Reference architecture

HPE Reference Architecture for VMware Cloud Foundation 9.0

HPE ProLiant Gen12 - vSAN and HPE Alletra Storage MP B10000

Contents

Executive summary

In today's fast-paced digital landscape, enterprises are challenged to deliver services faster, respond dynamically to customer demands, and modernize infrastructure to support innovation—all while controlling cost and complexity. To meet these demands, IT organizations are adopting hybrid cloud strategies that bring together the best of traditional infrastructure and modern cloud-native platforms.

VMware Cloud Foundation 9.0, developed by Broadcom, is a full-stack software-defined infrastructure platform that unifies compute, storage, networking, and lifecycle management. It provides a consistent private cloud operating model with built-in automation, scalability, and support for modern workloads across data centers and clouds.

To support this transformation, Hewlett Packard Enterprise (HPE) provides a validated infrastructure foundation that combines its industry-leading HPE ProLiant DL servers for compute, HPE Alletra MP storage arrays for high-performance, scalable external storage, and Aruba CX 8325 switches for high-throughput, low-latency networking. Together, they form a robust and flexible platform for deploying and operating VMware Cloud Foundation 9.0 in enterprise data centers. This reference architecture showcases how the solution delivers elastic, agile infrastructure that accelerates time to value, boosts innovation, and reduces total cost of ownership.

The reference architecture offers customers the flexibility to choose between two validated storage models:

— vSAN Express Storage Architecture (ESA), which uses high-performance internal NVMe drives within HPE ProLiant DL servers to deliver hyperconverged, software-defined storage.

— External Fibre Channel storage with HPE Alletra Storage MP B10000, ideal for customers with existing Fibre Channel SAN infrastructure or those preferring external, centralized storage arrays over hyperconverged options like vSAN.

This flexibility allows enterprises to align their storage strategy with existing investments, performance needs, and operational preferences.

Solution benefits include:

— Validated hybrid cloud architecture combining VMware Cloud Foundation 9.0, HPE ProLiant DL servers, and HPE Alletra MP Storage.

— Choice of vSAN ESA (NVMe-based hyperconverged) or Fibre Channel-based external storage, allowing flexible storage design based on customer needs.

— Lifecycle automation using vSphere Lifecycle Manager (vLCM), via the Hardware Support Manager (HSM) service built into the HPE OneView for VMware vCenter® (OV4vC) plug-in, to remediate firmware, drivers, and ESX™ updates within a single maintenance window—reducing operational overhead and simplifying patch management.

— Building blocks for running both traditional virtualized and modern containerized workloads.

— High-performance network infrastructure is delivered through Aruba CX 8325 top-of-rack (ToR) and Aruba 6300M out-of-band (OOB) switches, orchestrated by Aruba Fabric Composer, which provides dynamic, policy-based network provisioning and automation across the data center fabric. This combination enables reliable, low-latency connectivity, accelerates deployment, reduces configuration errors, and improves operational agility.

Target audience: This document is intended for IT decision-makers, as well as enterprise architects, system engineers, and system administrators who are evaluating or designing enterprise-ready private cloud solutions. It focuses on deployments using HPE ProLiant DL servers, HPE Alletra MP storage, and VMware Cloud Foundation.

Readers should have a solid understanding of VMware Cloud Foundation, enterprise networking, enterprise storage architectures, and the HPE ProLiant server platform.

Document purpose: The purpose of this document is to present a validated use case for building an enterprise-ready private cloud solution by combining the capabilities of VMware Cloud Foundation with HPE compute, storage, and networking infrastructure. The solution is designed to be general purpose, flexible, and easy to deploy, providing customers with a proven reference for the install of private cloud deployments. While the recommendations and configurations detailed here are based on tested scenarios, this document does not represent the only supported deployment model, nor does it aim to cover all possible deployment variations across diverse customer environments.

This Reference Architecture describes solution testing performed in September 2025.

Solution overview

This reference architecture outlines how VMware Cloud Foundation (VCF) 9.0 can be deployed and lifecycle-managed on HPE infrastructure components—including compute, storage, and networking—to deliver a scalable, flexible, and automated private cloud platform for enterprise workloads. The solution is designed to host business-critical applications with consistency and automation in a private cloud environment.

— **HPE ProLiant Servers** - HPE ProLiant DL380/DL360 Gen12 Servers as VMware Cloud Foundation's Domain Management and Workload Hosts.

— **HPE Alletra MP B10000 Storage** - Provides high-performance Fibre Channel-based external storage for both the management and workload domains. It serves as an alternative to vSAN ESA for customers preferring external SAN infrastructure.

— **HPE OneView** - A centralized infrastructure appliance platform that accelerates server provisioning, simplifies IT operations, and improves operational efficiency.

— **HPE OneView for VMware vCenter (OV4vC) -** An integrated plug-in application for VMware vCenter that integrates HPE server management capabilities into VMware vCenter. Serving as the vSphere Hardware Support Manager (HSM) enabling firmware and driver remediation through vSphere Lifecycle Manager (vLCM) and supports ongoing hardware monitoring and configuration tasks.

— **vSphere Lifecycle Manager (vLCM) -** A vCenter-integrated service that provides centralized, image-based lifecycle management of ESX hosts, including firmware and driver updates. vLCM simplifies patching and consistency across clusters.

— **VMware Cloud Foundation Lifecycle Management -** Delivered through VCF Operations, lifecycle management automates patching, upgrades, and remediation of VCF core components, ensuring consistency and reducing administrative overhead across the private cloud environment.

— **Aruba Fabric Composer (AFC)** - A software-defined orchestration solution that automates and simplifies network provisioning, operations, and policy enforcement across the Aruba CX switch fabric—enabling faster, more consistent network deployment and reduced operational complexity.

HPE and VMware Cloud Foundation Solution components

The VMware Cloud Foundation on the HPE ProLiant DL servers is validated with the following hardware and software components. For additional component details, refer to the VMware Cloud Foundation 9.0 Release Notes at https://techdocs.broadcom.com/us/en/vmware-cis/vcf/vcf-9-0-and-later/9-0/release-notes/vmware-cloud-foundation-90-release-notes.html. VMware Cloud Foundation is supported on vSphere-compatible server hardware which meets the minimum requirements for VMware Cloud Foundation and the desired workloads.

Figure 1 shows the logical architecture of the HPE validated VMware Cloud Foundation 9.0 deployed over HPE ProLiant DL Gen12 utilizing vSAN or FC as storage model both for Management and Workload domain.

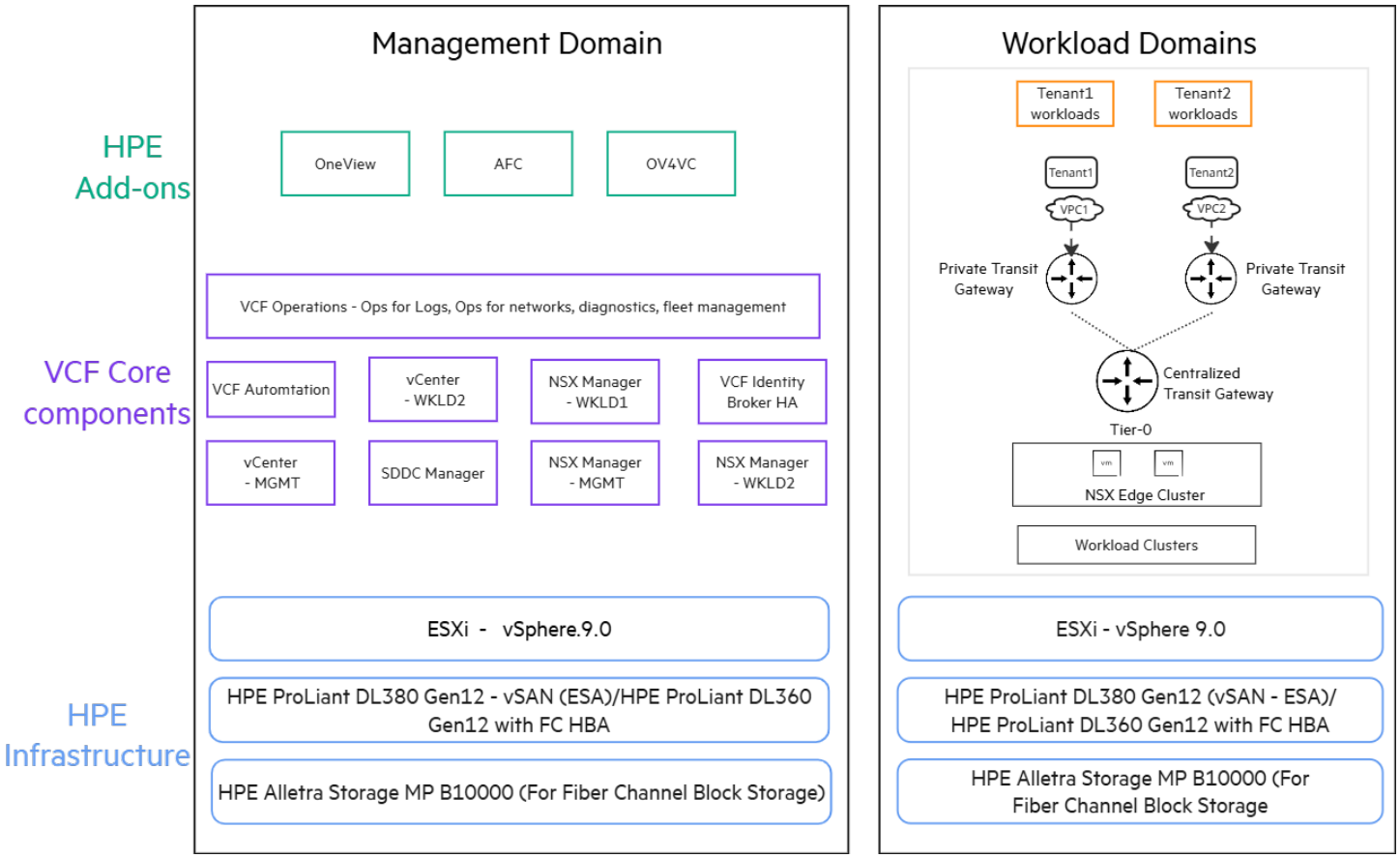

Figure 1. VMware Cloud Foundation 9.0 Logical Architecture utilizing external FC storage/vSAN both for Management and Workload domain

Hardware

Figure 2 shows physical rack layout of solution components of HPE validated VMware Cloud Foundation 9.0 supporting vSAN Express Storage Architecture (ESA) and Fibre Channel (VMFS on FC).

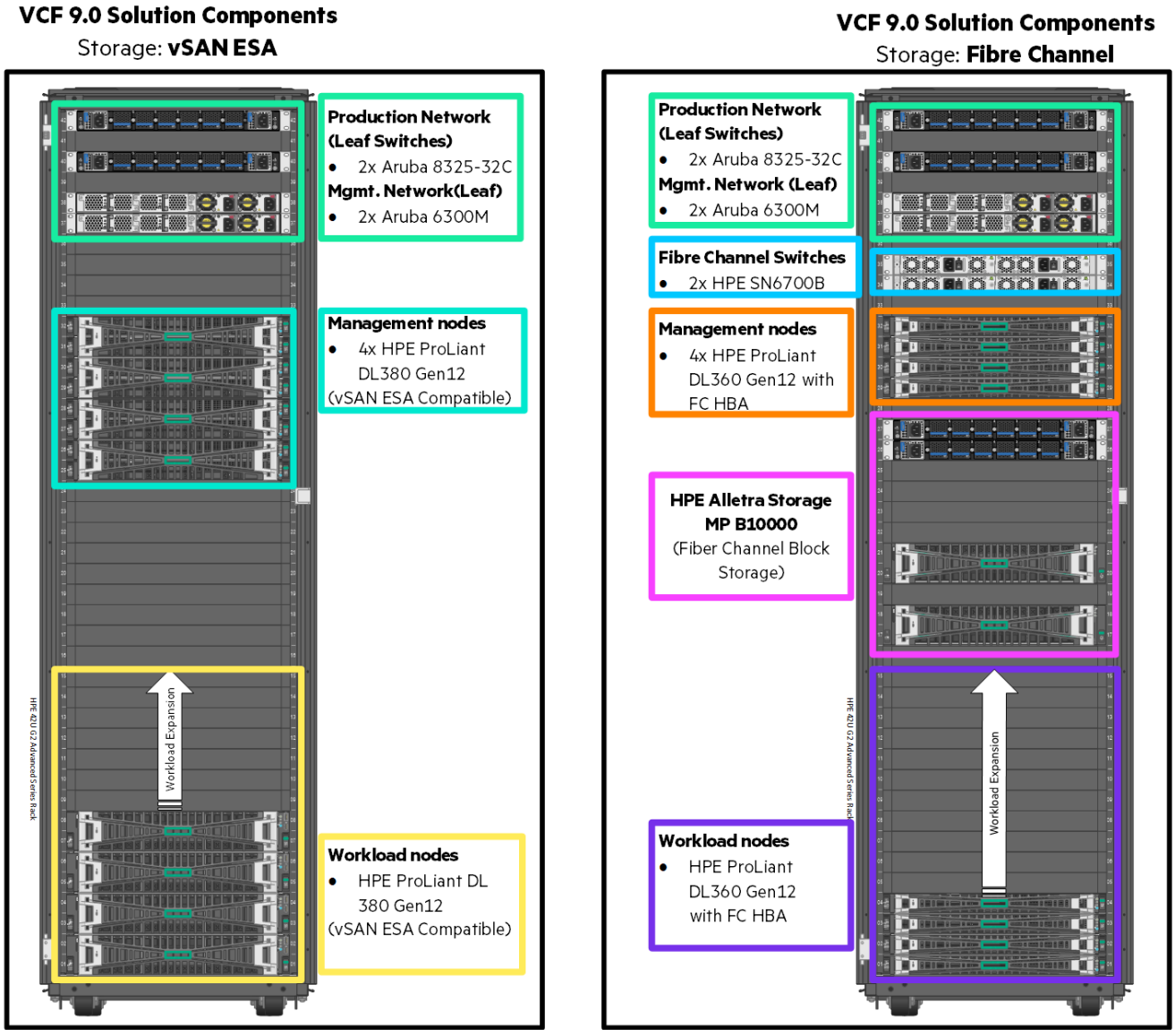

Figure 2. Physical rack layout of vSAN ESA and Fibre Channel architecture

Table 1 and Table 2 shows the hardware components used in this solution.

Table 1. HPE hardware components for VCF 9.0 vSAN Express Storage Architecture (ESA) storage

Components	Quantity	Description
HPE ProLiant DL380 Gen12 server (Management domain node)	4	2 x Intel® Xeon® 6730PP (2.5GHz/32-core/250W) 32 x 32GB RAM (Dual Rank x8 DDR5-6400 CAS-52-52-52 EC8 Registered Smart Memory Kit) 1 x HPE MR216i-p Gen11 x16 Lanes without Cache PCI SPDM Plug-in Storage Controller 2 x HPE 1.6TB SAS Mixed Use SFF BC Self-encrypting FIPS 140-2 PM7 SSD 8 x HPE 3.2TB NVMe Gen4 High Performance Mixed Use SFF BC U.3 PM1735a SSD 2 x Mellanox MCX631432AS-ADAI Ethernet 10/25Gb 2-port SFP28 OCP3 Adapter for HPE
HPE ProLiant DL380 Gen12 server (Workload domain node)	4	2 x Intel® Xeon® 6730PP (2.5GHz/32-core/250W) 32 x 32GB RAM (Dual Rank x8 DDR5-6400 CAS-52-52-52 EC8 Registered Smart Memory Kit) 1 x HPE MR216i-p Gen11 x16 Lanes without Cache PCI SPDM Plug-in Storage Controller 2 x HPE 1.6TB SAS Mixed Use SFF BC Self-encrypting FIPS 140-2 PM7 SSD 16 x HPE 3.2TB NVMe Gen4 High Performance Mixed Use SFF BC U.3 PM1735a SSD 2 x Mellanox MCX631432AS-ADAI Ethernet 10/25Gb 2-port SFP28 OCP3 Adapter for HPE
Aruba CX 8325 Switch	2	Aruba 8325-32C Power to Port Airflow 6 Fans 2 Power Supply Units
Aruba CX 6300M Switch	2	Aruba 6300M 48G Power to Port Airflow 2 Fans 1 Power Supply Unit

Table 2. HPE hardware components for VCF 9.0 Fibre Channel (VMFS on FC) storage

Components	Quantity	Description
HPE ProLiant DL360 Gen12 server (Management domain node)	4	2 x Intel Xeon 6737P 2.9GHz 32-core 270W Processor for HPE 32 x 32GB RAM (Dual Rank x8 DDR5-6400 CAS-52-52-52 EC8 Registered Smart Memory Kit) 1 x HPE MR216i-o Gen11 x16 Lanes without Cache OCP SPDM Storage Controller 2 x HPE 1.6TB SAS Mixed Use SFF BC Self-encrypting FIPS 140-2 PM7 SSD 1 x HPE InfiniBand NDR200/Ethernet 200GbE 2-port QSFP112 PCIe5 x16 MCX755106AC-HEAT Adapter 1 x HPE SN1610Q 32Gb 2-port Fibre Channel Host Bus Adapter
HPE ProLiant DL360 Gen12 server (Workload domain node)	3	2 x Intel Xeon 6730P 2.5GHz 32-core 250W Processor for HPE 12 x 16 GB RAM (Single Rank x8 DDR5-6400 CAS-52-52-52 EC8 Registered Smart Memory Kit) 1 x HPE MR216i-o Gen11 x16 Lanes without Cache OCP SPDM Storage Controller 2 x 1.6TB SAS Mixed Use SFF BC Self encrypting FIPS 140-2 PM7 SSD

Components	Quantity	Description
		1 x HPE InfiniBand NDR200/Ethernet 200GbE 2-port QSFP112 PCIe5 x16 MCX755106AC-HEAT Adapter 1 x HPE SN1610Q 32Gb 2-port Fibre Channel Host Bus Adapter
HPE Alletra Storage MP B10000	1	1 HPE Alletra Storage MP B10000 Base Cluster Configuration 2 HPE Alletra Storage MP B10240 Controller Node 4 HPE Alletra Storage MP 32Gb 4-port Fibre Channel OCP LPm37004 Host Bus Adapter 2 HPE Alletra STG MP 32-port 100GbE Switch Bundle 1 HPE Alletra Storage MP 10001 NVMe Configure-to-order Expansion Shelf 24 HPE Alletra Storage MP 3.84TB NVMe SFF Self-encrypting SSD
HPE B-series SN6700B SAN Switches	2	HPE SN6700B 64Gb 56/24 24p SFP28 FC Switch
Aruba CX 8325 Switch	2	Aruba 8325-32C Power to Port Airflow 6 Fans 2 Power Supply Units
Aruba CX 6300M Switch	2	Aruba 6300M 48G Power to Port Airflow 2 Fans 1 Power Supply Unit

HPE ProLiant DL380 Gen12 server

The secure 2P 2U server is a robust and versatile server designed to handle high demanding workloads in today's dynamic IT environment. It supports two Intel Xeon 6 processors, each with up to 144 cores per socket and memory capacity of up to 8TB . Equipped with high-speed PCIe Gen5 and Flexible I/O for accelerator options such as GPU, it provides a perfect balance of density and expandability along with support for a wide range of storage options. iLO 7 embedded management; and security enhancements. Designed for supreme versatility and resiliency while being backed by a comprehensive warranty makes it ideal for multiple environments from Containers to Cloud to Big Data. The solution utilizing the vSAN and storage solutions leverages four (4) HPE ProLiant DL380 Gen12 servers to deploy VMware Cloud Foundation Management Domain and four(4) HPE ProLiant DL380 Gen12 Servers to deploy VMware Cloud Foundation workload domain.

Figure 3. HPE ProLiant DL380 Gen12 server

HPE ProLiant DL360 Gen12 server

The HPE ProLiant Compute DL360 Gen12 is a compact 1U 2P server that delivers exceptional compute performance, memory density with scalability and high-speed data transfer rate. Powered by Intel® Xeon® 6 Processors with up to 144 cores, plus up to 8TB of DDR5 memory running at maximum 6400 MT/s, DL360 Gen12 can be scaled with a variety of front storage support, ranging from 3.5" 4x LFF, 2.5" 10x SFF as well as 20x E3.S NVMe drives. High performance Networking OCP cards and RAID 1 OS Boot Device can be configured at front cage for healthy airflow. The HPE ProLiant Compute DL360 Gen12 is an ideal hybrid cloud platform for enterprise applications and workloads. This is an intelligent sever in three pillars. Firstly, the intelligent multiple-purpose front cage design delivers extreme scalability through hybrid front storage including SFF, E3.S, OS Boot device and front OCP NIC (post launch). Secondly, the intelligent leak detection feature provides easy maintenance of Closed-loop Liquid Cooling and Direct Liquid Cooling modules. Last but not least, the new DL360 Gen12 Smart Chassis configuration feature designed in the One Config Advanced (OCA) offers extended thermal configuration capability and high scalability associated with high power CPU and high-bandwidth networking cards for Compute Nodes and Networking Nodes. Smart Chassis delivers a reduction of configuration time on cables and maximizes the usage of multi-purpose front cage design. The solution utilizing FC storage as storage solutions leverages four (4) HPE ProLiant DL360 Gen12 servers to deploy VMware Cloud Foundation Management Domain and three(3) HPE ProLiant DL360 Gen12 Servers to deploy VMware Cloud Foundation workload domain.

Figure 4. HPE ProLiant DL360 Gen12 server

HPE ProLiant Gen12 Servers Security Features

The HPE ProLiant Gen12 servers deliver exceptional security enhancements, optimizing both infrastructure security and performance for enterprise environments. These systems integrate advanced embedded security mechanisms, providing comprehensive protection for critical data and applications. Key features encompass:

— HPE ProLiant Gen12 servers feature advanced security with iLO 7, including Silicon Root of Trust for firmware validation, runtime verification, and automatic secure recovery.

— They incorporate a Secure Enclave ASIC for isolated cryptographic operations and quantum-resistant encryption readiness.

— FIPS 140-3 Level 3 certification ensures high-level compliance, while Zero Trust integration enforces continuous verification.

— Enhanced Server Data Security: Supports encryption and key management via iLO Managed Encryption, UEFI-managed encryption, and self-encrypting drives (SED) for robust data-at-rest protection, integrated with the Secure Enclave for tamper-resistant operations.

— One-Button Secure Erase: Enables NIST SP 800-88-compliant media sanitization for secure server decommissioning, ensuring data is irrecoverably wiped.

— Expanded Industry Compliance: Aligns with FIPS 140-3, NIST SP 800-53, NIST SP 800-171, and NIST SP 800-88 standards, including post-quantum cryptography (PQC) readiness via Silicon Root of Trust (SROT) for firmware validation.

HPE iLO

HPE Integrated Lights Out (iLO) is embedded in HPE ProLiant Gen12 platforms and provides server management that enables faster deployment, and simplified lifecycle operations while maintaining end-to-end security, thus increasing productivity. This is supported by iLO7 security features including:

1. Silicon Root of Trust, ensuring firmware validation to prevent tampering.
2. Runtime Firmware Verification, continuously checking integrity during operation.
3. Automatic Secure Recovery, reverting to a known-good firmware version if compromised.
4. Zero Trust Integration, enhancing compatibility with modern identity and access solutions.

HPE Alletra Storage MP B10000

HPE Alletra Storage MP B10000 is a unique, software-defined, scale-out data system that consolidates a high-performance all-flash object storage service, exabyte-scale capacity, and easy management for data intensive initiatives like data lakes, digital repositories, and backup with flash-accelerated recovery. The HPE Alletra Storage MP takes advantage of the industry's first disaggregated multi-protocol architecture, which makes it possible for you to scale from terabytes to exabytes on the same hardware. Cost savings are provided through the ability to efficiently scale capacity and performance independently.

It is a software-defined, multi-protocol storage platform that provides flexibility and high performance for both structured and unstructured data storage needs. It consists of standardized, composable building blocks — compute (node), capacity (JBOF), and switches — that can be configured for different software-defined storage personas and use cases. This enables you to uniquely deploy block, file or object workloads on common hardware and manage everything with a unified cloud experience through the HPE GreenLake cloud.

Figure 5 shows the front view of HPE Alletra Storage MP Enclosure.

Figure 5. Front view HPE Alletra Storage MP Enclosure

Figure 6 shows the rear view of HPE Alletra Storage MP Enclosure.

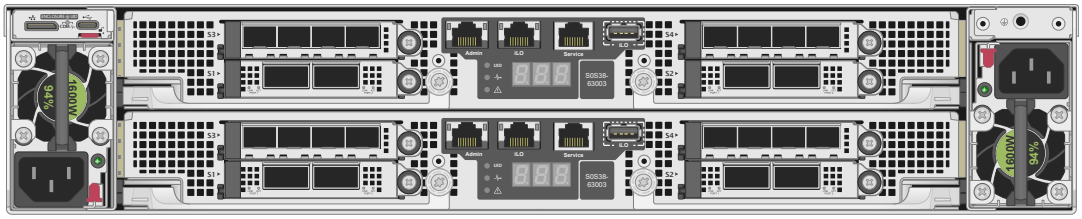

Figure 6. Rear view HPE Alletra Storage MP Enclosure

HPE Alletra Storage MP B10000 Drive Enclosure

HPE Alletra Storage MP B10000 Drive Enclosures extend the storage capacity of the storage array. Each enclosure contains multiple slots for either small or large form factor drives. Drive enclosures also contain Input/Output modules (cards), and a pair of PCMs (power-cooling modules) for redundant power and cooling of the enclosure.

Front View

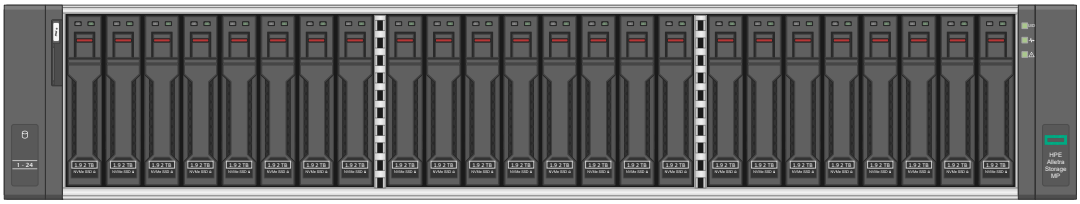

Figure 7. Front View of HPE Alletra Storage MP Drive Enclosure

Rear View

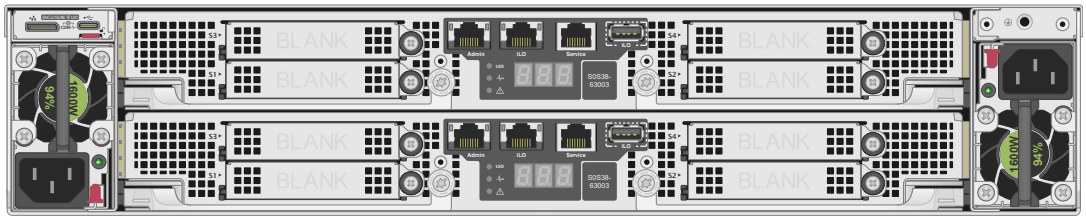

Figure 8. Rear view of HPE Alletra Storage MP

HPE Alletra Storage MP Switches

HPE Alletra Storage MP B10000 family of storage arrays support both switched and switchless architecture. For the purpose of this reference architecture, a switched storage array was used which is supported by HPE Alletra Storage MP Switches. These switches are used to connect HPE Alletra Storage MP B10000 controller nodes with disk enclosures and help with easy expansion of the storage capacity.

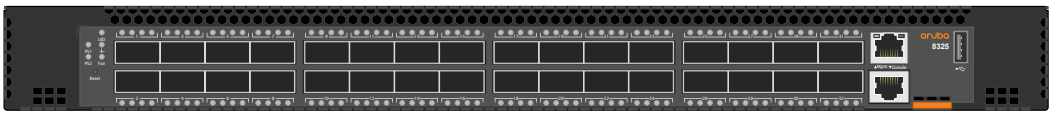

Figure 9.HPE Alletra Storage MP Switches

HPE B-series SN6700B SAN Switches

The HPE Storage Fibre Channel Switch B-series SN6700B is a high-performance, ultra-dense, highly scalable, and easy-to-use enterprise-class storage networking switch delivering Gen7 64Gb Fibre Channel (FC) capabilities. It is

designed to support data growth, demanding workloads, and data center consolidation in small to large scale enterprise infrastructures. Delivering 64Gb performance, customized high port density, and integrated network sensors, it accelerates data access, adapts to evolving requirements, and drives 24x7 businesses.

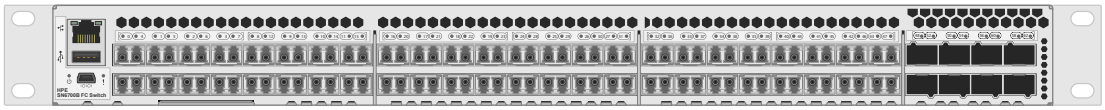

Figure 10. HPE Storage Fibre Channel SN6700B Switch

Aruba 8325 Top of Rack Switches

The Aruba 8325 Switches offers a flexible and innovative approach to addressing the application, security, and scalability demands of the mobile, cloud, and IoT era. These switches serve the needs of the next-generation core and aggregation layer, as well as emerging data center requirements at the Top of Rack (ToR) and End of Row (EoR). The Aruba 8325 series include industry-leading line rate ports 1/10/25GbE (SFP/SFP+/SFP28) and 40/100GbE (QSFP+/QSFP28) with connectivity in a compact 1U form factor.

