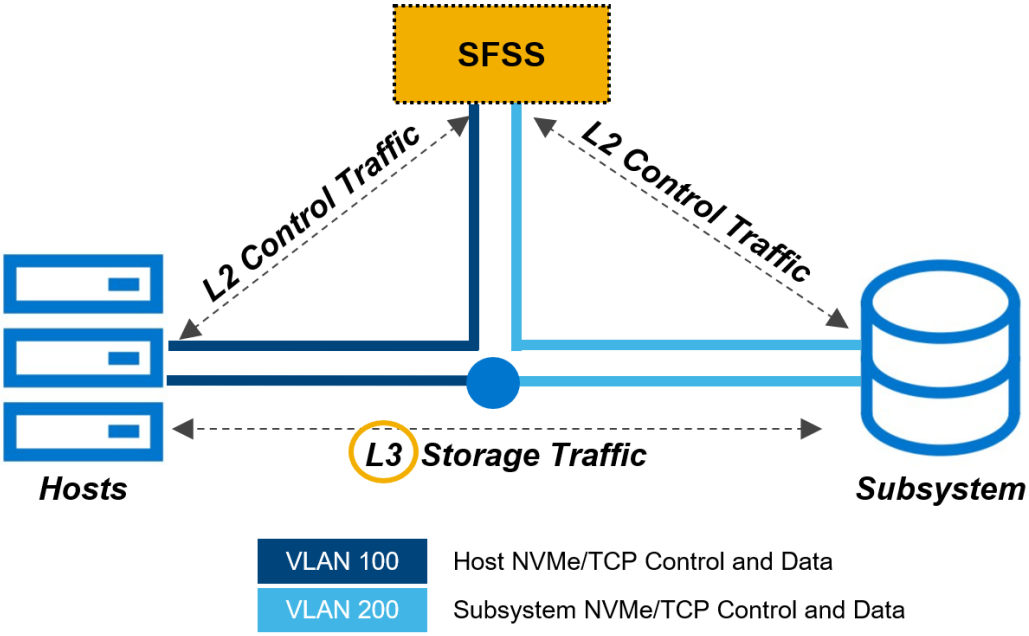


Figure 209. Layer 2 control and Layer 3 I/O traffic topology

Disable or remove an SFSS network interface

When SFSS communicates with its endpoints over Layer 3 it will only have one interface, it is necessary to disable or remove SFSS interfaces.

Disable SFSS interface

To disable an SFSS interface, perform the following steps:

1. Select the interface and then click **Edit**.
2. Change the **IPv4 Config** to **Manual**, enter the placeholder **IPv4 Address** of **0.0.0.0**, and the **IPv4 Prefix length** as **32.**
3. Change the **IPv6 Config** to **Manual**, enter the placeholder **IPv6 Address** of **::**, and the **IPv6 Prefix Length** as **64.**

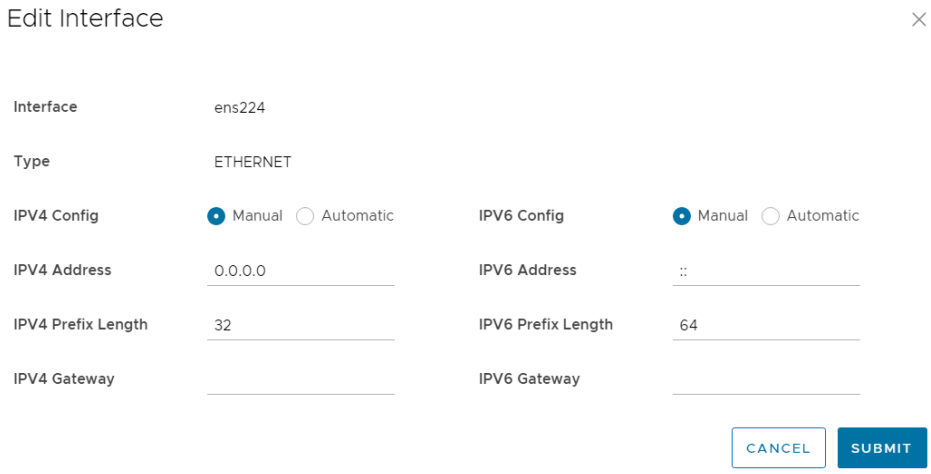


Figure 210. Edit interface screen

4. Click **Submit**.

Endpoints will not discover the interface.

