Using Dell PowerFlex NFS with VMware Cloud Foundation

October 2023

H19673

Implementation Guide

Abstract

This document provides guidance for using Dell PowerFlex NFS as Principal Storage for Workload Domains in VMware Cloud Foundation (VCF).

Dell Technologies PowerFlex Engineering

PowerFlex Engineering
Validated

Copyright

Contents

Contents

Chapter 1 Introduction

This chapter presents the following topics:

Executive summary

VMware Cloud Foundation, or VCF, is a complete software-defined infrastructure platform that encompasses all the required components to run a private, public, or hybrid cloud. The heart of VCF is the software-defined data center, or SDDC Manager. From the SDDC Manager, the user can control all aspects of the VCF environment, providing a single management interface. The other components of the VCF platform include vSphere for compute, vSAN for storage, NSX-T for networking, and the vRealize Suite (optional) for management.

VCF uses a concept of domains. The management domain comprises the heart of the VCF implementation and requires vSAN storage. Its main function is to run the VCF environment. A workload domain is designed to run customer workloads. Workload domains are managed by a single vCenter Server instance and can consist of one or more vSphere clusters. A workload domain offers the flexibility of using various storage solutions other than vSAN, such as FC, vVols, and NFS. This permits the use of more robust storage array solutions like NFS on PowerFlex.

Network File System (NFS) is a distributed file system protocol that allows users to access files over a network. NFS is a common choice with storage for workload domains because it is simple to implement and manage. When using NFS storage with VCF, it is important to pick a platform that meets the performance and scalability requirements of your workloads. PowerFlex is the perfect solution for VCF as its NAS implementation can scale up to 16 nodes, supports both NFS 3 and 4.1, and delivers superior performance when matched with a high performance, low latency network.

This paper provides an overview of how to implement NFS storage with VCF when deployed on a PowerFlex platform. It covers deployment of both the management and workload domain, configuration of NFS on PowerFlex, and best practices when using NFS with VCF.

Note: PowerFlex does not support VMware Virtual Volumes with PowerFlex 4.x, so it is not an available option for VCF storage.

Document purpose

This guide provides configuration details for implementing VMware Cloud Foundation on Dell servers and PowerFlex storage. It demonstrates how to use NFS file systems as principal storage for workload domains.

Note: Examples that are provided in this guide cover performing various VMware vSphere activities using PowerFlex systems and Dell software. These examples were developed for laboratory testing and may need tailoring to suit other operational environments. Any procedures that are outlined in this guide should be thoroughly tested before implementing in a production environment.

Note: The contents of this document are valid for the described software and hardware versions. For information about updated configurations for newer software and hardware versions, contact your VMware or Dell Technologies sales representative.

Audience

This document is intended for use by storage administrators, system administrators, and VMware vSphere administrators.

Readers of this document are expected to be familiar with the following topics:

- Dell PowerFlex system operation
- Dell software including the following: PowerFlex Manager (4.x)
- General storage concepts
- VMware Cloud Foundation, including vSphere, NSX, and vSAN
- VMware vSphere products and their operations

Wizard walkthroughs

Because users are expected to be familiar with the products and technologies that are covered in the guide, not every step of each wizard has an associated image. The steps are always documented, however.

Table 1. Revision history

Part number	Release date	Description
H19673	October 2023	Initial release

Terminology

The following table provides definitions for some of the terms that are used in this document.

Table 2. Terminology

Term	Definition
ITOM	IT Operational Management
LCM	Life Cycle Management – automation of patching and upgrades of VCF
BOM	Bill of Materials
MDM	Meta Data Manager
SDC	Storage Data Client
SDS	Storage Data Server
VDS	vSphere Distributed Switch (defined and managed by vCenter)
VM	Virtual Machine
VI	Virtual Infrastructure – used in reference to a workload domain
VCF	VMware Cloud Foundation

Chapter 2 Product overview

This chapter presents the following topics:

PowerFlex family overview

PowerFlex software-defined infrastructure enables broad consolidation across the data center, encompassing almost any type of workload and architecture. The software-defined architecture offers automation and programmability of the complete infrastructure and provides scalability, performance, and resiliency to enable effortless adherence to stringent workload SLAs.

The PowerFlex family provides a foundation that combines compute and high-performance storage resources in a managed unified fabric. PowerFlex comes in flexible deployment options (rack, appliance, or custom nodes and in the public cloud) that enables independent (two-layer), HCI (single-layer), or mixed architectures. PowerFlex is ideal for high-performance applications and databases, building an agile private-hybrid cloud, or consolidating resources in heterogeneous environments.

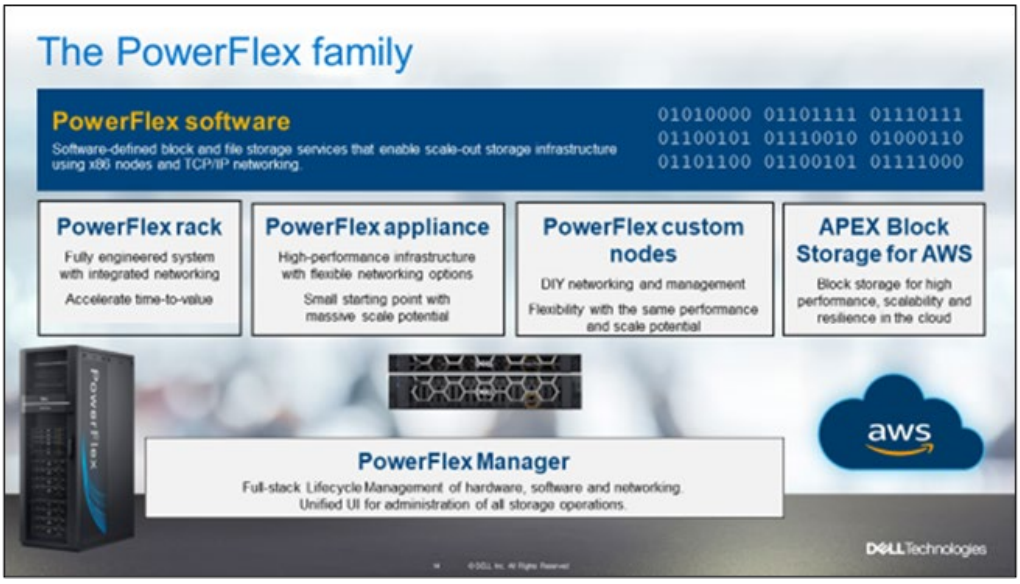

Figure 1. PowerFlex family

PowerFlex software components

Software is the key differentiation in the PowerFlex offering. PowerFlex software components not only provide software-defined storage services, but also help simplify infrastructure management and orchestration. This software enables comprehensive IT Operational Management (ITOM) and Life Cycle Management (LCM). These capabilities span compute and storage infrastructure, from BIOS and Firmware to nodes, software, and networking.

PowerFlex

PowerFlex is the software foundation of PowerFlex software-defined infrastructure. It is a scale-out block and file storage service that is designed to deliver flexibility, elasticity, and simplicity with predictable high performance and resiliency at scale.

PowerFlex Manager

PowerFlex Manager is the software component in the PowerFlex family that enables ITOM automation and LCM capabilities for PowerFlex systems. Starting with PowerFlex 4.0, the unified PowerFlex Manager brings together three separate components from previous releases: PowerFlex Manager, the core PowerFlex UI, and the PowerFlex

gateway. The new PowerFlex UI runs in Kubernetes and embraces a modern development framework.

PowerFlex file services

PowerFlex File Controllers, also known as File Nodes, are physical nodes that enable PowerFlex software defined File Services. They host the NAS Servers, which in turn host tenant namespaces and file systems, mapping PowerFlex volumes to the file systems presented by the NAS Servers. All major protocols are supported, such as NFS, SMB-CIFS, FTP, and NDMP. Both NFS 3 and 4 are supported. PowerFlex file service is supported from PowerFlex 4.0.

PowerFlex CSI and CSM

An important component outside of PowerFlex that enables a flexible consumption model for Kubernetes is the PowerFlex CSI driver. It was developed as a part of the Dell Kubernetes strategy. After the CSI driver for PowerFlex is loaded into Kubernetes, it can be used to provision persistent volumes from the underlying PowerFlex storage resource. If the Kubernetes deployment is running low on PowerFlex storage resources, you can add PowerFlex storage nodes to increase the system capacity and performance.

The CSI driver connects the PowerFlex system and Kubernetes deployments. It is a storage broker agent which dynamically provisions volumes from PowerFlex through the PowerFlex API gateway to the Kubernetes cluster. Once the volume is available on PowerFlex, it is immediately mapped to the requesting pod. If a pod is destroyed or rescheduled, the CSI plug-in ensures that the volumes are remapped upon rescheduling of that pod.

Customers running Kubernetes clusters on PowerFlex use the Dell Container Storage Modules (CSM), which extend the CSI driver capabilities. These modules:

- Provide enterprise storage capabilities to Kubernetes for cloud-native stateful applications.
- Reduce management complexity, so that developers can independently use enterprise storage with ease and automate daily operations.
- Extend storage functionality and capabilities beyond using the CSI driver alone.

These modules include snapshot, observability, authorization, application mobility, and resiliency.

PowerFlex supports multiple operating systems and different deployment options for on-premises and public cloud deployment models (available in AWS). PowerFlex is validated with the leading Kubernetes distributions as shown in Figure 2.

Figure 2. PowerFlex for different Kubernetes distributions

PowerFlex deployment architectures

PowerFlex software-defined infrastructure excels in deployment flexibility. PowerFlex can be deployed in a two-layer (independent compute and storage layers), single-layer (Hyperconverged Infrastructure, or HCI), or a mixture of the two architectures (Mixed).

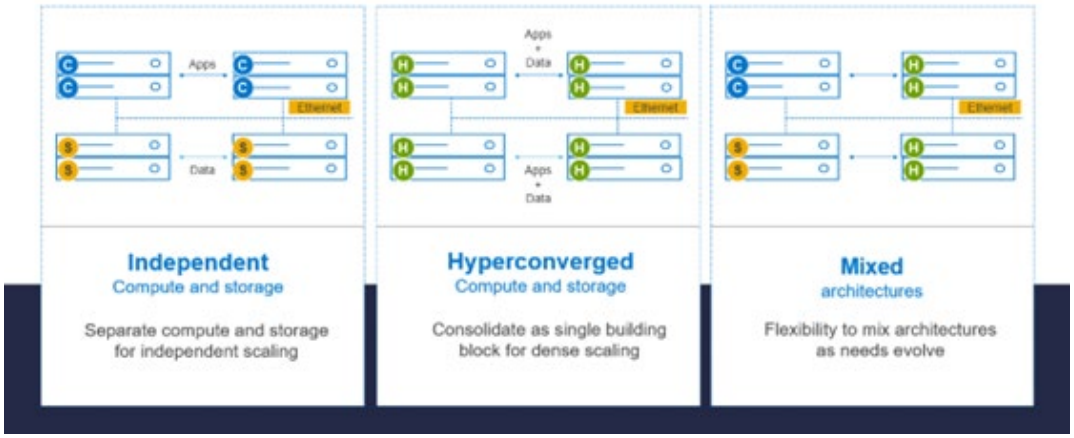

Figure 3. PowerFlex architectures

Independent architecture

In an independent architecture or two-layer architecture, some nodes provide storage capacity for data in applications. Other separate and independent nodes provide compute resources for applications and workloads. Compute and storage resources can be scaled independently by adding nodes to the cluster while it remains active. This separation of compute and storage resources helps to minimize software licensing costs in certain situations. This architecture can be ideal for high-performance databases and application workloads.

Hyperconverged architecture

In an HCI architecture, each node in the cluster contributes storage and compute resources simultaneously to the applications and workloads. This architecture allows you

to scale your infrastructure uniformly with building blocks that add both storage and compute resources. This architecture is appropriate for data center and workload consolidation.

Mixed architecture

A mixed architecture has a combination of both the HCI and Independent architectures. As shown previously in Figure 3, there would be some storage only nodes, compute only nodes, and hyperconverged nodes as part of the same PowerFlex cluster. This architecture is desirable when working with an existing compute infrastructure and adding high-performance software-defined infrastructure. This architecture can also be a starting point for a two-layer deployment design as external workloads are migrated to PowerFlex.

PowerFlex consumption options

PowerFlex rack

PowerFlex rack is a software-defined infrastructure platform that delivers flexibility, elasticity, and simplicity with predictable performance and resiliency at scale. It combines compute and high-performance storage resources in a managed unified network. This rack-based engineered system, with integrated networking, enables customers to achieve the scalability and management requirements of a modern data center.

PowerFlex appliance

PowerFlex appliance is a PowerEdge server which has been configured to be a node in a software-defined infrastructure deployment that runs PowerFlex software components. This offering allows customers the flexibility and savings to bring their own compatible networking.

PowerFlex Custom Nodes

PowerFlex Custom Nodes are validated server building-blocks that are configured for use with PowerFlex. They are available with thousands of configuration options and are available for customers who prefer to build their own environments.

Dell APEX Block Storage for AWS

PowerFlex software can also be deployed in the public cloud. It is available in the Amazon Marketplace as Dell APEX Block Storage for AWS (formerly known as PowerFlex cloud storage). PowerFlex on AWS offers the same on-premises benefits of high-performance, linear scalability, and high resilience as with cloud. PowerFlex also adds cloud-specific benefits, such as large volume sizes, extreme performance based on NVMe drives, and predictable scalability. With PowerFlex on AWS, you can also get higher Multi Availability Zone (Multi AZ) resiliency when PowerFlex Fault sets are distributed across multiple AWS Availability Zones. For more information, see Dell APEX Block Storage for AWS.

VCF

VMware Cloud Foundation (VCF) is a complete software-defined management solution that consists of VMware vSphere, VMware NSX-T Data Center, VMware vSAN, and vRealize Suite. The installation of VCF is driven by VMware Cloud Builder. The various components serve the following roles:

- VMware Cloud Builder: A virtual appliance the user deploys that automates the building of the management domain of VCF by accepting the planning guide (xls) as input. Subsequent domains are provisioned through the SDDC Manager.

- SDDC Manager: Automates the life cycle management of VCF. It enables patching and upgrades, firmware application, and the general day to day operation of VCF.
- VMware vSphere: Virtualizes the bare-metal servers using the ESXi software and aggregates them in the vCenter Server.
- VMware NSX-T Data Center: Provides the networking for the VCF solution along with security and automation. NSX-t is designed for both private and public clouds.
- VMware vSAN: Aggregates local or direct-attached storage in a single pool that can be shared across all ESXi hosts in the VCF environment. vSAN is a required component of the management domain.
- vRealize Suite Lifecycle Manager: An optional component of VCF which, when deployed, can be used to enable other vRealize Suite products. These products can manage infrastructure and applications in the private or public cloud.

VMware portrays the high-level VCF implementation as depicted in Figure 4.

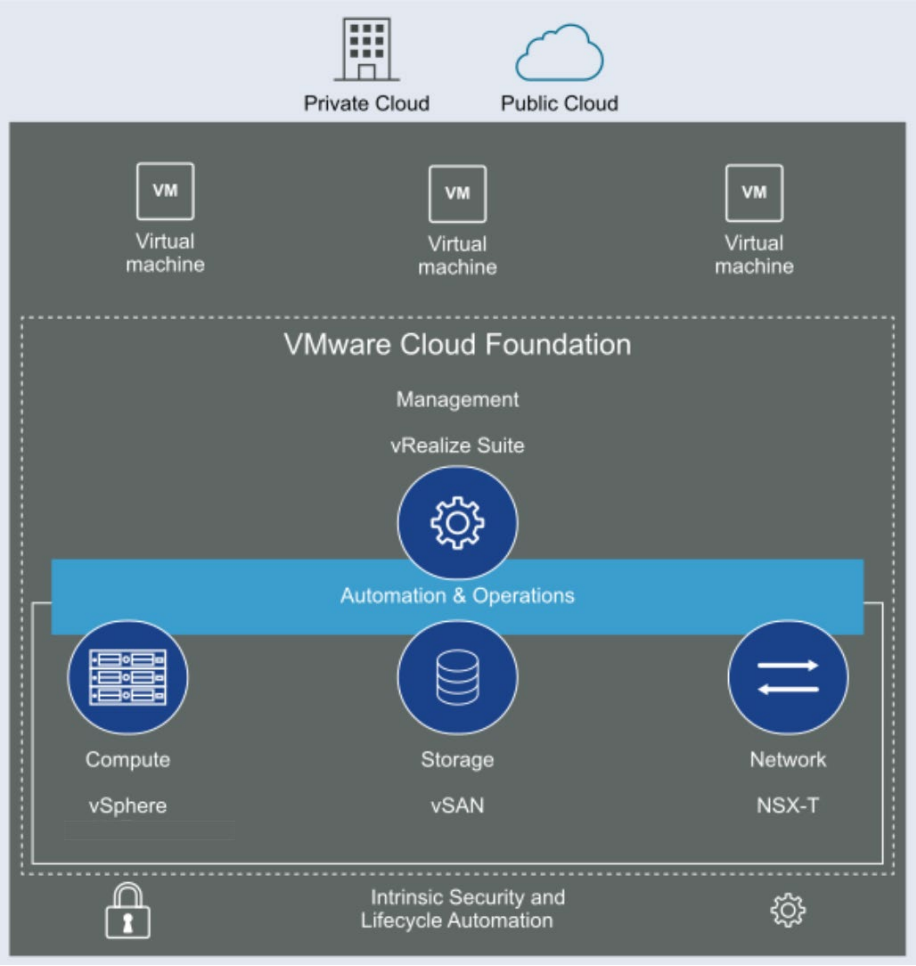

Figure 4. VMware Cloud Foundation

Chapter 3 Environment and system requirements

This chapter presents the following topics:

Introduction

The following sections cover the requirements for implementing VCF on a PowerFlex 4.x system using NFS as principal storage for the workload domain.