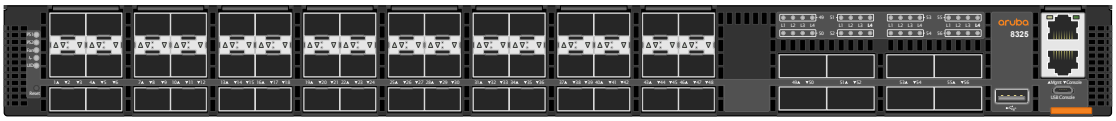

Figure 11. Aruba 8325 32Y8C Switch

Aruba 6300M Out of Band Management Switches

The Aruba CX 6300 Switch Series is a modern, flexible, and intelligent family of stackable switches ideal for enterprise network access, aggregation, core, and data center top of rack (ToR) deployments. Created for game-changing operational efficiency with built-in security and resiliency, the Aruba 6300 switches provide the foundation for high-performance networks supporting IoT, mobile, and cloud applications.

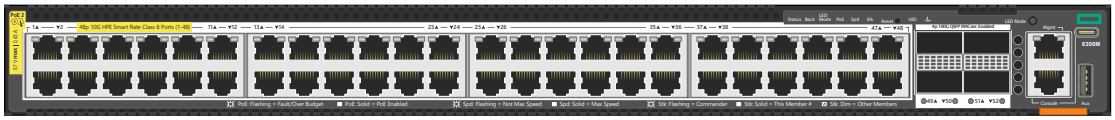

Figure 12. Aruba 6300M Switch Software

Tables 3, 4 and 5 list the software components used in this solution.

Table 3. HPE software and firmware components

Component	Version
HPE ProLiant Gen12 server's Service Pack for ProLiant (SPP)	2025.09.00.00
HPE OEM image for vSphere 9.0	9.0.0.0 (Build: 24813472) (VMware-ESXi-9.0.0-24813472-HPE-900.0.0.12.2.0.4-oct2025.iso)
HPE Add-On	HPE ESXi 9.0 Add-On 900.0.0.12.2.0.0.4 (HPE-900.0.0.12.2.0.4-oct2025-Addon-depot.zip)
Aruba CX 6300M Switch	10.13.1110 (ArubaOS-CX_6400-6300_10_13_1110.swi)
Aruba CX 8325 Switch	10.13.1110 (ArubaOS-CX_8325_10_13_1110.swi)
HPE G3 Metered and Switches PDUs	3.2.5

Component	Version
HPE Alletra Storage MP Block OS	10.4.8

Table 4. VMware software components

Component	Version	Build number
VCF Installer	9.0.0.0	24755599
VMware ESX	9.0.0.0	24813472
VMware vCenter	9.0.0.0	24755230
VMware vSAN ESA Witness	9.0.0.0	24755427
VMware vSAN File Services	9.0.0.0	24755229
VMware vSAN OSA Witness	9.0.0.0	24755428
VMware NSX	9.0.0.0	24733063
SDDC Manager	9.0.0.0	24703748
VMware Cloud Foundation Operations	9.0.0.0	24695812
VMware Cloud Foundation Operations fleet management	9.0.0.0	24695816
VMware Cloud Foundation Operations for logs	9.0.0.0	24695810
VMware Cloud Foundation Operations for networks	9.0.0.0	24694676
VMware Cloud Foundation Automation	9.0.0.0	24701403
VMware vSphere Supervisor	9.0.0.0	24686447
VMware Cloud Foundation Download Tool	9.0.0.0	24703747
VMware Cloud Foundation Operations Identity Broker	9.0.0.0	24695128

Refer the Bill of Materials (BOM) for the complete VMware Cloud Foundation software products.

Table 5. HPE Solution Integration software for VMware

HPE Value added Software	Version
HPE OneView for VMware vCenter plug-in	11.7
HPE OneView (Virtual Appliance)	10.0
Aruba Fabric Composer	7.2.0

For more information on VMware Cloud Foundation 9.0 software and firmware, refer to the HPE Firmware and Software Compatibility Matrix for VMware Cloud Foundation 9.0.

VMware Cloud Foundation

VMware Cloud Foundation (VCF) 9.0 is a comprehensive private cloud platform that combines the agility and scale of public cloud with the security and performance of private cloud. It simplifies the entire lifecycle of cloud infrastructure, from installation to day-to-day management, enhancing efficiency and security. VCF offers centralized automation with self-service cloud automation, blueprints, and centralized APIs/SDKs, supporting both VMs and containers, including GPU support. It leverages VMware's world-class virtualization engine to ensure feature parity between VMs and containers, providing a developer-ready infrastructure without compromising performance. Additionally, VCF supports Fibre Channel storage as principal or supplemental storage for the management domain and workload domains.

It introduces a unified, streamlined infrastructure management experience for Cloud Admins through a centralized console that consolidates capacity planning, tenant management, governance policy configuration, and security monitoring. With tools like VCF Diagnostics and Application Topology and Network Analysis, issue resolution becomes faster and performance optimization more efficient. For Platform Engineers, VCF 9.0 offers a versatile, consumption-ready environment supporting VMs, Kubernetes, and containers, along with enhanced multi-tenancy and self-service capabilities that boost productivity, enforce governance, and accelerate application delivery in modern development workflows.

Figure 13 shows the overview of VMware Cloud Foundation components.

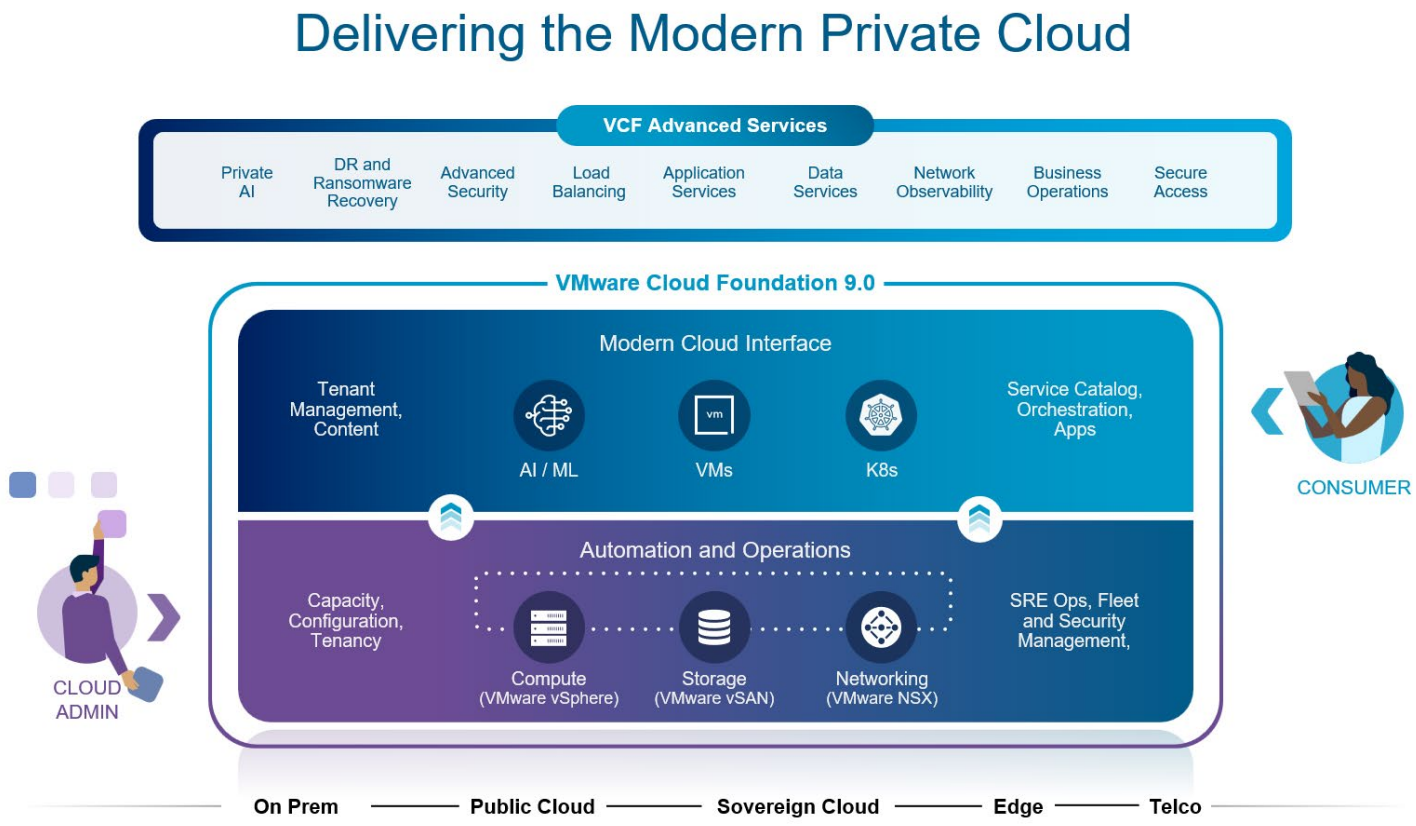

Figure 13. VMware Cloud Foundation (Courtesy: Broadcom)

VMware Cloud Foundation Key Concepts

VCF 9.0 introduces a few new logical constructs related to building and managing private cloud deployment. A few key concepts are listed as follows. For a more detailed description, visit the VCF Taxonomy documentation.

VCF Instance: VCF instance consists of a management domain with SDDC Manager, vCenter, and NSX Manager and workload domains with vCenter and NSX Manager.

VCF Fleet: VCF Fleet includes a primary management domain with single VCF Operations and VCF Automation and one or more VCF instances.

VCF Private Cloud: VCF Private Cloud includes one or more VCF Fleets.

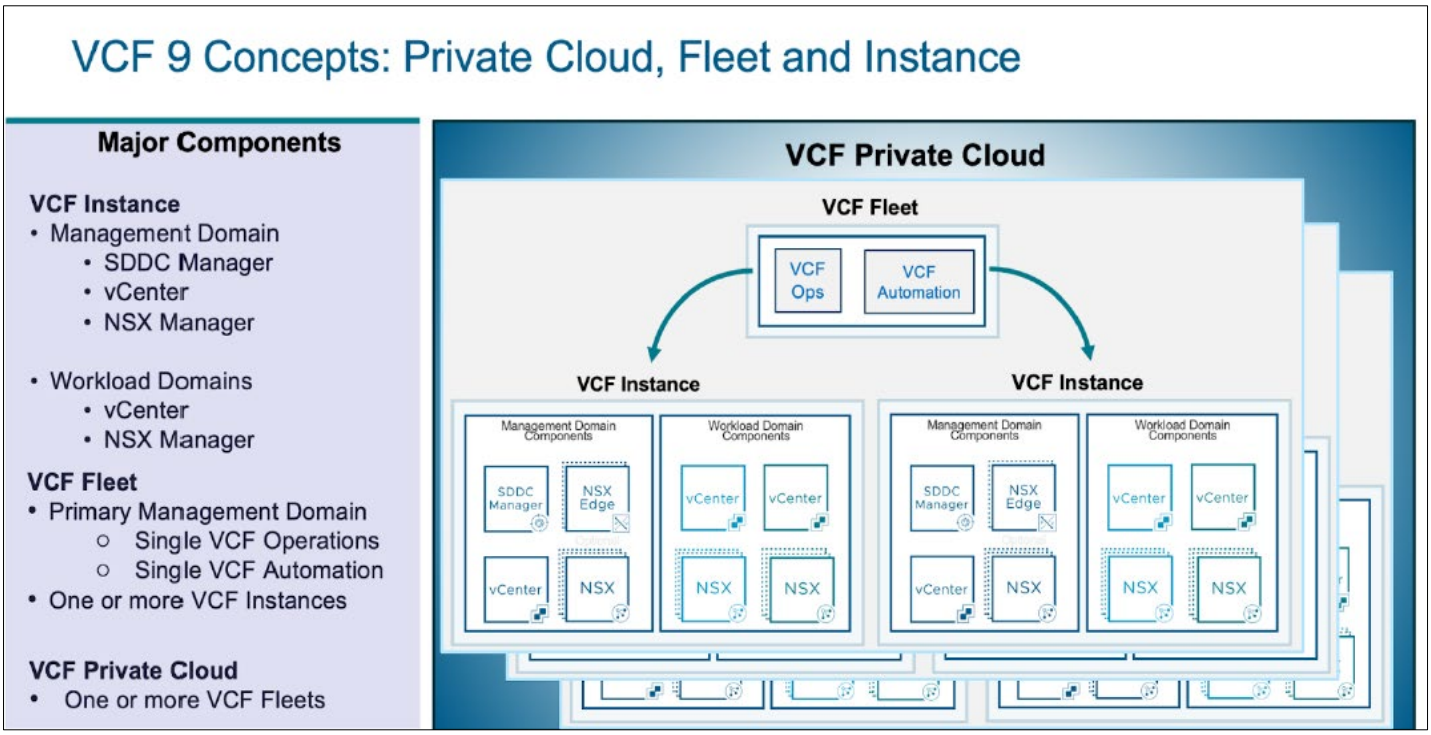

Figure 14. VMware Cloud Foundation Key Concepts (Courtesy Broadcom)

VMware Cloud Foundation components

The core components of VMware Cloud Foundation are as follows:

VCF Installer

VMware Cloud Foundation 9.0 includes VCF Installer, which is a new virtual appliance that provides automated deployment and configuration workflows for the VCF environment. The VCF Installer appliance UI and JSON input functionality now replace the Deployment Parameter Worksheet Cloud Builder appliance. Where the VCF Installer is deployed impacts how it can be used within the environment and for future deployments. For more information refer to What is the VMware Cloud Foundation Installer?.

SDDC Manager

SDDC Manager provides management capabilities for the underlying virtual infrastructure and uses binaries to deploy new workload domains, and to patch and upgrade existing ones.

VMware vCenter

VMware vCenter provides management of a VMware virtualized environment with one or more ESX hosts. By default, all vCenters are deployed with their own dedicated vCenter Single Sign-On (SSO) domain. ESX host commissioning and NSX edge deployments can be performed via vCenter.

VMware ESX

ESX is a type 1 hypervisor used to implement virtualization on bare-metal systems. ESX provides compute virtualization within the software-defined data center, and it is a foundational building block for implementing a private cloud. VMware vSphere Lifecycle Manager provides the functionality to upgrade and patch ESX. VMware vSphere Lifecycle Manager along with HPE OneView Hardware Support Manager (HSM) plug-in can also perform server firmware, drivers, and software updates in the same maintenance window as the ESX server operating system updates.

VMware vSAN

VMware vSAN is a software-defined storage solution, aggregates local or direct-attached capacity devices of all ESX hosts in a cluster and creates a single storage pool shared across all ESX hosts in the vSAN cluster. With HPE ProLiant Gen12 servers for ESX hosts deliver exceptional compute performance, memory density scalability and high-speed data transfer rate to run vSAN on VMware Cloud Foundation (VCF).

vSAN ESA is a hardware-optimized architecture designed for modern NVMe-based storage devices, offering high performance and simplified management compared to the original storage architecture (OSA).

VMware NSX

VMware NSX® is the network virtualization solution in VMware Cloud Foundation™ (VCF) that enables scale-out network connectivity, agile multi-tenant operations, and a simplified network consumption model. NSX works with all leading switch fabric management solutions in the industry to provide consistent configuration and workload mobility. NSX brings network services closer to the application workload, enabling efficient traffic forwarding and simpler network segmentation. It also provides a complete set of logical networking capabilities and services, including logical switching, routing, load balancing, virtual private cloud (VPC), virtual private network (VPN), and monitoring. Virtual Private Cloud (VPC) is a logically isolated, tenant-specific virtual network that provides a dedicated environment. It is a way to create secure, isolated environments within a larger VCF private cloud, allowing users to manage their own networks, subnets, and security policies.

VMware Cloud Foundation Operations

Starting with VMware Cloud Foundation™ (VCF), VCF Operations is the central control plane for managing the entire VMware Cloud Foundation (VCF) instance, offering a streamlined approach to operations, monitoring, and lifecycle management. Fleet management within VCF Operations allows admins to oversee multiple VCF instances from a single console. This includes centralized lifecycle management and consistent upgrades across environments, identity and access management (IAM and SSO), certificate and password management, tag management, configuration management & drift assessment and license management.

VMware Cloud Foundation Automation

In VMware Cloud Foundation™ (VCF), VCF Automation provides Supervisor services (VM, K8s, Network, Volume, DB etc.) so that application teams can provision IaaS in a self-service manner as needed, without going through a cumbersome ticketing process. Through the Kubernetes CLI/UI/API, users can create Supervisor Namespaces, create VMs, create vSphere Kubernetes Service (VKS) clusters, log into the VKS cluster, apply applications and perform Day 2 actions on provisioned IaaS resources in a secure private cloud. Additionally, it supports policy-based governance, infrastructure as code, Kubernetes and network automation, private AI automation, SDDC infrastructure consumption, workload lifecycle management, and orchestration and extensibility.

HPE Value added Software

HPE OneView

HPE OneView is a management appliance used to deploy and maintain infrastructure faster, simplify IT operations, and increase productivity. It lets businesses simplify and automate today's complex hybrid IT infrastructure. Through software-defined intelligence, HPE OneView takes a template-driven approach for deploying, provisioning, updating, and integrating compute, storage, and networking infrastructure.

HPE OneView for VMware vCenter

HPE OneView for VMware vCenter is a VMware vCenter plug-in that provides comprehensive server hardware management capabilities for HPE servers within a VMware environment. It offers features such as monitoring, firmware updates, vSphere/ESX image deployment, remote control, and power optimization. Integrated within this plug-in is the HPE Hardware Support Manager (HSM), which enables coordinated lifecycle management by allowing firmware updates to be applied during the same maintenance window as ESX operating system updates—often with a single reboot—through seamless integration with vSphere Lifecycle Manager (vLCM).

HPE Aruba Fabric Composer

Aruba Fabric Composer is an intelligent, API-based, software-defined orchestration solution that simplifies and accelerates leaf-spine network provisioning and day-to-day operations across rack-scale compute and storage infrastructure. Aruba Fabric Composer orchestrates is a discrete set of switches as a single entity called a fabric which significantly simplifies operations and troubleshooting. Aruba's data center orchestration solution is fully infrastructure and application-aware providing automation of various configuration and lifecycle events.

Design and configuration guidance

This guidance describes the deployment of a VCF Fleet in a Single Site with a single availability zone. The VCF Operations and Automation components are deployed in a High Availability model within the single VCF instance. Utilize the VCF Planning and Preparation Workbook which is a Microsoft Excel workbook which gathers input for your intended deployment specifications including resource sizing.

A VCF Fleet provides a scalable starting point for deploying the first VCF Instance, with the flexibility to expand to multiple instances while maintaining centralized operations with self-service and IaaS models for workload and services consumption with the ability to support both VM and container-based workloads and leverage a variety of storage options including vSAN and external storage solutions.

For more details refer to the Design Blueprints for VMware Cloud Foundation at, Design Blueprints for VMware Cloud Foundation.

VMware Cloud Foundation 9.0 Storage options

While there are several storage options supported in VMware Cloud Foundation 9.0 listed here , the reference architecture provides guidance on vSAN ESA or Fibre Channel Storge Models as storage options for management and workload domains.

vSAN Express Storage Architecture (ESA)

VMware vSAN 9.0 introduces the vSAN Express Storage Architecture (ESA), a new architecture designed to enhance performance and efficiency. ESA leverages high-performance NVMe drives and a single-tier storage pool, replacing the traditional two-tier disk group model of vSAN OSA.

Fiber Channel

The Virtual Machine File System on Fibre Channel provides block-level storage access over a Fibre Channel network. The Fibre Channel storage from HPE Alletra Storage MP is used as principal storage for both Management domain and Workload domains.

Deployment process for VCF 9.0

The following figure shows the high-level workflow for the deployment of VMware Cloud Foundation 9.0.

Broadcom provides a journey map illustrating the install experience of deploying a new VCF deployment. Refer to the VCF 9.0 Customer Journey map for more information including duration of tasks.

Figure 15 shows the high-level workflow for the deployment of VMware Cloud Foundation 9.0 utilizing the vSAN Storage

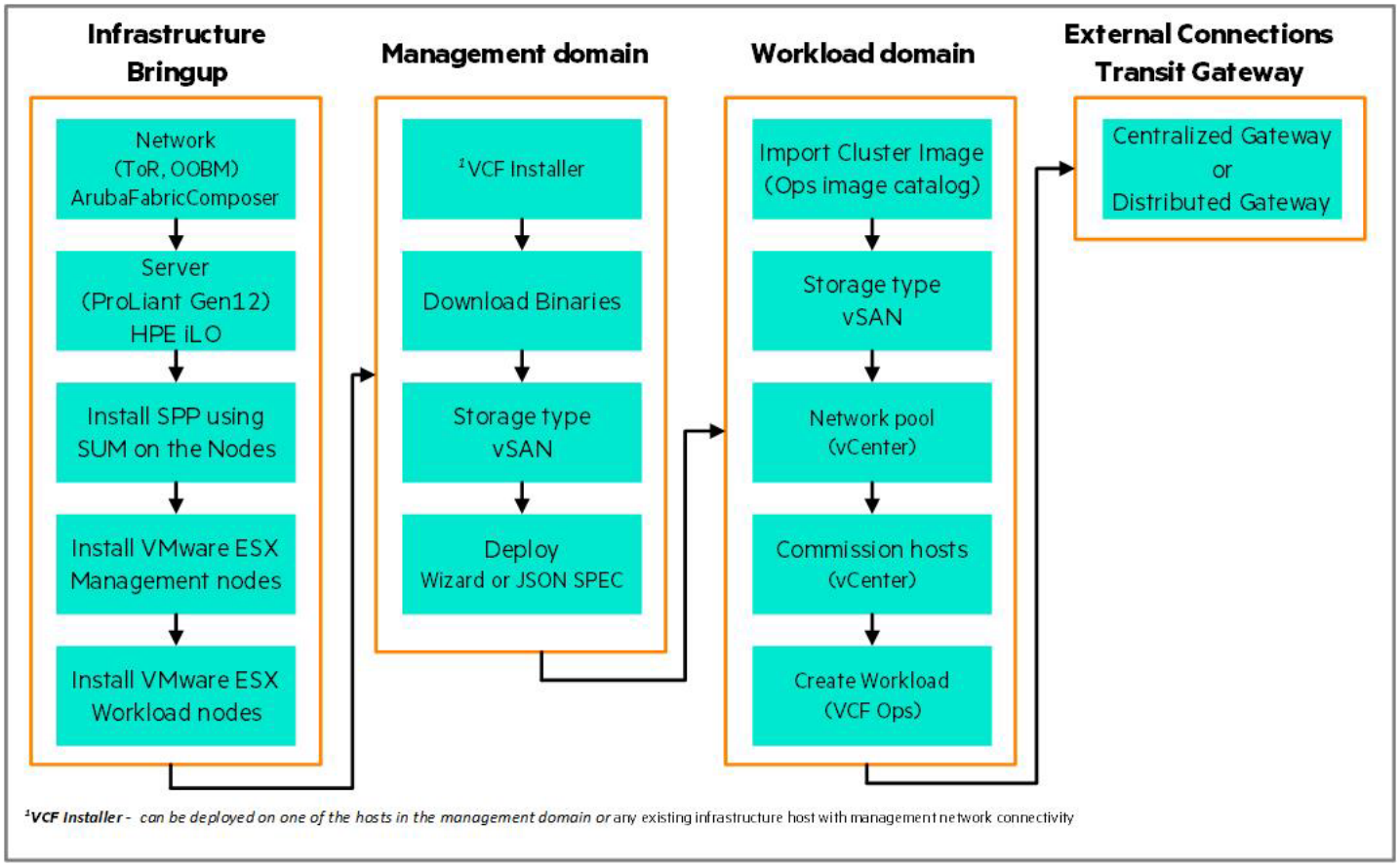

Figure 15. Deployment process for VCF 9.0 utilizing vSAN storage

Figure 16 shows the high-level workflow for the deployment of VMware Cloud Foundation 9.0 utilizing the FC storage

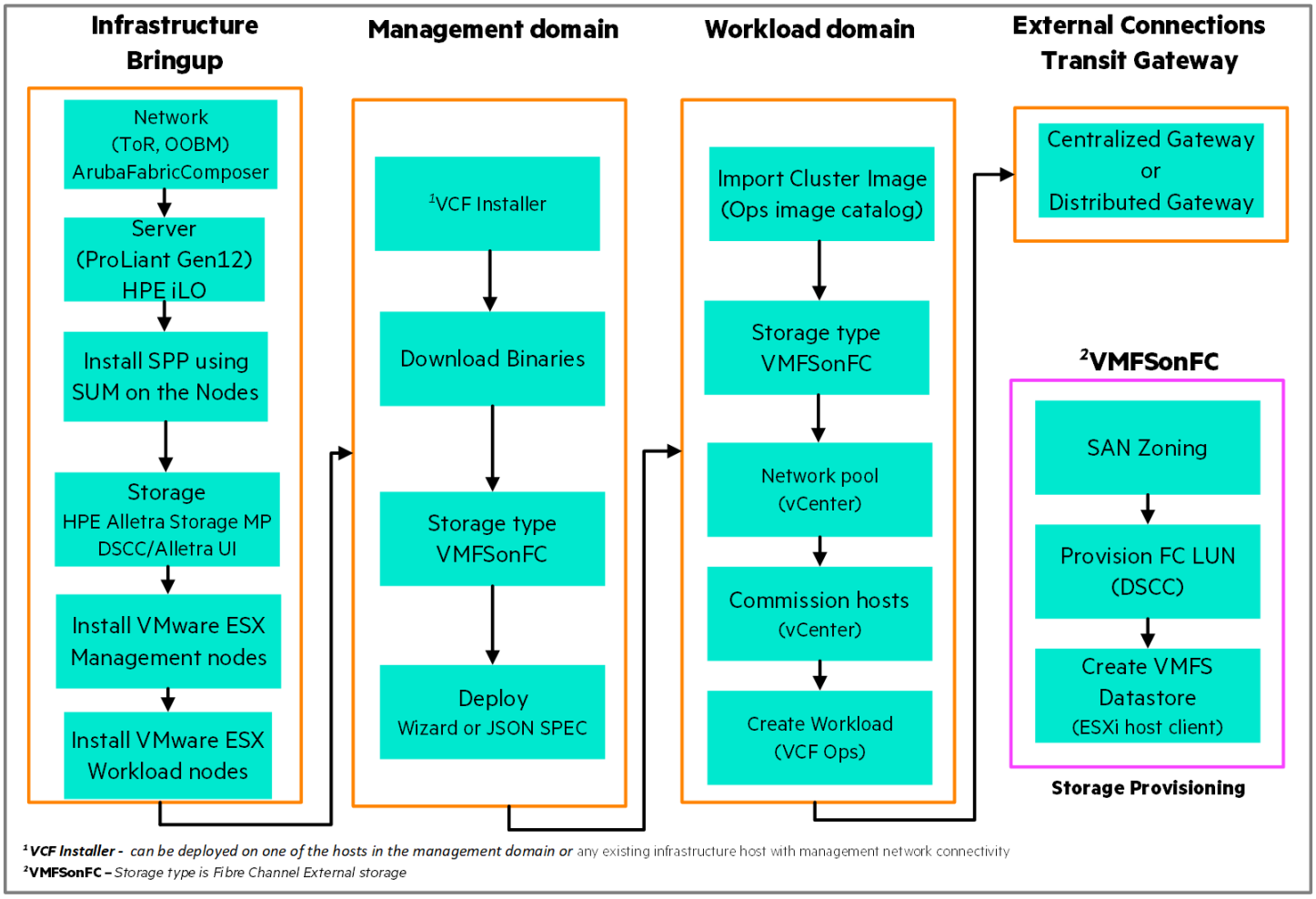

Figure 16. Deployment process for VCF 9.0 utilizing FC storage

Infrastructure Configuration

Network

Aruba CX 6300M Switches configuration

Aruba CX 6300M switches are the out-of-band management switches in this solution. Both Aruba CX 6300M switches are configured for Virtual Switching Framework that virtualizes two physical devices into one Virtual Fabric to provide high availability and scalability. All the HPE ProLiant DL Server's iLO connects to the solution management network configured on Aruba CX 6300M switches. HPE Integrated Lights-Out enables the remote management of HPE ProLiant DL Servers securely from anywhere on this solution management network.

Aruba CX 8325 Switches configuration

Aruba CX 8325 Switches should be connected and configured for Virtual Switching Extension (VSX) that virtualizes the control plane of two aggregation switches to function as one device at layer 2 and as independent devices at layer 3.

All the VLANs required for VMware Cloud Foundation deployment should be created on Aruba 8325 top-of-rack (ToR) switches. The Ethernet ports on the HPE Aruba CX 8325 Switches should be trunk enabled allowing all VLANs required for the VMware Cloud Foundation stack.