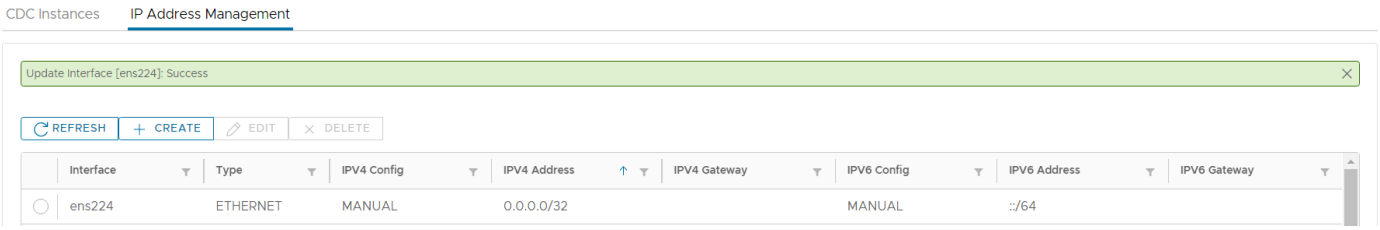


Figure 211. Interface disabled and hidden from Endpoints

Remove interface

NOTE: If you are unsure of which interface to remove, compare the MAC addresses in the **VM Settings** and the **SFSS shell** `ifconfig` output. To run `ifconfig` in SFSS, go to the **Web Console**, type **2** to enter the **Debug** menu, and then enter `shell`, and from the prompt, enter `ifconfig`.

To remove a network adapter from the VM, perform the following steps:

1. Power-off the SFSS virtual machine.
2. When prompted to confirm the shutdown process, click **YES**.
3. Right-click the VM and click **Edit Settings**.
4. Hover over the interface to be removed, and then click the **X** icon to the right of the **Connected** listing.