Prerequisites

The following prerequisites must be met before implementing VCF on PowerFlex using NFS as principal storage. They are meant to be high level as some tasks related to them are covered in the paper.

- A PowerFlex system must be installed and configured with the File option (SDNAS). PowerFlex supports File in node pairs from 2 to 16. The type of PowerFlex system (such as appliance or custom node) is not critical to the solution.
- Six Dell servers with sufficient networking, memory, CPU, and storage to satisfy the requirements of VCF and vSAN. VCF uses the policy of Bring Your Own Network (BYON) and therefore the VMware compatibility guide no longer certifies vSAN Ready Nodes, rather the customer should use the VCF Planning Guide. Note that the two servers used for the workload domain will not require storage for vSAN as they are using NFS.
- Licenses must be obtained for PowerFlex and all the VCF components in use.

VCF components

Each version of VCF includes a bill of materials (BOM) which dictates the versions for each component of the solution. VMware offers no ability to substitute. For example, even if there is a newer update for ESXi at the time of installation, VMware requires the version on the BOM. The versions are shown in Table 3.

Table 3. Bill of Material

Software Component	Version	Build Number
Cloud Builder VM	4.5.2	22223457
SDDC Manager	4.5.2	22223457
VMware vCenter Server Appliance	7.0 Update 3m	21784236
VMware ESXi	7.0 Update 3n	21930508
VMware vSAN Witness Appliance	7.0 Update 3l	21424296
VMware NSX-T	3.2.3.1	22104592
VMware vRealize Suite Lifecycle Manager	8.10	21950667

Network topology

At the physical layer, two Top of Rack (TOR) switches are used for redundancy and load-balancing purposes. There are four connections from each Dell host, two to TOR A and two to TOR B. VCF requires two of the connections to form the vSphere Distributed Switch (VDS).

The following table shows the different networks that are configured for this solution.

Note: All VLANs are tagged except for management (1109). An untagged VLAN requires setting VLAN ID to 0 in vSphere.

Table 4. Network VLANs

Network type	VLAN ID
Management	0
vMotion	1612
vSAN	1613
NSX-T Host Overlay	1614

PowerFlex topology

The PowerFlex 4.x system consists of five nodes, three for the MDM cluster and two for File. The characteristics of these servers are covered in Table 5.

Table 5. PowerFlex node configurations

Dell Model	MDM Role	SDS	File Node	CPU	Memory	Storage	Network
R650	Primary	Yes	No	2 * Intel(R) Xeon(R) Gold 6336Y CPU @ 2.40GHz (Core Count 24)	512 GB (16 * 32 GB, 2933 MT/s DRAM DDR-4), 32 GB (2 * 16 GB, 2933 MT/s NVDIMM-N DDR-4)	2 * 447.13 GB (SATA SSD), 10 * 1490.42 GB (SAS SSD)	2 * Mellanox ConnectX-5 EN 25GbE SFP28 Adapter
R650	Secondary	Yes	No	2 * Intel(R) Xeon(R) Gold 6336Y CPU @ 2.40GHz (Core Count 24)	512 GB (16 * 32 GB, 2933 MT/s DRAM DDR-4), 32 GB (2 * 16 GB, 2933 MT/s NVDIMM-N DDR-4)	2 * 447.13 GB (SATA SSD), 10 * 1490.42 GB (SAS SSD)	2 * Mellanox ConnectX-5 EN 25GbE SFP28 Adapter
R650	Tie Breaker	Yes	No	2 * Intel(R) Xeon(R) Gold 6336Y CPU @ 2.40GHz (Core Count 24)	512 GB (16 * 32 GB, 2933 MT/s DRAM DDR-4), 32 GB (2 * 16 GB, 2933 MT/s NVDIMM-N DDR-4)	2 * 447.13 GB (SATA SSD), 10 * 1490.42 GB (SAS SSD)	2 * Mellanox ConnectX-5 EN 25GbE SFP28 Adapter
R650	None	No	Yes	2 * Intel(R) Xeon(R) Gold 6336Y CPU @ 2.40GHz (Core Count 24)	512 GB (16 * 32 GB, 2933 MT/s DRAM DDR-4), 32 GB (2 * 16 GB, 2933 MT/s NVDIMM-N DDR-4)	2 * 447.13 GB (SATA SSD), 10 * 1490.42 GB (SAS SSD)	2 * Mellanox ConnectX-5 EN 25GbE SFP28 Adapter
R650	None	No	Yes	2 * Intel(R) Xeon(R) Gold 6336Y CPU @ 2.40GHz (Core Count 24)	512 GB (16 * 32 GB, 2933 MT/s DRAM DDR-4), 32 GB (2 * 16 GB, 2933 MT/s NVDIMM-N DDR-4)	2 * 447.13 GB (SATA SSD), 10 * 1490.42 GB (SAS SSD)	2 * Mellanox ConnectX-5 EN 25GbE SFP28 Adapter

VCF servers

The VCF environment as described in this paper consists of six servers, four for the management domain and two for the workload domain. Although the specifications of all servers are the same, they are listed below in Table 6 for completeness.

Table 6. VCF server configurations

Dell Model	Management Domain	Workload Domain	CPU	Memory	Storage	Network
R650	Yes	No	2 * Intel(R) Xeon(R) Gold 6336Y CPU @ 2.40GHz (Core Count 24)	512 GB (16 * 32 GB, 2933 MT/s DRAM DDR-4), 32 GB (2 * 16 GB, 2933 MT/s NVDIMM-N DDR-4)	2 * 447.13 GB (SATA SSD), 10 * 1490.42 GB (SAS SSD)	2 * Mellanox ConnectX-5 EN 25GbE SFP28 Adapter
R650	**Yes**	No	2 * Intel(R) Xeon(R) Gold 6336Y CPU @ 2.40GHz (Core Count 24)	512 GB (16 * 32 GB, 2933 MT/s DRAM DDR-4), 32 GB (2 * 16 GB, 2933 MT/s NVDIMM-N DDR-4)	2 * 447.13 GB (SATA SSD), 10 * 1490.42 GB (SAS SSD)	2 * Mellanox ConnectX-5 EN 25GbE SFP28 Adapter
R650	**Yes**	No	2 * Intel(R) Xeon(R) Gold 6336Y CPU @ 2.40GHz (Core Count 24)	512 GB (16 * 32 GB, 2933 MT/s DRAM DDR-4), 32 GB (2 * 16 GB, 2933 MT/s NVDIMM-N DDR-4)	2 * 447.13 GB (SATA SSD), 10 * 1490.42 GB (SAS SSD)	2 * Mellanox ConnectX-5 EN 25GbE SFP28 Adapter
R650	**Yes**	No	2 * Intel(R) Xeon(R) Gold 6336Y CPU @ 2.40GHz (Core Count 24)	512 GB (16 * 32 GB, 2933 MT/s DRAM DDR-4), 32 GB (2 * 16 GB, 2933 MT/s NVDIMM-N DDR-4)	2 * 447.13 GB (SATA SSD), 10 * 1490.42 GB (SAS SSD)	2 * Mellanox ConnectX-5 EN 25GbE SFP28 Adapter
R650	No	**Yes**	2 * Intel(R) Xeon(R) Gold 6336Y CPU @ 2.40GHz (Core Count 24)	512 GB (16 * 32 GB, 2933 MT/s DRAM DDR-4), 32 GB (2 * 16 GB, 2933 MT/s NVDIMM-N DDR-4)	2 * 447.13 GB (SATA SSD), 10 * 1490.42 GB (SAS SSD)	2 * Mellanox ConnectX-5 EN 25GbE SFP28 Adapter
R650	No	**Yes**	2 * Intel(R) Xeon(R) Gold 6336Y CPU @ 2.40GHz (Core Count 24)	512 GB (16 * 32 GB, 2933 MT/s DRAM DDR-4), 32 GB (2 * 16 GB, 2933 MT/s NVDIMM-N DDR-4)	2 * 447.13 GB (SATA SSD), 10 * 1490.42 GB (SAS SSD)	2 * Mellanox ConnectX-5 EN 25GbE SFP28 Adapter

vSAN

The following are the prerequisites to build the required vSAN storage setup for VCF:

- One SAS or SATA host bus adapter (HBA), or a RAID controller that is in passthrough mode or RAID 0 mode.
- For cache storage: One SAS or SATA solid-state disk (SSD) or PCIe flash device.
- For capacity storage: An All-flash disk group configuration that must have at least one SAS, or SATA solid-state disk (SSD), or PCIe flash device.

Generally, the first bullet point is standard for most servers so that is unlikely to cause a problem with vSAN. For the other two bullet points, there is a known issue where during the validation of the Planning Guide VMware is unable to identify devices for use with vSAN. VCF requires a ratio of one cache device to seven capacity devices. If the disks are available and visible on ESXi, but they are not recognized, it is possible to manually assign them as vSAN-eligible. This is a two-step process which is outlined below.

Formatting

The first issue is common during the validation step of the install. VMware reports that the devices on the servers have existing partitions, which render them ineligible for vSAN. To determine which devices are problematic, issue the command `vdq -qH` in ESXi to view all the devices and check the **State** row. An example is shown in Figure 5:

```
[root@austin243:~] vdq -qH
     DiskResult[6]:
          Name:  t10.NVMe____Dell_Ent_NVMe_FIPS_CM6_RI_1.92TB_______0130D00CE28EE38C
       VSANUUID:
          State:  Ineligible for use by VSAN
         Reason:  Has partitions
          IsSSD?:  1
IsCapacityFlash?:  0
          IsPDL?:  0
       Size(MB):  1831420
     FormatType:  512e
  IsVsanDirectDisk?:  0
```

Figure 5. Ineligible for vSAN due to existing partitions

For this particular issue, the solution is to wipe the existing partition. This can be achieved by using the utility `partedUtil` to create a new gpt partition on the disk, clearing out the existing ones. The following is an example of the CLI command:

```
partedUtil mklabel
/vmfs/devices/disks/t10.NVMe____Dell_Ent_NVMe_FIPS_CM6_RI_1.92TB__
______0130D00CE28EE38C gpt
```

While the command itself does not return any response, running the `vdq` command once more shows that the **State** of the disk is now eligible, as shown in Figure 6.

```
     DiskResult[6]:
          Name:  t10.NVMe____Dell_Ent_NVMe_FIPS_CM6_RI_1.92TB_______0130D00CE28EE38C
       VSANUUID:
          State:  Eligible for use by VSAN
         Reason:  None
          IsSSD?:  1
IsCapacityFlash?:  0
          IsPDL?:  0
       Size(MB):  1831420
     FormatType:  512e
  IsVsanDirectDisk?:  0
```

Figure 6. Eligible for vSAN

Capacity versus cache

The second issue for vSAN occurs when the devices are all of the same type, as they are on the servers in this environment. In such cases VMware treats all the devices as cache storage and thereby leaves no devices for capacity, which is required. This appears to be the most common of the two issues, and impacted the environment detailed in this paper. Fortunately, VMware provides a CLI command to "tag" devices as "capacityFlash" so that VCF will claim all tagged devices as capacity devices, and any non-tagged devices as cache, thereby satisfying the requirements for building the vSAN cluster. Since vSAN needs at least one cache device, it is best to tag all available devices for capacity, save one. Use the following command to tag devices:

```
esxcli vsan storage tag add -t capacityFlash -d
t10.NVMe____Dell_Ent_NVMe_FIPS_CM6_RI_1.92TB________0130D00CE28EE3
8C
```

After running the command in Figure 7 and querying the disk, the row **IsCapacityFlash?** now shows a positive '1'.

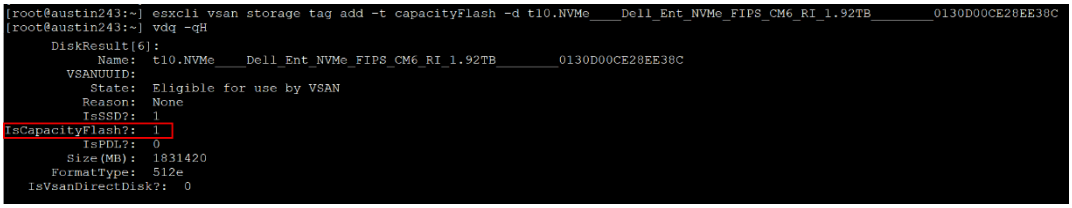

Figure 7. Setting the vSAN capacity tag

With the devices tagged, the Cloud Builder installer can create the vSAN cluster. In this environment, which includes 11 devices, VCF creates three vSAN disk groups for each host. Two of the disk groups will have three capacity devices and one cache device, and one of the disk groups will have two capacity devices and one cache device. One of these hosts is shown in Figure 8.

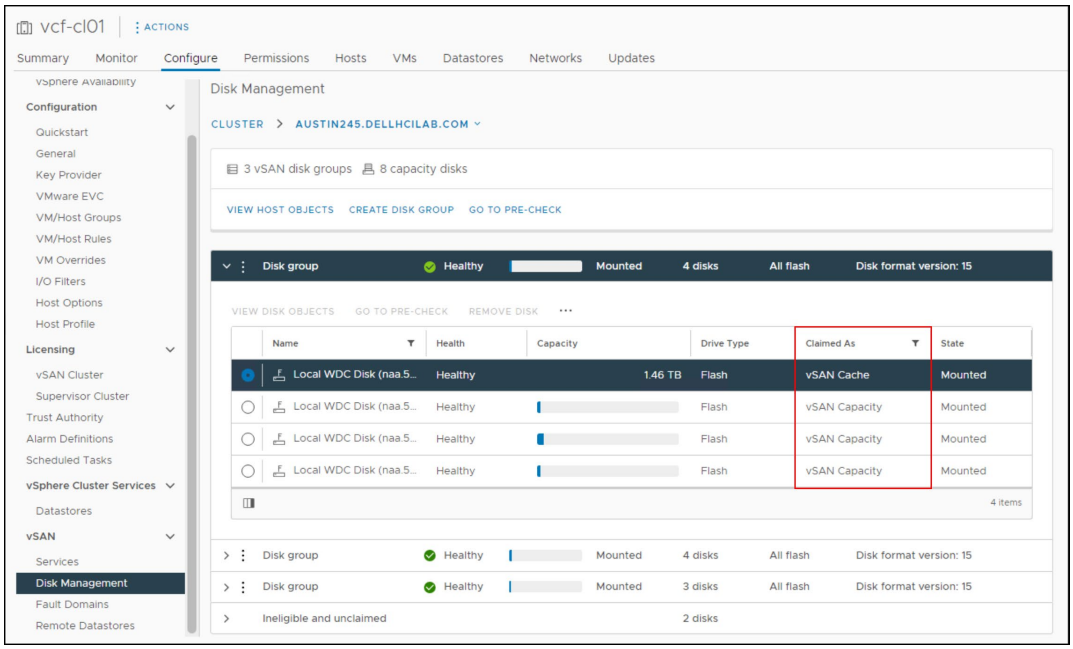

Figure 8. vSAN disk groups in VCF

Domains

VCF uses a concept called domains. Domains are essentially a set of resources such as servers, storage, and software. There are two types of domains in VCF: management and workload. There is one management instance per VCF. The management domain is the set of resources that runs VCF. The management domain is the control center of the environment, handling all aspects of life cycle management through an optional component, VMware vRealize Lifecycle Manager. The basic management functions are handled through the SDDC Manager, which is the interface to VCF, much like vCenter is to clusters of ESXi. VCF does not support controlling the management domain directly through the vCenter, though its hosts are managed by one.

Workload domains are deployed from the SDDC Manager and consist of their own vCenter, cluster, hosts, and storage. These workload domains are typically used to run the applications for a business. Unlike the management domain, the workload domain offers great flexibility in storage, so customers with array storage can take full advantage of the features of an array for their applications. The number of workload domains is only limited by the resources available to support them. An example of a VCF instance with two workload domains is shown in Figure 9.