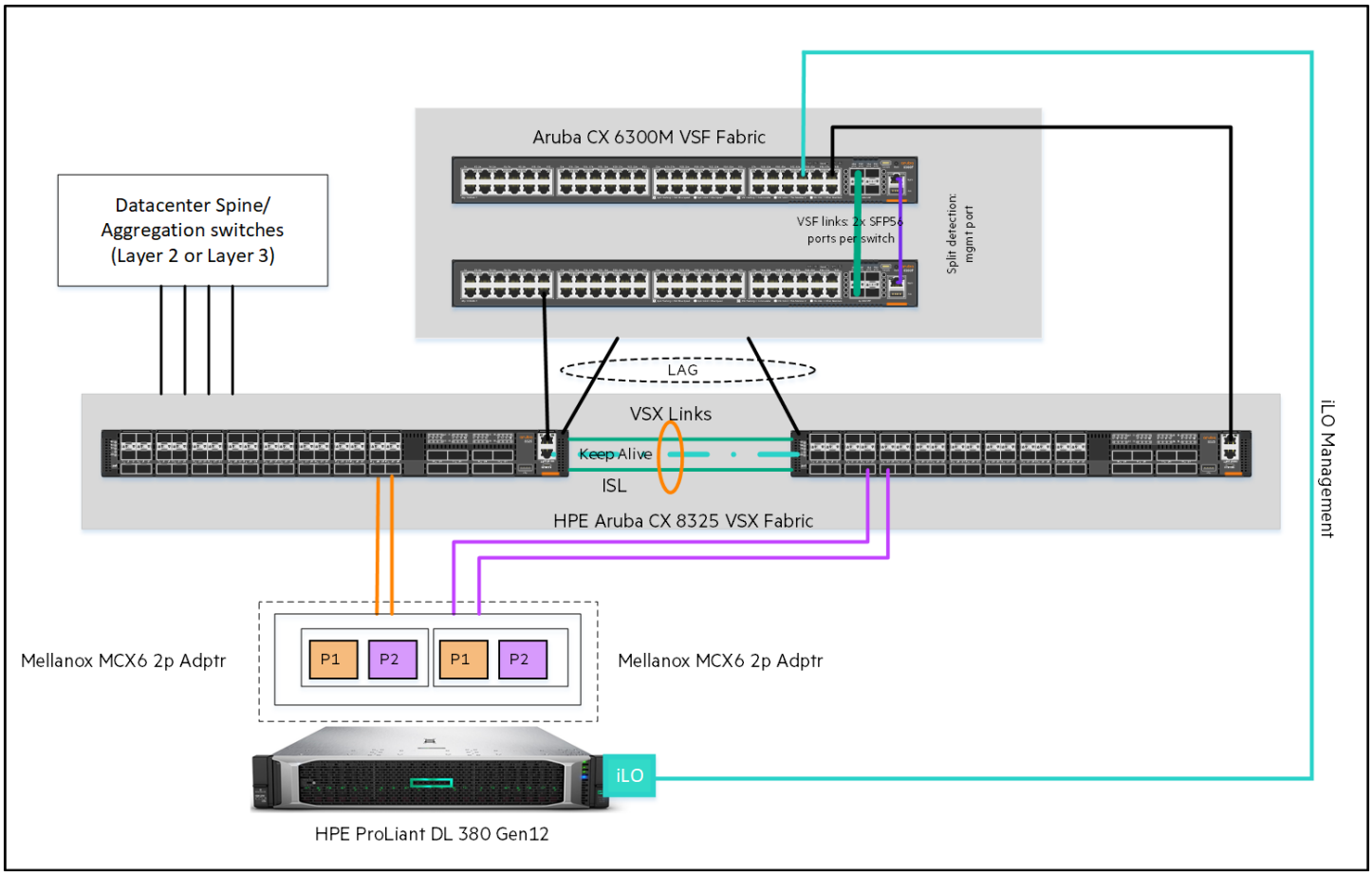

Figure 17. Network layout with Aruba Switches for DL380 Gen12

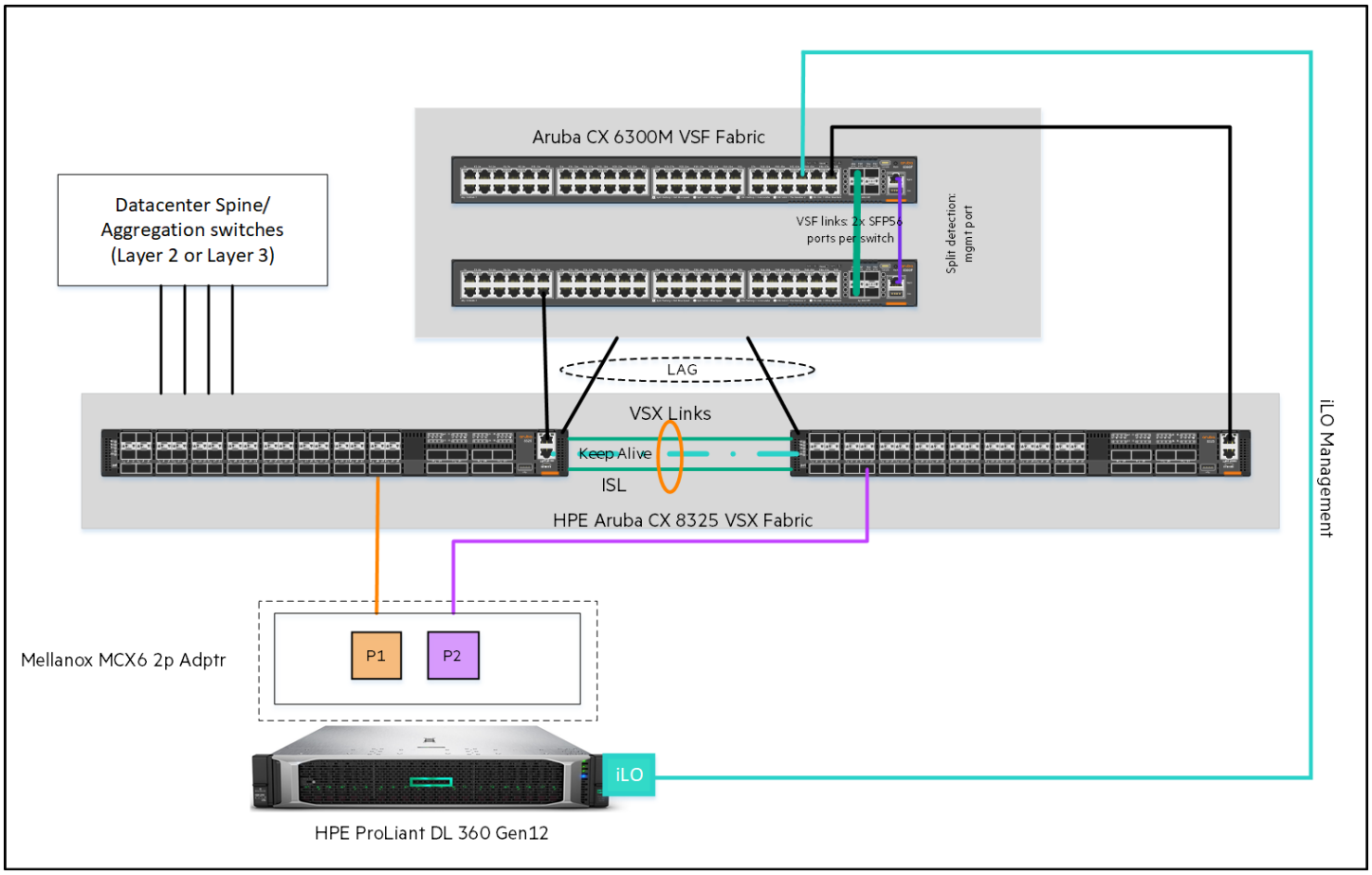

Figure 18. Network layout with Aruba Switches for HPE ProLiant DL360 Gen12 Servers.

Aruba Fabric Composer

In this solution, Aruba CX 6300 OOBM management switches and Aruba CX 8325 data switches are orchestrated from the single AFC user interface providing connectivity visualizations and automation of onsite deployments and day-to-day operations.

Aruba Fabric Composer available in OVA format is deployed as a virtual machine on a standalone ESX server. This ESX server has connectivity to the solution management network and is also used to host other infrastructure virtual machines such as NTP and DNS, which are necessary to deploy this cloud solution. To begin with, both Aruba CX 6300M switches and Aruba CX 8325 switches are initialized and configured with management IPs that belong to the solution management network. A pair of Aruba CX 6300 OOBM switches and Aruba CX 8325 switches are on boarded to AFC as part of the Aruba fabric before proceeding to configure VLANs needed to support VMware Cloud Foundation deployment. AFC UI helps avoid command-line interface to perform all network configurations, providing increased visibility and control.

Figure 19 shows both OOBM and data switches onboarded to Aruba Fabric Composer.

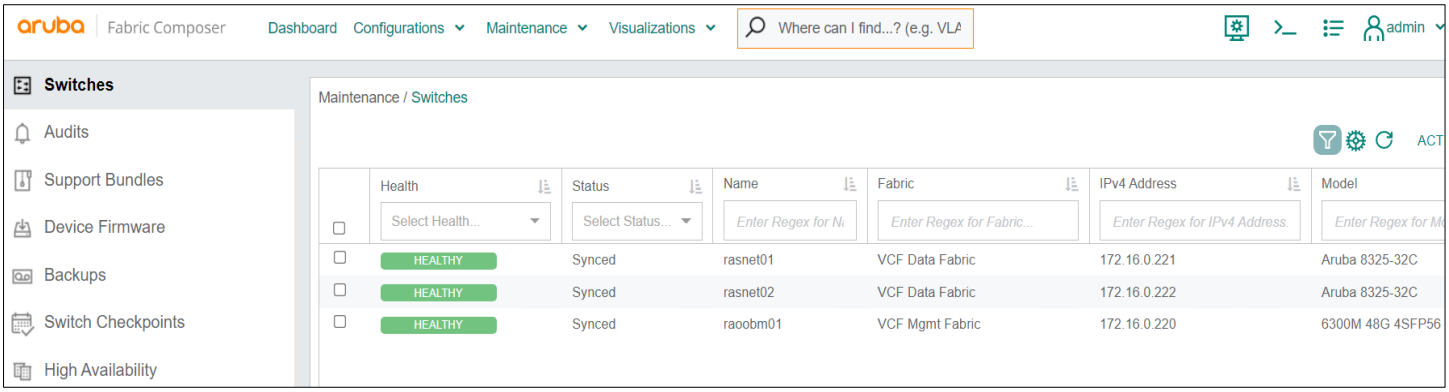

Figure 19. Aruba switches onboard to Aruba Fabric Composer

Aruba VSX, if not already configured, can also be configured from the Aruba Fabric Composer. Multi-Chassis Link Aggregation Group between OOBM and data switches can also be configured through Aruba Fabric Composer.

Figure 20 shows MC-LAG (10) and Aruba 8325 VSX Inter-Switch Link LAG (256) configured through AFC.

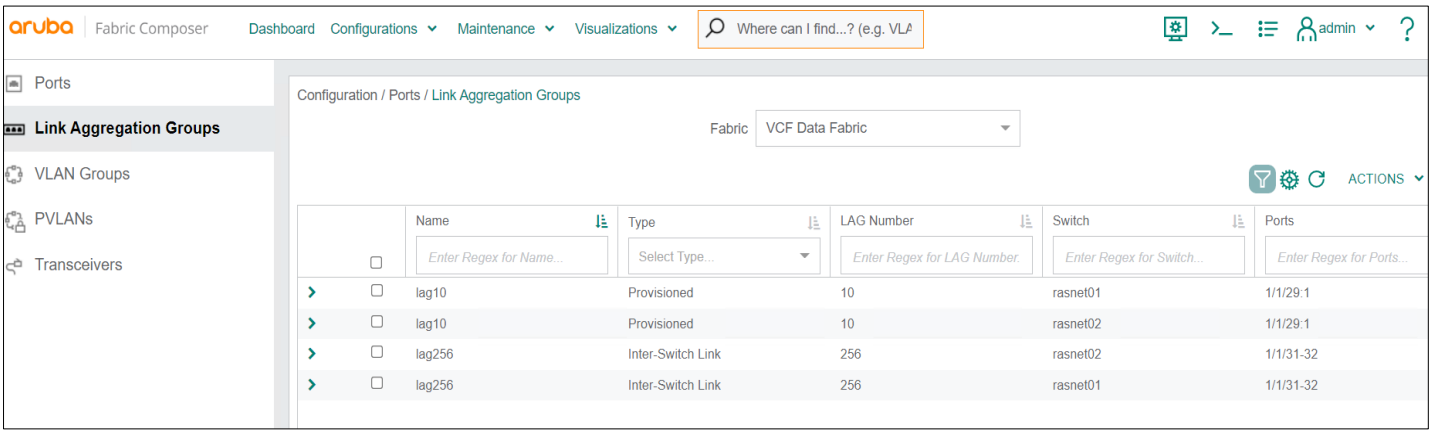

Figure 20. MC-LAG and ISL configured through Aruba Fabric Composer

VLANs required for VMware Cloud Foundation deployment should be configured on both Aruba CX 8325 switches. Since the control plane is separate for paired Aruba CX 8325 switches, each interface VLANs must be created on both switches.

Figures 21 and 22 show one of the switch virtual interfaces created on Aruba CX 8325 switch with an active gateway through the AFC.

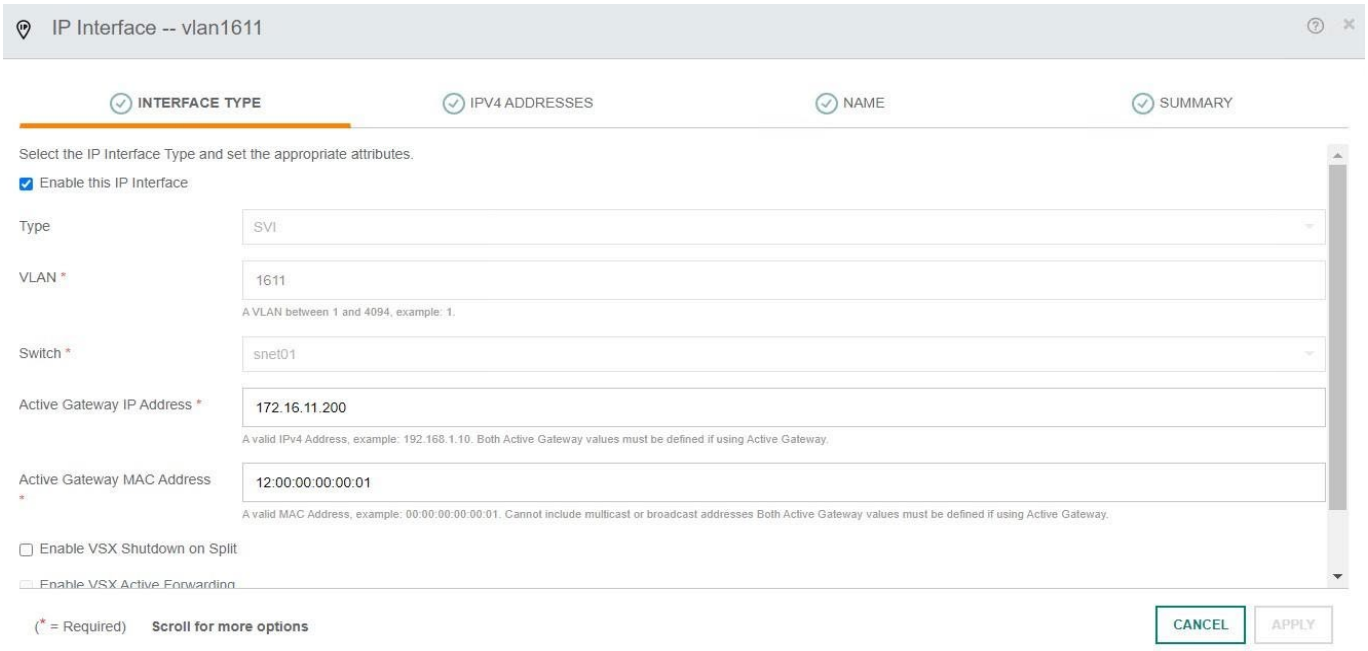

Figure 21. Interface VLAN created through Aruba Fabric Composer

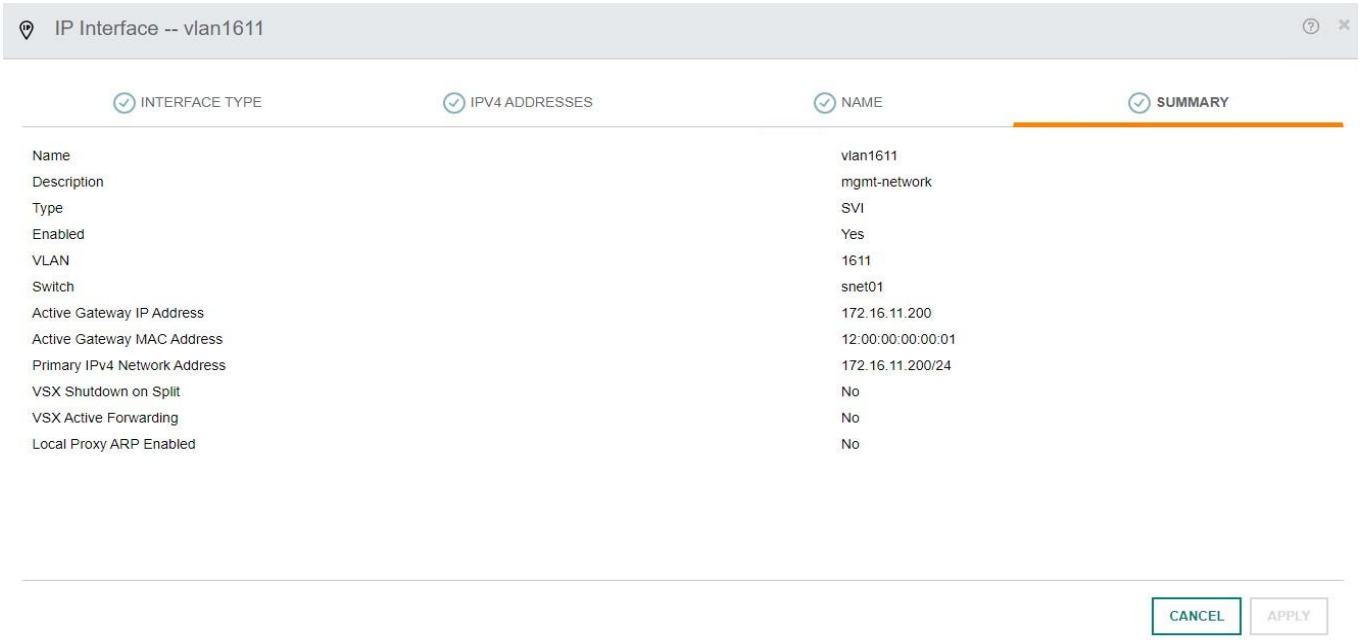

Figure 22. Summary of Interface VLAN created through Aruba Fabric Composer

All the interface VLANs required for VMware Cloud Foundation management domain deployment, workload domain deployment, and edge cluster deployment are configured through Aruba Fabric Composer. Figure 23 shows the solution VLANs configured through the Aruba Fabric Composer.

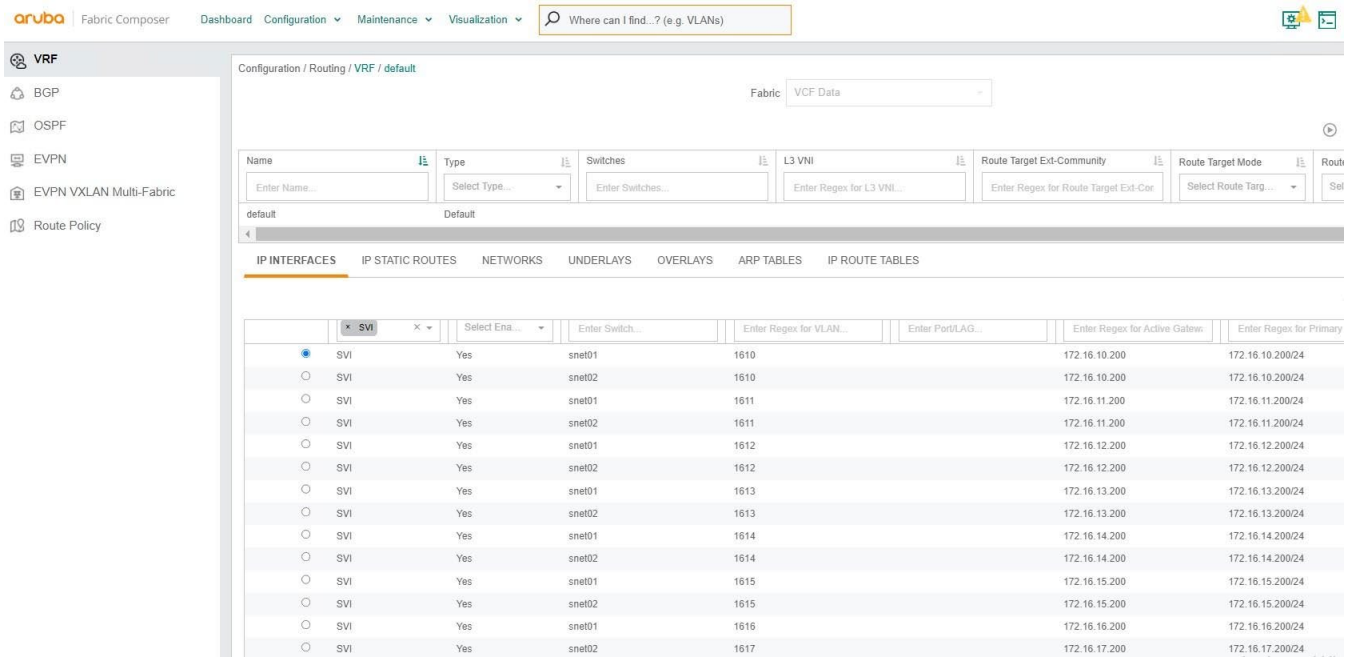

Figure 23. Solution VLANs created through Aruba Fabric Composer

Servers

HPE ProLiant DL Gen12 Server Configuration

Prepare the servers to be utilized in the VCF environment. Each server must have a compatible version of vSphere ESX installed to meet the minimum criteria. For an extensive list of the criteria, refer to the Commission ESX Host documentation.

Configuring a static IP address (iLO 7 Configuration Utility)

Follow the steps to assign a static IP address to the VCF management domain and Workload domain cluster nodes:

1. Restart or power on the server.
2. Press **F9** in the server POST screen.
3. Click **System Configuration**.
4. Click **iLO 7 Configuration Utility**.
5. Click **Network Options**.
6. Select **OFF** in the DHCP Enable menu.
7. Enter values in the IP Address, Subnet Mask, and Gateway IP Address boxes.
8. To save the changes and exit, press **F12**.
9. To save and exit, click **Yes** - Save Changes.
10. Exit the System Utilities and resume the normal boot process, click **Exit** and resume system boot.

Configuring the Virtual NIC feature (iLO 7 Web Interface)

The Virtual NIC feature enables a secure connection to iLO directly from the host operating system. Use this feature directly at the host server or through a Remote Console connection. You can interact with iLO by using the web interface, SSH, or the iLO RESTful API.

The Virtual NIC feature is useful when you want to:

— Access iLO when the network configuration prevents connection through the management network. For example, use a Virtual NIC connection when you have access to the production network but cannot access the iLO dedicated management network.

— Access iLO when there is no NIC cable attached to the host or iLO.

The factory default Virtual NIC setting is enabled for iLO 7. When you reset iLO to the factory default settings, the Virtual NIC setting returns to the default setting for the installed version of iLO. Firmware upgrades or downgrades do not change this setting.

1. Connect to the iLO Web interface by typing https://iLO_IP_Address.
2. Click **iLO Settings** in the left navigation pane and click **Access**.
3. Confirm that Virtual NIC is set to Enabled in the Other Interfaces section.
4. If Virtual NIC is not set to Enabled, enable it.
5. Click icon next to the Other Interfaces. The Other Interfaces window opens.
6. Select the Virtual NIC check box.
7. iLO notifies you that pending changes require a reset to take effect. click **Reset iLO**.
8. iLO prompts you to confirm the request.
9. Click **Yes**, reset iLO.
10. After the reset is complete, the Virtual NIC feature is enabled, and it is detected by the host server OS.

Adding user accounts (iLO 7 Configuration Utility)

Follow the steps to set up iLO accounts on the VCF management domain and workload domain cluster nodes.

1. Restart or power on the server.
2. Press **F9** in the server POST screen.
3. Click **System Configuration**, click **iLO 7** Configuration Utility, click User Management, and then click Add User.
4. Select the privileges for the new user.
5. Enter the username and login name in the New Username and Login Name boxes.
6. Enter the **password**.
7. To close the confirmation dialog box, click OK.
8. Create as many user accounts as needed, and then press **F12** to save the changes and exit the system utilities.
9. When prompted to confirm the changes, click Yes - Save Changes to exit the utility and resume the boot process.

Enable Virtualization Technology on Server

1. From the System Utilities screen, select **System Configuration > BIOS/Platform Configuration (RBSU) > Workload Profile.**
2. Under Workload Profile drop down menu select **Virtualization – Max Performance**.
3. Save and reboot to apply your Workload Profile.

Installing a license key

Follow the steps to install iLO license keys on the VCF management domain and Workload domain cluster nodes:

1. Click **iLO Settings** in the left navigation pane and click Licensing. The Licensing page appears.
2. Click **Install License**. The Install License window appears.
3. Enter a license key in the Activation Key box.
4. Click **Install**.
5. iLO prompts you to confirm that you have read and accept the EULA. Click, **-` I agree**. The license key is now enabled.

Note

For more information about configuring iLO 7 please refer to the HPE iLO 7 User Guide. https://support.hpe.com/hpesc/public/docDisplay?docId=sd00005342en_us&page=index.html.

Installing Service Pack for ProLiant using HPE SUM

HPE Service Pack for ProLiant can be installed using the HPE Smart Update Manager(SUM).

HPE Smart Update Manager application is an innovative tool for updating firmware of HPE ProLiant Servers. It has a browser based GUI as well as a scriptable interface using legacy command line interface and input file mode.

HPE SUM is available within the Service Pack for ProLiant(SPP) Software. HPE SUM can run both on Windows and Linux Platform.

The following procedure describes firmware update procedure on HPE ProLiant DL Gen12 Servers using HPE SUM available in the HPE Service pack for ProLiant software. The following activity can be done using any Laptop with Windows OS installed which is to be used for initial configurations. HPE Service Pack for ProLiant software can downloaded from the https://support.hpe.com/docs/display/public/a00sppdocen_US/spp/#/.

1. HPE Service Pack for ProLiant is available as an ISO file. Right Click the ISO file in the File Explorer and select Mount from the Context menu.
2. After mounted, check the drive letter on which it is mounted.
3. Open command prompt and navigate to the drive on which SPP is mounted.
4. Run the launch_sum.bat utility.

5. The command will open the HPE SUM browser based GUI. In the GUI, Click **Smart Update Manager** menu click **BaseLine Library** and add a baseline and provide the path to Service Pack for ProLiant packages.

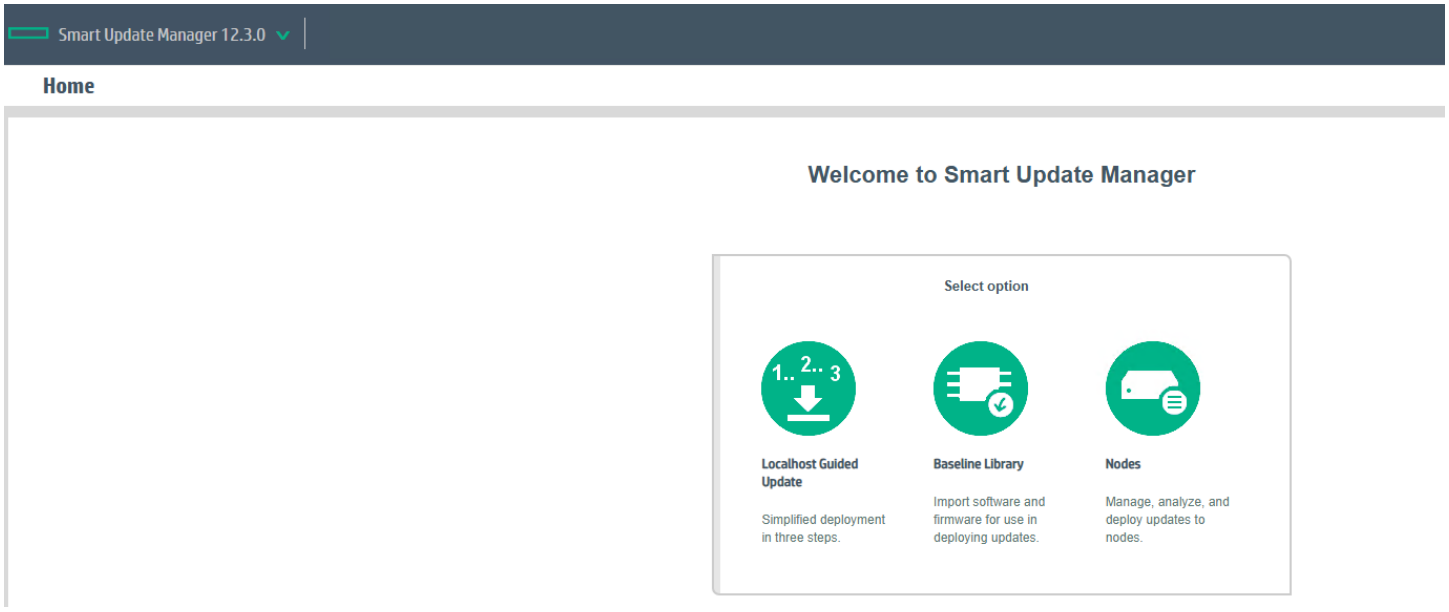

Figure 24. HPE SUM Home interface

6. The HPE SPP software to be installed on the HPE ProLiant DL Servers acts as a baseline and need to be uploaded. Click **Baseline Library** and Click **Add baseline**.