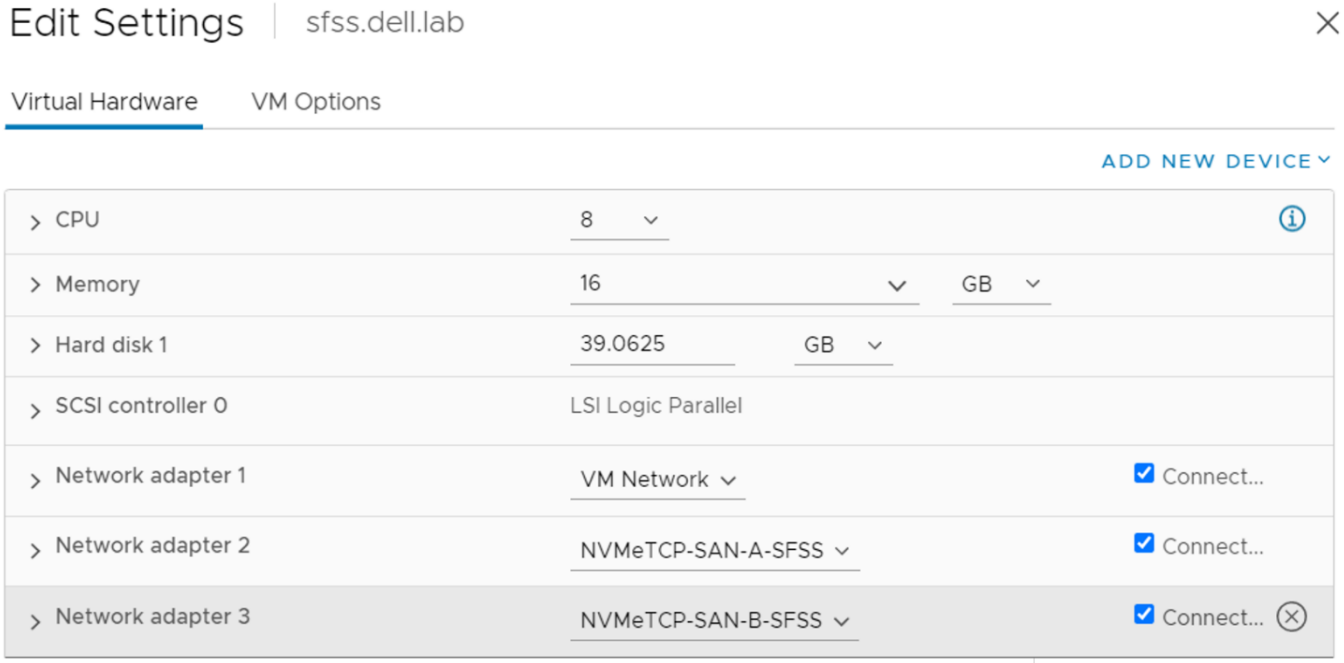


Figure 212. Network adapter selection screen

5. Click **OK**.

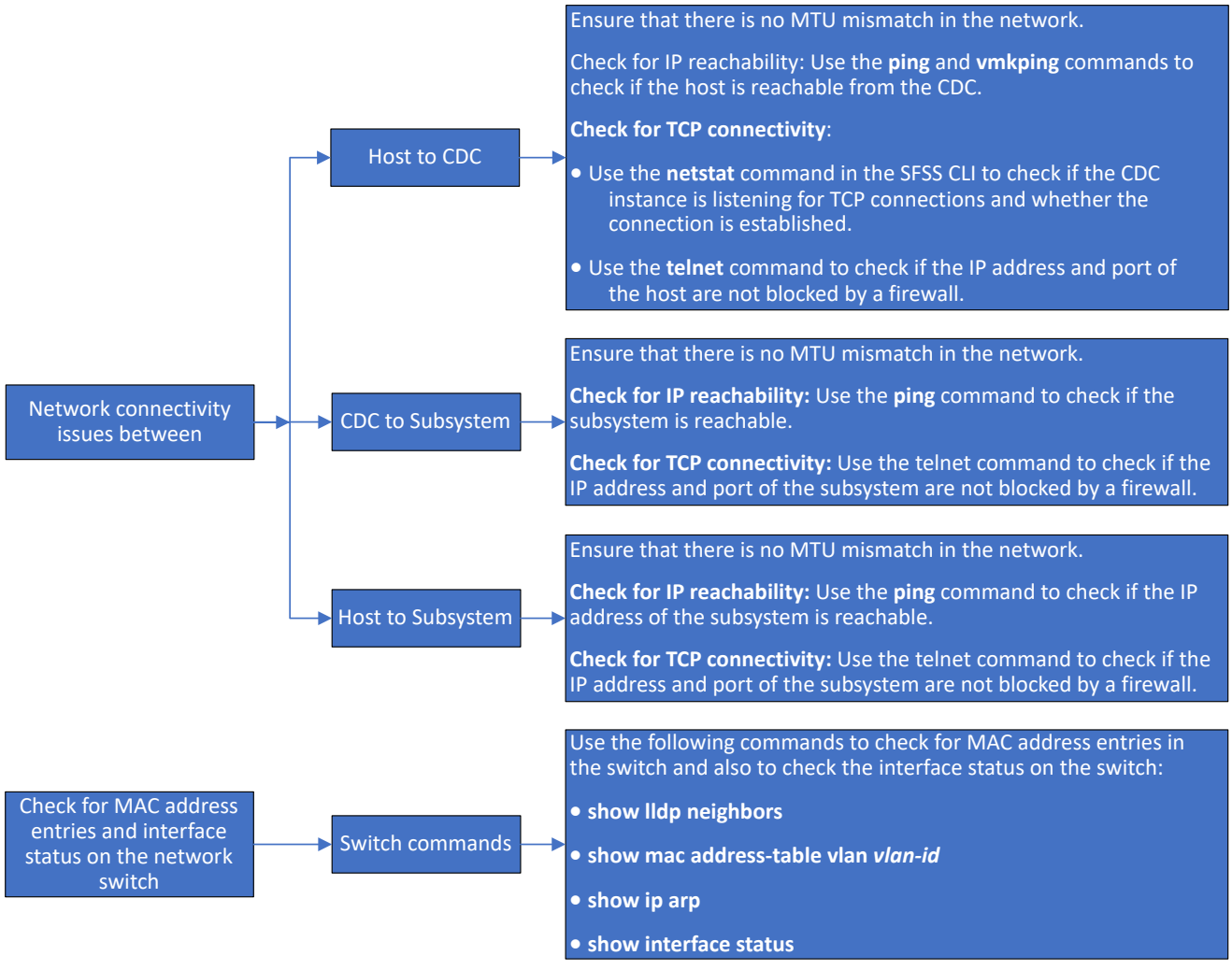
C

Troubleshooting

NOTE: For more troubleshooting information, see the SmartFabric Storage Software Troubleshooting Guide.

Check the network infrastructure

The following sections provide steps to troubleshoot network connectivity issues at the different layers in a network.



Connectivity issues between the ESXi host and CDC

Perform the following checks to ensure that TCP connection is established successfully.

NOTE: See the VMware Knowledge Base Article 2020669 for troubleshooting TCP connectivity issues on the ESXi host.

1. Enter the `telnet` command on the ESXi host to look for TCP port connectivity issues. The output shows that the IP address and port are not blocked by a firewall.

```
[root@esxi05:~] telnet 172.18.21.250 8009
Trying 172.18.21.250...
Connected to 172.18.21.250.
Escape character is '^]'.
```

   If the `telnet` command is not available on the ESXi host, use the `netcat (nc)` command to check for TCP port connectivity.

```
[root@esxi05:~] nc -z 172.18.21.250 8009
Connection to 172.18.21.250 8009 port [tcp/*] succeeded!
```

   The `netcat` command output shows that the TCP connection is established.

2. Check if the CDC instance is reachable from the ESXi host. Enter the `vmkping` command on the ESXi host. Ensure that there is no MTU mismatch in the network. Endpoint registration fails if there is an MTU mismatch in the network.