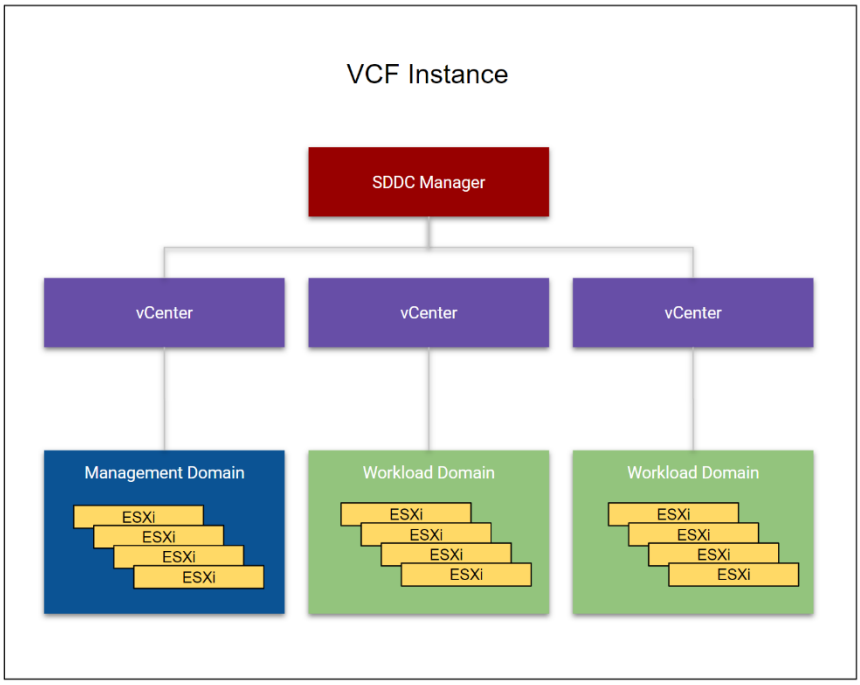

Figure 9. VCF instance with two workload domains

While the management and workload domains typically include separate hardware, for those customers with less server resources, or want a smaller footprint or even a POC lab, it is possible for the management domain to also be a workload domain. This is known as a consolidated architecture. In such a configuration the same vSAN that is used for the management domain can also be used for the workload domain, alleviating the need for more disk.

Storage

Storage plays an important role in VCF as vSAN is part of the solution. There are two different categories of storage in VCF, each serving different functions in the solution. They are called principal and supplemental. Principal storage is what is required to deploy a domain–management (vSAN only) or workload–or to deploy a new cluster in an existing workload (including the management domain). It can be of type vSAN, FC, vVols, or NFS. Supplemental storage is the storage that can be added to any existing management or workload domain to offer more space post deployment. Supplemental storage supports all the types of principal storage, as well as iSCSI and the PowerFlex specific SDC. These storage options are shown in Figure 10.

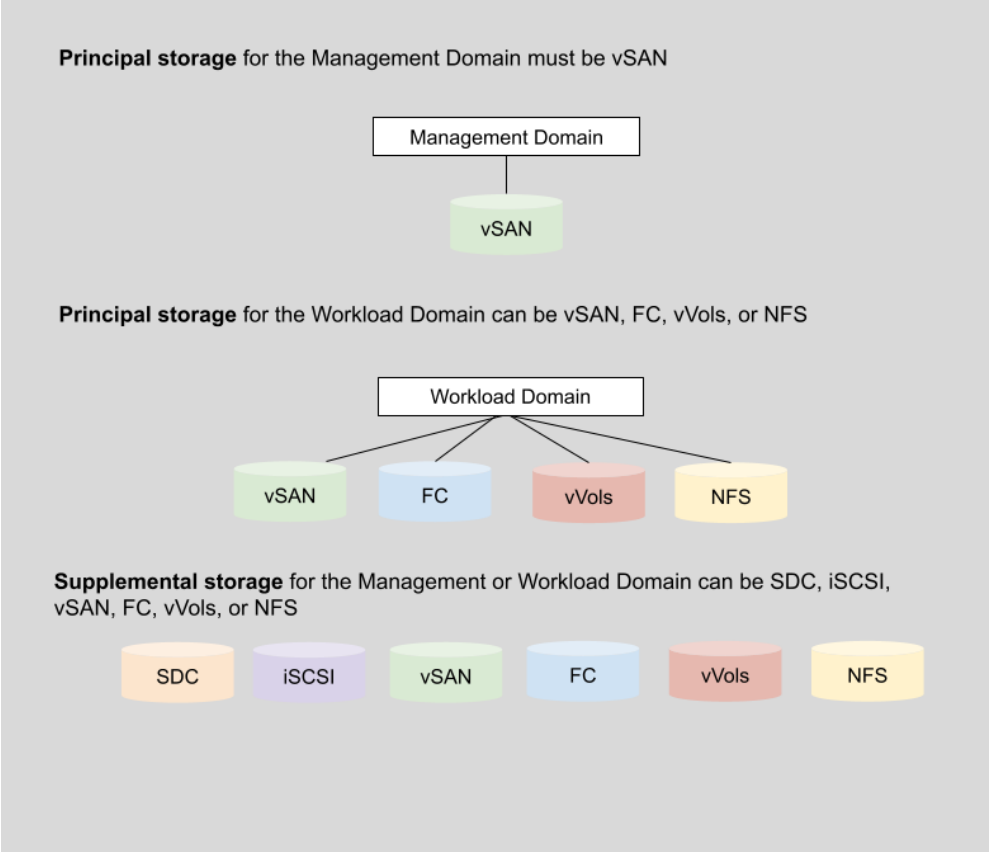

Figure 10. VCF storage options

As noted, vSAN is the only supported principal storage for the management domain. VMware requires vSAN in the management domain in order to have full control over storage life cycle management from creation to deletion. VCF does not provide this level of control for non-vSAN storage and thus requires the user to manage the life cycle. The entire VCF solution can run on vSAN with no other storage (and VMware strongly recommends this), but at a minimum vSAN must be used to deploy the management domain.

Note: The VCF release covered in this paper is 4.5.2. In the most recent VCF releases, VMware added support for NVMeoF for supplemental storage. See the VMware documentation for specific releases and their storage support.

Vendor storage support

VMware does not publish storage support for VCF by vendor, rather they rely on the VMware Compatibility Guide for Storage/SAN (https://www.vmware.com/resources/compatibility/search.php?deviceCategory=san). If the vendor is listed as supporting the protocol for the version of ESXi in the BOM, then it is supported with VCF. For example, Dell PowerFlex is listed as supporting ESXi 7 and 8 running on NFS, therefore NFS can be used as principal or supplemental storage with VCF.

Chapter 4 Deployment

This chapter presents the following topics:

Introduction

The following sections detail the installation of VCF using the VMware Cloud Builder.

VCF installation

Although VCF consists of vSphere, vSAN, NSX, and the vRealize Suite, it does not require that the user install each of these components independently. The installation of the base component of VCF, or management domain, is accomplished using the VMware Cloud Builder which contains all the necessary software built in.

There are three steps to installation.

1. Prepare the environment. This is achieved through the Planning and Preparation Workbook that VMware provides. There are three tabs—Credentials, Hosts and Networks, and Deploy Parameters—where the user inputs IPs, NSX and SDDC Manager information, and passwords among other entries.
2. Image all servers with the ESXi version that is listed in the Bill of Materials. This is a straightforward install, choosing among the available methods, and then minor modifications post-install of setting IPs, hostname, and so on. This is the only software that the VMware Cloud Builder does not install.
3. Install VMware Cloud Foundation. This requires first deploying the VMware Cloud Builder appliance which is a wizard-driven application that accepts the prepared workbook as input to create the management domain.

The following section walks through the installation of the management domain.

VMware Cloud Builder

The VMware Cloud Builder is a virtual appliance with a UI that guides the user through the VCF installation using the **vcf-ems-deployment-parameter.xls** spreadsheet which VMware terms the **Planning and Preparation Workbook**. The appliance is best deployed on an existing ESXi host or vCenter with access to the networking of the VCF environment. Once deployed, log in as the **admin** user. The screen in Figure 11 appears, providing the user with two options for a VCF installation: standard or VxRail. As this setup includes independent servers, leave the default radio button selected.

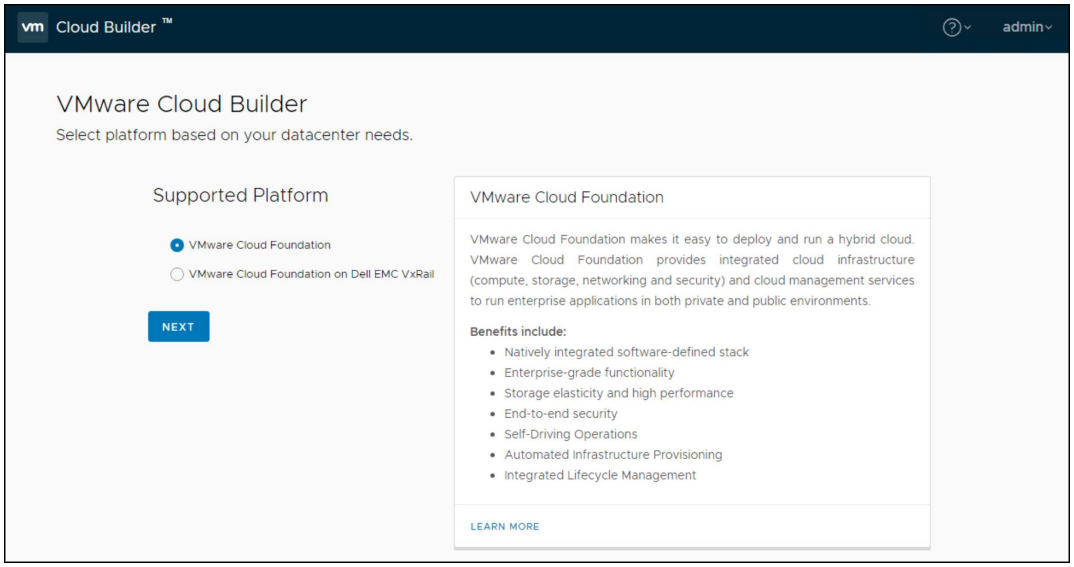

Figure 11. VCF installation initial screen

Note: While the VMware Cloud Builder is the preferred method for a VCF installation, there is a VCF CLI which can be used. The major difference between the UI and CLI is the ability to highly customize a CLI installation. Environments with unique networking requirements, for example, may require the use of the CLI.

In the next page, shown in Figure 12, VMware lists all the prerequisites for a VCF installation. Although this information is available in the standard documentation, it is scattered there and not presented in as clear a manner as here. Dell recommends using the available **DOWNLOAD** or **PRINT** options in the upper right corner to save a copy of this and review it prior to checking the box and proceeding. The Cloud Builder will not validate every prerequisite prior to installing, so failure to complete them can result in installation failure. Although the installer can be retried at the point of failure after fixing the issue, there is no guarantee that it will succeed. Manually cleaning up a failed install is a time-consuming, and error-prone task so it should be avoided.

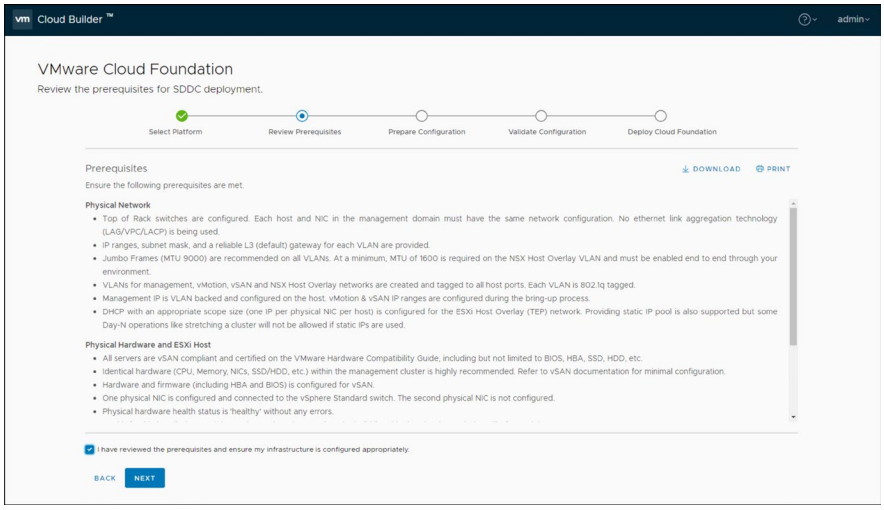

Figure 12. VCF installation prerequisites

Once the prerequisites are user-validated, there are three steps the UI walks the user through:

1. Download Workbook – if not done already VMware provides the ability to do so here.
2. Complete Workbook – an acknowledgment by the user.
3. Upload File – upload the completed workbook.

These three steps are shown completed in Figure 13.

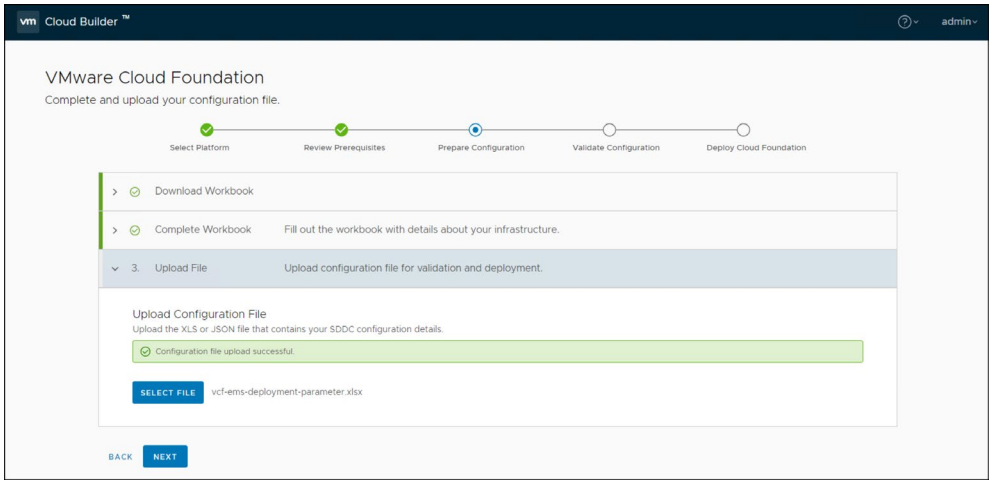

Figure 13. VCF installation – File upload

If the user selects **NEXT**, VMware will then attempt to validate the workbook against the environment as shown in Figure 14. As previously mentioned, it will not validate all prerequisites, though it endeavors to cover most. When failures occur, they must be rectified and the validation retried. For example, the vSAN configuration is a common problem area and may need a manual resolution as explained in the section titled vSAN.

Note that VMware will not prevent installation for warnings. In a lab setup, warnings may be acceptable, but should not be present for a production installation.

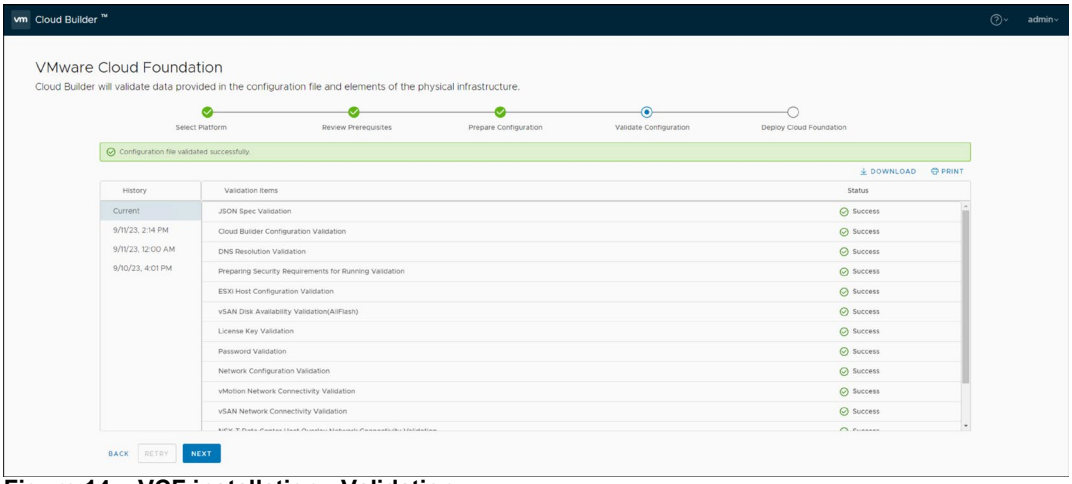

Figure 14. VCF installation - Validation

With validation complete, a final warning is given as in Figure 15. Before proceeding, ensure that all prerequisites are complete in addition to the validation. Although the dialog box indicates that only SDDC is being installed, it does include all the VCF components.

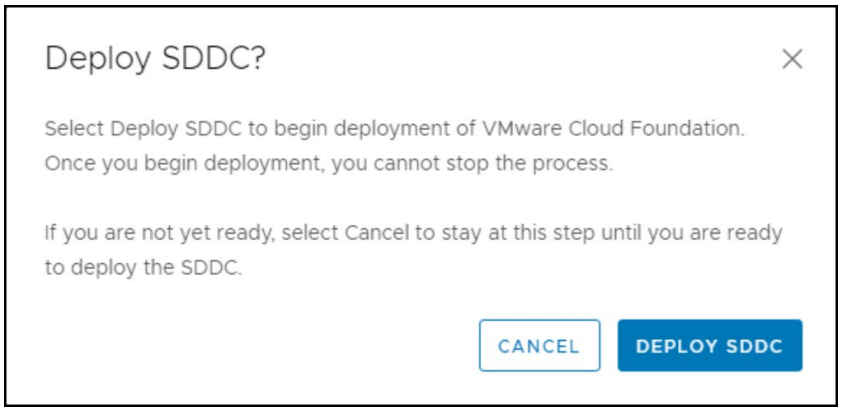

Figure 15. VCF installation – Deployment warning

The deployment time varies according to the environment and is measured in hours. Any errors during installation must be resolved, and the deployment retried. There is no cleanup or reset.