7. In the Add baseline Screen Provide details for location of the package folder present with the HPE SPP software. Select location type as UNC path . Enter the directory path as shown in Figure 25.

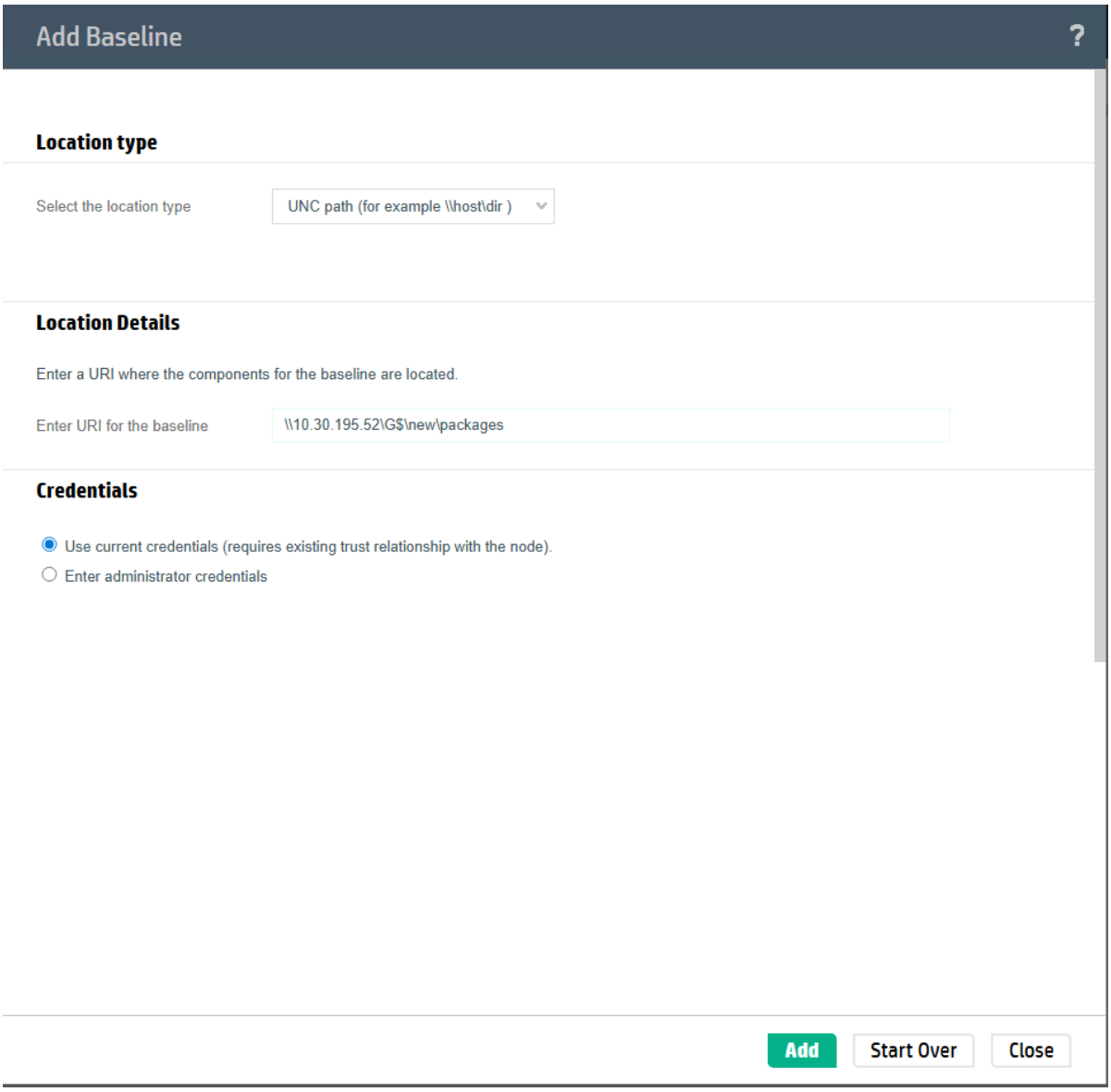

Figure 25. Add Baseline to HP SUM

8. After the baseline is created, add the HPE ProLiant Server node for which Firmware needs to be updated.

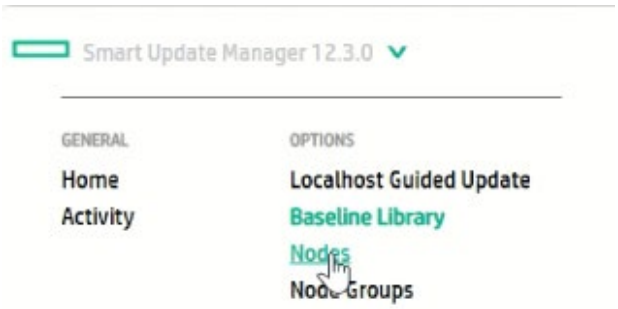

Figure 26. Nodes

9. In the Add Node Screen Provide details ILO IP address of the HPE ProLiant Server Node. Select the Baseline as created in step 5 for the HPE SPP Software.

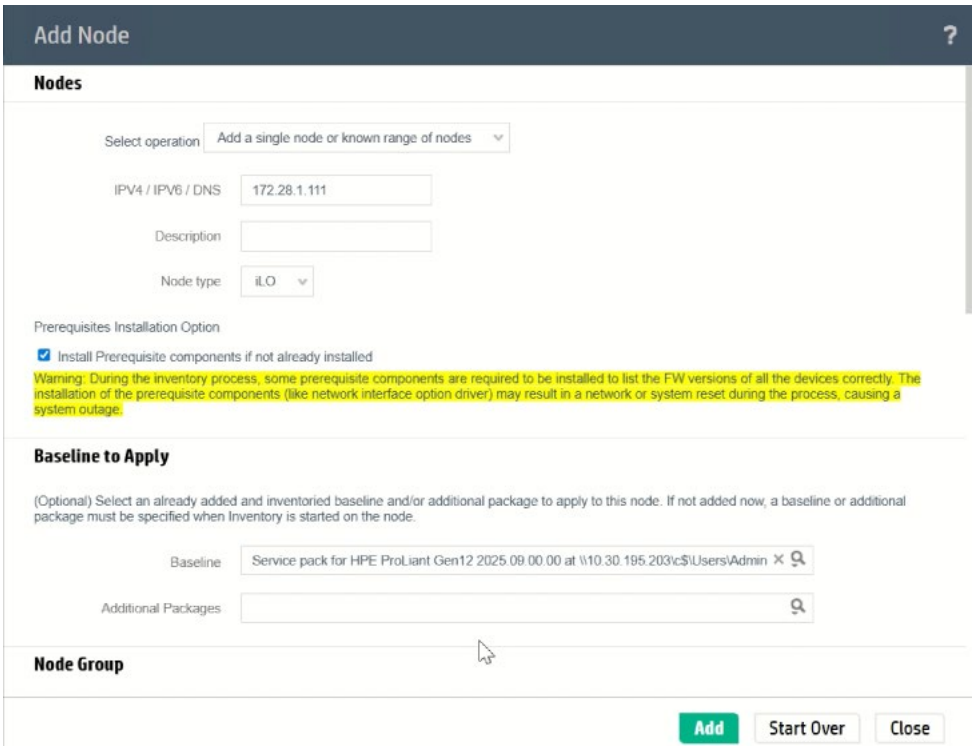

Figure 27. Add Node

10. After the Node is successfully added click **Inventory**.

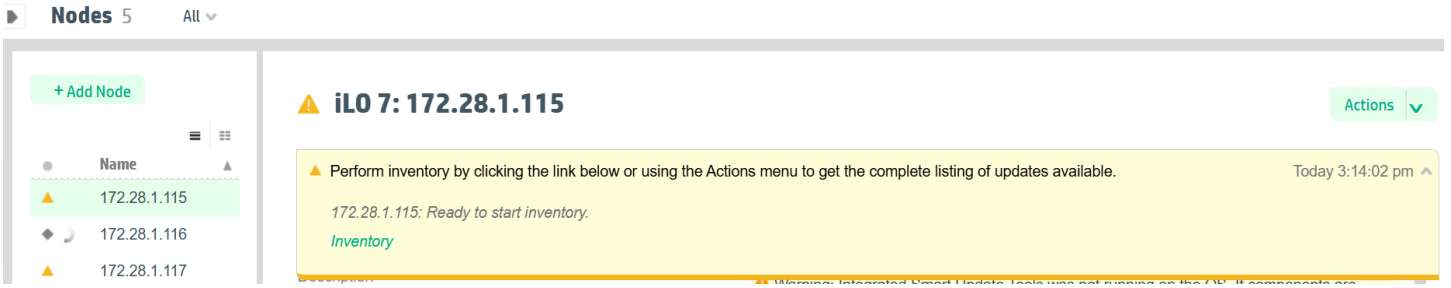

Figure 28. Inventory

11. In the Inventory screen , beside Baselines select the baseline created using the Service Pack for ProLiant(SPP). Click **Inventory** tab to start the process.

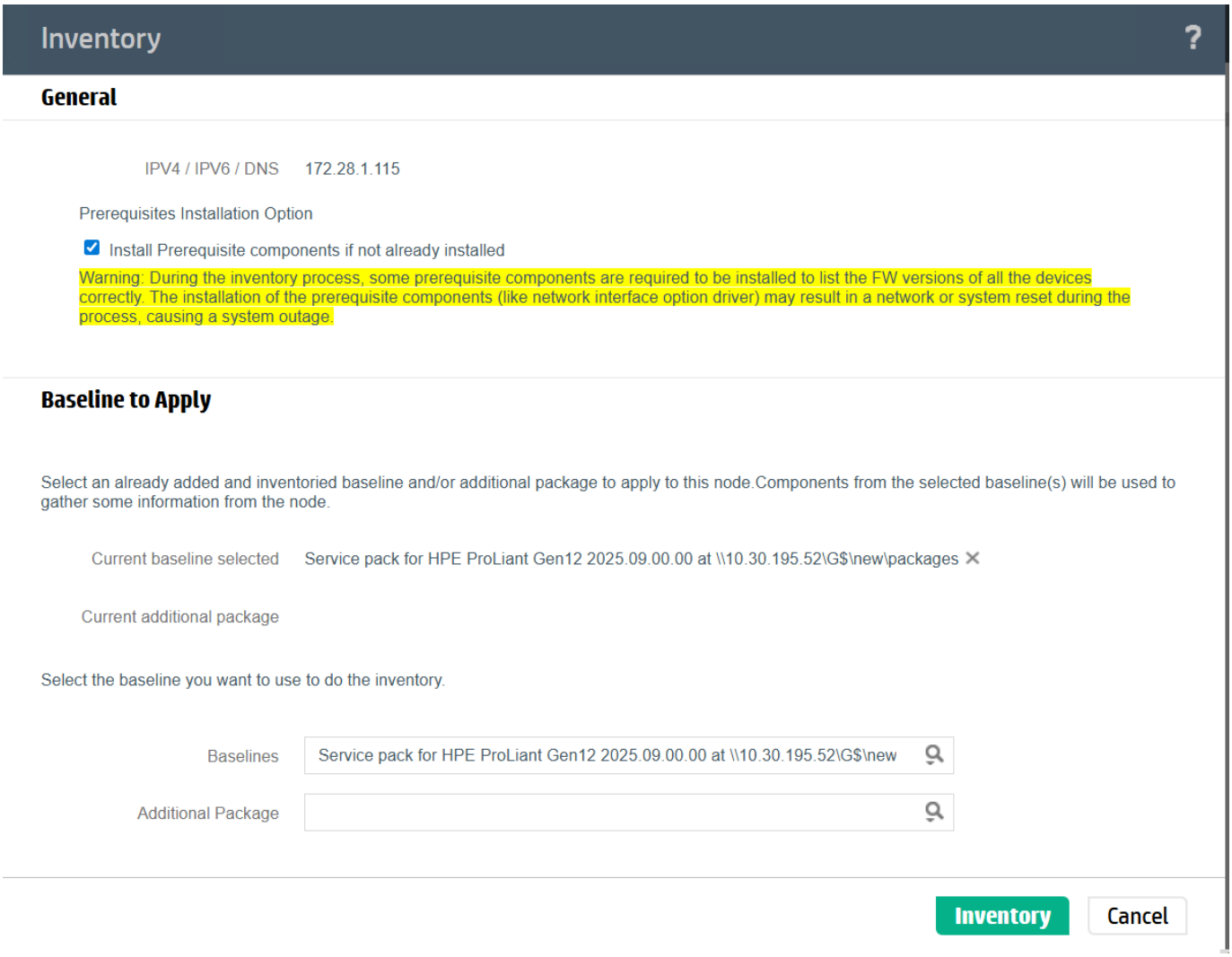

Figure 29. Inventory Configurations

This Inventory create a comparison chart for currently installed Firmware in the HPE ProLiant DL Servers and updated Version of the Firmware present in HPE SPP for the respective components.

12. Click **Review and Deploy** to Install the Firmware updates after completion of Inventory.

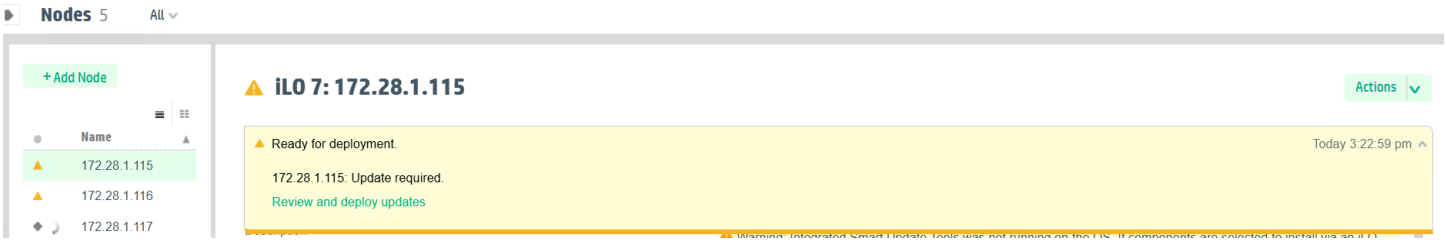

Figure 30. Review and Deploy

13. Open the Deploy wizard showcasing the current version of Firmware installed and updated version of the Firmware available in SPP. Click **Deploy tab** to start the Deployment process to install the updated Firmwares.

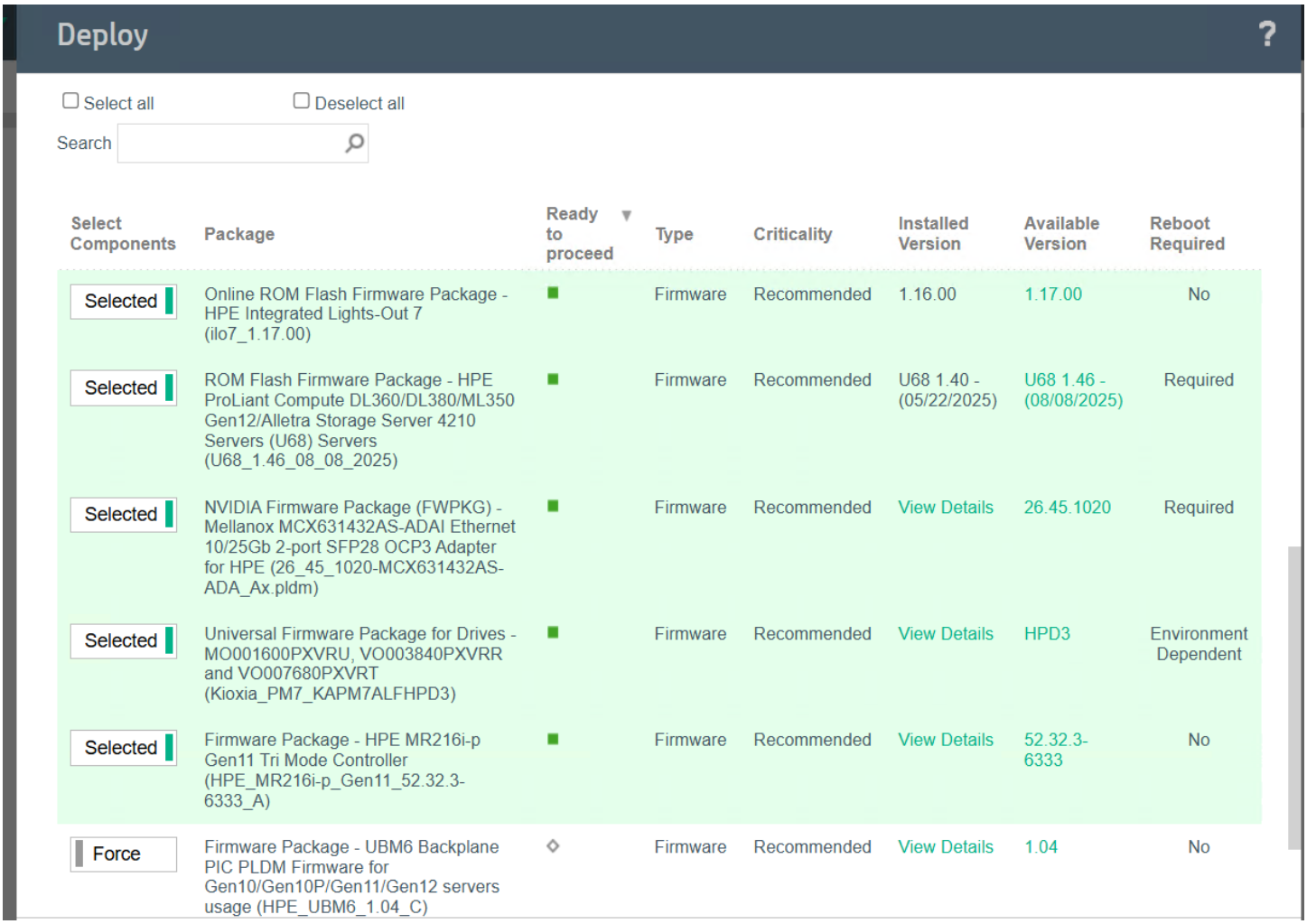

Figure 31. Firmware matrix based on installed version and available version

14. After the Firmware updates is completed for all the nodes, ESXi Host operating systems can be installed on all the nodes.

Create Logical disk for deploying ESX

1. Reboot the Server and press **F9** for boot options.
2. Go to **System Configuration > Select MR controller for boot OS drive > Main Menu > Configuration Management > Create Logical Drive**.
3. Select and click the two Drives for operating system.
4. On the data loss Warning screen, click Confirm, click Yes, this will take you to the Create Logical Drive page.
5. On the Create Logical Drive page, from the Select RAID Level dropdown select RAID1.
6. On the Create Logical Drive page click to **Select Drives**.
7. On the Select Drives page, under **CHOOSE UNCONFIGURED DRIVES**, click **Check All** to select the OS drives and click **Apply Changes**.
8. On the Success page, click **OK**. This will take you back to the Create Logical Drive page.

9. On the Create Logical Drive page, in the Logical Drive Name field, provide a name for the OS drive.
10. Click **Save Configuration**.
11. On the Warning screen click **Confirm** and Yes.
12. On the Success page, click **OK**.
13. Exit.

Deploy ESX and Configure the HPE ProLiant DL Gen12 Server

Deploy ESX on all management and workload domain servers booting from a RAID 1 configuration on the local boot drives.

1. Configure VLAN ID, IP Address, DNS server IP, and FQDN for all the ESX nodes through ESX DCUI.
2. Configure Network Time Protocol (NTP) on an ESX host using the ESX host client.
3. Start SSH and NTP services on an ESX host using the vSphere Client.
4. Update the VLAN ID of the VM Network to 'VM Management VLAN'.
5. Regenerate certificates and restart the services on all ESX hosts to ensure the correct common name is reflected on certificates based on newly added host FQDN.

   ```
   # /sbin/generate-certificates
   ```
6. Reboot the ESX host.

Storage

Validated HPE Alletra Storage MP logical diagram

Figure 32 shows the architecture of storage networking (host to storage connectivity) used in this reference architecture. SAN switches in the solution enables Fibre Channel connectivity between host and storage system. Pair of HPE Storage Fibre Channel Switch B-series SN6700B switches form fabric 1 and fabric 2. Proper zoning is done using a combination of domain/port numbers and WWNs.

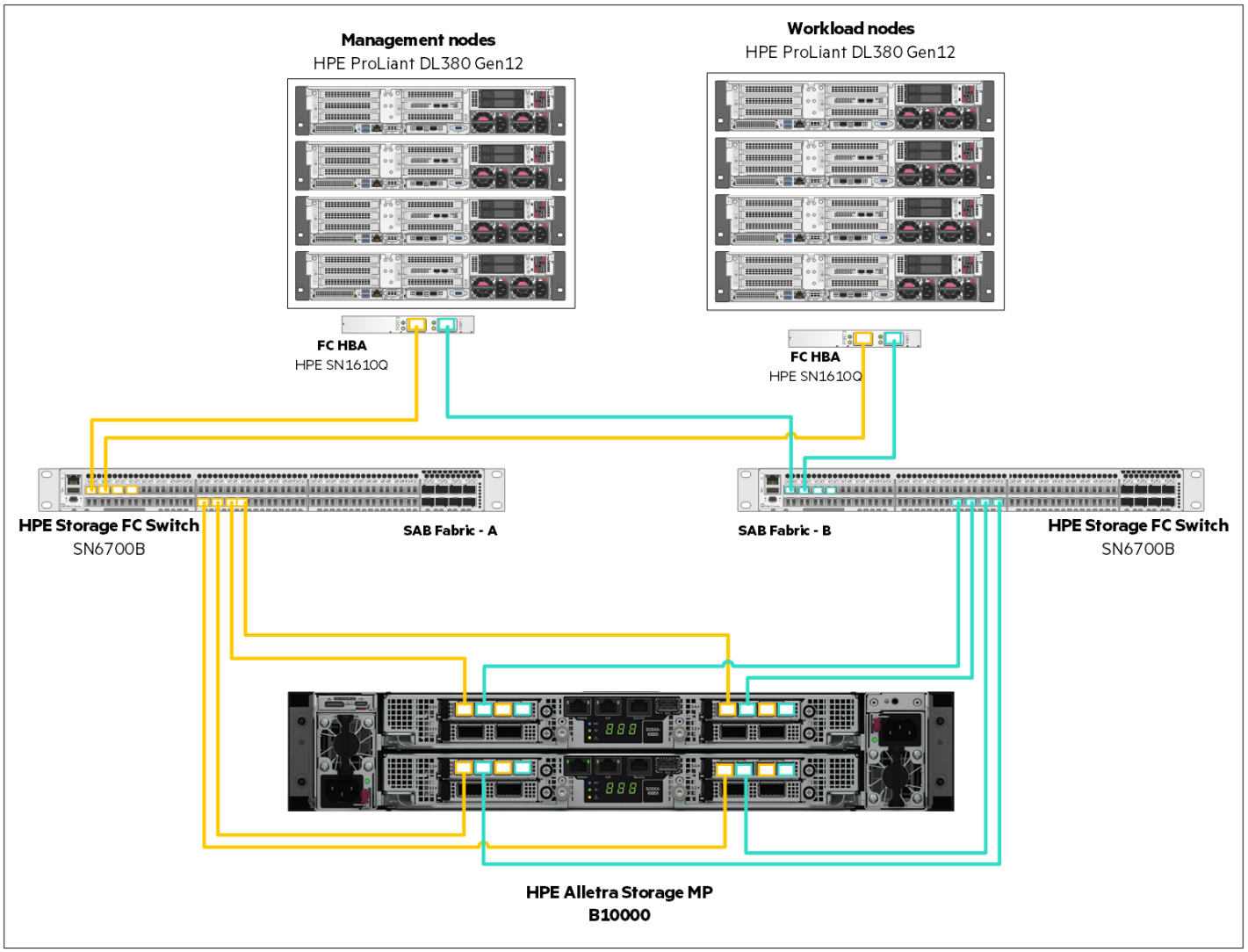

Figure 32. HPE Storage Networking (FC) design

Storage Provisioning

The FC Storage will be provisioned to the management and workload nodes using Virtual Machine File System (VMFS). Version 6 of the Virtual Machine File System is a clustered file system that enables multiple nodes in the cluster to concurrently access a shared datastore. In this setup, storage is provided by the HPE Alletra Storage MP B10000 array and accessed via Fibre Channel for clustered workloads that require shared storage access.

Note

The storage provisioning process requires that physical connectivity is properly established between the HPE management and workload nodes, the HPE Alletra MP B10000 storage array, and the associated HPE network switches. Additionally, the storage array must be initialized and accessible via the HPE Data Services Cloud Console (DSCC) to enable configuration management, monitoring, and lifecycle operations. This reference architecture assumes that these foundational setup steps are complete. Following this, appropriate Fibre Channel zoning must be configured on the switches to establish secure and isolated communication paths between each compute host and the storage array.

SAN Zoning

The following section describes the example zoning guidelines for HPE Fibre Channel switches:

1. Create aliases for HPE Alletra Storage MP host ports:
   a. SSH to the Alletra management IP and capture the port WWNs of controller nodes by executing % showport.
   b. Construct array host port aliases as per standard policy: “SiteNumber+Rack_array-hostname_Node:Slot:Port_SANSwitchPort”.
   c. SSH to the SAN switch using management IP and appropriate login credentials. Configure the aliases using the below CLI syntax and associate the storage host port with the WWPN captured from the array’s showport output:

      ```
      #alicreate “<standard_naming_convention>”, “<WWPN from Alletra host port>>”
      ```

      For example:

      ```
      #alicreate "S1R1_array2_N0S3P1_P10", "20:31:00:02:AC:02:C7:E5"
      ```

      Note

      An alias must be created for every HPE Alletra port that is cabled to SAN switch and is online.

   d. Save the configuration by running `cfgsave` on the SAN switch and verify the aliases created by running `alishow`.
   e. SSH to another SAN switch and repeat steps c and d as applicable.

Table 6. HPE Alletra ports cabled to SAN switch for 2 node and 4 node configurations

Array	MP B10000 Slot 3 ports		MP B10000 Slot 4 ports	
Two-node	0:3:1	1:3:1	0:4:1	1:4:1
	0:3:2	1:3:1	0:4:2	1:4:2
	0:3:3	1:3:3	-	-
	-	-	0:4:4	1:4:4
Four-node	2:3:1	3:3:1	2:4:1	3:4:1
	2:3:2	3:3:2	2:4:2	3:4:2
	2:3:3	3:3:3	-	-
	-	-	2:4:4	3:4:4

2. Create aliases for WWPNs of VCF workload domain hosts.
   a. Login to the iLO IP of each workload host and capture the port WWNs (WWPN) of FC adapters under System Information > Network.
   b. SSH to the SAN switch using management IP and appropriate login credentials. Construct workload host aliases as per data centers standard policy.

   Example: “SiteNumber+Rack_server-serialnumber_Slot:Port_SANSwitchPort”.

c. Configure the aliases using the below CLI syntax and associate the storage host port with the WWPN captured from the array's showport output:

```
#alicreate "<standard_naming_convention>", "<WWPN from HP-VM host port>>"
```

For example:

```
#alicreate "S1R1_3M1D1X110P_S1P1_P0", "51:40:2e:c0:20:3f:69:c4"
```

Note

An alias must be created for every host port that is cabled to SAN switch and is online.

d. Save the configuration by running `cfgsave` on the SAN switch and verify the aliases created by running `alishow`.

e. SSH to another SAN switch and repeat steps c and d as applicable.

3. Create Zones to link workload servers HBA ports to the storage array's host ports, as shown below example mapping table.

Table 7. Mapping of Alletra ports and workload server ports for 2 node and 4 node configurations

Host Grouping	Source Port	Workload servers	HPE Alletra Storage MP B10000 port mapping
1	PCIe HBA prt 1	<1,3,5,7,9,11, 13,15,17 ... fx = last host # in range +2>	N0:S3:P1, N1:S3:P1, N2:S3:P1 & N3:S3:P1
	PCIe HBA prt 2		N0:S3:P2, N1:S3:P2, N2:S3:P2 & N3:S3:P2
2	PCIe HBA prt 1	<2,4,6,8,10,12,14,16,18... fx = last host # in range +2>	N0:S4:P1, N1:S4:P1, N2:S4:P1 & N3:S4:P1
	PCIe HBA prt 2		N0:S4:P2, N1:S4:P2, N2:S4:P2 & N3:S4:P2

4. SSH to the SAN switch using management IP and appropriate login credentials.

5. Configure the zone using the following CLI syntax:

```
#Zonecreate "SiteNumber+Rack_server-serialnumber_array-hostname_SlotPorts",
"<server_alias>; <HPE Alletra MP Node#_port_alias>; <HPE Alletra MP Node#_port_alias>; <HPE
Alletra MP Node#_port_alias>;<HPE Alletra MP Node#_port_alias>"
```

For example:

```
#zonecreate  "S1R1_3M1D1X110P_array2_S3P2",
"S1R1_3M1D1X110P_S1P2_P0;S1R1_array2_N0S3P2_P10;S1R1_array2_N1S3P2_P14"
```

Note

Zone creation must be done for all the VCF management domain and workload domain hosts.