```
[root@esxi05:~] vmkping -I vmk2 172.18.21.250 -s 9000
PING 172.18.21.250 (172.18.21.250): 9000 data bytes
9008 bytes from 172.18.21.250: icmp_seq=0 ttl=64 time=0.307 ms
9008 bytes from 172.18.21.250: icmp_seq=1 ttl=64 time=0.283 ms
9008 bytes from 172.18.21.250: icmp_seq=2 ttl=64 time=0.239 ms

--- 172.18.21.250 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.239/0.276/0.307 ms
```

3. Enter the following `netstat` command on the SFSS VM to check if CDC is listening for TCP connections.

```
root@sfss:/home/stfs# sudo netstat -tulpn | grep LISTEN | grep 8009
tcp        0      0 172.18.21.250:8009      0.0.0.0:*               LISTEN
3327/kube-proxy
```

   The IP address, 172.18.21.250 is the IP address of the CDC instance. You can see from the output that the CDC instance is listening for TCP connections.

4. (Optional) On the SFSS VM, you can use the `netstat` command to ensure that the TCP connection is established:

```
root@sfss:/home/stfs# sudo netstat -an | grep ESTABLISHED | grep 8009
tcp        0      0 172.18.21.250:36464     172.18.21.250:8009      ESTABLISHED
```

Connectivity issues between the CDC and the subsystem

On the SFSS VM, check if the subsystem is reachable and ensure that the IP address and port of the subsystem are not blocked by a firewall.

1. To check if the IP and port are not blocked, enter the `telnet` command.

```
root@sfss:/home/stfs# telnet 172.18.21.191 8009
Trying 172.18.21.191...
Connected to 172.18.21.191.
Escape character is '^]'.
```