The UI will time out during deployment, but logging back in will always return the user to the current status. A completed installation is seen in Figure 16. Selecting **FINISH** brings up the **SDDC Deployment Complete** dialog box where **SDDC Manager** can be launched.

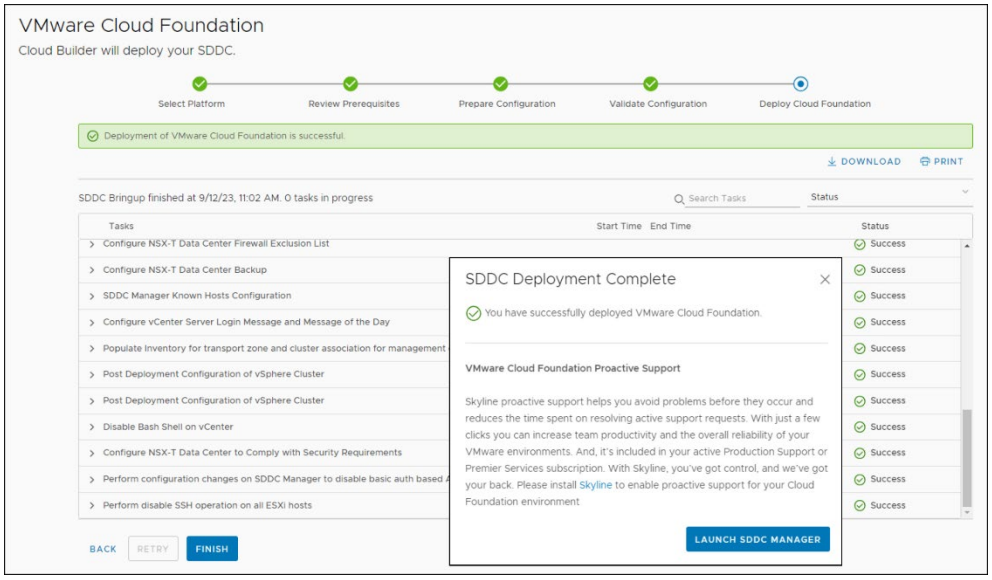

Figure 16. VCF installation - Complete

The **SDDC Manager Dashboard** appears as in Figure 17. From here, the workload domain can be deployed. This will be covered in the subsequent sections.

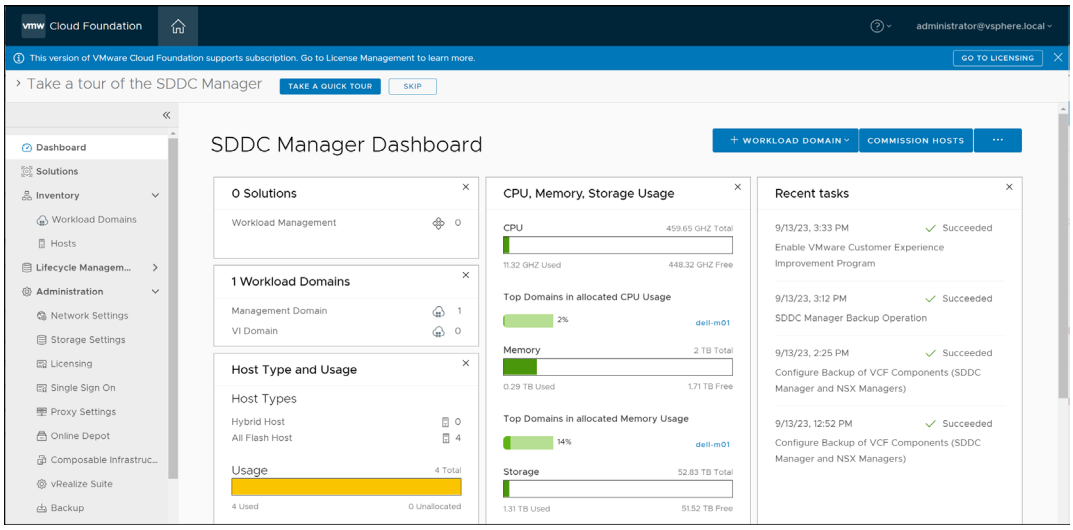

Figure 17. SDDC Manager Dashboard

Chapter 5 NFS Configuration

This chapter presents the following topics:

Introduction

The following sections detail the setup of an NFS file system on PowerFlex for use with a VCF workload domain.

Prerequisites for NFS Storage

VMware presents the following prerequisites for using NFS storage as principal storage for a workload domain:

- A minimum of two ESXi hosts available in SDDC Manager with NFS storage. This is an exception to the rule of three hosts for a workload domain, which is still the recommended minimum amount.
- An NFS Server that meets the NFS Storage Guidelines and Requirements found in the vSphere Storage Guide. Specifically, NFS version 3 is required for principal storage, though version 4 is supported when using NFS as supplemental.
- A Network Pool created in SDDC Manager that includes details for the vMotion and NFS networks to be used for the cluster.
- The FQDN/IP and the mount point folder name of the NFS server.

NFS file system

Before creating the NFS file system, ensure that there is an available NAS server. In this example, the server called **NAS_Production** with an IP of 100.80.130.223 is used as shown in Figure 18.

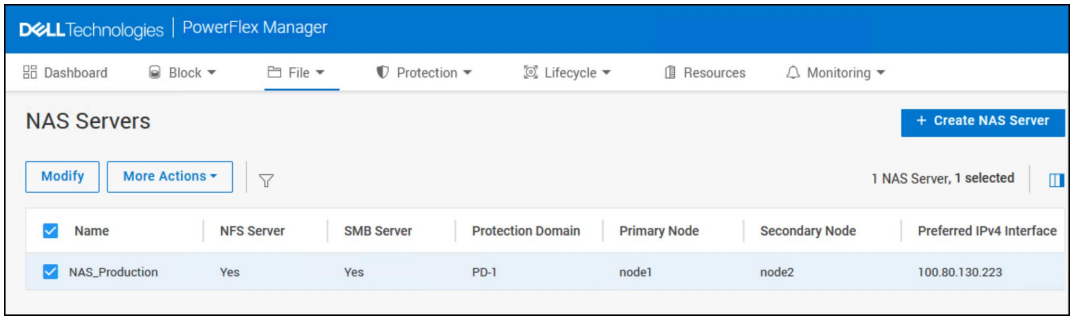

Figure 18. Production NAS server

Follow the steps to create an NFS file system in the PowerFlex UI.

1. Go to **File > File Systems**. Select **+ Create File System** as in Figure 19.

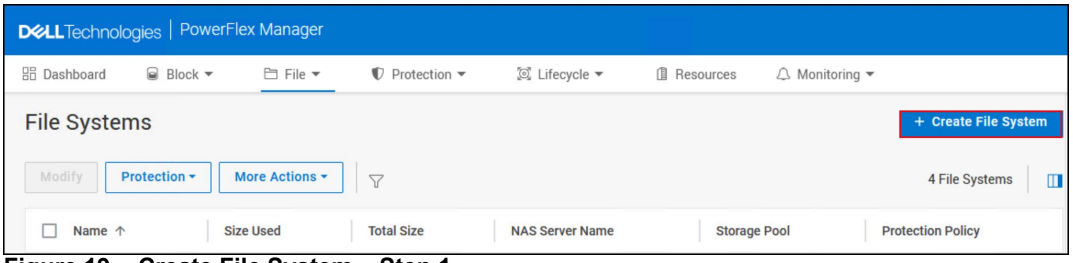

Figure 19. Create File System – Step 1

2. Select the previously noted **NAS Server** and click **Next** as in Figure 20. No additional settings are necessary as SMB is not being used.

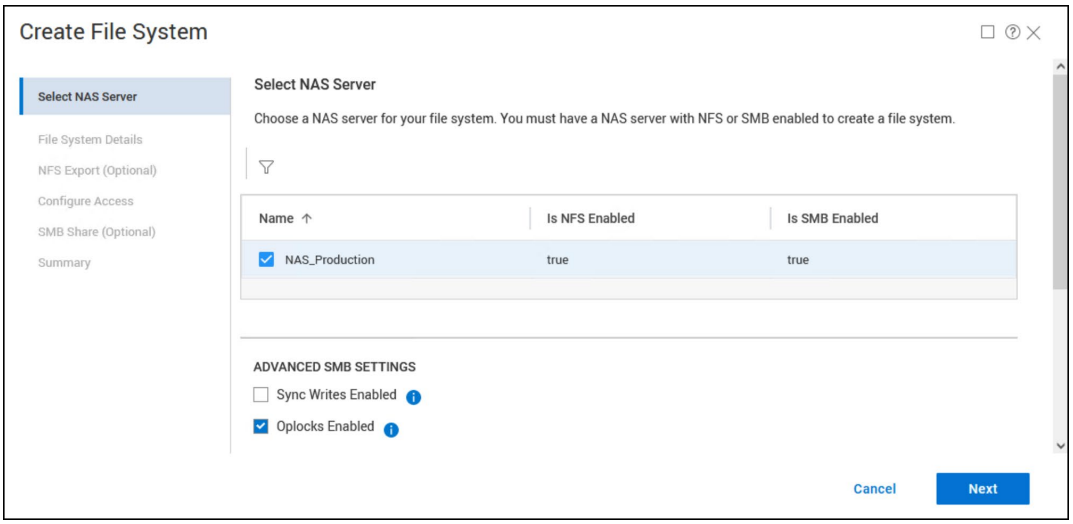

Figure 20. Create File System – Step 2

3. In order for VCF to access the file system for the workload domain installation, create an NFS export. Provide a name and alternatively a description and click **Next** as in Figure 21.

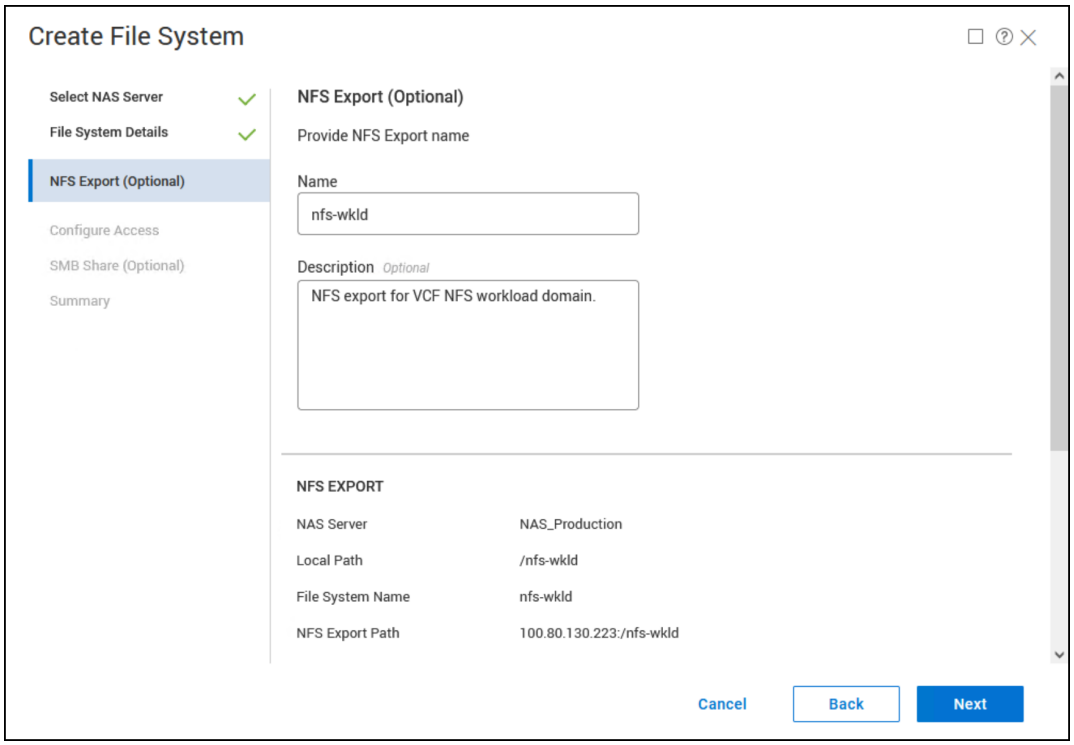

Figure 21. Create File System – Step 3

4. For ESXi to mount the NFS file system, grant the file system access. There is a base security, Sys, and advanced security in the form of Kerberos. In the example shown in Figure 22, the simplest security is set, **Sys.** The **Default Access** must be set to **Read/Write, allow Root** in order for ESXi to mount the file system. Since VCF requires NFS 3, the more advanced Kerberos security options cannot be used. There is no need to add a specific host. Click **Next**.

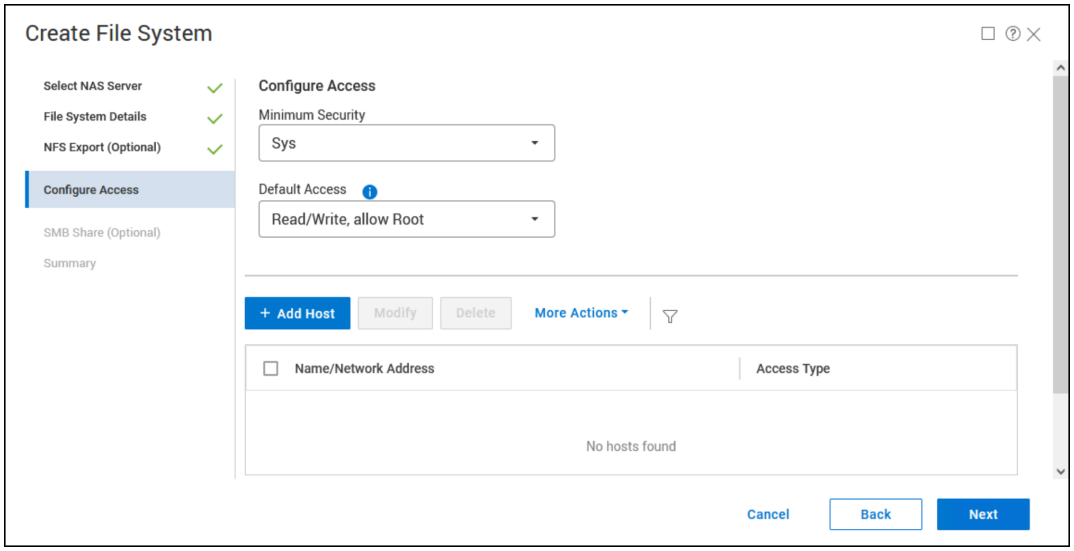

Figure 22. Create File System – Step 4

5. In the next screen, the **SMB Share** is optional. Go to the **Summary** page and click **Create File System** to complete the wizard as in Figure 23. Note in the summary that PowerFlex allows more than one IP for the export. The resulting NFS file system is highlighted in Figure 24.

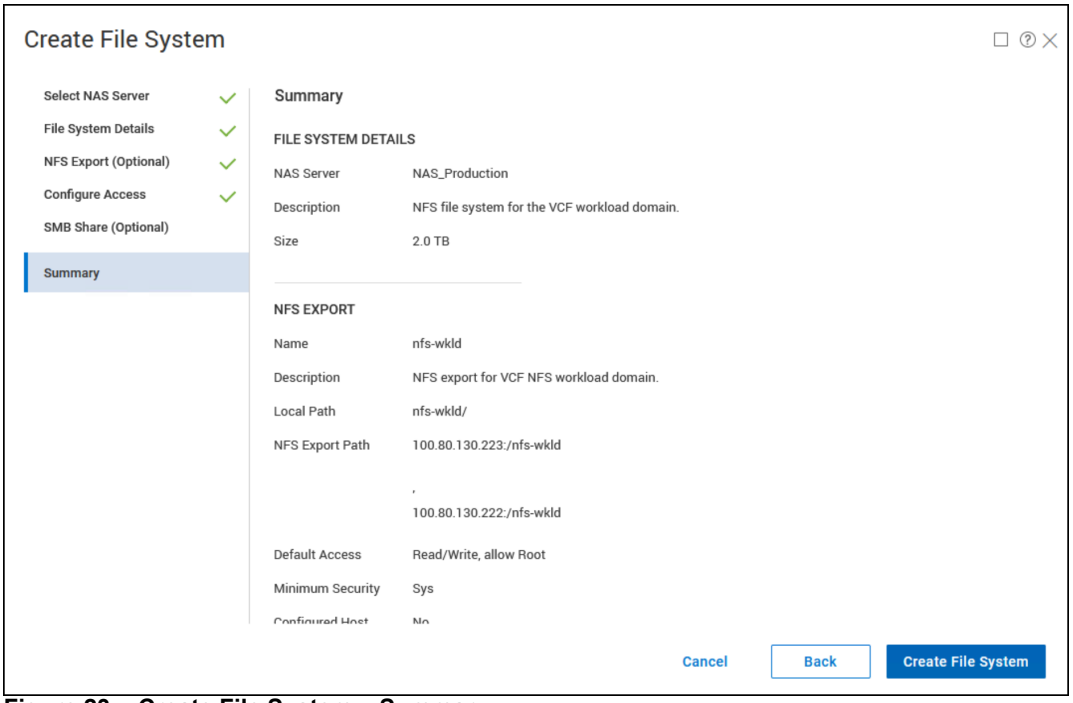

Figure 23. Create File System – Summary

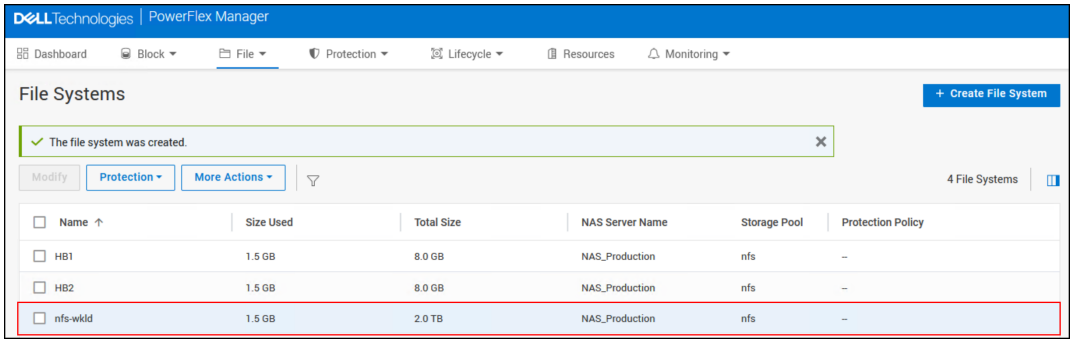

Figure 24. nfs-wkld file system

Protection for NFS on PowerFlex

One of the benefits of using array-based storage instead of vSAN for workload domains is the ability to use the features of the array, such as local replication. VMware does offer VM-based snapshots, but they are unable to offer a consistent copy of all objects that are part of the NFS datastore like array technology can. Such copies can serve multiple purposes, from cloning, to restores and backups. And as workload domains are designed to run production applications, it is essential to have a backup strategy in case of failure.