6. Save the configuration by executing `cfgsave` on the SAN switch.

7. Create and activate the configuration by running following commands on SAN switch:

```
# cfgcreate  "VCF-SAN-A", "zones"
```

For example:

```
cfgcreate "VCF-SAN-A",
"S1R1_3M1D1X110P_array2_S3P1;S1R1_3M1D1X110M_array2_S4P1;S1R1_3M1D1X110N_array2_S3P1;S1R1_3
M1D1X110L_array2_S4P1"

# cfgenable VCF-SAN-A
```

8. Verify the effective configuration on the SAN switch by executing `cfgactvshow`.
9. SSH to another SAN switch and repeat steps b to e as applicable.

Provisioning a Fibre Channel (FC) storage LUN and creating VMFS datastore

Create a Host Group using Data Services Cloud Console

1. In Data Services Cloud Console, launch Data Ops Manager.
2. Under Menu, select Data Access and click + under Host Groups.
3. In the Create Host Group section, add a host to the host group by clicking + Create.
4. In the Create Host dialog, provide a host name, select FC as the protocol, choose VMware (ESX) as the operating system, and then click **Next**.
5. In the Initiators section, click + Create. In the Add FC Initiator provide the FC Qualified Name (WWNs) of the host, click Add then click **Done**.
6. Click **Next**, then click Create to complete the host creation process.
7. Repeat steps 3-5 to add all the Management domain hosts to the host group.
8. Click **Next** on the Create Host Group dialog to verify the Management domain hosts details, then click **Create**.

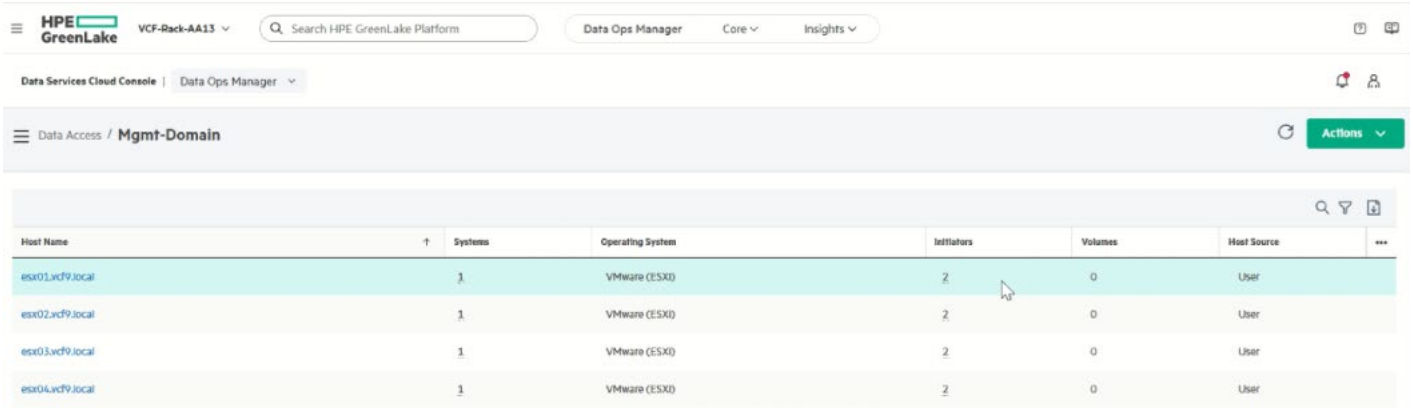

Figure 33. Host set created on DSCC Data Ops Manager

Create a Volume Set and Export Volume to Host Group on Data Services Cloud Console

1. To create and export a volume to host group, launch Block Storage in Data Services Cloud Console.
2. Under Menu, select Storage and click + and select the right storage tier and the workload type.
3. Enter the name for the volume, number of volumes and their respective size.
4. Select the already created host group under which group of hosts need access to this storage?
5. Under protection policy, select No Protection and click **Continue**.
6. Leave the rest of the options to default and in the Review screen, click **Submit**.

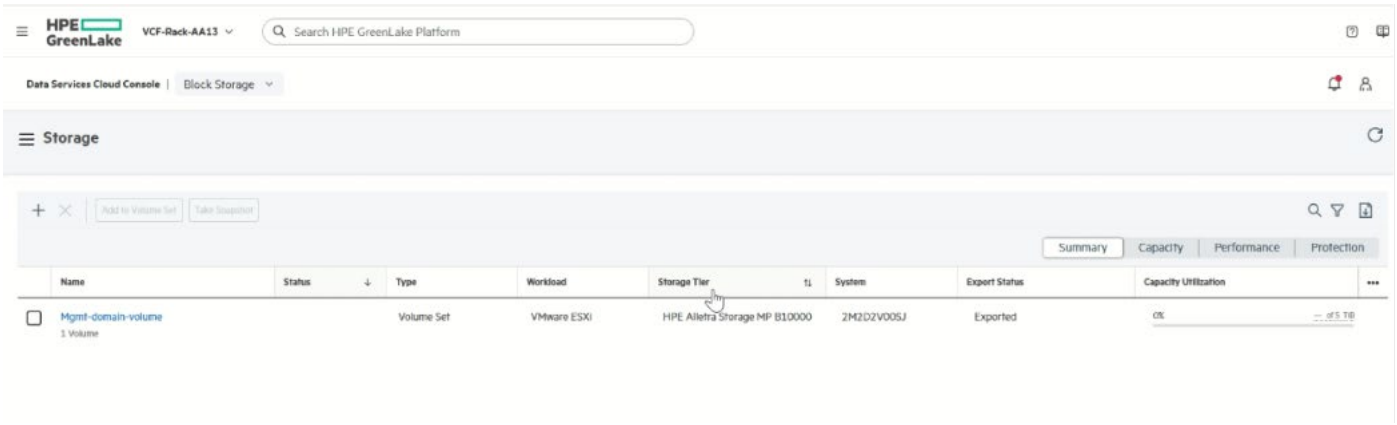

Figure 34. Volume and volume set created on DSCC Block Storage

Verify Provisioned Volumes (LUNs) on VCF management hosts

Scan the FC host bus adapters on each host of the VCF management hosts using the following commands:

```
# esxcli storage core adapter rescan --all
This command forces the host to rediscover all physical paths to storage devices
# esxcli storage nmp device list
lists all the Fibre Channel LUNs and multipathing information
```

```
[root@vcf-m01esx01:~] esxcli storage nmp device list
naa.60002ac0000000000000790002c89c
   Device Display Name: 3PARdata Fibre Channel Disk (naa.60002ac0000000000000790002c89c)
   Storage Array Type: VMW_SATP_ALUA
   Storage Array Type Device Config: {implicit_support=on; explicit_support=off; explicit_all
ow=on; alua_followover=on; action_OnRetryErrors=off; {TPG_id=10,TPG_state=AO}{TPG_id=11,TPG_s
tate=ANO}}
   Path Selection Policy: VMW_PSP_RR
   Path Selection Policy Device Config: {policy=latency,latencyEvalTime=180000,samplingCycles
=16,curSamplingCycle=16,latencyDeviation=10,useANO=0; CurrentPath=vmhba4:C0:T1:L0: NumIOsPend
ing=0,latency=153}
   Path Selection Policy Device Custom Config:
   Working Paths: vmhba4:C0:T1:L0, vmhba5:C0:T0:L0
   Is USB: false
```

Figure 35. Storage LUN

Create VMFS Datastore on Management domain hosts

VMware vSphere® VMFS is a high-performance cluster file system (CFS) that enables virtualization to scale beyond the boundaries of a single system.

1. Launch VMware Host Client for any one host using IP Address or FQDN.
2. Click **Storage** in the VMware Host Client inventory and click **Datastores**.
3. Click **New datastore**, The New datastore wizard opens.
4. On the Select creation type page, select Create new VMFS datastore and click **Next**.
5. On the Select device page, select where to create the new VMFS partition.
6. Enter a Name for the new datastore.
7. Select a device (Example: 3PARdata Fibre Channel Disk).
8. Click **Next**.

9. On the Select partitioning options page, select use full disk to partition the device and click **Next**.
10. On the Ready to complete page, review the configuration details and click **Finish**.
11. Connect to each host using ESX Host Client. Verify the newly created datastore is visible. If not, Rescan the Adapter or Device.

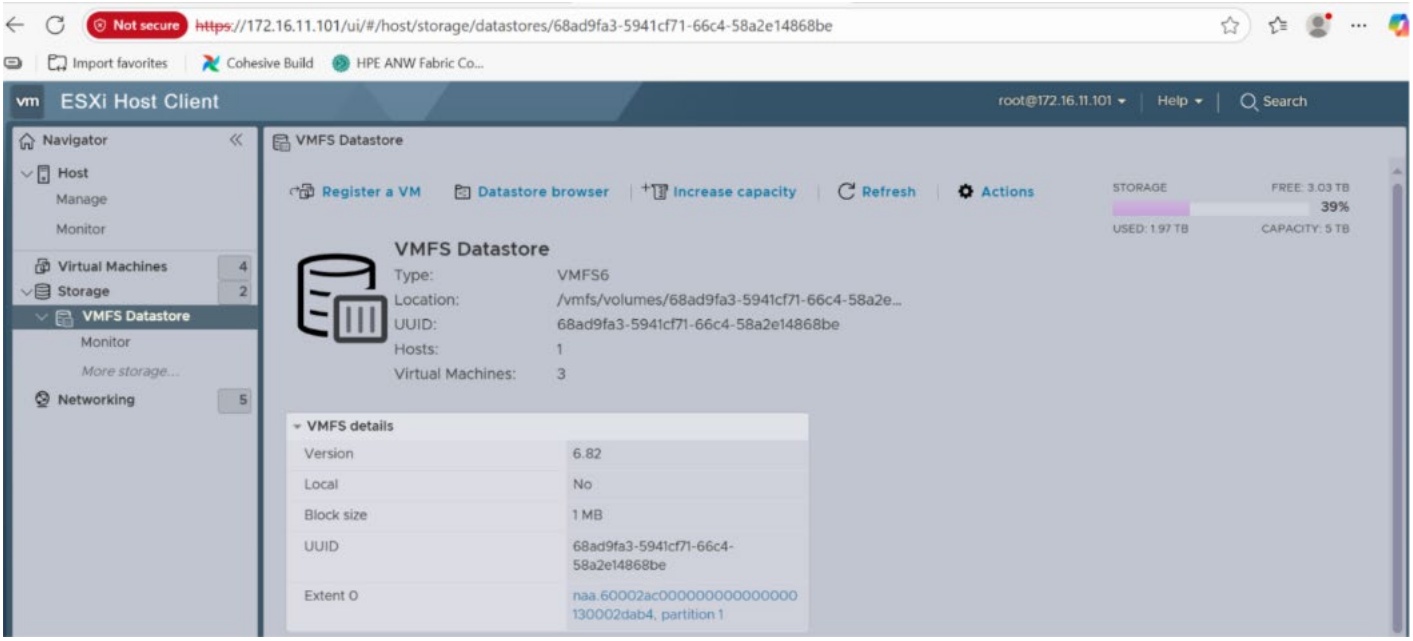

Figure 36. Verify Datastore on each Management host

Storage Deployment – vSAN ESA vs FC

Table 8. Storage Deployment – vSAN ESA vs FC

Deployment Step	vSAN ESA based deployment	Fibre Channel–based Deployment
Datastore Provisioning	vSAN datastore from NVMe disks on hosts	VMFS datastore from external Fibre Channel (FC) LUNs
Network Configuration	Dedicated vSAN network for mgmt and workload	No vSAN network required
Network Pools	Includes both vMotion and vSAN traffic	Includes only vMotion traffic
Management Domain Storage Type	vSAN ESA	VMFS on Fibre Channel (FC)
Workload Host Commissioning	Storage option selected: vSAN	Storage option selected: VMFS on FC
Workload Domain Storage Type	vSAN	VMFS on FC

VCF Management domain bringup

This section outlines the deployment process for the VCF Management Domain using the VCF Installer, which is the standard deployment tool for VMware Cloud Foundation 9.0. Unlike earlier versions such as VCF 5.x that supported parameter sheet–based deployment, VCF 9.0 introduces a more streamlined approach by supporting deployment either through a graphical user interface (UI) or a JSON configuration file via the VCF Installer. Resource requirements for the VCF installer can be reviewed in the Deploy the VMware Cloud Foundation Installer appliance documentation.

VCF 9.0 supports multiple storage options for the management domain, including vSAN, VMFS on Fibre Channel (FC), and NFS.

Note

The steps described are for the storage option VMFS on Fibre Channel (FC). For customers opting to use vSAN as a storage option, guidelines are provided in this document wherever needed.

Deploy VCF Installer

1. Download the VCF Installer appliance OVA file.
2. Deploy VCF Installer on the first HPE ProLiant DL server chosen for the management domain.
3. Log in to vSphere Host Client of the first management domain host and go to Virtual Machines and click Create / Register VM and select Deploy a virtual machine from an OVF template or OVA file to start the deployment wizard for deploying the appliance.

   Note

   VCF Installer can either be deployed on any ESX host that will be used for management domain, or it can be deployed on an existing infrastructure host with management network connectivity to all the management domain hosts.

Table 9 shows the details of each screen and performs the required action.

Table 9. Deployment wizard actions for each screen

Installation	Action Needed
Select OVF and VMDK files	Enter a name for the virtual machine Click to select files “VCF-SDDC-Manager-Appliance-9.0.0.0.24703748.ova”
Select storage	Local datastore of the ESX host
License agreements	Click “I Agree” button
Deployment options	Select the network for Network1 VM Network
Additional settings	Enter Passwords Host Name <FQDN> NTP Servers Network details DNS Domain Name

Installation	Action Needed
	Domain Name Servers
Ready to complete	Review and click “FINISH” button

Download the VCF 9.0 binaries

1. VCF binaries are downloaded and staged on to VCF Installer. The binaries can be downloaded by setting up either online or offline depot.
2. Refer the Broadcom page on Downloading Binaries to VCF Installer for downloading VCF binaries.

Figure 37 shows the VCF 9.0 binaries are downloaded and made available to the VCF installer.

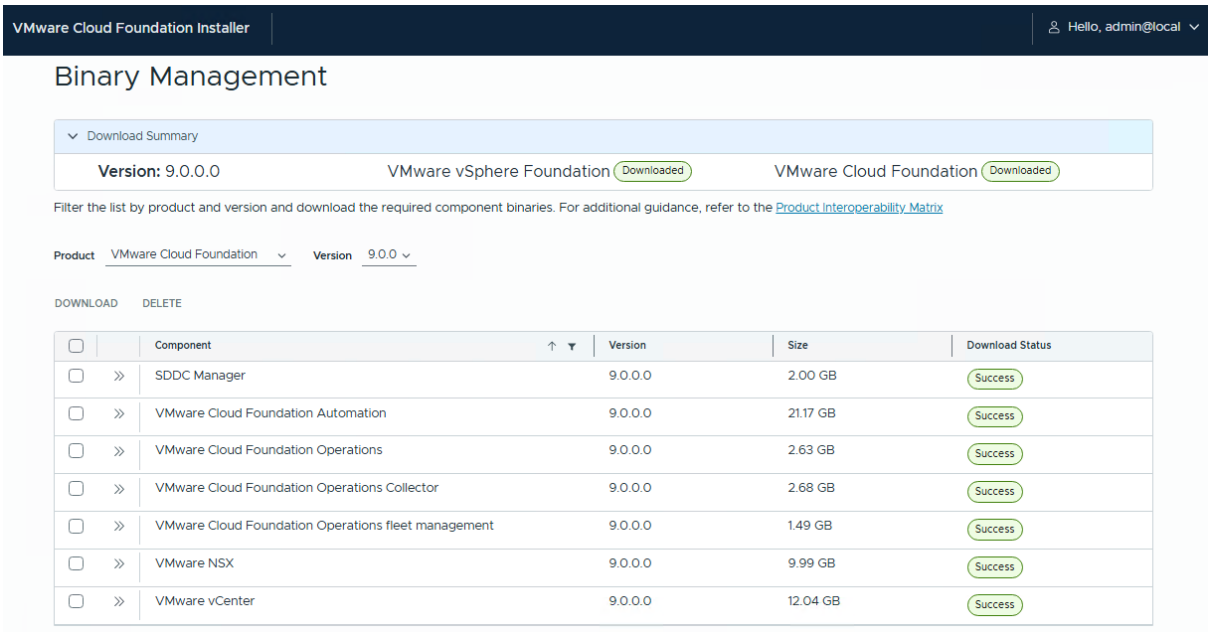

Figure 37. VCF 9.0 Binaries staged onto VCF Installer

Deploy VCF Management Domain

Prerequisites

To complete the VCF Deployment, the following requirements are to be met:

— FDQNs used for different components – vCenter, NSX (Managers and VIP), VCF Operations (Primary, Data, Replica, Fleet Management and Operations Collector nodes), VCF Automation and SDDC Manager must be resolvable by the Domain Name System.

— Network subnet, mask, and gateway details for Management, VM Management, vMotion, vSAN and Host Overlay network.

Note

To deploy using a JSON file, use the JSON spec file and edit the values with appropriate details for the environment used. On VCF Installer, select Deploy with JSON Specification, upload the JSON file, validate and deploy.

The following procedure describes how to deploy using the deployment wizard:

In a web browser, log in to the VMware Cloud Foundation Installer appliance administration interface: https://installer_appliance_FQDN.

1. Click **Deployment Wizard >> VMware Cloud Foundation**.
2. Select Deploy a new VCF fleet and click **Continue**.
3. Click **Next** at Existing Components page.