2. To check if the subsystem is reachable, from the SFSS VM, use the `ping` command.
   - **Normal ping**

```
root@sfss:/home/stfs# ping 172.18.21.191
PING 172.18.21.191 (172.18.21.191) 56(84) bytes of data.
64 bytes from 172.18.21.191: icmp_seq=1 ttl=64 time=0.164 ms
64 bytes from 172.18.21.191: icmp_seq=2 ttl=64 time=0.138 ms
64 bytes from 172.18.21.191: icmp_seq=3 ttl=64 time=0.172 ms
64 bytes from 172.18.21.191: icmp_seq=4 ttl=64 time=0.153 ms
64 bytes from 172.18.21.191: icmp_seq=5 ttl=64 time=0.137 ms
64 bytes from 172.18.21.191: icmp_seq=6 ttl=64 time=0.139 ms
```

```
--- 172.18.21.191 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 84ms
rtt min/avg/max/mdev = 0.137/0.150/0.172/0.018 ms
```

- **Jumbo ping, if high MTU is used**

  NOTE: Endpoint registration fails if there is an MTU mismatch in the network.

```
root@sfss:/home/stfs# ping 172.18.21.191 -s 8972
PING 172.18.21.191 (172.18.21.191) 8972(9000) bytes of data.
8980 bytes from 172.18.21.191: icmp_seq=1 ttl=64 time=0.242 ms
8980 bytes from 172.18.21.191: icmp_seq=2 ttl=64 time=0.156 ms
8980 bytes from 172.18.21.191: icmp_seq=3 ttl=64 time=0.148 ms
8980 bytes from 172.18.21.191: icmp_seq=4 ttl=64 time=0.094 ms

4 packets transmitted, 4 received, 0% packet loss, time 74ms
```

Connectivity issues between the ESXi host and the subsystem

On the ESXi host:

1. Use the `telnet` command to check if the IP address of the subsystem and port are not blocked. If the `telnet` command is not available, use the `netcat` (`nc`) command:

```
[root@esxi05:~] nc -z 172.18.21.191 8009
Connection to 172.18.21.191 8009 port [tcp/*] succeeded!
```

2. Use the `vmkping` command to check if the subsystem is reachable from the ESXi host.

```
[root@esxi05:~] vmkping 172.18.21.191
PING 172.18.21.191 (172.18.21.191): 56 data bytes
64 bytes from 172.18.21.191: icmp_seq=0 ttl=64 time=0.155 ms
64 bytes from 172.18.21.191: icmp_seq=1 ttl=64 time=0.116 ms
64 bytes from 172.18.21.191: icmp_seq=2 ttl=64 time=0.107 ms

--- 172.18.21.191 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.107/0.126/0.155 ms
```

Check MAC address entries and interface status on the network switches

Check if the switches have learned the endpoint MAC addresses. Enter the following commands on the switches. The examples listed below are obtained from an OS10 switch:

- `show lldp neighbors`

```
SAN-A# show lldp neighbors
Loc PortID      Rem Host Name           Rem Port Id           Rem Chassis Id
-------------------------------------------------------------------------------
ethernet1/1/1   Not Advertised       b8:ce:f6:10:b1:b8      b8:ce:f6:10:b1:ba
ethernet1/1/1   Not Advertised       b8:ce:f6:10:b1:b8      b8:ce:f6:10:b1:b8
ethernet1/1/2   Not Advertised       b8:ce:f6:10:b1:94      b8:ce:f6:10:b1:96
ethernet1/1/2   esxi02.dell.lab     b8:ce:f6:10:b1:94      vmnic4
ethernet1/1/3   Not Advertised       b8:ce:f6:10:b1:d0      b8:ce:f6:10:b1:d2
ethernet1/1/3   esxi03.dell.lab     b8:ce:f6:10:b1:d0      vmnic4
ethernet1/1/4   Not Advertised       b8:ce:f6:10:b1:b4      b8:ce:f6:10:b1:b6
ethernet1/1/4   esxi04.dell.lab     b8:ce:f6:10:b1:b4      vmnic4
ethernet1/1/31  Not Advertised       00:60:16:d3:77:f4      00:60:16:d3:77:f4
ethernet1/1/31  Dell EMC PowerStore  00:60:16:d3:77:e4      cyc-coreos
ethernet1/1/32  Not Advertised       00:60:16:d3:55:bc      00:60:16:d3:55:bc
ethernet1/1/32  Dell EMC PowerStore  00:60:16:d3:55:ac      cyc-coreos
mgmt1/1/1       Rack126-N2048        Gi1/0/33               88:6f:d4:da:e2:53
```