PowerFlex offers snapshot capability for all NFS file systems through both UI and CLI. The following walks through creating a snapshot in the UI interface.

In the UI, log in and go to **File > File Systems**. Then, select the desired file system where the workload domain will be provisioned, in this case **nfs-wkld.** Select **Protection > Create Snapshot** from the menu as in Figure 25.

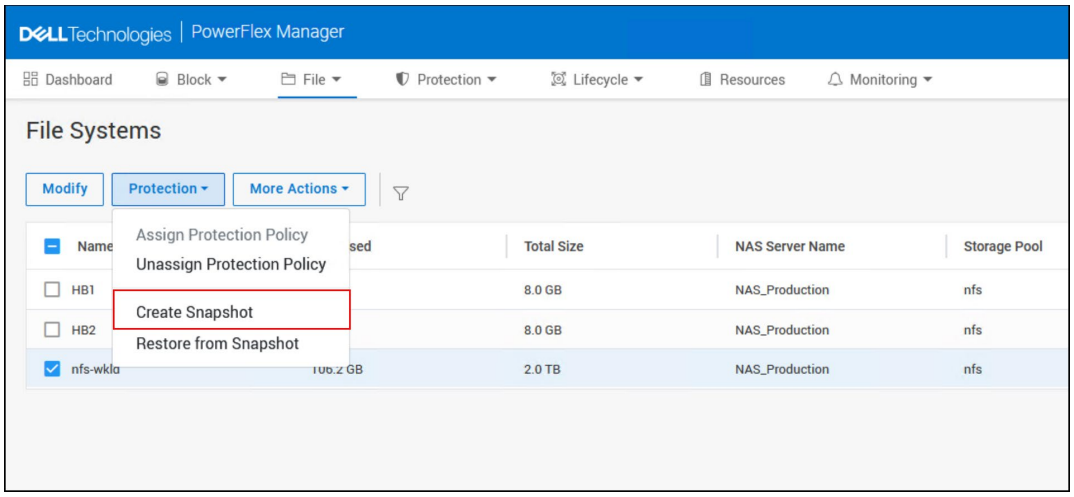

Figure 25. File system snapshot

PowerFlex presents the following three types of snapshots shown in Figure 26:

- **Protocol (read-only):** Creates a read-only snapshot that can be mounted and accessed later through NFS export or SMB share.
- **Snapshot:** Creates a read-only auto mounted snapshot accessible through the snapshot directory in the file system.
- **Protocol (read/write):** Creates a read/write snapshot that can be mounted and accessed later through NFS export or SMB share.

The retention period is set to one week by default. One can set a different retention period or select the **No Automatic Deletion** for indefinite retention.

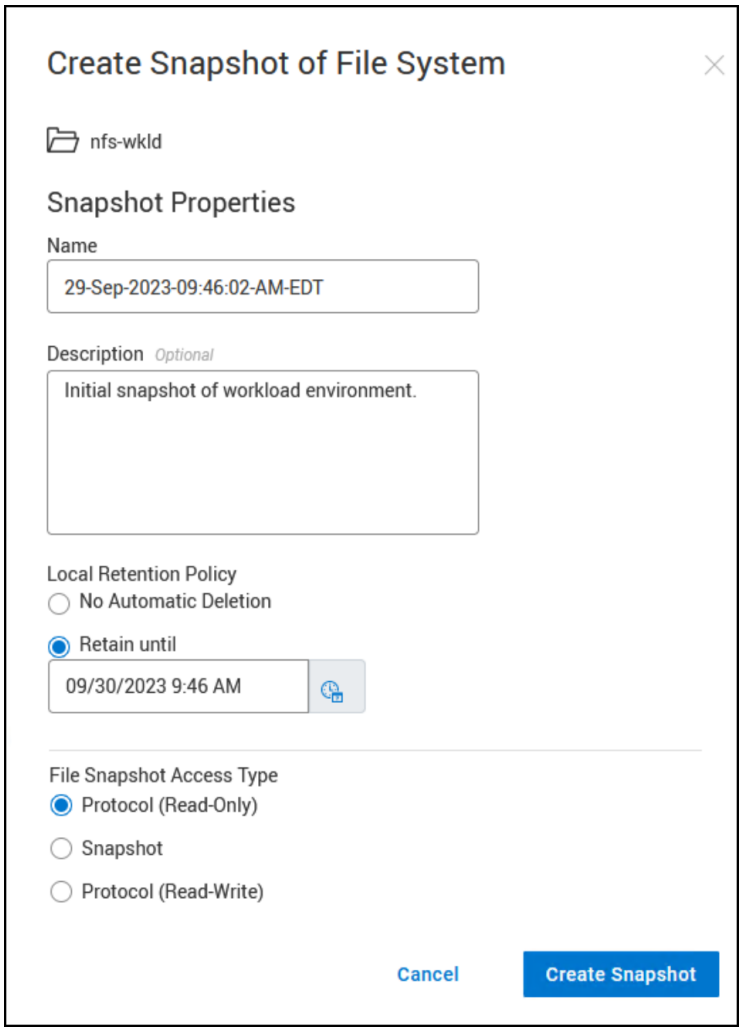

Figure 26. Snapshot options

For the purposes of backup and restore, a protocol (read-only) snapshot is the best option because it is only mounted when required and does not permit overwriting the data. A protocol (read/write) snapshot would be useful for test or development purposes. Finally, the “snapshot” snapshot, unlike the other two, is made available immediately to the system through the existing NFS file system. This type of snapshot is useful to do a quick restore of objects in the file system since it is made immediately available. In VMware, the way to access it is through the **snapshot directory** of the NFS datastore. This directory does not show up, even when listing hidden files. The user must know that the snapshot exists and change the directory into it. Alternatively, if the same NFS datastore is also available as an SMB share, the snapshot is available by right clicking the share, selecting **Properties** and then the **Previous Versions** tab as seen in Figure 27.

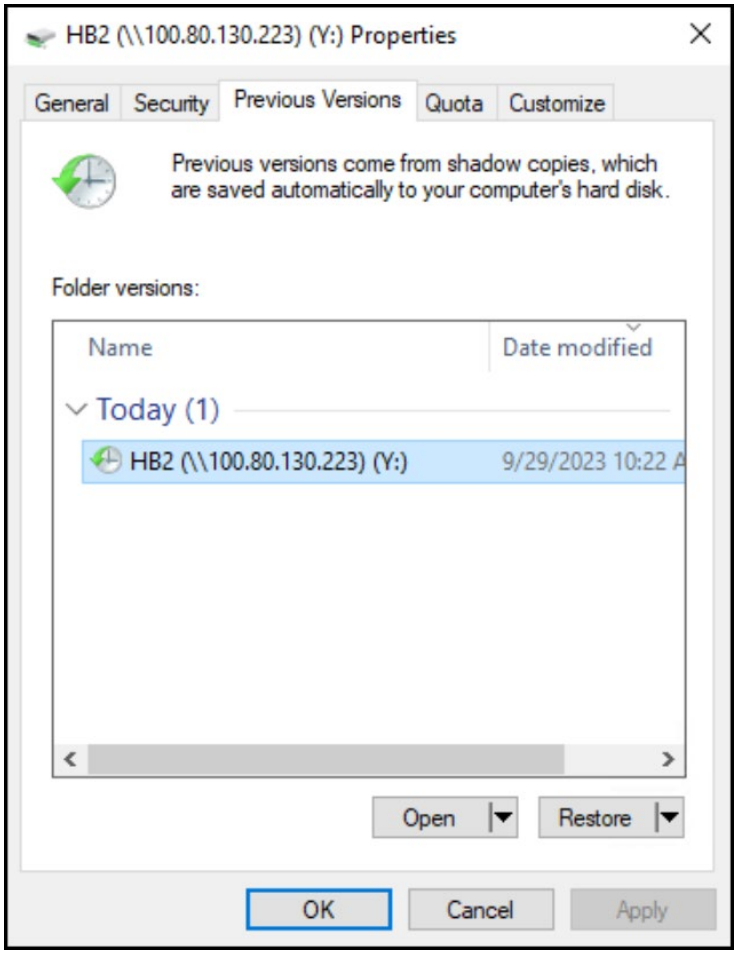

Figure 27. Snapshot access in an SMB share

By opening the folder, the objects in the snapshot are available for restore. If restoring VMs, be sure to first shut them down and unregister them, to avoid any issues.

Protection policies

In additional to individual snapshots, PowerFlex provides the ability to setup protection policies which consist of snapshot rules that automate how often to take snapshots of an NFS file system and how long to retain them. An NFS file system may only have a single protection policy assigned to it. To create a protection policy:

1. Go to **File > File Protection**.
2. Under the **Protection Policies** tab, select **+Create**.
3. Enter in a name and description (optional) into the dialog box that appears, and then select **+Create Rule**.

   These steps are shown in Figure 28.

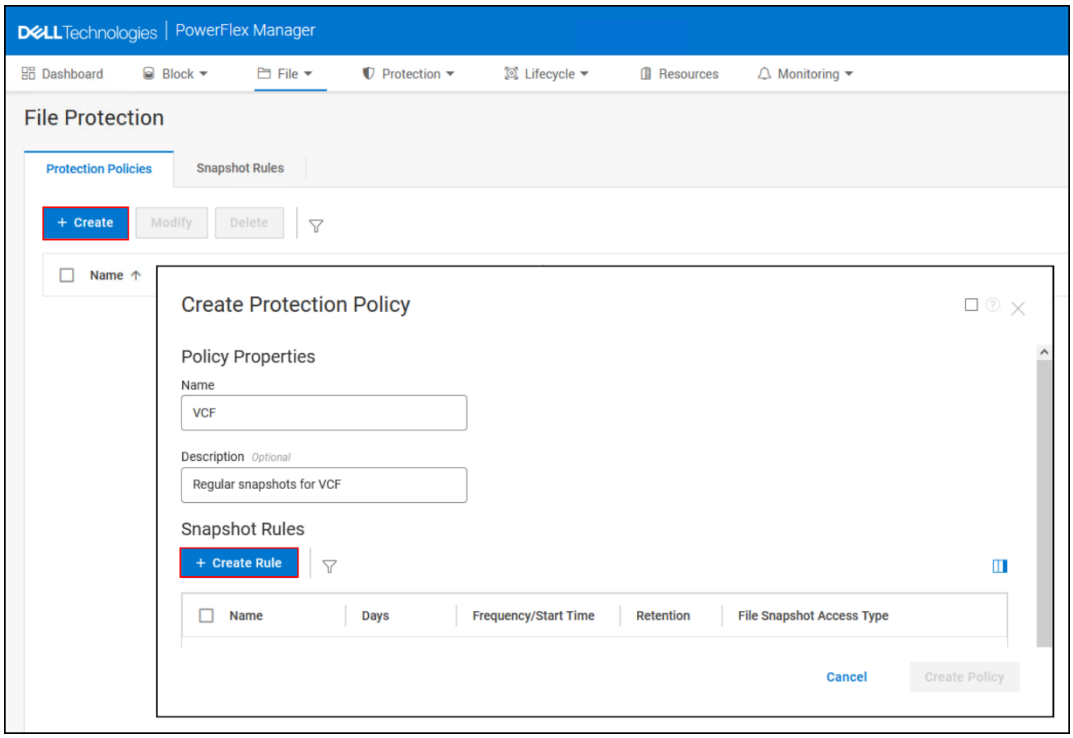

Figure 28. Create protection policy

4. In the rule dialog, enter a name and then select either a **Time of day** or **Every** to select an hourly cadence. When **Time of day** is selected, the radio buttons under **Days** become available.

   In the example in Figure 29, the rule is set to take a read-only snapshot every four hours and retain the snapshots on a cycle of 120 hours. This leads to 30 snapshots being taken before the first snapshot taken is removed.

5. Select **Create** to complete.

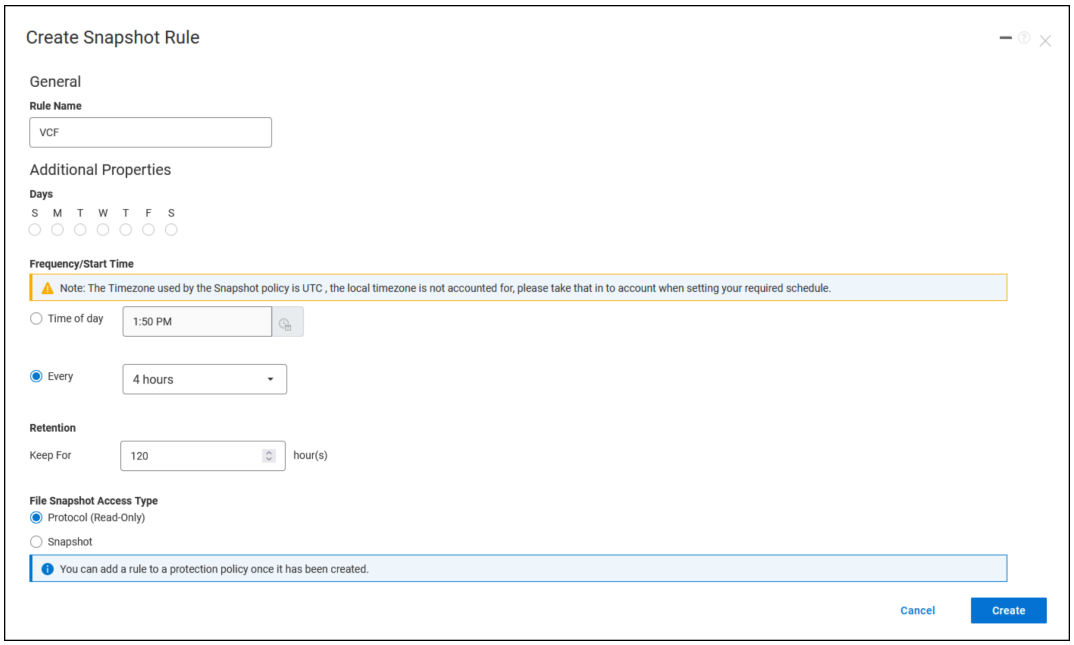

Figure 29. Create Rule

The rule is assigned automatically to the policy.

6. Select **Create Policy** to complete the process as in Figure 30.

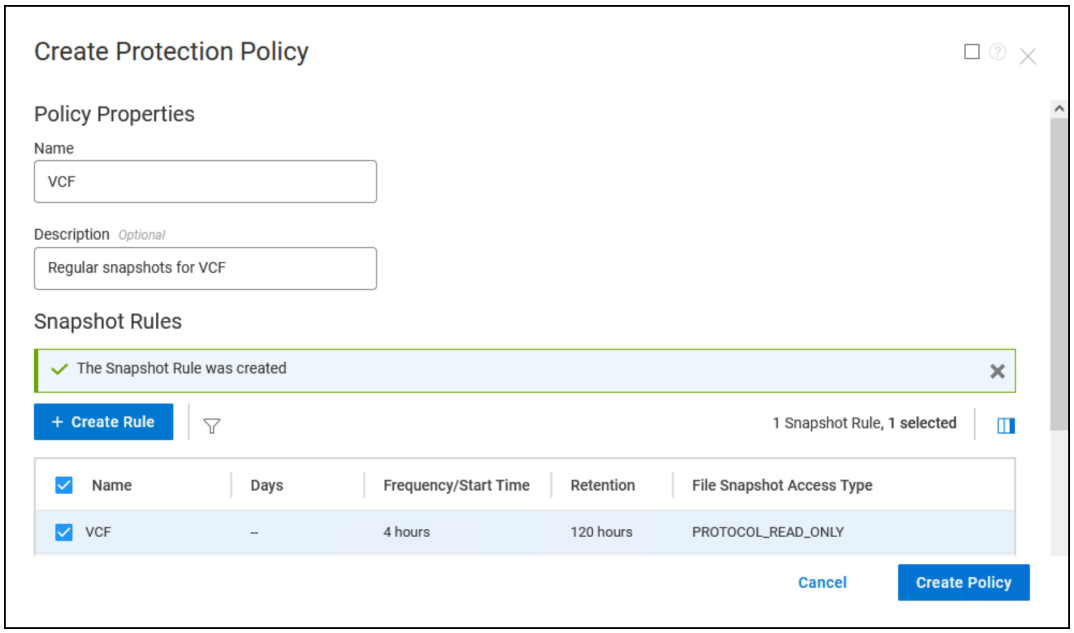

Figure 30. Create policy - Complete

The final step is to assign the newly created policy to the workload file system.