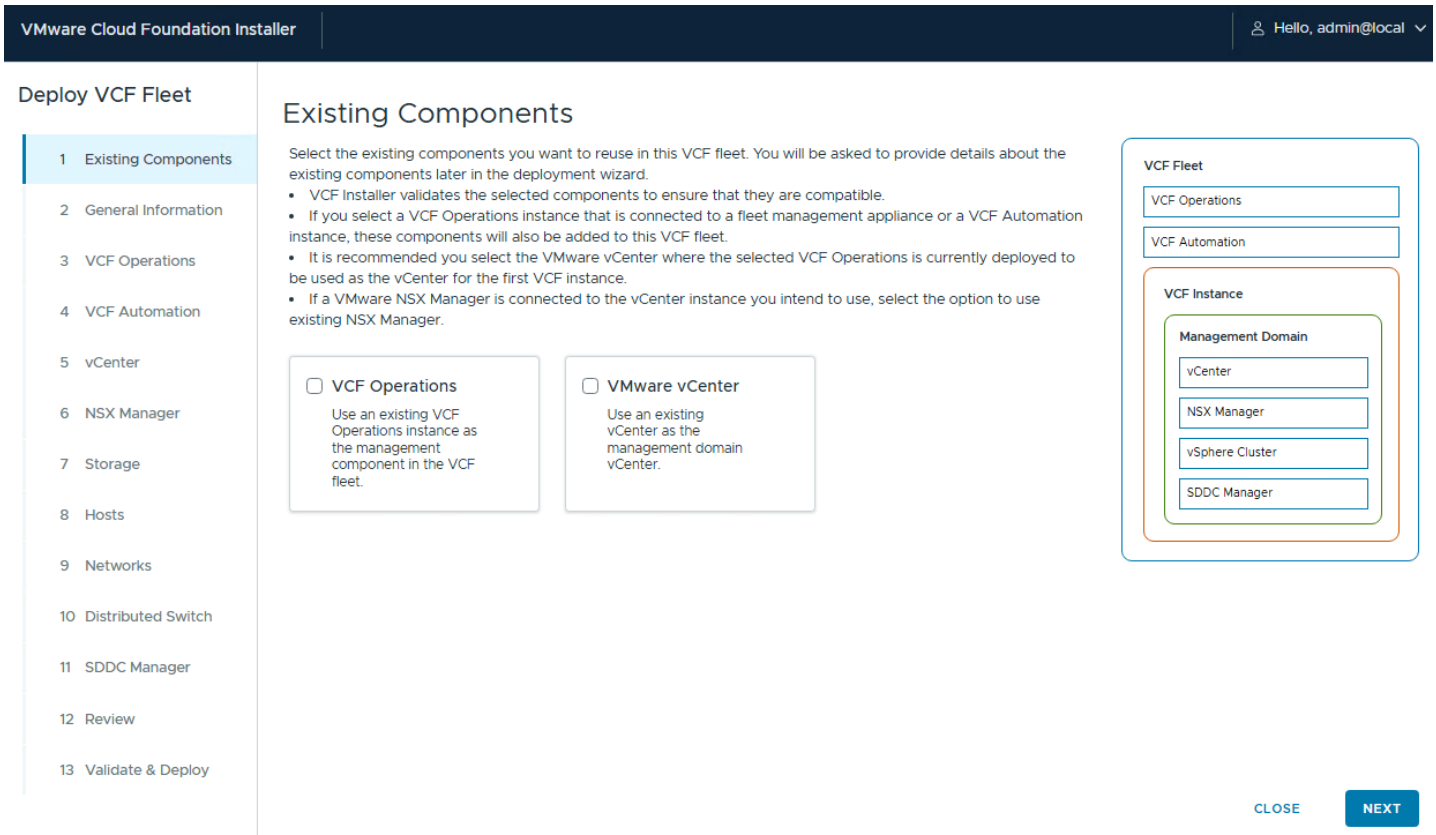

Figure 38. VCF Fleet

4. Provide the general information details for your deployment.

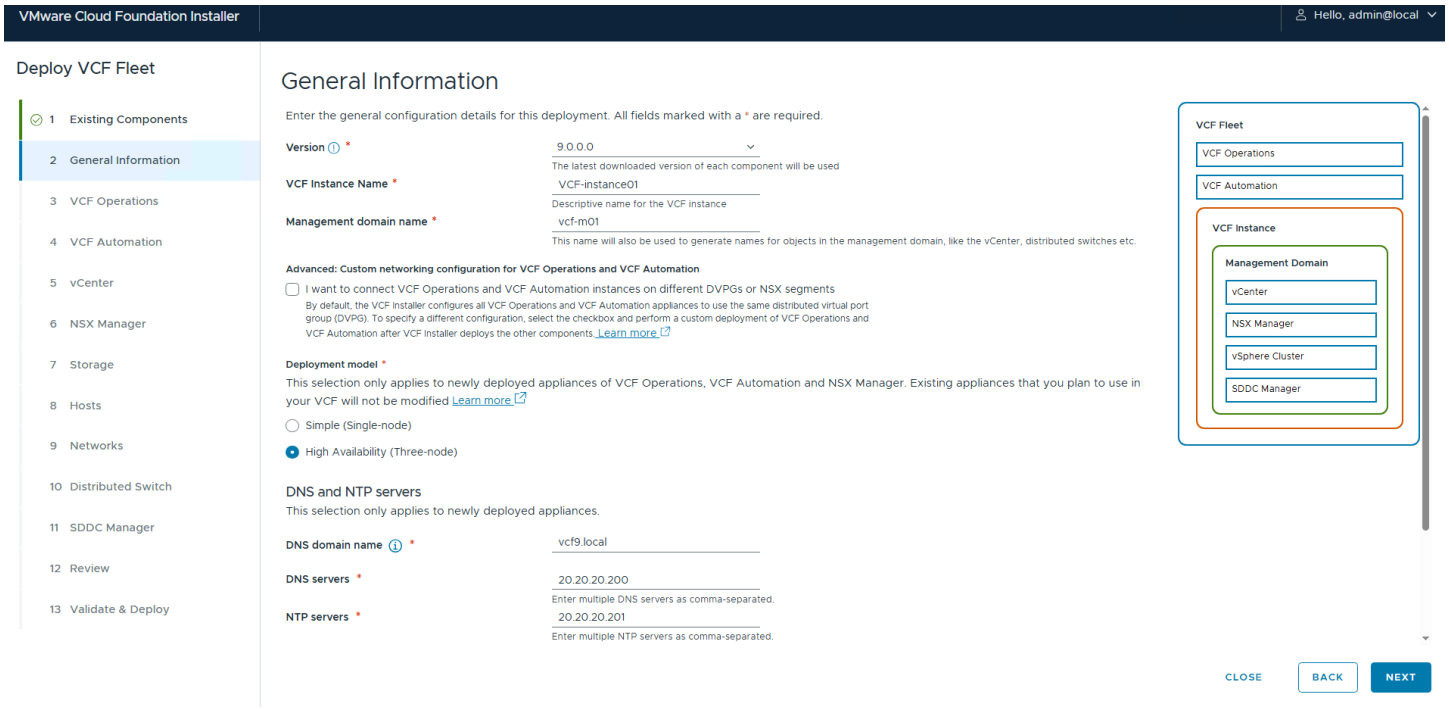

Figure 39. General information

5. Enter the VCF Operations details.

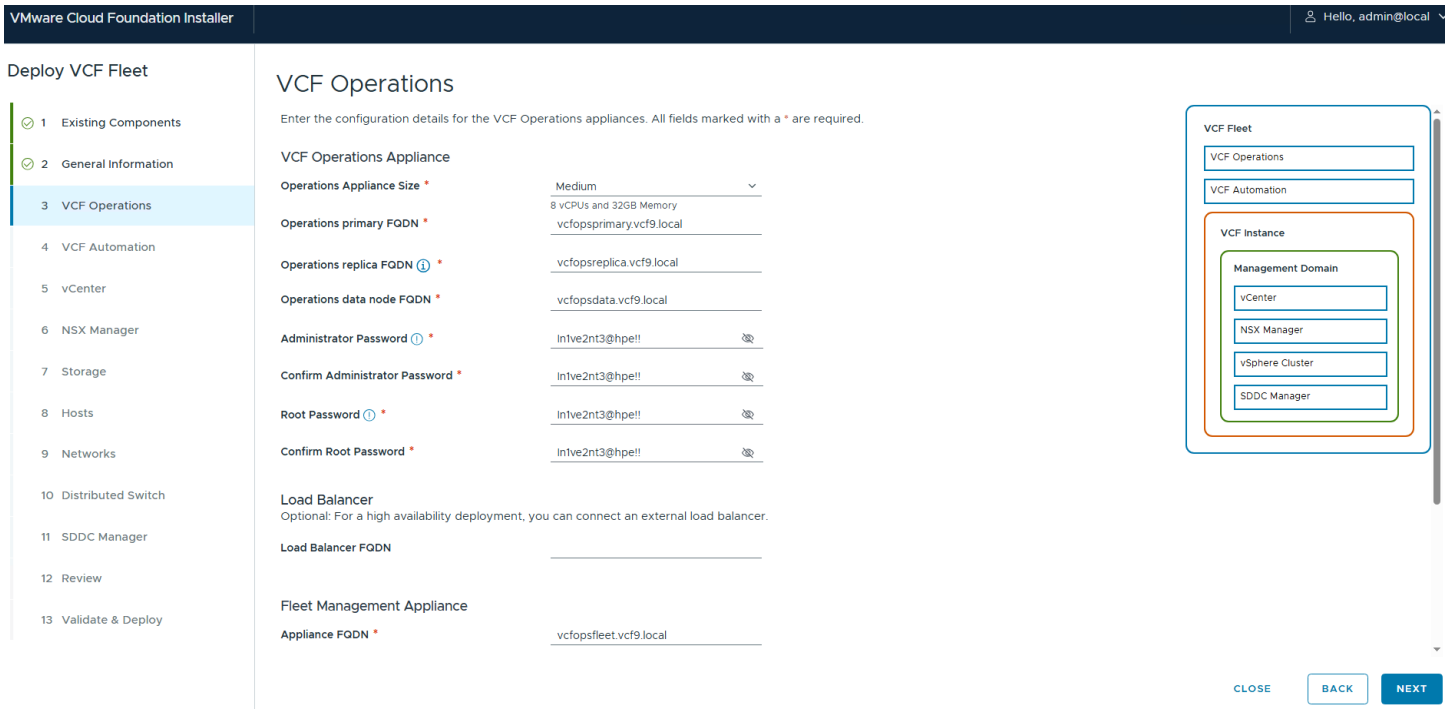

Figure 40. VCF Operations

6. Enter the VCF Automation details.

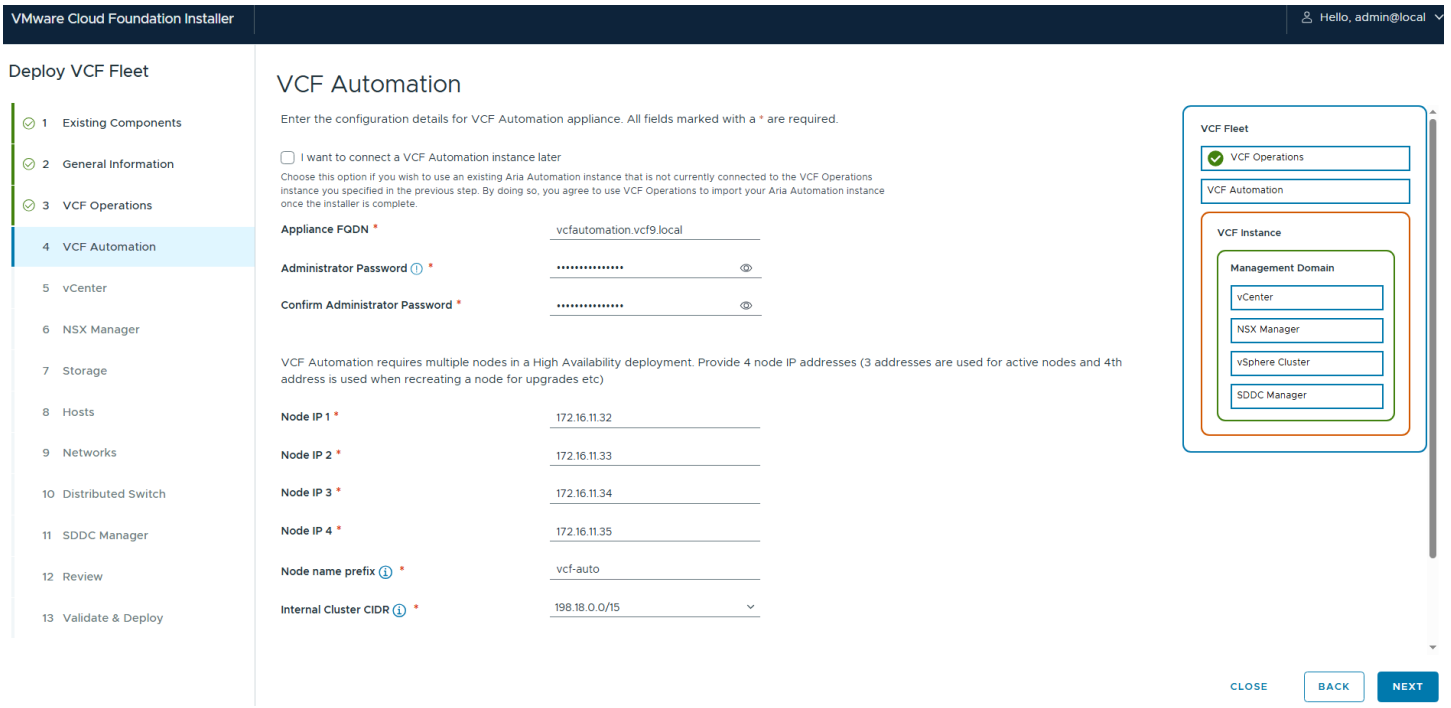

Figure 41. VCF Automation

7. Enter the vCenter details.

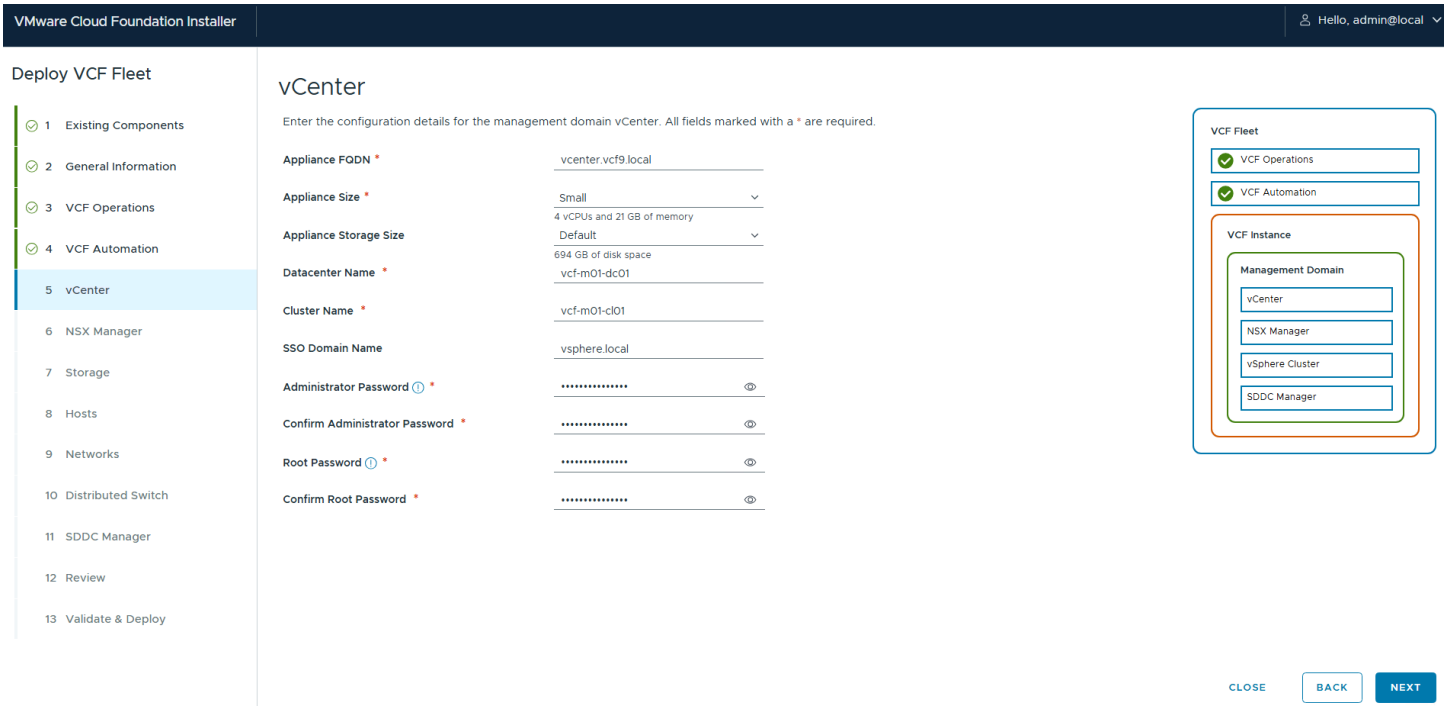

Figure 42. vCenter

8. Enter the NSX Manager details.

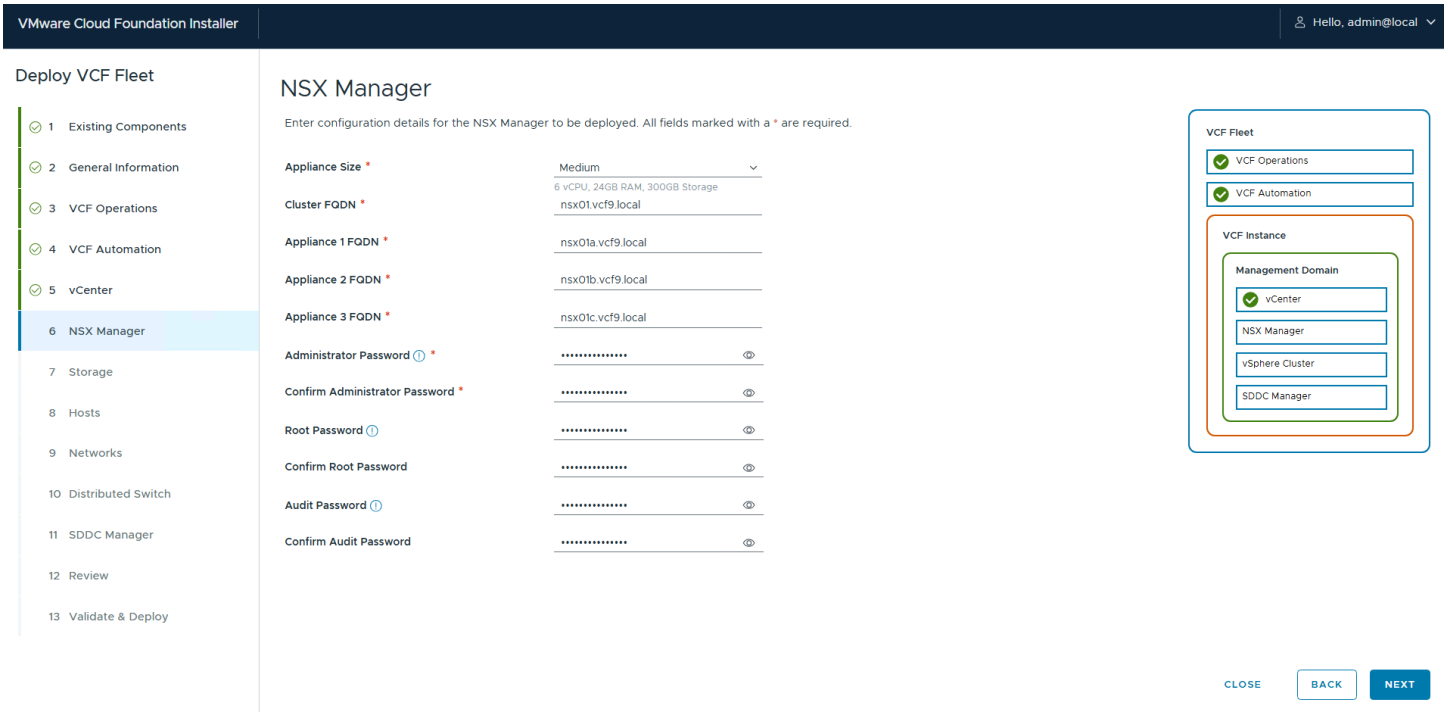

Figure 43. NSX Manager

9. Choose a storage option and enter the storage details.

   In this example storage option is VMFS on Fibre Channel (FC), enter the datastore name.

Note

If you are deploying vSAN Based management domain, choose the storage option as vSAN and provide the name of the vSAN datastore.

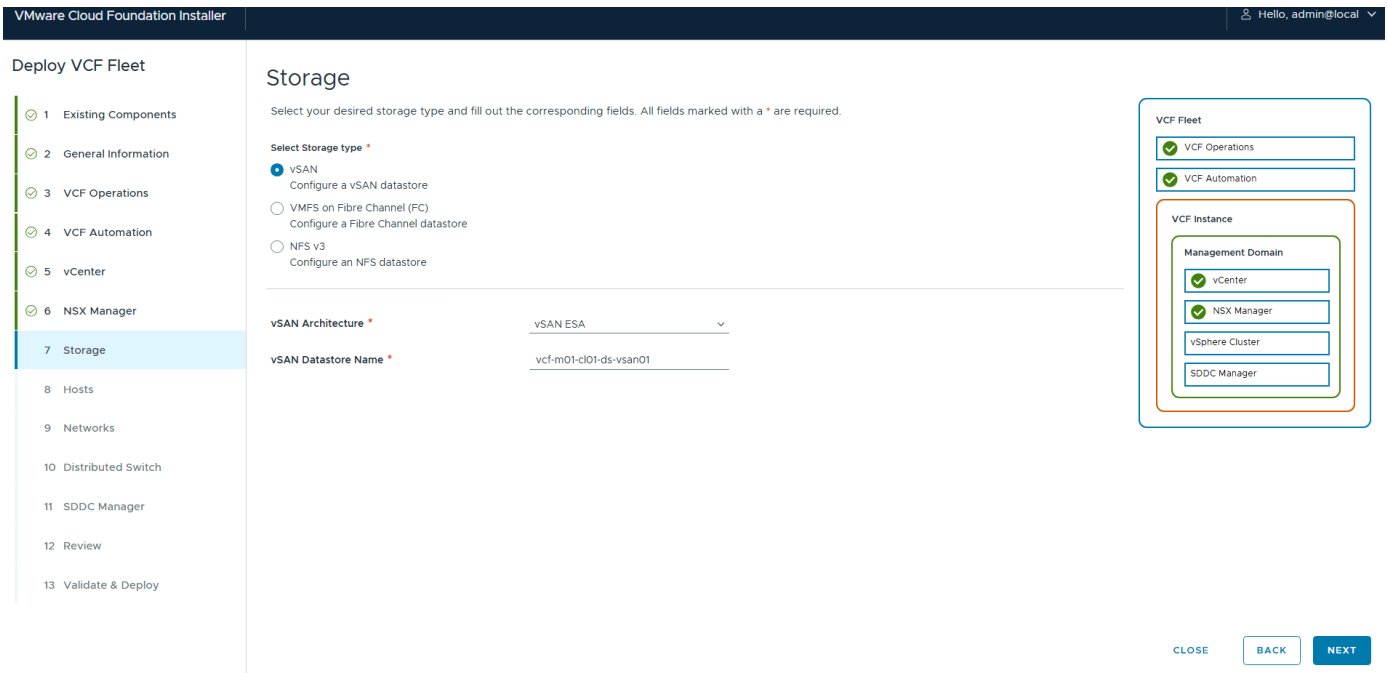

Figure 44. vSAN as Storage option for vSAN based management domain

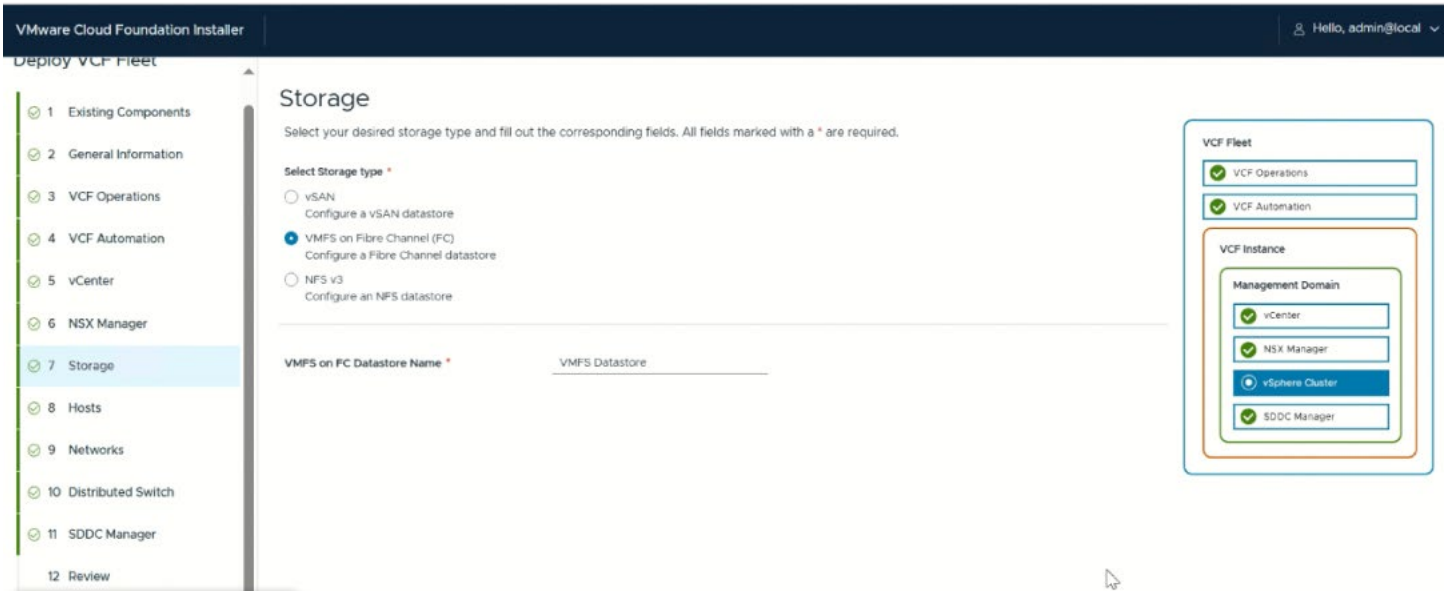

Figure 45. VMFS on FC datastore

10. Enter the ESX host details.

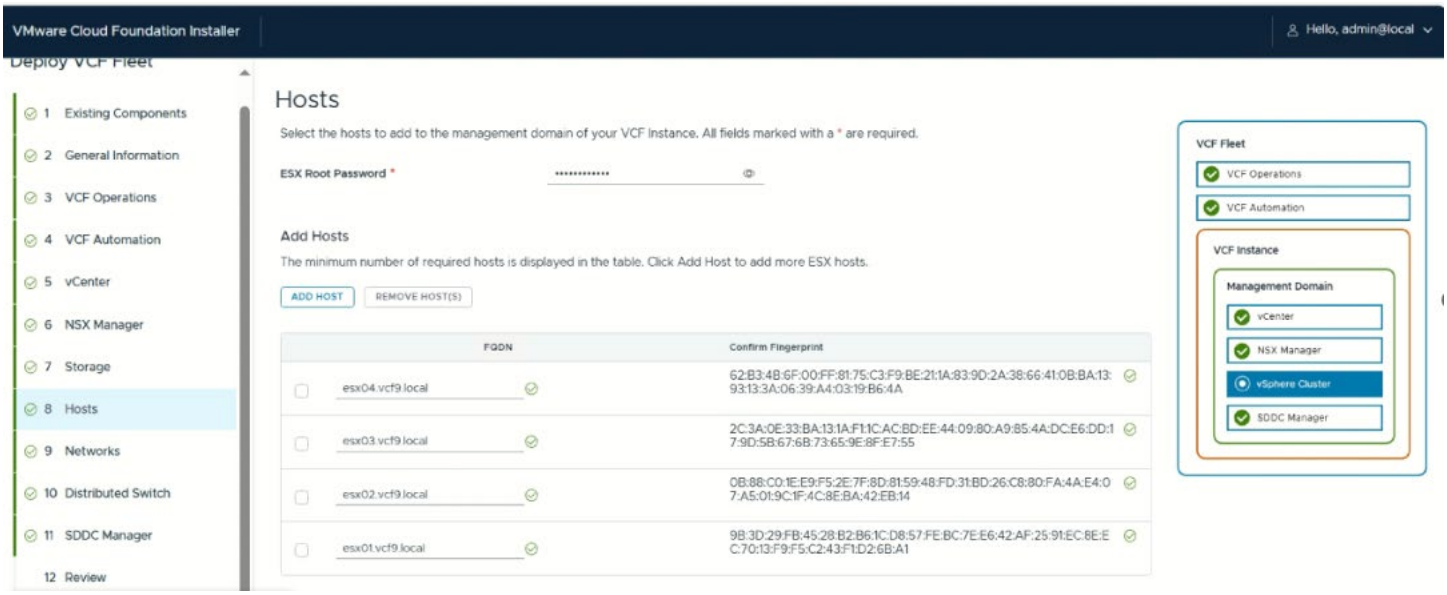

Figure 46. Add ESX Hosts

11. Enter details about the networks.

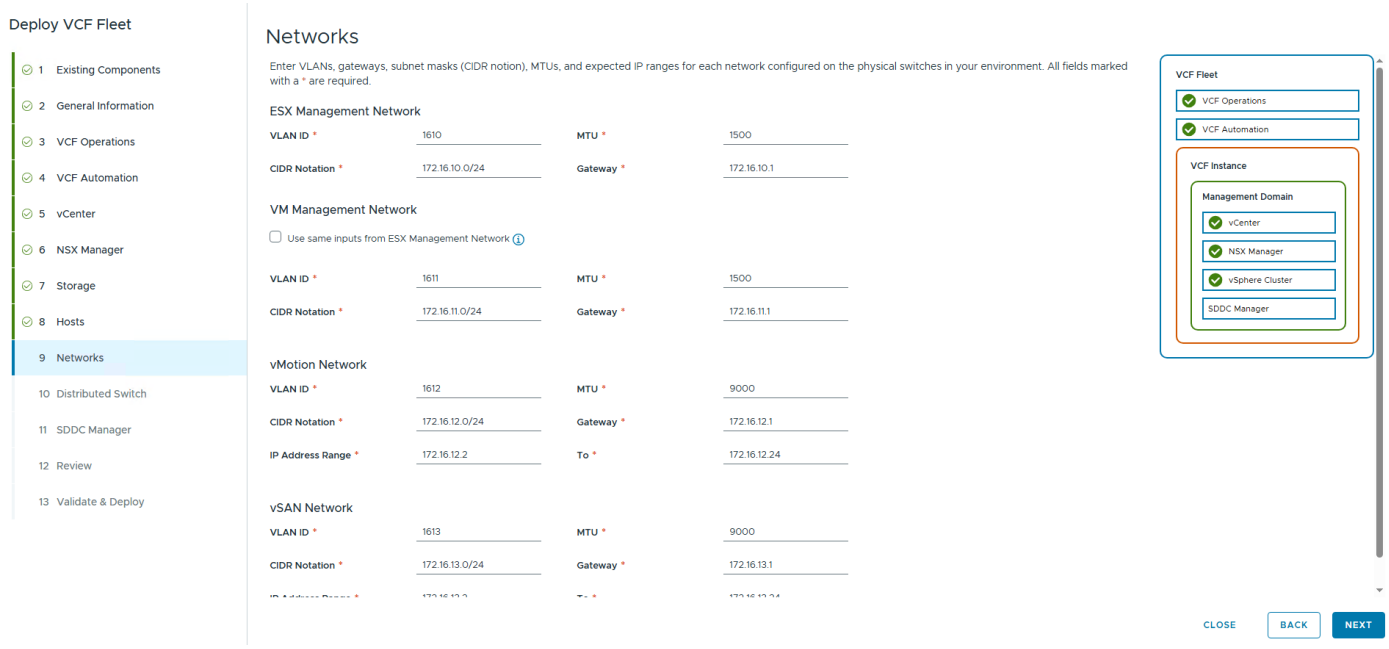

Figure 47. Networks

12. Enter the Distributed Switch details.

Note

VCF 9.0 supports various profiles based on traffic separation and number of Distributed Switches. In this reference architecture for vSAN we have tested the NSX Traffic Separation profile. It provides a segregation for NSX traffic.

Figure 48 shows distributes switch created for NSX Traffic Separation.

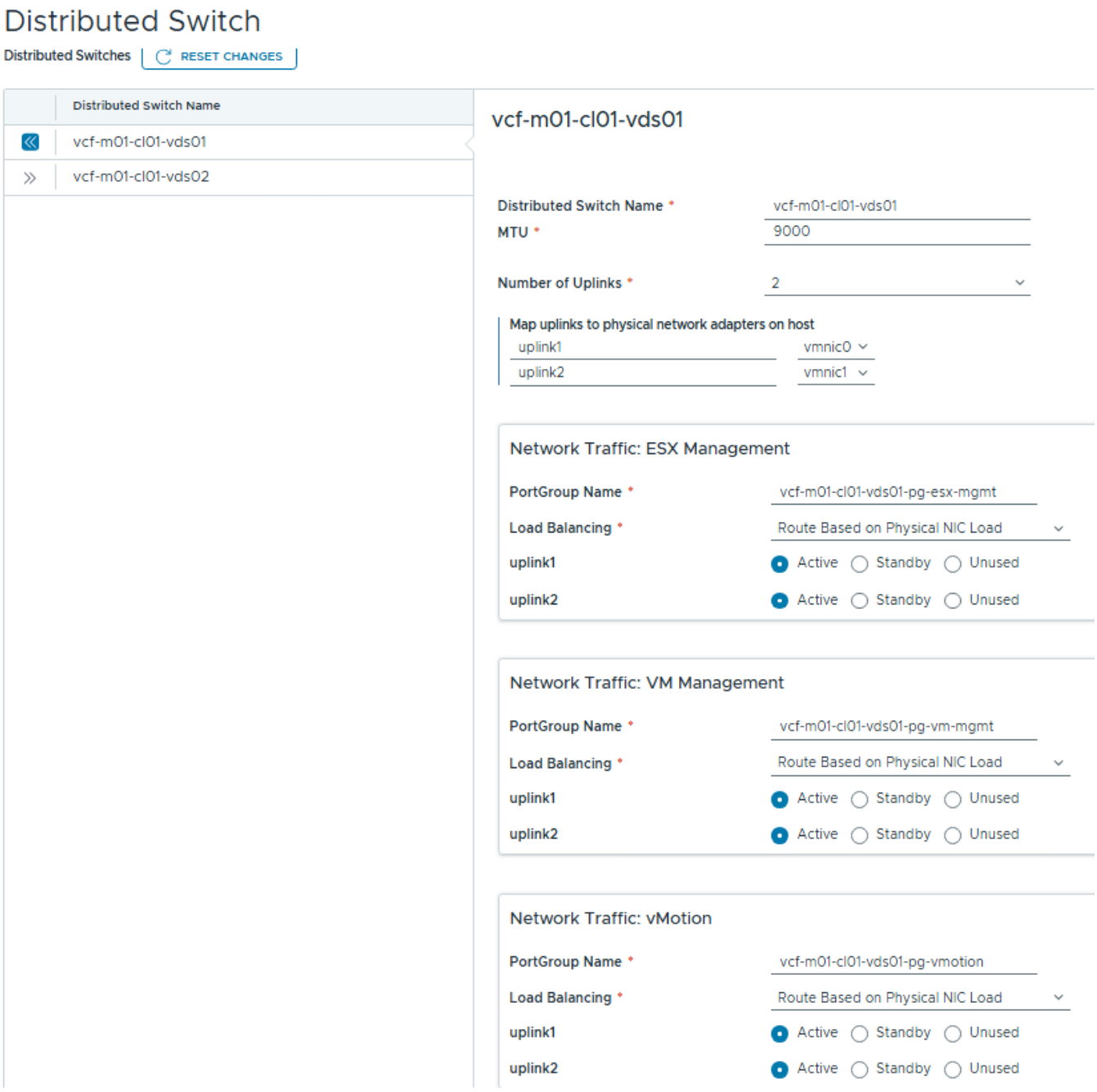

Figure 48. Distributed switch

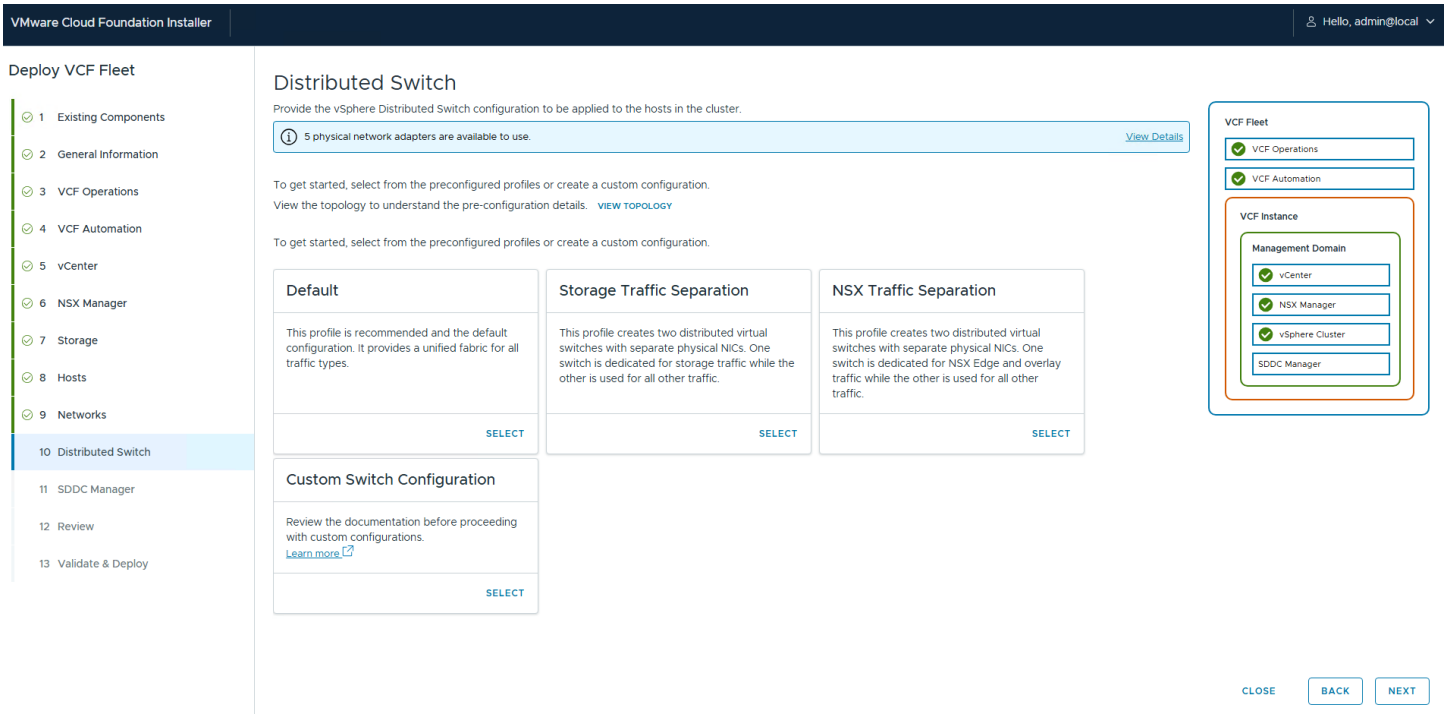

Figure 49. Distributed Switch configuration for management traffic

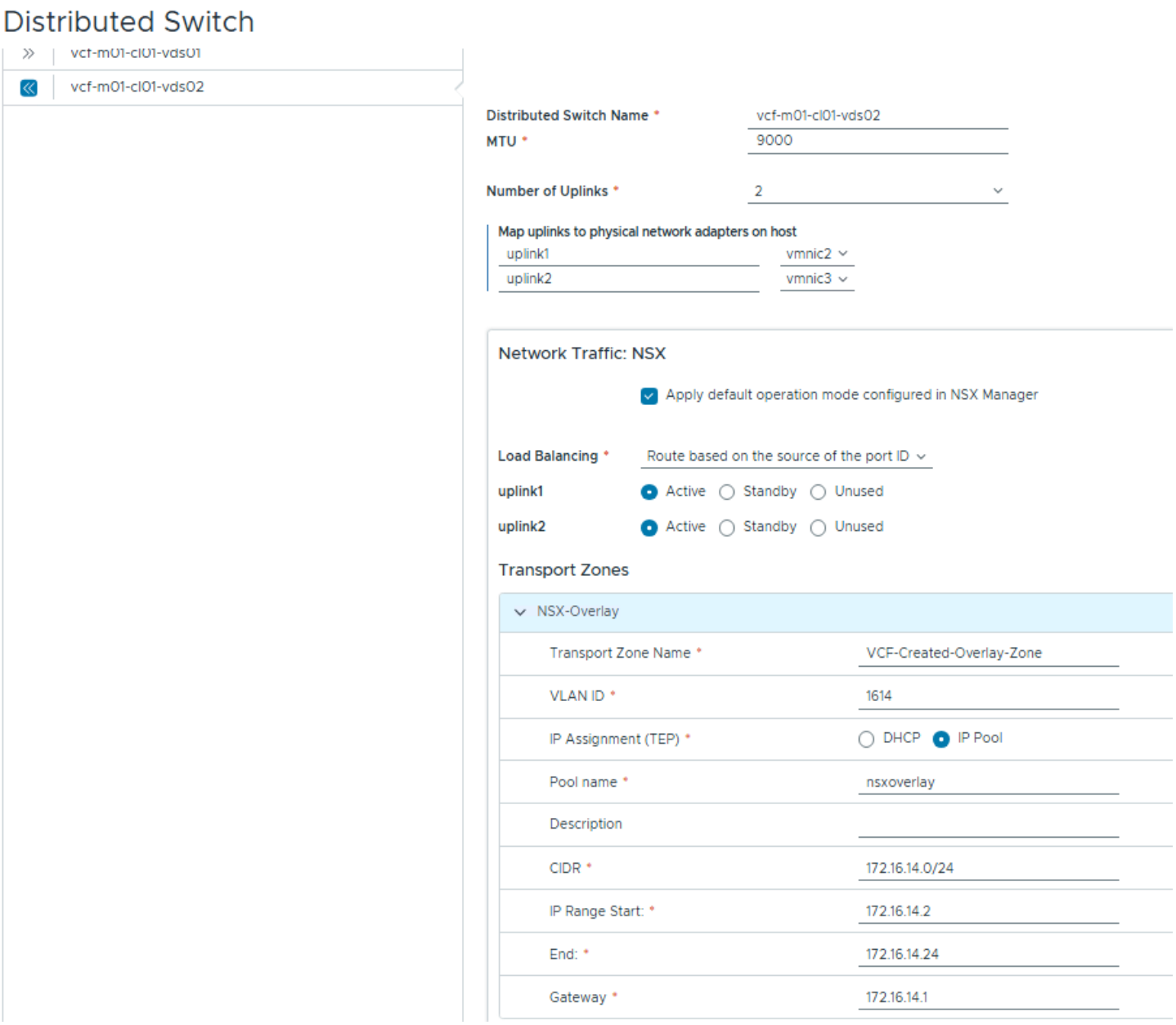

Figure 50. Distributed switch configuration for NSX traffic

Note

VCF 9.0 support various profiles based on traffic separation and number of Distributed Switches. In this reference architecture , for VMFS on FC use case, we have tested Default profile. It provides a unified fabric for all traffic types using a single vSphere Distributed Switch.