- `show mac address-table vlan vlan-id`

```
SAN-A# show mac address-table
Codes: pv <vlan-id> - private vlan where the mac is originally learnt
VlanId     Mac Address       Type      Interface
1821     00:50:56:61:70:9f  dynamic  ethernet1/1/2
1821     00:50:56:6c:06:de  dynamic  ethernet1/1/3
1821     00:50:56:6e:36:0b  dynamic  ethernet1/1/4
1821     00:50:56:a4:2e:0e  dynamic  ethernet1/1/1
1821     3a:7a:18:a7:09:69  dynamic  ethernet1/1/32
1821     f2:da:6e:ed:c2:58  dynamic  ethernet1/1/31
```

- `show ip arp`

```
SAN-A# show ip arp
Codes: pv <vlan-id> - private vlan where the mac is originally learnt
Address       Hardware address   Interface    Egress Interface
-------------------------------------------------------------------
172.18.21.102 00:50:56:61:70:9f   vlan1821     ethernet1/1/2
172.18.21.103 00:50:56:6c:06:de   vlan1821     ethernet1/1/3
172.18.21.104 00:50:56:6e:36:0b   vlan1821     ethernet1/1/4
172.18.21.191 f2:da:6e:ed:c2:58   vlan1821     ethernet1/1/31
172.18.21.250 00:50:56:a4:2e:0e   vlan1821     ethernet1/1/1
```

Check for the interface status using the `show interface status` command:

```
SAN-A# show interface status
------------------------------------------------------------------------
Port       Description   Status Speed  Duplex Mode Vlan Tagged-Vlans
------------------------------------------------------------------------
Eth 1/1/1  esxi01          up    25G   full    T    1   1821
Eth 1/1/2  esxi02          up    25G   full    T    1   1821
Eth 1/1/3  esxi03          up    25G   full    T    1   1821
Eth 1/1/4  esxi04          up    25G   full    T    1   1821
Eth 1/1/31 PowerStore-R1.. up    25G   full    T    1   1821
Eth 1/1/32 PowerStore-R1.. up    25G   full    T    1   1821
```

Verify the Infrastructure

To verify the infrastructure, follow the steps below:

1. In the web console, enter **2** to access the **Debug** menu.

```
################################################################################
Welcome to Dell Smart Fabric Storage Software (SFSS) management
################################################################################

   Menu
--------------------------------------------------------------------------------
1. Show version
2. Debug
3. Password/SSL configuration menu
4. Show EULA
5. Interface configuration menu
6. Reboot
7. Logout

Enter selection [ 1 – 7 ] :
```

2. Enter **shell** to access the SFSS shell interface.

```
################################################################################
Welcome to Dell Smart Fabric Storage Software (SFSS) management
################################################################################

   Menu
--------------------------------------------------------------------------------
1. Show version
2. Debug
```

```
3. Password/SSL configuration menu
4. Show EULA
5. Interface configuration menu
6. Reboot
7. Enter selection [ 1 - 7 ] : 2

Enter Module name (app-alerts, app-redis, app-rest, cdcproxy, centralnz, discovery,
license,
redis-deployment, syslogng, shell): shell_
```

3. Verify if the following containers are running. Run the following commands:
   - **kubectl get pods**—Verify that the status of the containers is **Running**.

```
root@sfss:/home/stfs# kubectl get pods
NAME                                          READY   STATUS    RESTARTS   AGE
stfs-app-alerts-deployment-6f69fb5499-69cxm   1/1     Running   0          6d23h
stfs-app-redis-deployment-79b869bc67-v69lp    1/1     Running   0          6d23h
stfs-app-rest-deployment-7bd4bf7c8f-jv46v     1/1     Running   0          6d23h
stfs-cdcproxy-deployment-1-0                  1/1     Running   0          6d20h
stfs-cdcproxy-deployment-1-1                  1/1     Running   0          6d20h
stfs-centralnz-deployment-1-689db9475f-jmc8q  2/2     Running   0          6d20h
stfs-discovery-1                              1/1     Running   0          6d20h
stfs-license-857786785-qmx2v                  1/1     Running   0          6d23h
stfs-monitor-655b869dfd-j6bbk                 1/1     Running   0          6d23h
stfs-redis-deployment-1-6cd4c6788c-5m487      1/1     Running   0          6d20h
stfs-syslogng-6966f8dcf8-mvx28                2/2     Running   0          6d23h
```