7. Go to **File > File Systems**. Check the box next to the workload domain file system, **nfs-wkld**, and from the **Protection** menu select **Assign Protection Policy** in Figure 31.

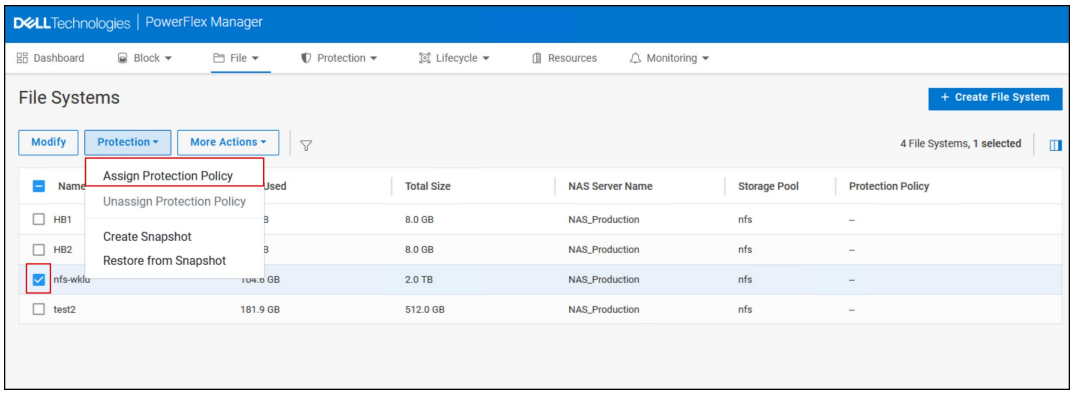

Figure 31. Assign protection policy

8. Use the checkbox to pick the desired policy, then **Apply**. A warning will appear and the user should select **Assign** as in Figure 32.

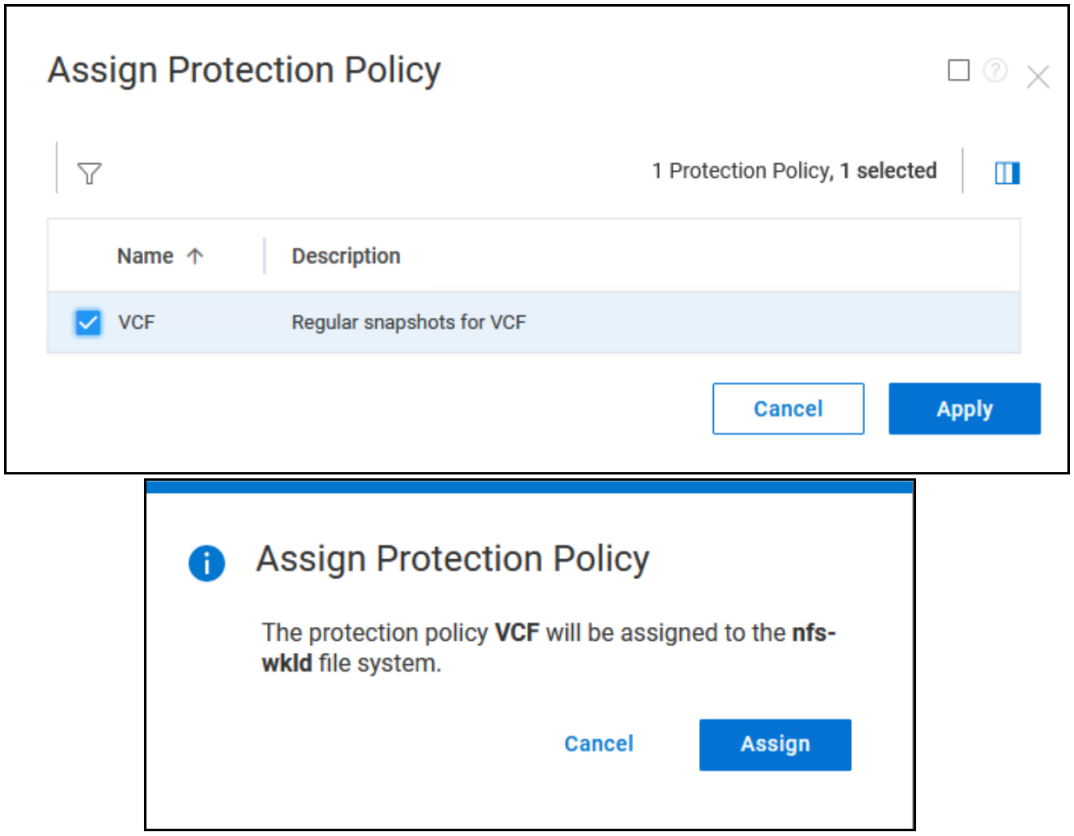

Figure 32. Assign policy

The policy is now applied and PowerFlex will take the snapshots automatically, providing local replication for backups, restores, and cloning. The installation of the workload can now proceed on the protected file system.

NFS best practices

There are a few best practices to follow when using NFS. Some are specific to VMware, while others are generic to NFS storage. In general, however, VCF requirements are going to map to the NFS best practices.

As NFS is IP-based network storage, it is essential that NFS traffic is separated from the other traffic like management in the VCF environment. Servers should use an MTU of 9000 or Jumbo Frames, to take full advantage of the bandwidth. In addition, a minimum of two 10 GigE NICs are required for VCF. If the environment supports larger networks like 25 GigE, which are present in this environment, it is preferable. VCF will “team” these NICs together when building the workload domain.

There are some VMware limits of note. By default, VMware restricts the number of NFS mounted datastores to eight for both NFS 3 and 4, however they do support 256 with a parameter change. Generally, Dell does not recommend changing the value unless it is necessary.

VMware controls both the heartbeating and locking of the NFS datastore. It has heartbeating parameters which VMware uses to check the health of the NFS 3 datastore. The mechanism is designed such that it allows recovery if a connection is lost for some short time period. The locking is also under the full control of VMware. The mechanism by which this is done does not need adjusting.

Chapter 6 Configuring VCF workload domain on NFS

This chapter presents the following topics:

Introduction

In order to deploy the workload domain, the user must first commission ESXi hosts to SDDC Manager. Essentially these hosts are added as inventory which are then available for deployment. Depending on the storage assigned to them, they could be added to the existing management domain and become part of the vSAN environment or as a workload domain (HCI configuration) or, as in this case, used to create a separate workload domain. To do the latter, principal storage must be assigned to the hosts, in this example NFS.

NFS workload deployment

In order to deploy a new workload domain on NFS using the SDDC Manager, there are two prerequisites:

1. A dedicated storage networking IP pool must be created for NFS traffic.
2. A minimum of two prepared and commissioned ESXi hosts are available in inventory.

The steps must be completed in this order as the SDDC Manager requests the storage pool during the commissioning of the hosts.

NFS network pool

To create a network pool for NFS, in SDDC Manager:

1. Go to **Administration > Network Settings**. Under the **Network Pool** tab select **+CREATE NETWORK POOL** as in Figure 33.

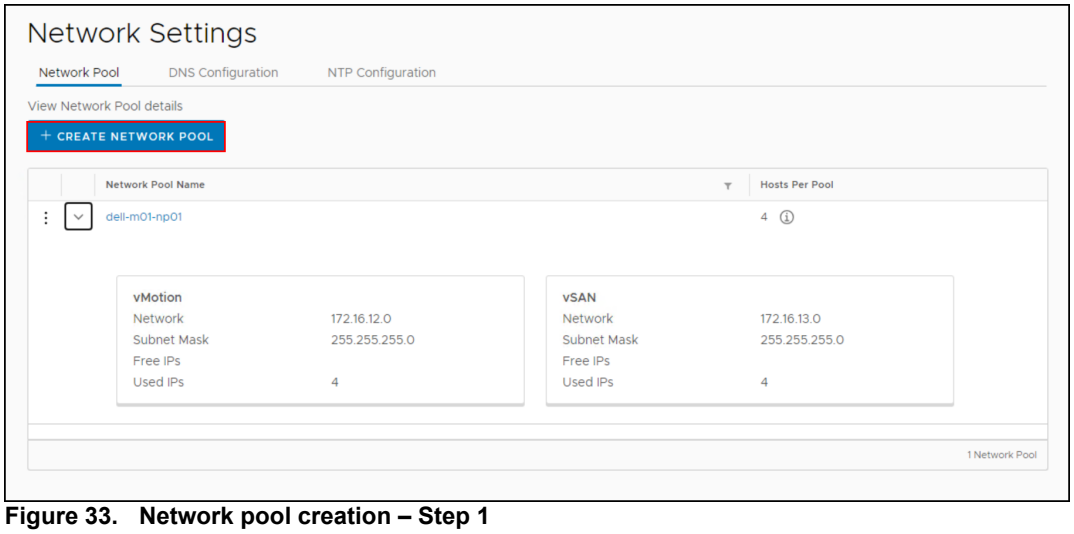

Figure 33. Network pool creation – Step 1

2. In the dialog box shown in Figure 34, check the box next to **NFS**.

Note: The **vMotion** box is checked automatically and is required as part of the pool configuration.

3. Enter in a network pool name and the IP information for both NFS and vMotion. The NFS IP information should be the same network that is used in the

PowerFlex File configuration so that the exports are accessible by VCF. Select **SAVE** to complete the wizard.

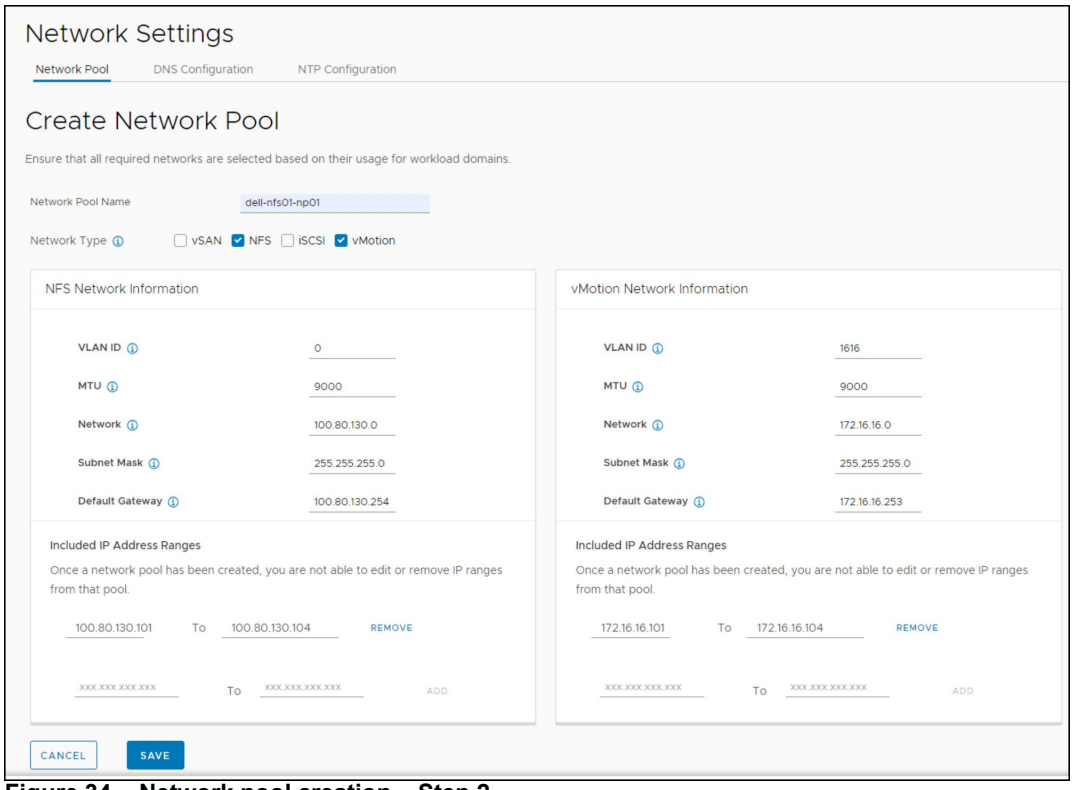

Figure 34. Network pool creation – Step 2

The final result is shown in Figure 35. As there are no hosts commissioned, the value for **Hosts Per Pool** is zero.

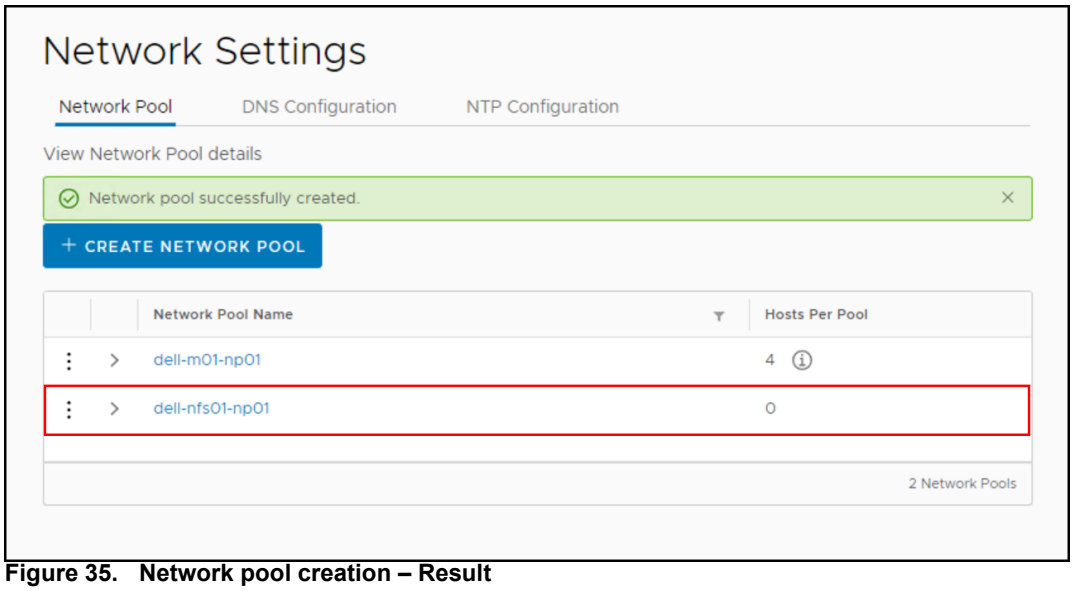

Figure 35. Network pool creation – Result

Commission hosts

Commissioning hosts essentially means adding them to the SDDC Manager inventory so they are available for use in the new workload domain. Hosts must be prepared for commissioning in the same way they were for the VCF base installation. Following the BOM, install the correct version of ESXi and configure hostname and networking. Once complete, in SDDC Manager complete the following steps:

1. Go to **Inventory > Hosts** and select **COMMISSION HOSTS** in the right-hand-corner as in Figure 36.

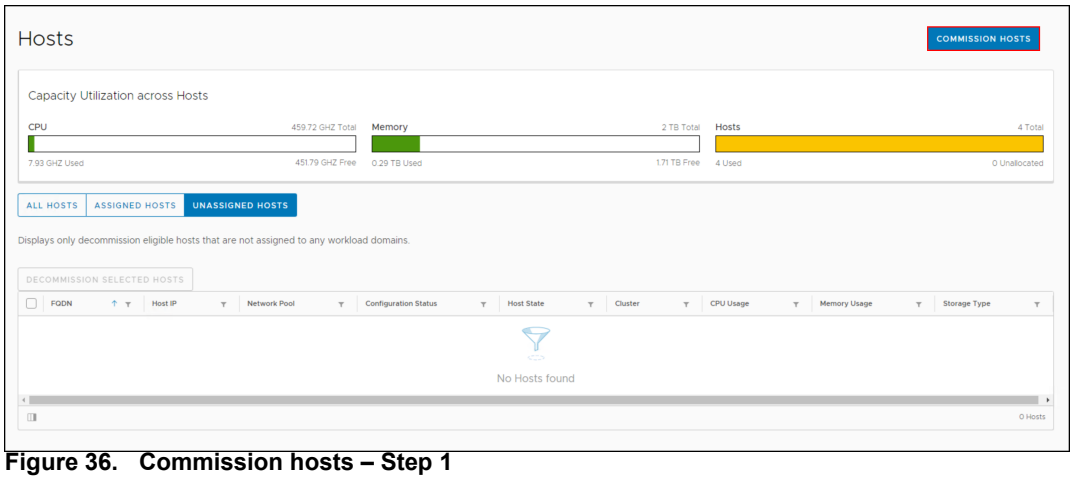

Figure 36. Commission hosts – Step 1

2. The first screen that appears is a checklist that the user is required to validate before proceeding. Although VMware calls this a checklist, it is simply a list of prerequisites. This list is not as extensive as that for VCF but is nevertheless important to validate. Be sure all items are complete before selecting the **PROCEED** button as in Figure 37.