The following screenshots represent the settings for Default Profile for vDS for VMFS on FC use case.

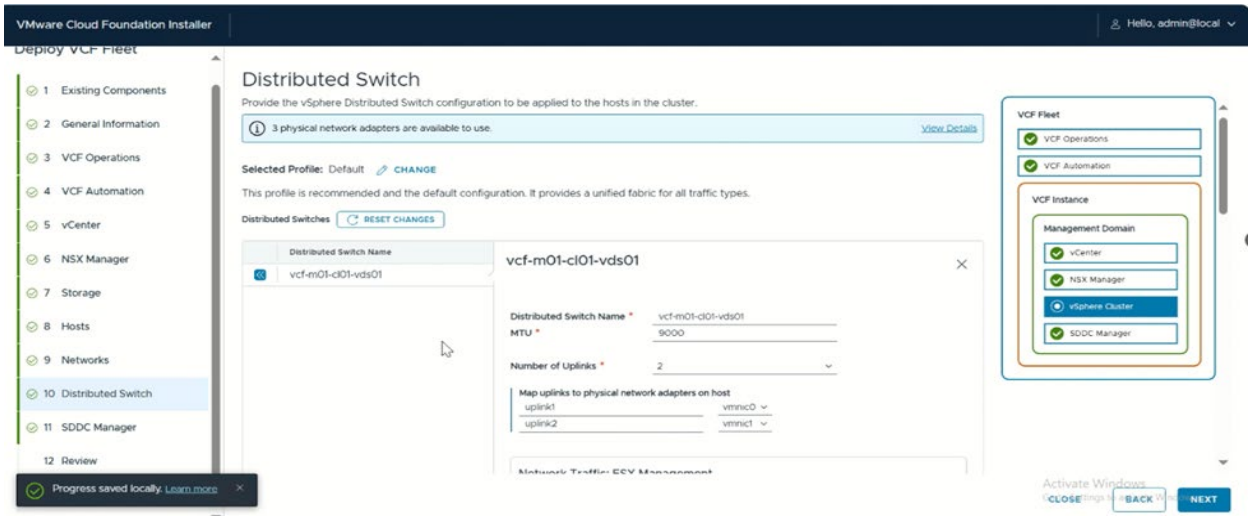

Figure 51. Distributed switch configuration for Default Profile

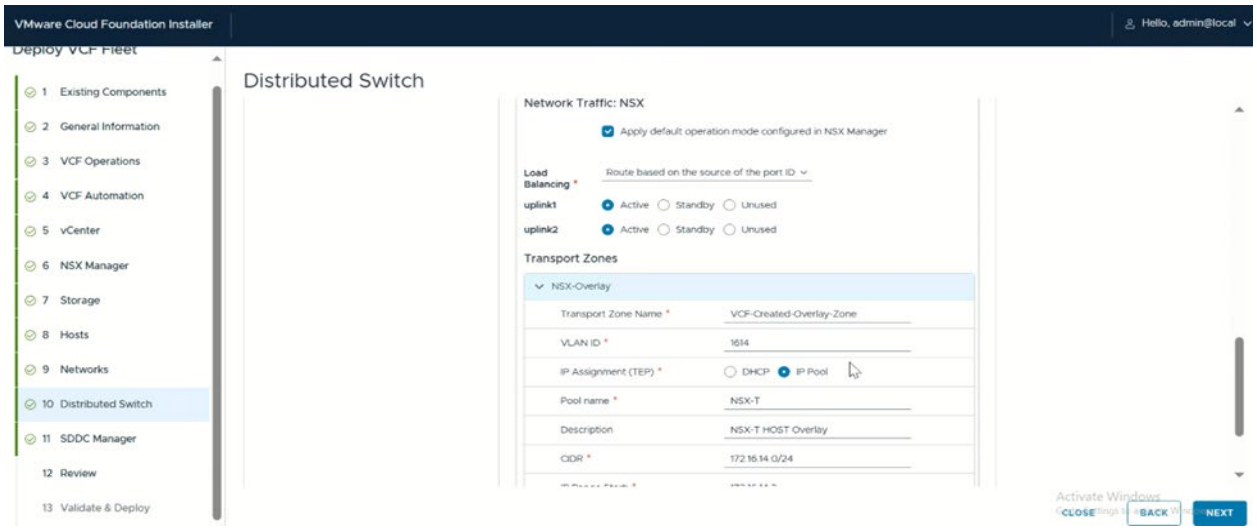

Figure 52. Transport Zone configuration for Default Profile vDS

13. Enter SDDC Manager details.

Note

If the VCF Installer appliance is deployed on one of the hosts in the management domain; during the deployment process, the installer appliance will be converted into the SDDC Manager appliance. The next screenshot would only prompt to provide the installer appliance password.

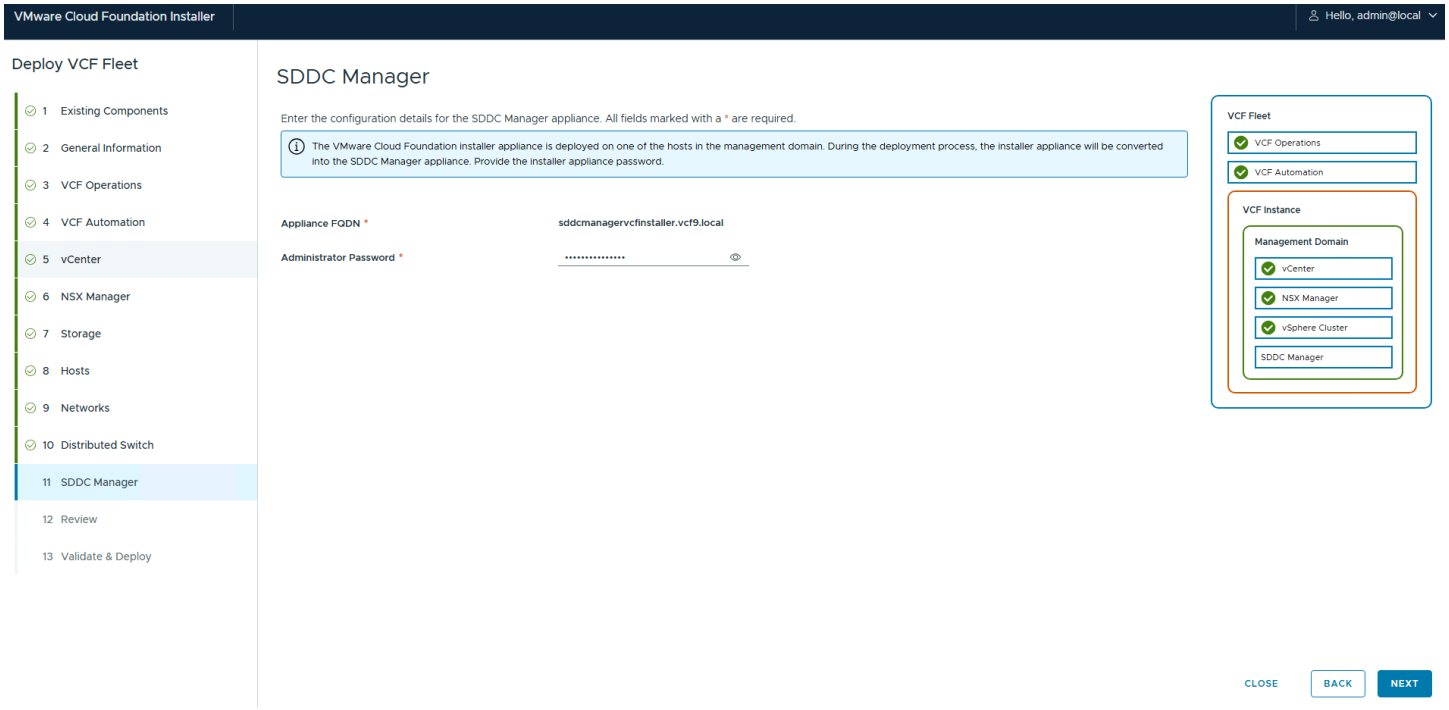

Figure 53. SDDC Manager

14. Review the deployment information.

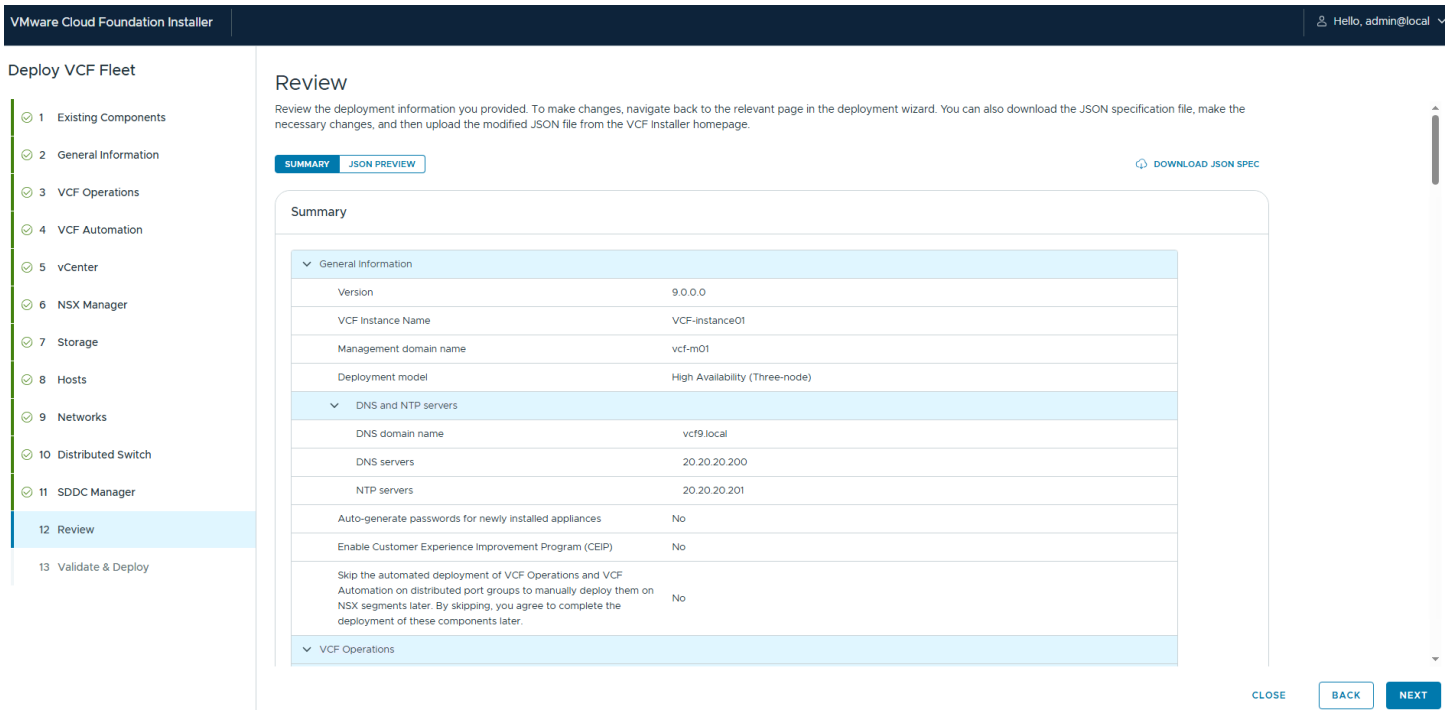

Figure 54. Review

Validate and Deploy

The VCF installer will now validate the information provided in the deployment wizard and report any warnings or errors. Warnings can be addressed or acknowledged. Errors must be resolved before deployment. Navigate back to the relevant pages as appropriate, address the issue(s), and re-run the validations.

When all validations are acknowledged or successfully complete, click **Deploy**.

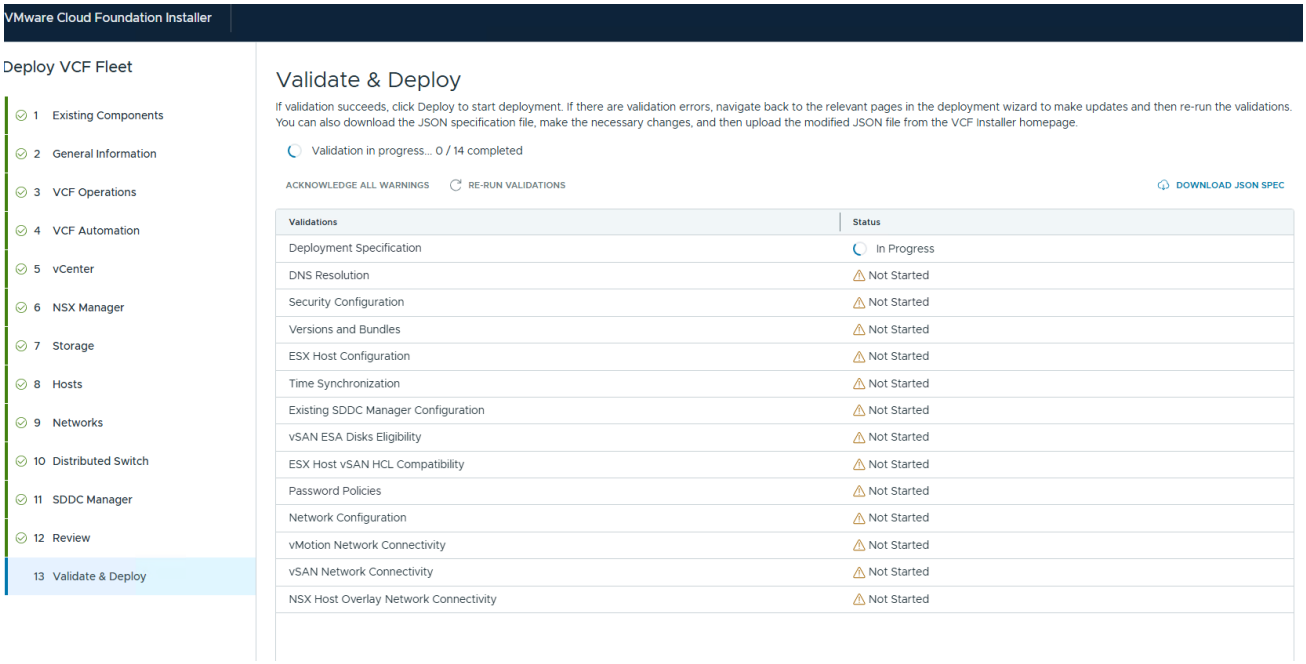

Figure 55. Validate and Deploy

Note

Figure 55 Validate and Deploy can be monitored here. If there are any errors, review the failed tasks in the tasks panel, address the issue(s) and retry the deployment. Optionally download the JSON spec file, for future deployments.

VCF Operations for unified visibility

To review a deployed VCF instance, access the VCF Operations interface, which provides a unified view of VCF deployments, including management and workload domains. This interface allows you to monitor the health of VCF components.

Figure 56 shows the newly deployed VCF Instance.

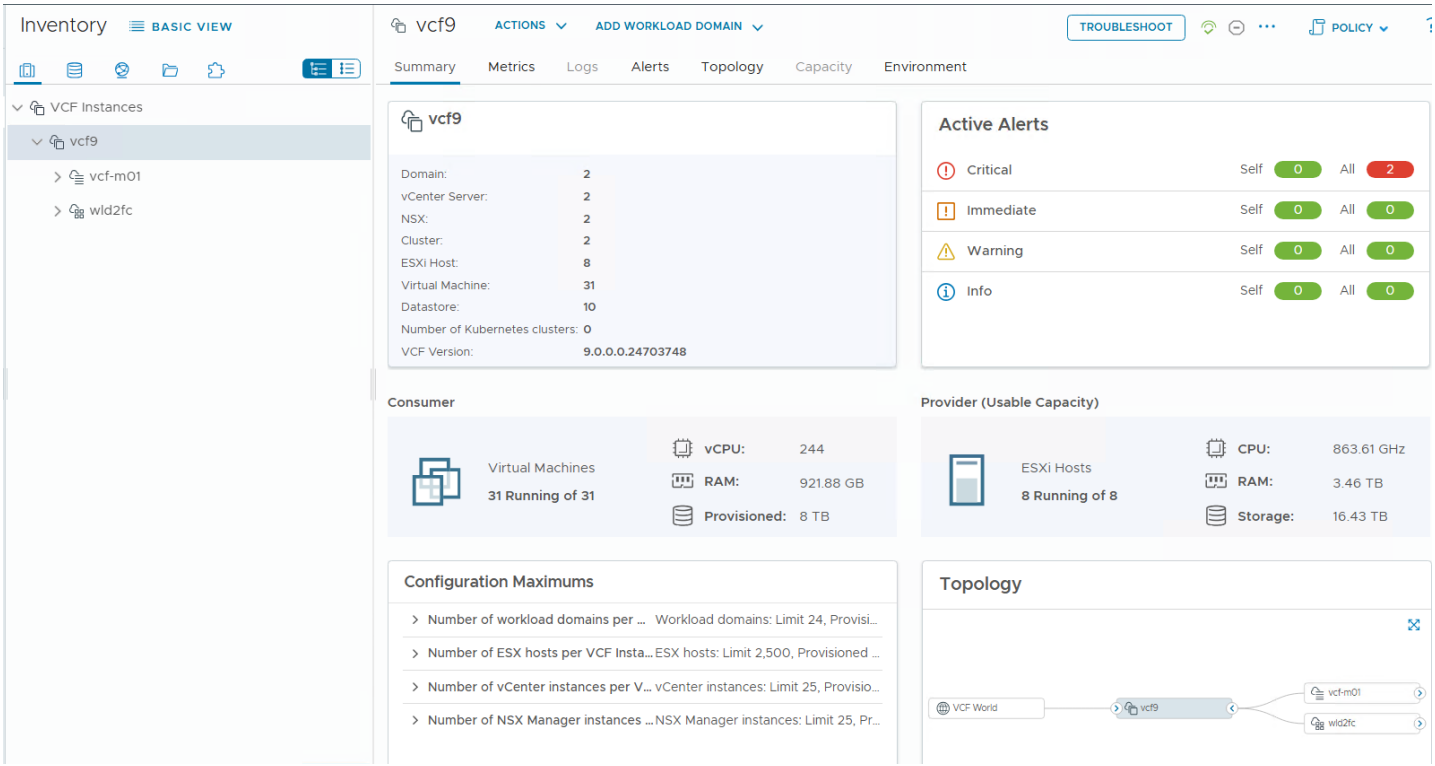

Figure 56. VCF Instance

VCF workload domain creation

VCF workload domains support vSAN, VMFS on Fibre Channel or NFS as primary storage options. The workload domain scenario deployment steps, described here, are based on “VMFS on Fibre Channel (FC)” storage.

Built in vSphere as a control plane, the VMware vSphere Supervisor enables native deployment and management of Kubernetes Clusters, and vSphere Pods along with traditional workloads by adding objects to the vCenter inventory such as namespaces and VKS clusters.

Note

If the customers opts to use vSAN, guidance is provided in the document on the changes needed for the vSAN based deployment workflow.

This section describes the deployment of the workload domain enabled with vSphere Supervisor services.

The following are the prerequisites for workload domain deployment:

Define vSphere Lifecycle Manager Cluster Image

A vSphere Lifecycle Manager cluster image must be available for the default vSphere cluster of the workload domain. A cluster image relevant for the HPE ProLiant Gen12 server must be created on the management vCenter and imported to VCF Operations image catalog. To import the image to VCF Operations image catalog.

1. Navigate to **VCF Operations > Fleet Management > Lifecycle > Expand the VCF Instance** and select the **deployed VCF Instance > Image Management tab**.
2. Click **Import Image**. Choose Import from a vCenter option.
3. Select the management vCenter from vCenter drop down and the table will be updated with images available from the vCenter Lifecycle manager. If you do not see an appropriate image, click the "**go to Image Library**" link to log into the management vCenter and create the appropriate image. Once created, return to this VCF Operations import image UI and click **refresh** to update the list.
4. Select the cluster image with HPE Vendor add-on appropriate for the respective HPE ProLiant DL Gen12 server.
5. Click **Import**.

Create Network pool

To add ESX hosts to the global inventory, you must create or expand a network pool. A network pool must include at a minimum, the vMotion network information. Depending on the type of storage you are using, you must provide network information for vSAN, NFS, and iSCSI.

Note

Starting with VCF 9.0, some host and cluster operations from SDDC Manager are integrated into management domain vCenter. Network pool creation and ESX Host commissioning is done through **vSphere Client > Global Inventory > Hosts** to leverage them for the workload domain deployment.

Properly sizing a network pool is critical to prevent future issues. Refer to "size a network pool" documentation for additional details.

1. From the management vCenter UI main menu, click **Global Inventory Lists > Hosts > Network Pools**.
2. Click **Create Network Pool**.
3. Enter a name for the network pool.
4. Select the network type(s).

5. Provide network information for the selected network type(s).

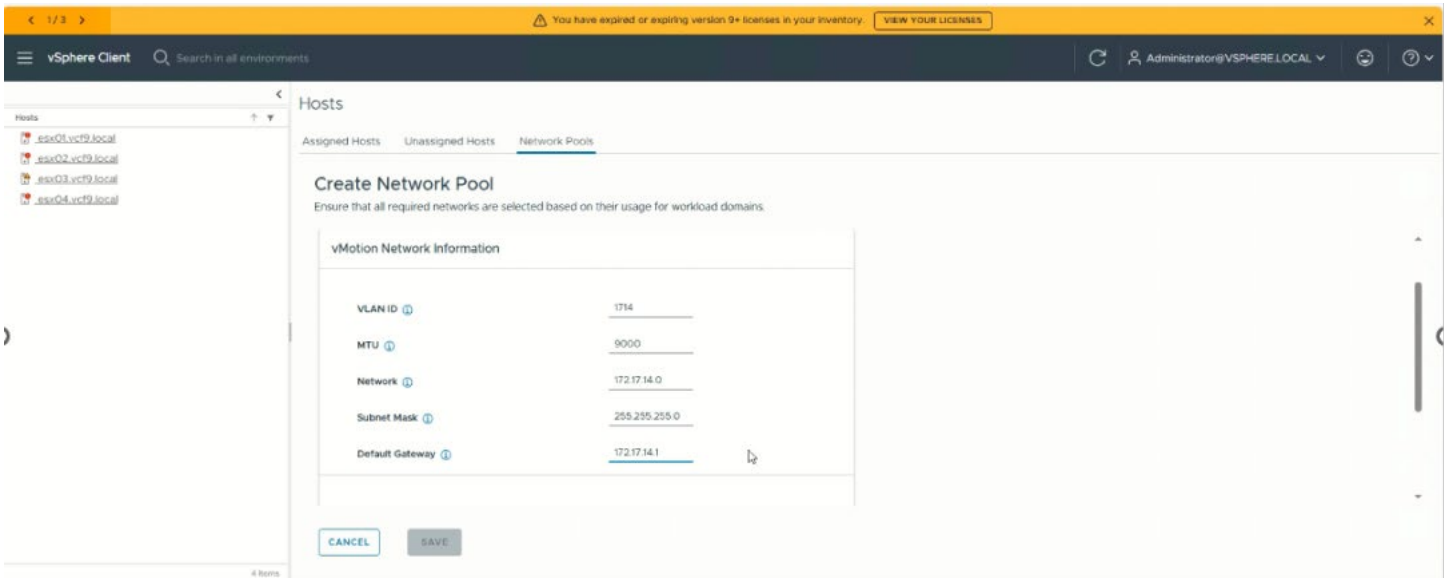

Figure 57. Network pool

Commission Hosts

Commission ESX hosts for use in a VCF domain. During the commissioning process, the ESX hosts are associated with a network pool and added to the global inventory. When an ESX host is added to a workload domain, an IP address from the network pool's IP range is assigned to it.

To perform this task from the management vCenter UI main menu, click **Global Inventory Lists > Hosts > Unassigned Hosts.**

1. Click **Commission Hosts**.
2. On the Checklist page, review the prerequisites are met and confirm by clicking **Select All**.
3. Click **Proceed**.
4. Select whether you want to add hosts one at a time or import multiple hosts at once from a JSON file.
5. Select Add New and enter the host FQDN, Storage Type and Network Pool Name.
6. Click Add to move the server to the "Hosts Added" table. Repeat the "Add New" entry for all servers to be configured for this workload domain.
7. Verify that the server fingerprint is correct for each host and then activate the Confirm All Fingerprints toggle.
8. Click **Validate All** to validate the host information. Ensure all hosts are marked as "Valid".
9. Click **Next**.

10. On the Review page.

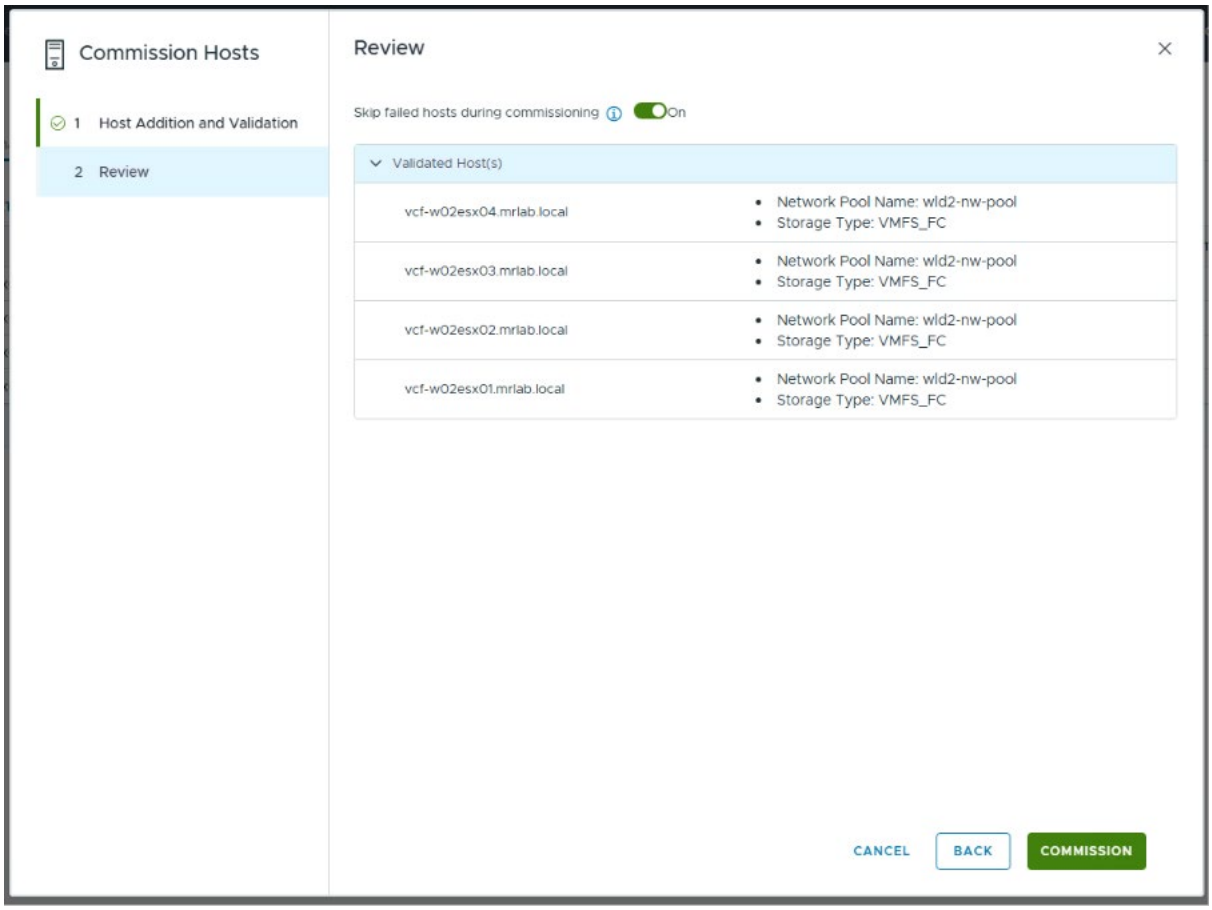

Figure 58. Commission hosts

11. Click **Commission**.
12. The successfully commissioned hosts are added to the Unassigned hosts table in the global inventory list.