   - **kubectl get svc**—Verify that the `stfs-app` services are listed.

```
root@sfss:/home/stfs# kubectl get svc
NAME                        TYPE        CLUSTER-IP     EXTERNAL-IP     PORT(S)
                                  AGE
kubernetes                  ClusterIP   172.18.1.1     <none>          443/TCP
                                  6d23h
stfs-app-alerts-svc         ClusterIP   172.18.1.223   <none>          50054/TCP
                                  6d23h
stfs-app-redis-svc          NodePort    172.18.1.189   172.18.2.1
6379:32322/TCP                                  6d23h
stfs-app-rest-svc           NodePort    172.18.1.233   172.18.2.1
9005:31486/TCP                                  6d23h
stfs-cdc-rest-service-1     NodePort    172.18.1.124   172.18.2.1
9006:30172/TCP                                  6d20h
stfs-cdcproxy-service-1     NodePort    172.18.1.150   172.18.21.250
8009:30884/TCP                                  6d20h
stfs-centralnz-service-1    ClusterIP   172.18.1.23    <none>          50052/TCP
                                  6d20h
stfs-license                ClusterIP   172.18.1.56    <none>          50053/TCP
                                  6d23h
stfs-redis-1                ClusterIP   172.18.1.52    <none>          6380/TCP
                                  6d20h
stfs-syslogng               NodePort    172.18.1.42    172.18.2.1      11514:30709/
UDP,6381:31562/TCP,11614:32404/TCP   6d23h
```

   - **kubectl get nodes**—Verify that the SFSS node status is **Ready**.

```
root@sfss:/home/stfs# kubectl get nodes
NAME   STATUS   ROLES                  AGE    VERSION
sfss   Ready    control-plane,master   6d23h   v1.21.1
```

4. Type **exit** and press the **Enter** key to return to the main menu.

```
root@sfss:/home/stfs# exit
exit
press [enter] to go back to main menu...
```

5. Select **7** to **Logout**.

```
################################################################################
Welcome to Dell Smart Fabric Storage Software (SFSS) management
################################################################################

   Menu
```

```
--------------------------------------------------------------------------------
1. Show version
2. Debug
3. Password/SSL configuration menu
4. Show EULA
5. Interface configuration menu
6. Reboot
7. Logout

Enter selection [ 1 - 7 ] : 7
```

D

Additional Information

Technical resources

Dell Technologies Storage Networking Info Hub

Dell Technologies eSupport - Storage Networking

Dell Technologies SmartFabric Storage Software Product Page

Dell Technologies NVMe over Fabrics Product Page

Dell Technologies Interactive Demo: Deploying SmartFabric Storage Software (SFSS) for NVMe over TCP

Dell Networking Info Hub

Dell Networking OS10 Info Hub on eSupport

Dell SmartFabric OS10 User Guide Release 10.5.0

Networking Solutions Support and Interoperability Matrix

Dell PowerSwitch S3048-ON Documentation

Dell PowerSwitch S4148-ON Documentation

Dell PowerSwitch S4048-ON Documentation

Dell PowerSwitch S5248F-ON Documentation

Dell PowerSwitch Z9264F-ON Documentation

PowerStore: Info Hub - Product Documentation and Videos

Dell Networking Transceivers and Cables

Dell OpenManage Network Integration for VMware vCenter

Dell OS10 SmartFabric Services FAQ

Dell Technologies Solve Online

Dell SmartFabric Services with PowerEdge Servers, PowerStore Storage Appliance, and Isilon Storage

Manuals and documentation for PowerEdge R640

Dell Networking L3 Design for Leaf-Spine with OS10EE

Support and feedback

For technical support, visit https://www.dell.com/support.

We encourage readers to provide feedback on the quality and usefulness of this publication by sending an email to Dell_Networking_Solutions@Dell.com.