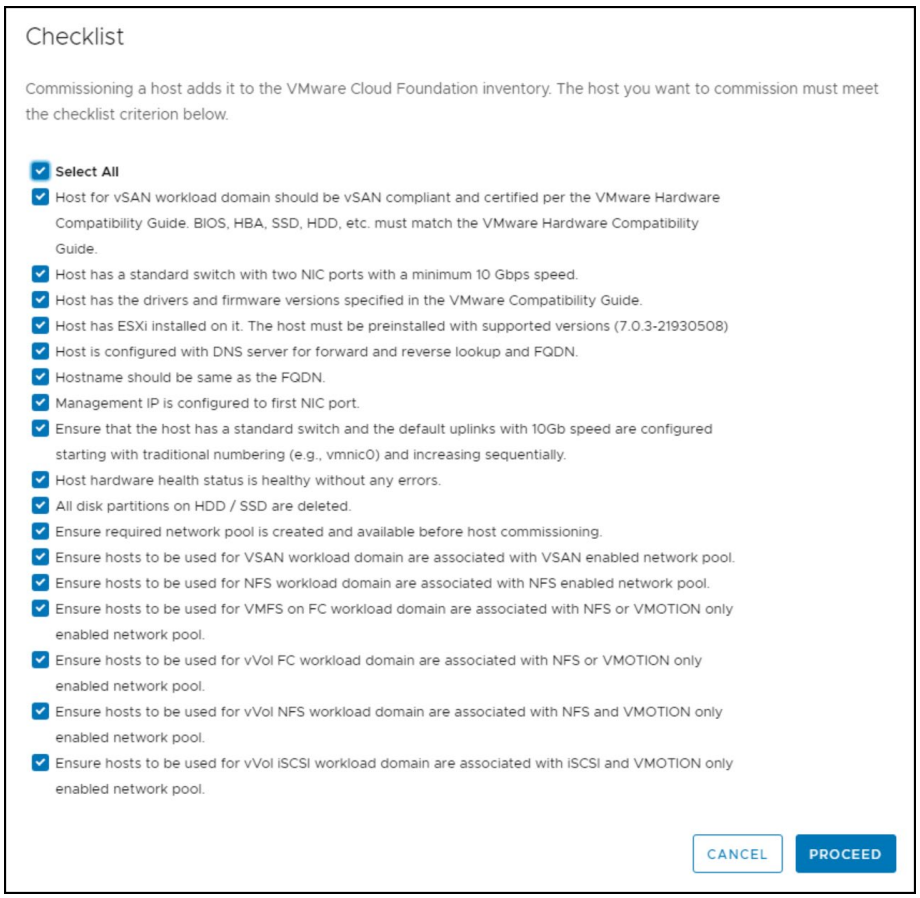

Figure 37. Commission hosts – Step 2

3. In the next step, add each host that is to be part of the workload domain on NFS.
4. In Figure 38, several steps are consolidated for brevity. They are:
   a. Each host gets added as shown in the top half of the image.
   b. Select the **NFS** radio button, enter the hostname, select the previously created network pool, and add the username and password.
   c. As each host is added, the fingerprint must be confirmed and then the host validated. In the example below both hosts are added with the fingerprint confirmed and the prerequisites validated.
   d. Select **NEXT** to move to review.

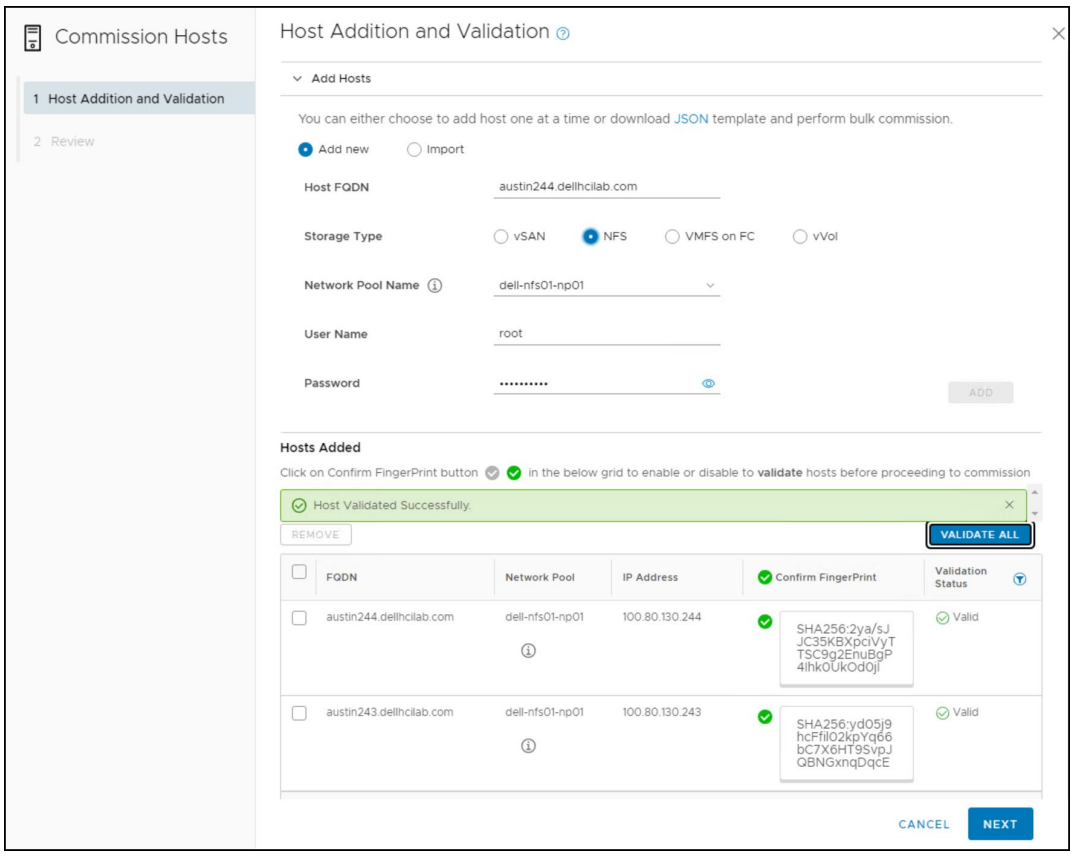

Figure 38. Commission hosts – Step 3

5. Before selecting the **COMMISSION** button in Figure 39, review the validated hosts. Despite the hosts passing validation in the previous step, there is still a chance that a host fails to commission. To that end, VMware offers a toggle at the top which lets the wizard skip failed hosts. Though this is unlikely, for example a network failure before commission, it is best to leave it set on. A failed host can be repaired and then commissioned again afterwards. The commissioning process does take some time to complete. The SDDC Manager displays the status as the hosts are added.

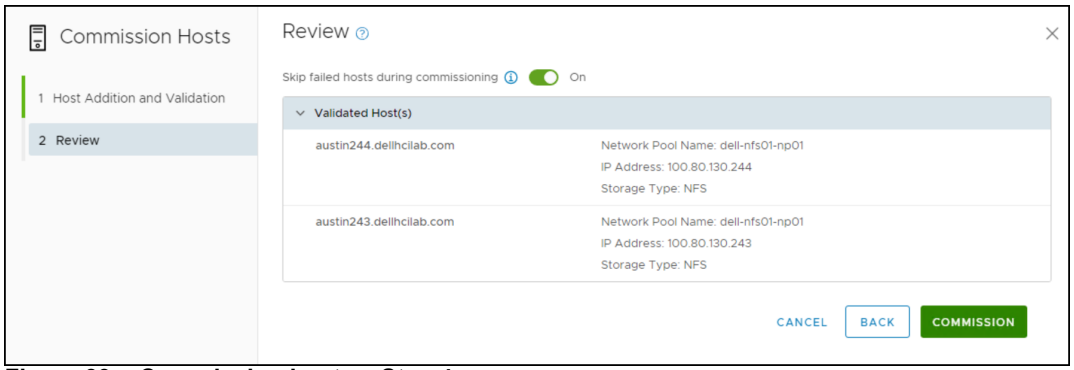

Figure 39. Commission hosts – Step 4

Upon completion, the new hosts displays as unassigned in the **Hosts** panel in Figure 40, and can now be used for the workload domain.

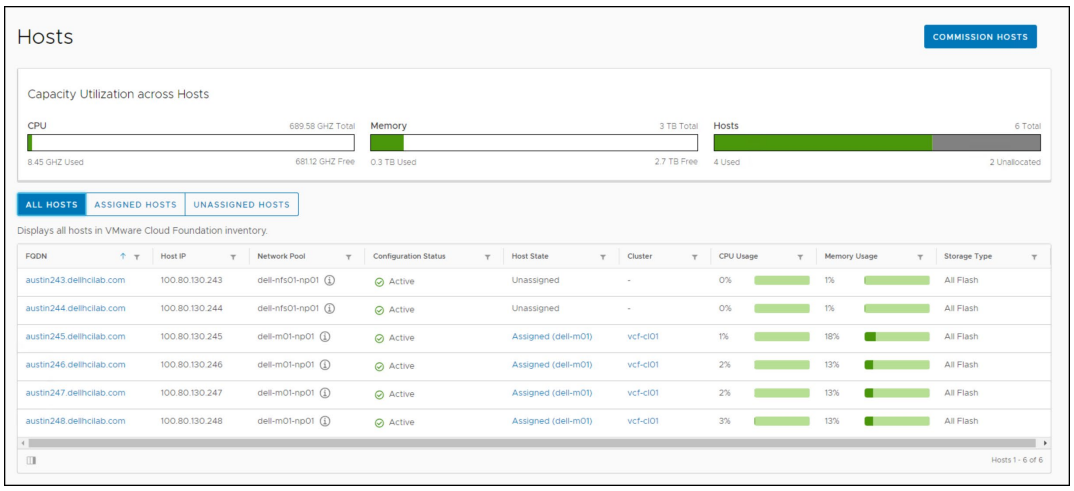

Figure 40. Unassigned hosts

Workload wizard

The following walk through covers the creation of the workload domain using the SDDC Wizard.

Within SDDC Manager, select **Workload Domains** from the **Inventory** menu on the left. Click **+ WORKLOAD DOMAIN > VI Workload Domain** in Figure 41. This initiates the workload wizard.

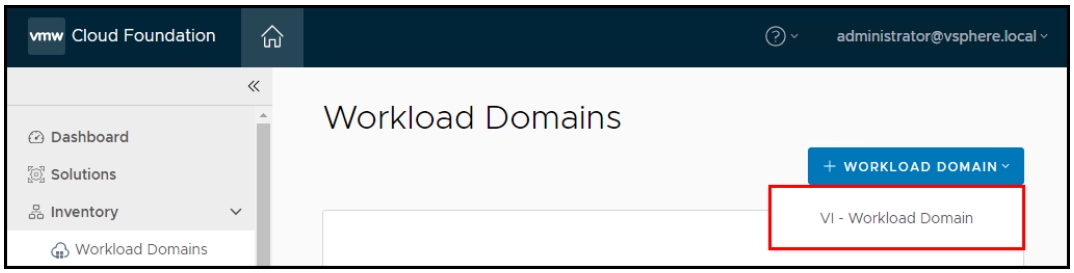

Figure 41. Add VI – Workload Domain

1. In the first step of the wizard the user can indicate if they will use two commissioned hosts, rather than three. To do this, check the box labeled **Manage clusters in this workload domain using images** shown in Figure 42. VCF only allows two hosts with NFS if using an image. This image does not need to include additional software and firmware beyond the ESXi software.

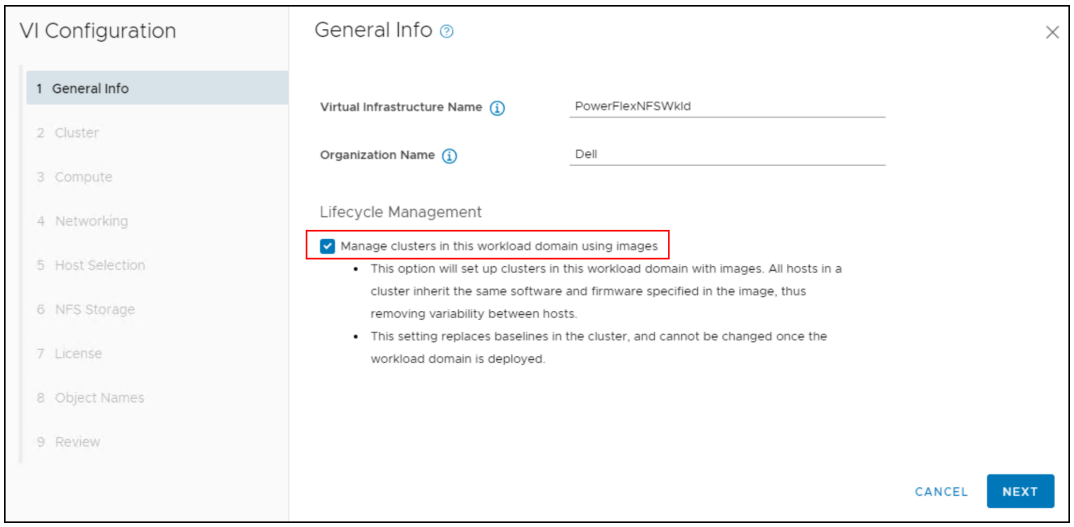

Figure 42. Workload domain – Step 1

If an image is already being used, go to the next step in the wizard. If an image is not in use, create one using any available vCenter using the same base version, such as, 7.x, as that in the BOM.

a. Within a vCenter, right-click the datacenter and select **New Cluster….** The new cluster wizard will start. In the first screen, check the box next to **Manage all hosts in the cluster with a single image**. When the options for how to setup the image appear, leave the default radio button **Compose a new image** selected, as shown in Figure 43. There is no need to provide a name for the cluster as it is temporary.

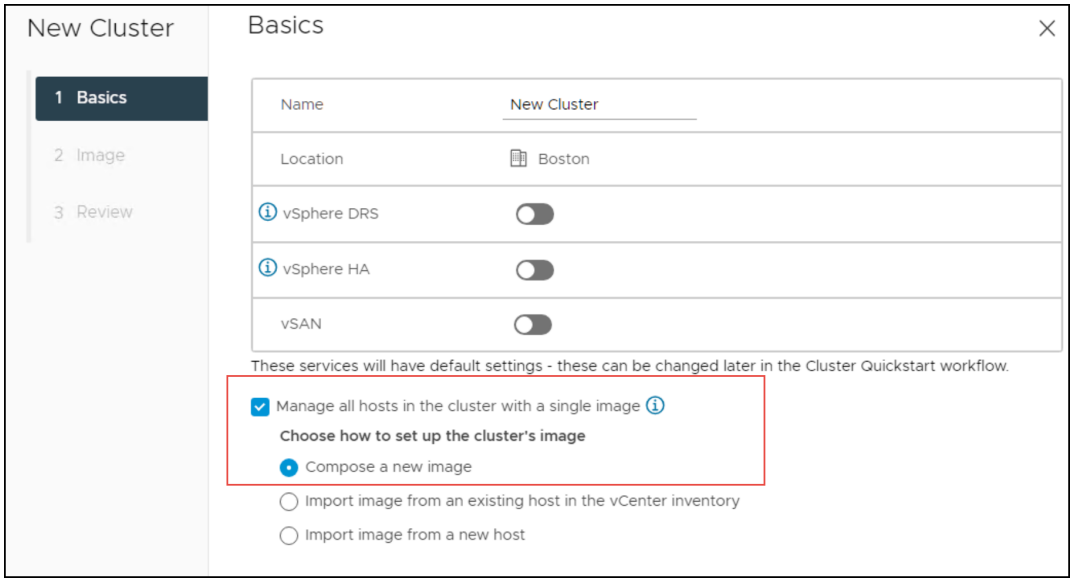

Figure 43. Create a new image – Step 1

b. Use the drop-down box to select the correct **ESXi Version** that matches exactly the commissioned hosts in SDDC Manager. Every available ESXi

patched version of the base one will be available. Leave the remaining options blank.

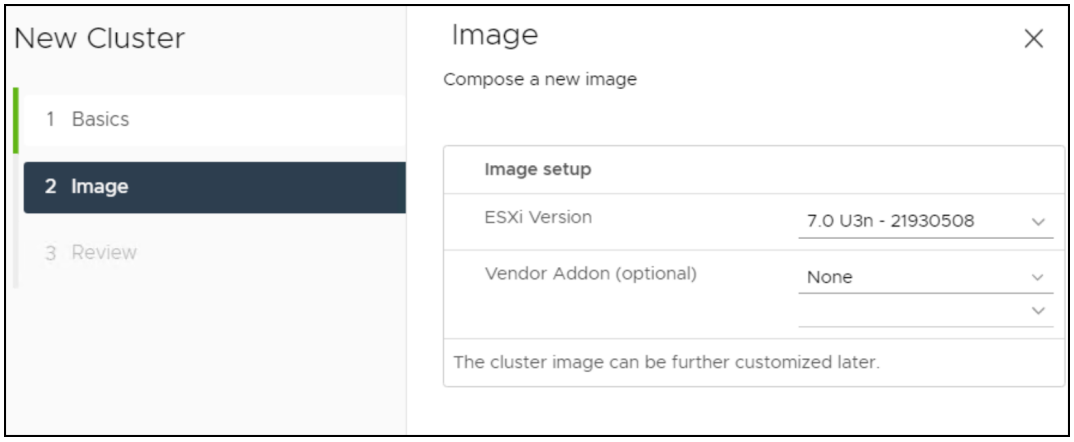

Figure 44. Create a new image – Step 2

c. List the ESXi version as the only component of the image. This is desirable and expected. The image is now part of the vCenter. The workload domain wizard provides the user the ability to either connect directly to the vCenter to pull the image or import the image. Either option is perfectly acceptable. In this environment, the image was imported after exporting from the vCenter as shown in Figure 45.

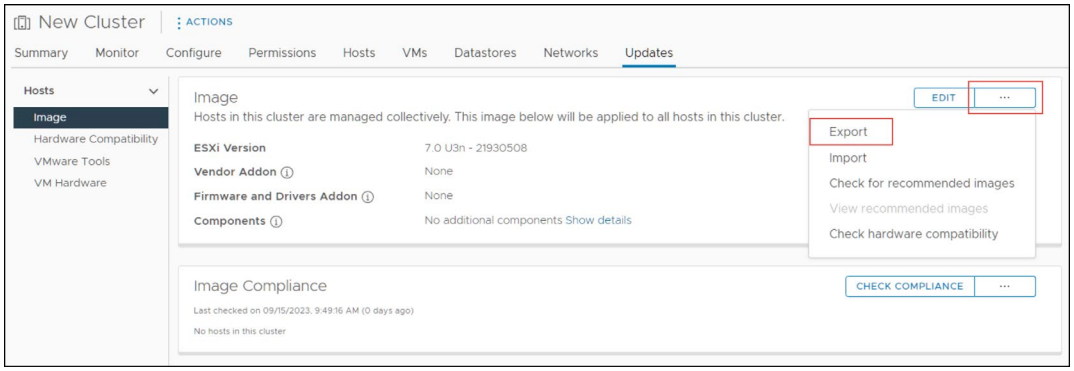

Figure 45. Exporting the image file from the vCenter

2. Returning to the workload wizard in Figure 46, enter a cluster name and for this example import the newly created image.

Note: ESXi is the only component in the image, which means both the commissioned hosts will validate successfully against it.

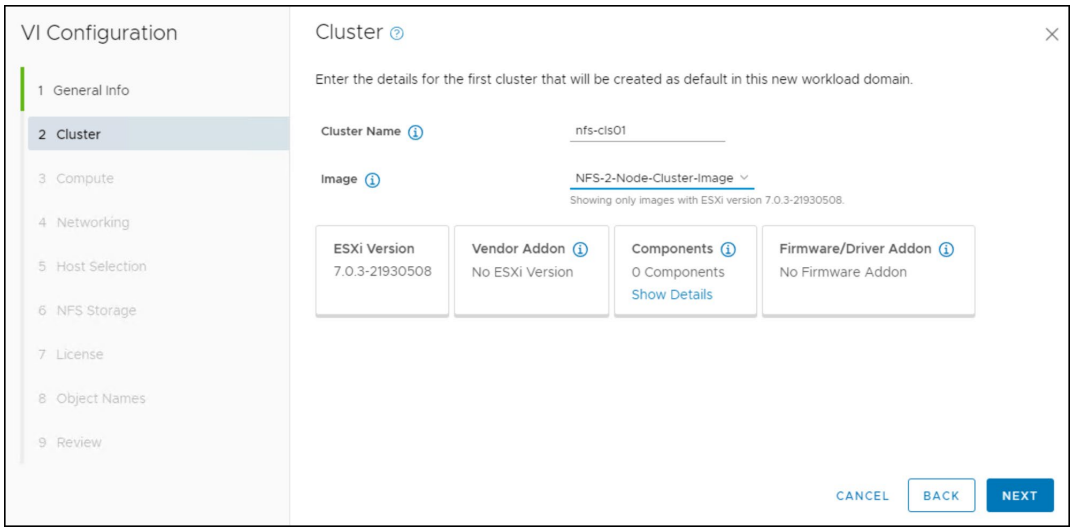

Figure 46. Workload domain – Step 2

3. Provide a FQDN for the new vCenter that will house the workload domain, along with IPs and root password. The new vCenter will share the PSC of the management domain vCenter, so it will be in Enhanced Link Mode.
4. The wizard requires three host FQDNs and IPs for the NSX environment, along with a cluster FQDN. In addition, passwords and an Overlay Network must be filled in. As this NSX environment could be independent of the management domain, this overlay network need not be the same, but it can be.
5. The user selects the previously commissioned hosts as in Figure 47. Since an image was selected in step two, the wizard indicates only two hosts are required. If the user forgot to select an image, the wizard will show that three hosts are required.

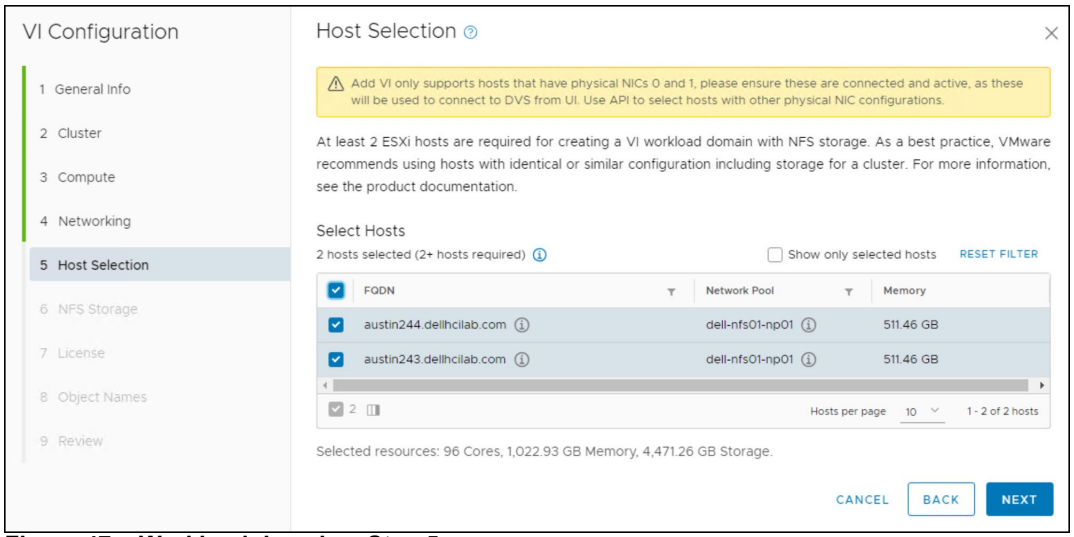

Figure 47. Workload domain – Step 5

Note: The warning in the previous image contains a critical message that the user should heed, since the wizard will not prevent the user from continuing if their hosts do not comply. The message clearly states that the first two physical NICs recognized by ESXi will be used. For many customers, those two NICs may not be the ones that are cabled. For example, in this environment the physical NICs appeared as in Figure 48 for one of the hosts. The first two NICs are not cabled, while the second two are. VCF expects vmnic0 to be assigned to switch vSwitch0 prior to installation and vmnic1 to be available.

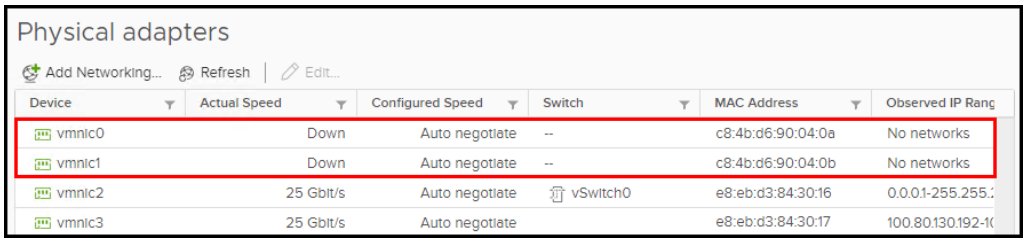

Figure 48. Physical NICs prior to re-order

The only solution VCF offers to this situation is to use the API, rather than the UI. If the user is comfortable with that solution, then it can certainly be done. If not, however, it is possible to re-order how ESXi discovers the NICs. VMware offers the following knowledge base article which details the process to re-order: https://kb.vmware.com/s/article/2091560. In short, the user creates aliases so that the vmnic order can be switched. In this environment the following alias exchanges were made, switching vmnic2 to vmnic0 and vmnic3 to vmnic1:

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/
deviceInternal alias store --bus-type pci --alias vmnic0 --
bus-address m0000306f
localcli --plugin-dir /usr/lib/vmware/esxcli/int/
deviceInternal alias store --bus-type pci --alias vmnic2 --
bus-address m0000206f
localcli --plugin-dir /usr/lib/vmware/esxcli/int/
deviceInternal alias store --bus-type logical --alias vmnic0
--bus-address "pci#m0000306f#0"
localcli --plugin-dir /usr/lib/vmware/esxcli/int/
deviceInternal alias store --bus-type logical --alias vmnic2
--bus-address "pci#m0000206f#0"

localcli --plugin-dir /usr/lib/vmware/esxcli/int/
deviceInternal alias store --bus-type pci --alias vmnic1 --
bus-address m00003079
localcli --plugin-dir /usr/lib/vmware/esxcli/int/
deviceInternal alias store --bus-type pci --alias vmnic3 --
bus-address m000020d3
localcli --plugin-dir /usr/lib/vmware/esxcli/int/
deviceInternal alias store --bus-type logical --alias vmnic1
--bus-address "pci#m00003079#0"
```

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/
deviceInternal alias store --bus-type logical --alias vmnic3
--bus-address "pci#m000020d3#0"
```

Once these commands are complete, a reboot of the ESXi host will re-order the NICs. For one of the hosts, the new order is shown in Figure 49.

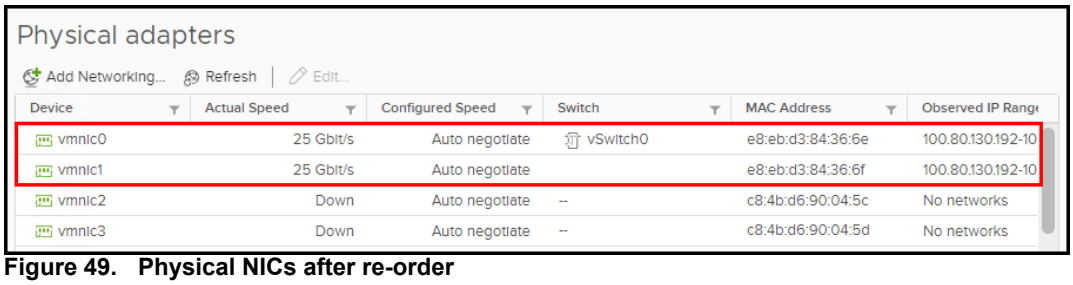

Figure 49. Physical NICs after re-order

6. Input the previously created NFS file system as in Figure 50 along with a datastore name. There are not restrictions around the name so long as it adheres to normal vSphere rules.

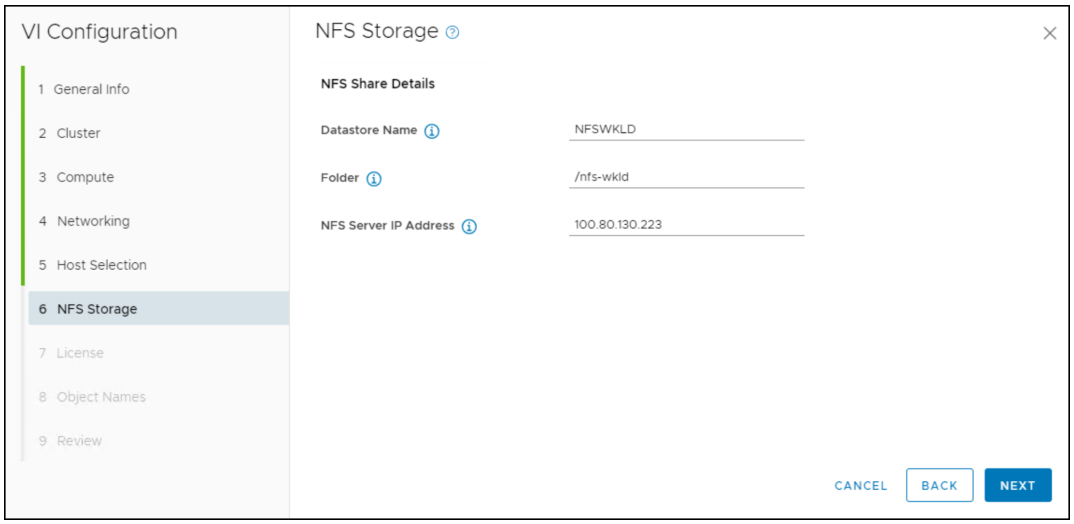

Figure 50. Workload domain – Step 6

7. Step 7 displays the existing licenses form the management domain by drop-down box for NSX Data Center and VMware vSphere. The user will not need to manually input a new license unless there are not enough available.
8. In Step 8, the wizard summarizes the generated names that it will use for networking. This is simply informative as they cannot be altered.
9. Finally, review the entries and select **FINISH**.

The SDDC Manager now undertakes the creation of the workload domain on NFS. The user can watch the progress of creation by checking the **Configuration Status** column under **Inventory > Workload Domains** as in Figure 51. The creation will take some time.

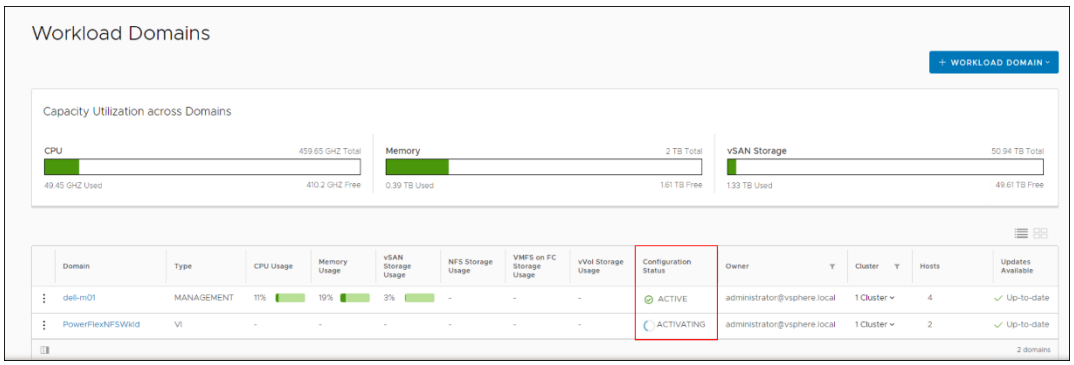

Figure 51. Workload domain creating

Once complete, use the hyperlink for the **PowerFlexNFSWkld** domain to drill-down into the workload domain. Select **Hosts** to see the ESXi hosts for the domain and note that the **Data Store Type** column is **NFS** as in Figure 52. The domain is now ready for application deployment.

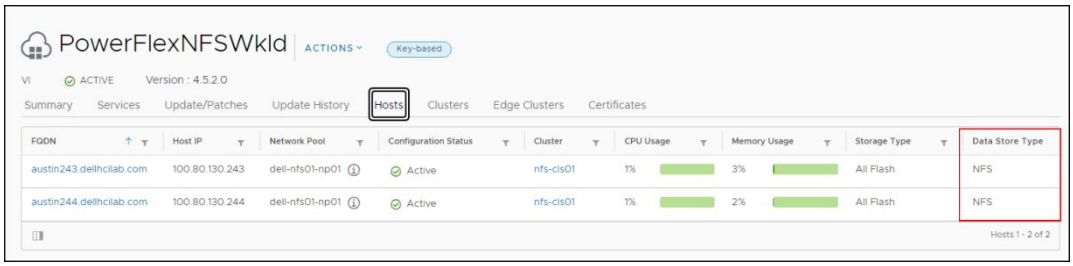

Figure 52. Workload Domains in SDDC Manager

Chapter 7 Conclusion

This chapter presents the following topics:

Summary

VMware Cloud Foundation provides a complete, unified platform to build both a private and public cloud, combining compute, storage, networking, and management. VCF offers the flexibility of using various storage options for workload domains from FC to NFS, running on external arrays like PowerFlex.

NFS storage is a popular choice for workload domains in VCF because it is simple to implement and manage and can deliver high performance. When using NFS on PowerFlex it enables the VCF environment to become highly resilient, scalable, and able to handle the most demanding workload domains.

By following the guidelines outlined in this paper, the user can ensure a successful implementation of a PowerFlex NFS storage solution on VCF.

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on the solution and the solution documentation. Contact the Dell Technologies Solutions team by email.

Authors: Drew Tonnesen, Dell Technologies PowerFlex Engineering

Contributors: Dell Technologies Solution Information Development & Design team

Chapter 8 References

This chapter presents the following topics:

Dell Technologies documentation

The following Dell Technologies documentation provides additional and relevant information. Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

- Dell PowerFlex documentation

VMware documentation

The following VMware documentation provides additional and relevant information:

- VMware Cloud Foundation documentation
- vSAN documentation
- NSX documentation
- vRealize Suite documentation