Create a new workload domain using VCF Operations

The workload domain with a vSphere Supervisor feature can be used for VCF Automation's self-service consumption capabilities. To enable this, toggle on the 'Enable vSphere Supervisor' in the General Information tab of the create workload domain deployment workflow (see Figure 59. Workload General information). The enablement of the vSphere Supervisor feature implies requirements on the NSX network connectivity. For more information refer to vSphere Supervisor Platform option to configure network connectivity and Virtual Private Cloud (VPC) External IP Blocks is included during the bring up of workload domain via VCF Operations. Connectivity between NSX Virtual Networking and VCF physical infrastructure can be configured in two ways: Virtual Networking and VCF physical infrastructure can be configured in two ways:

Centralized Gateway: If Centralized Connectivity is selected, the configuration occurs post workload domain deployment and is essential for enabling self-service capabilities and VCF Automation. It provides a variety of NSX services such as DHCP, NAT, VPN, and security, offering comprehensive network management. The detailed configurations are outlined in the following section.

Distributed Gateway: Distributed Connectivity offers a simplified external connectivity model without the need for deploying edge nodes. It features streamlined configuration with limited services. For external connectivity of the distributed gateway, an external Gateway IP address and VLAN are required.

Note

Centralized Networking connectivity is required for the deployment if vSphere Supervisor is deployed as part of the Workload domain deployment. Centralized Connectivity is required if the plan is to integrate the workload domain with VCF Automation.

Create Workload domain workflow

1. In VCF Operations, select **Inventory > Detailed View**.
2. Expand VCF Instances and browse to the VCF instance in which you want to create a new workload domain.
3. Click **Add Workload Domain > Create New**.
4. Review the prerequisites, click **Select All**, and click **Proceed**.
5. Enter the General Information details including Enable vSphere Supervisor and click **Next**.

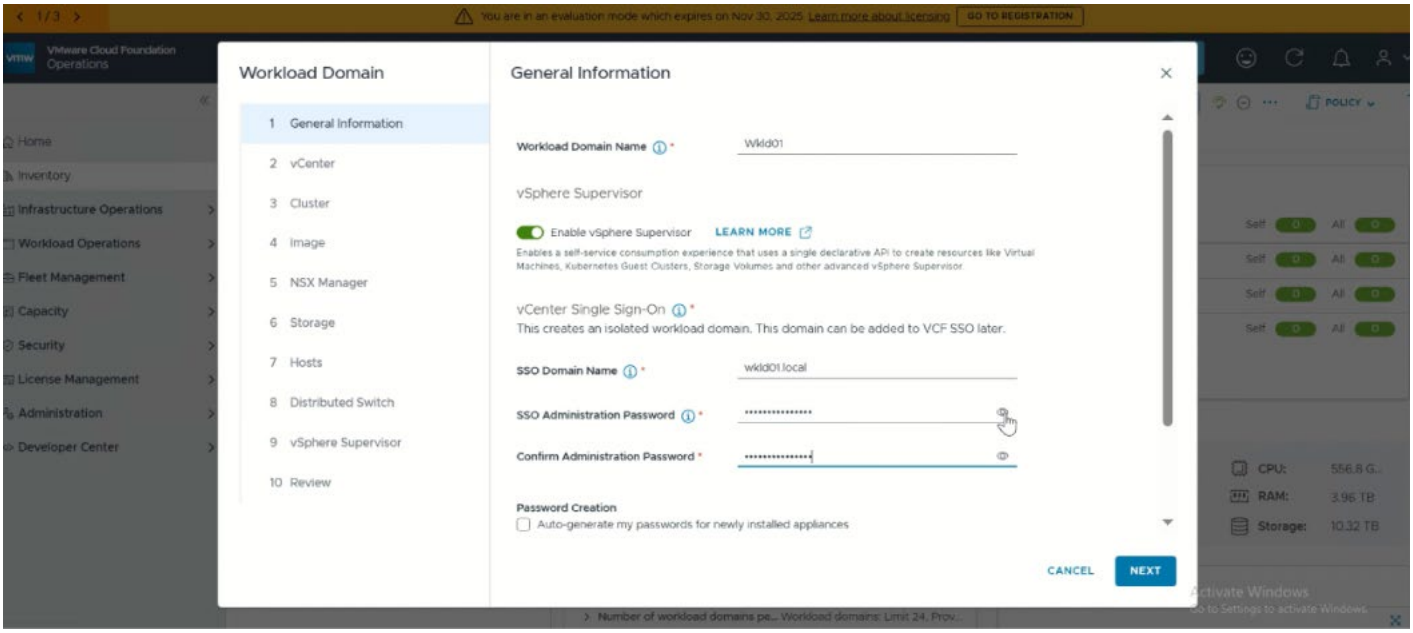

Figure 59. Workload General Information

6. Enter the vCenter details and click **Next**.

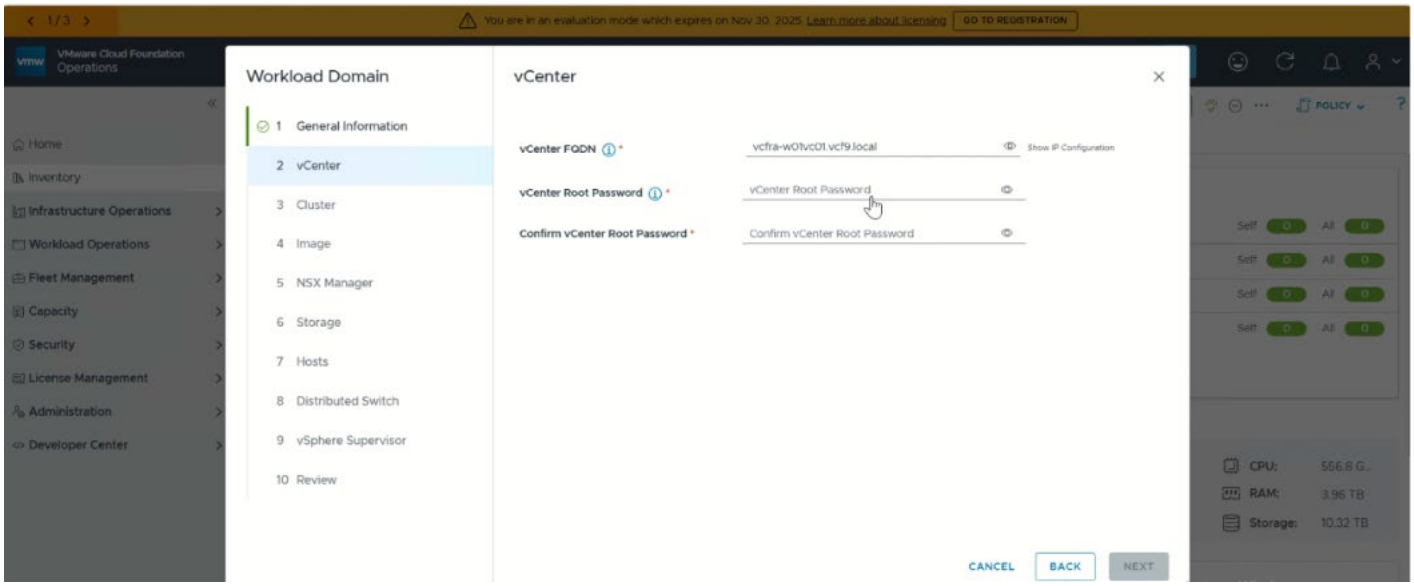

Figure 60. Workload vCenter

7. Enter the Cluster details and click **NEXT**.

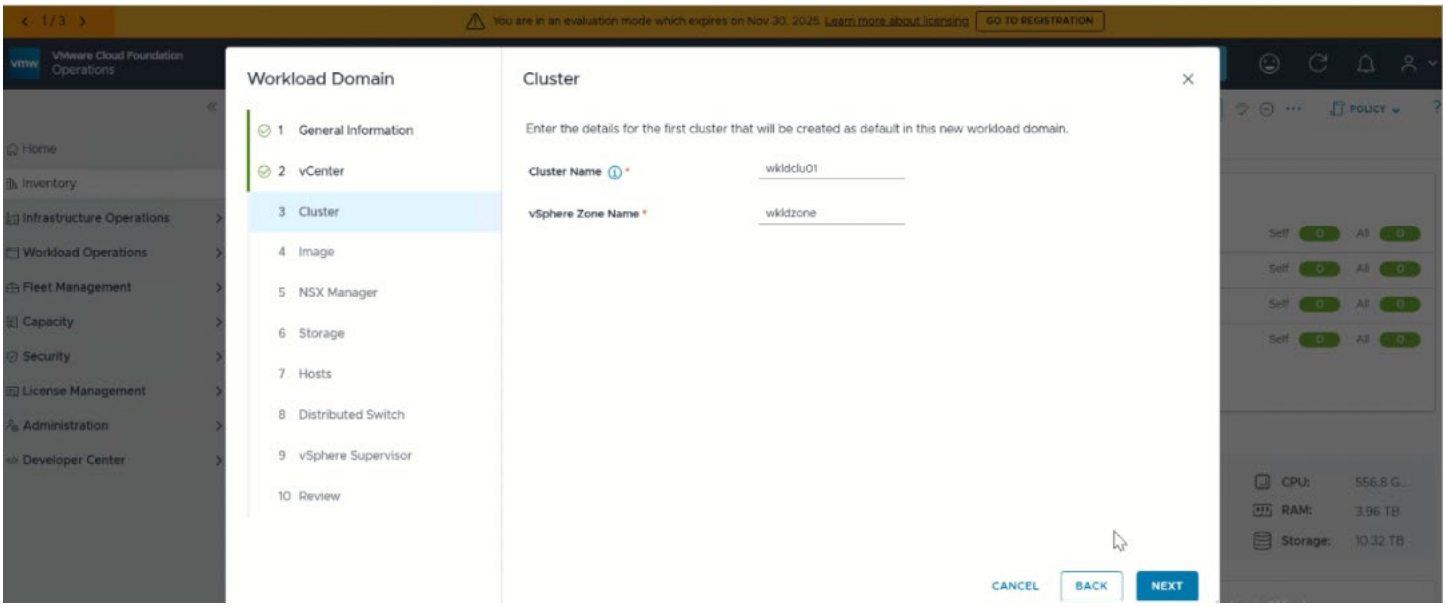

Figure 61. Workload Cluster

8. Select a cluster image and click **NEXT**.

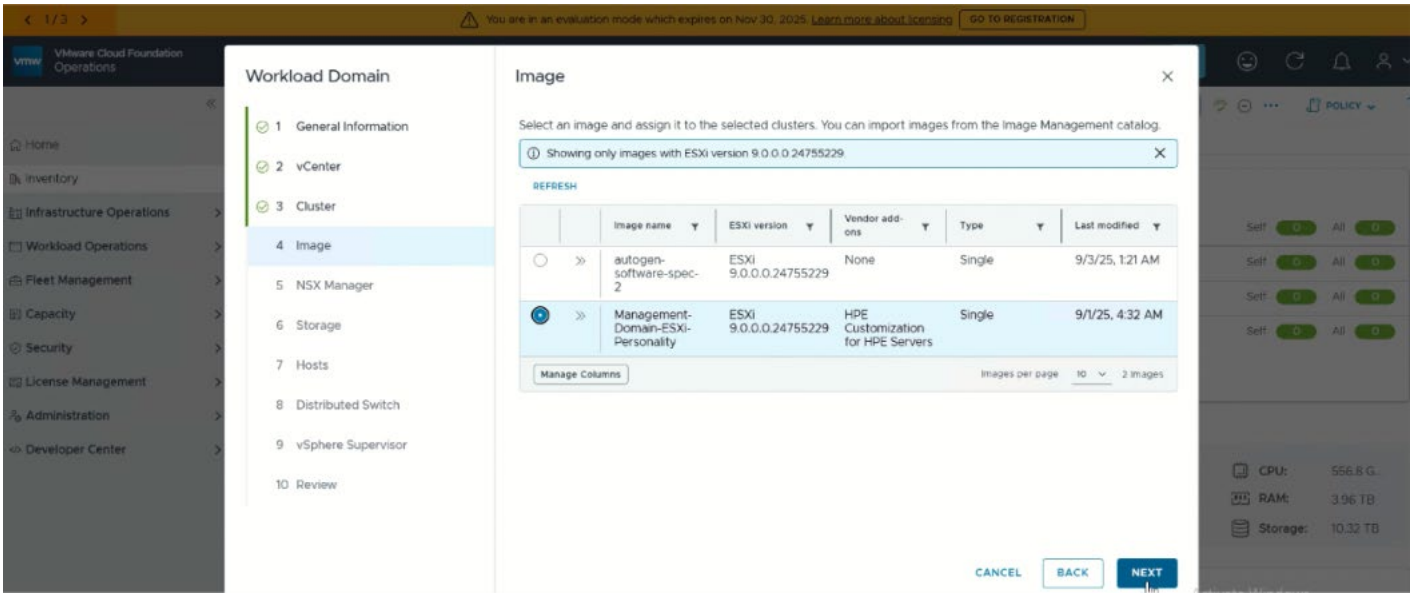

Figure 62. Workload Image

9. Enter the NSX Manager details and click **NEXT.**

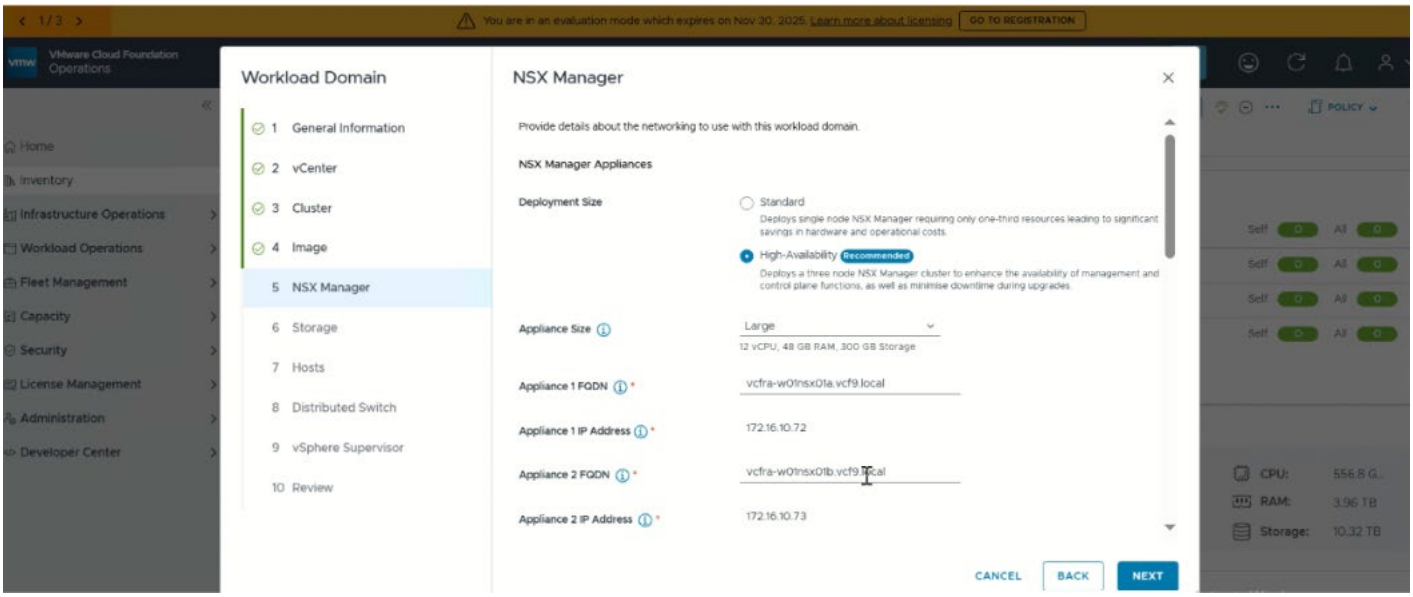

Figure 63. Workload NSX Manager

Note

Since “vSphere Supervisor” enabled for this workload domain, Centralized Connectivity is the default option as noted in Figure 64.

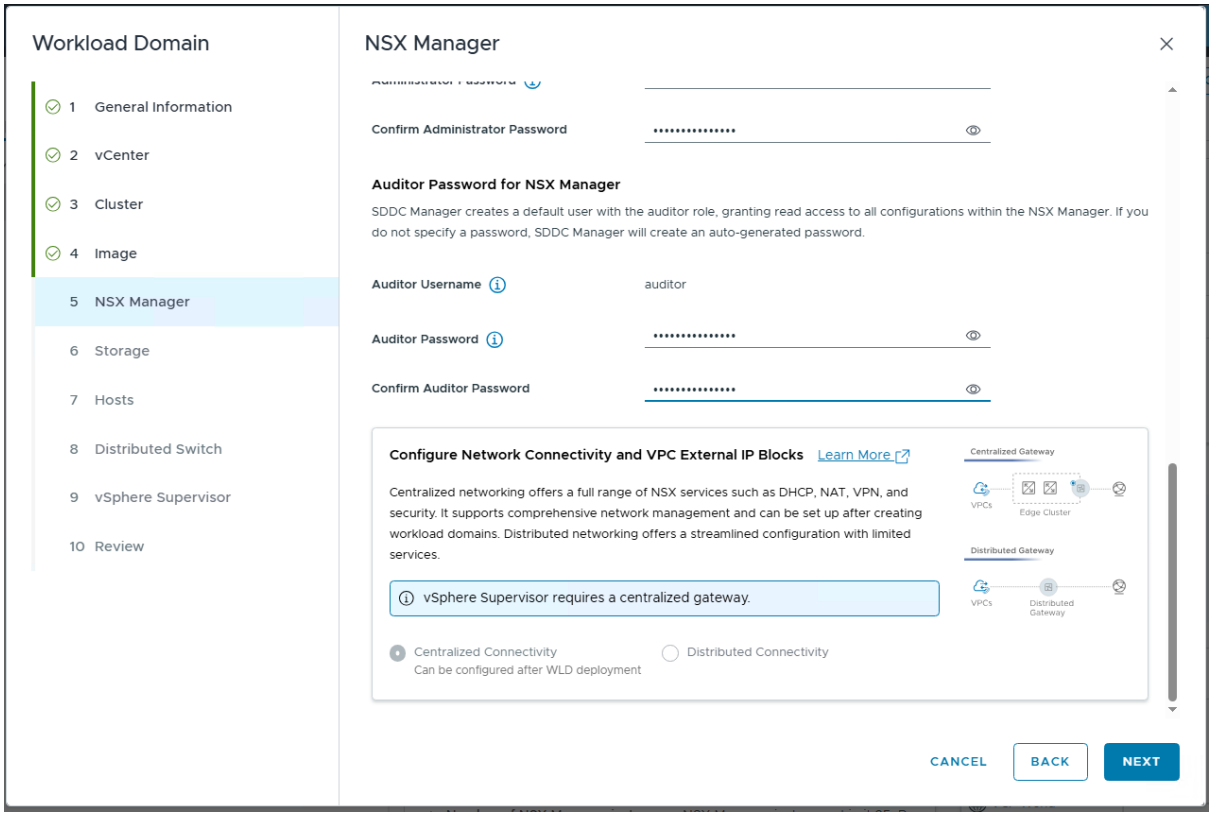

Figure 64. Workload NSX Manager continued

10. Enter the appropriate Storage details for this workload domain and click **NEXT.**

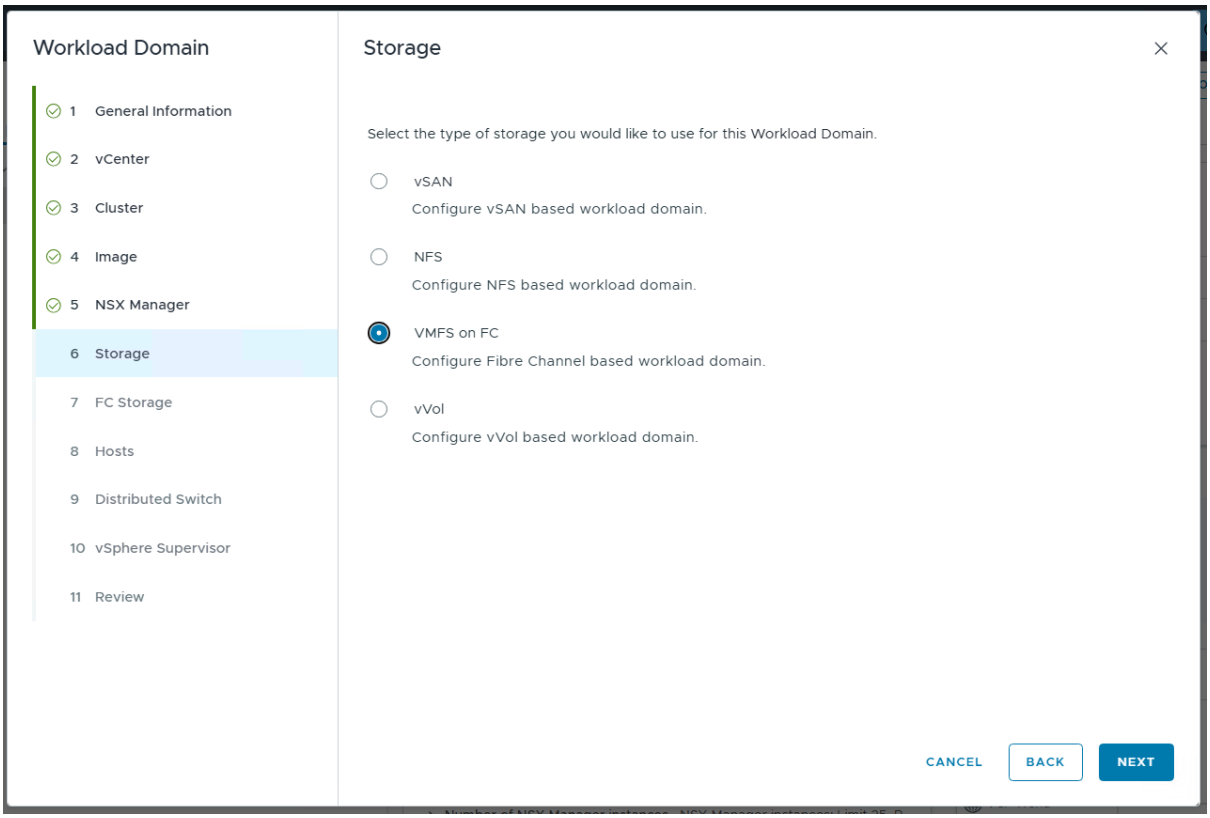

Figure 65. Workload storage

Note

If utilizing vSAN as the storage for the workload domain, select "vSAN" during step 6 of the workflow, then choose "vSAN ESA" (Express Storage Architecture), and for vSAN Cluster type select vSAN HCI.

11. FC Storage, enter Datastore Name created for each host during the storage provisioning phase.

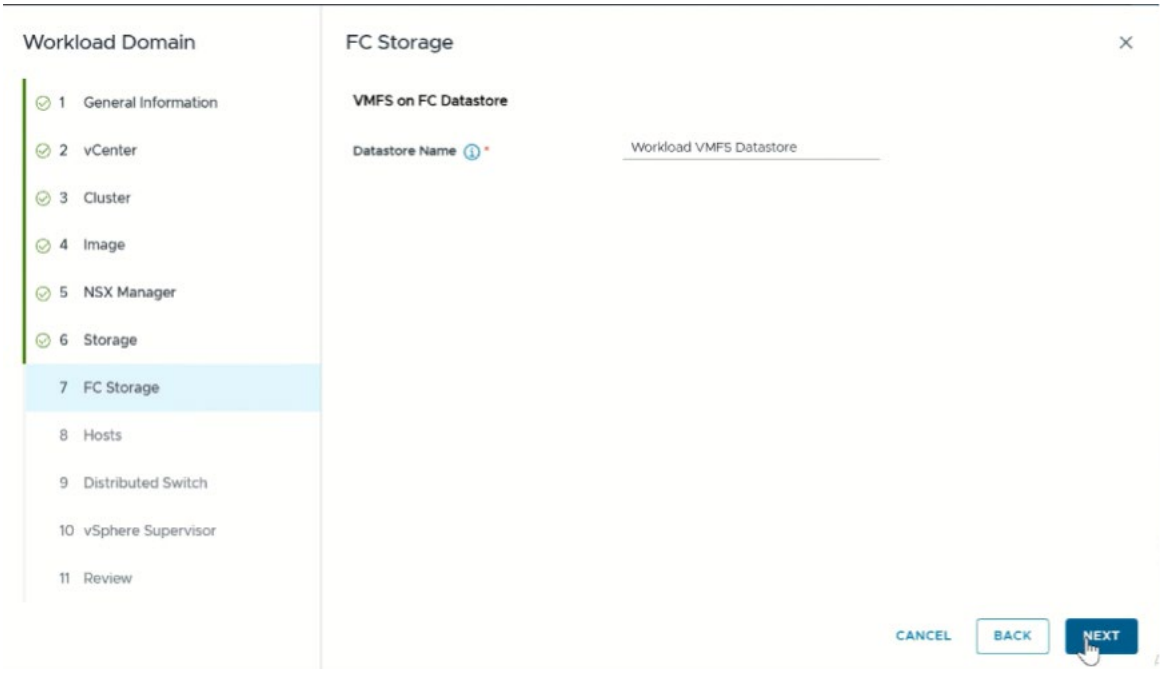

Figure 66. FC Datastore

12. Select the ESX hosts to use for creating the workload domain and click **Next**.

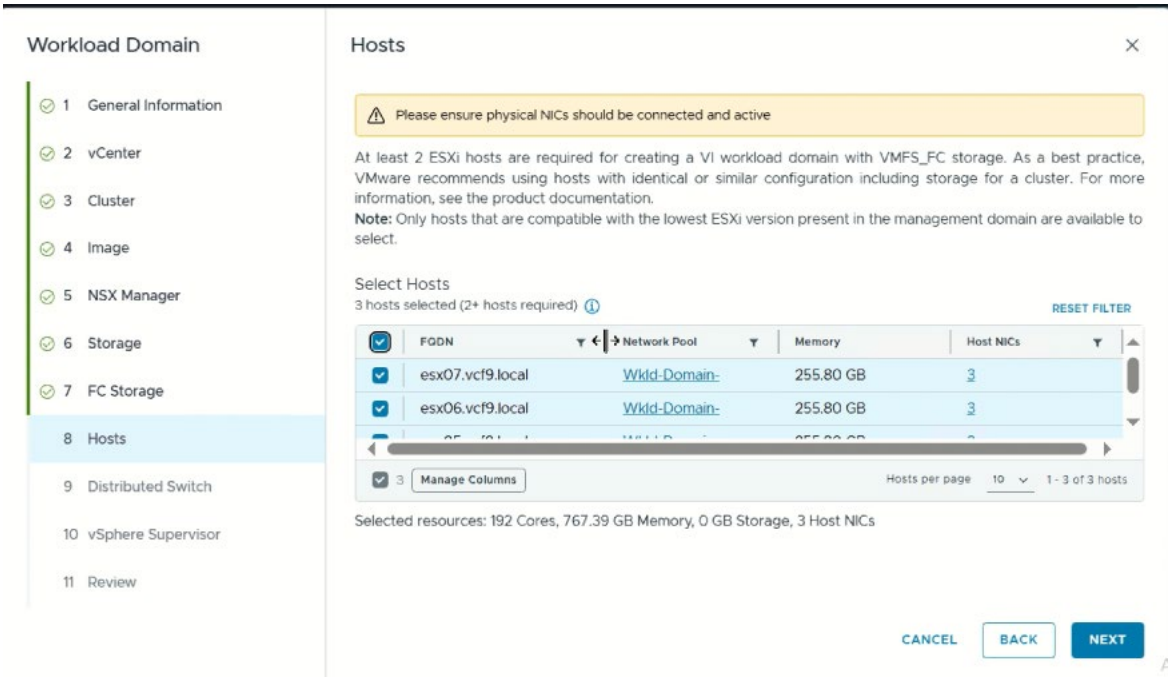

Figure 67. Hosts

15. Enter the Distributed Switch details and click **Next**.
    a. Click **SELECT**, to select **Default** Preconfigured profiles for the VDS.
    b. On Distributed Switch page.
    c. Click **Edit** on the Distributed Switches Banner to enter **VLAN ID** for NSX-Overlay Traffic Transport VLAN.

d. On NSX section, Enter **VLAN ID** for NSX-Overlay Traffic Transport VLAN.

e. Click **SAVE CHANGE**.

f. Click Acknowledge for VLAN ID edit.

g. Click **NEXT**.

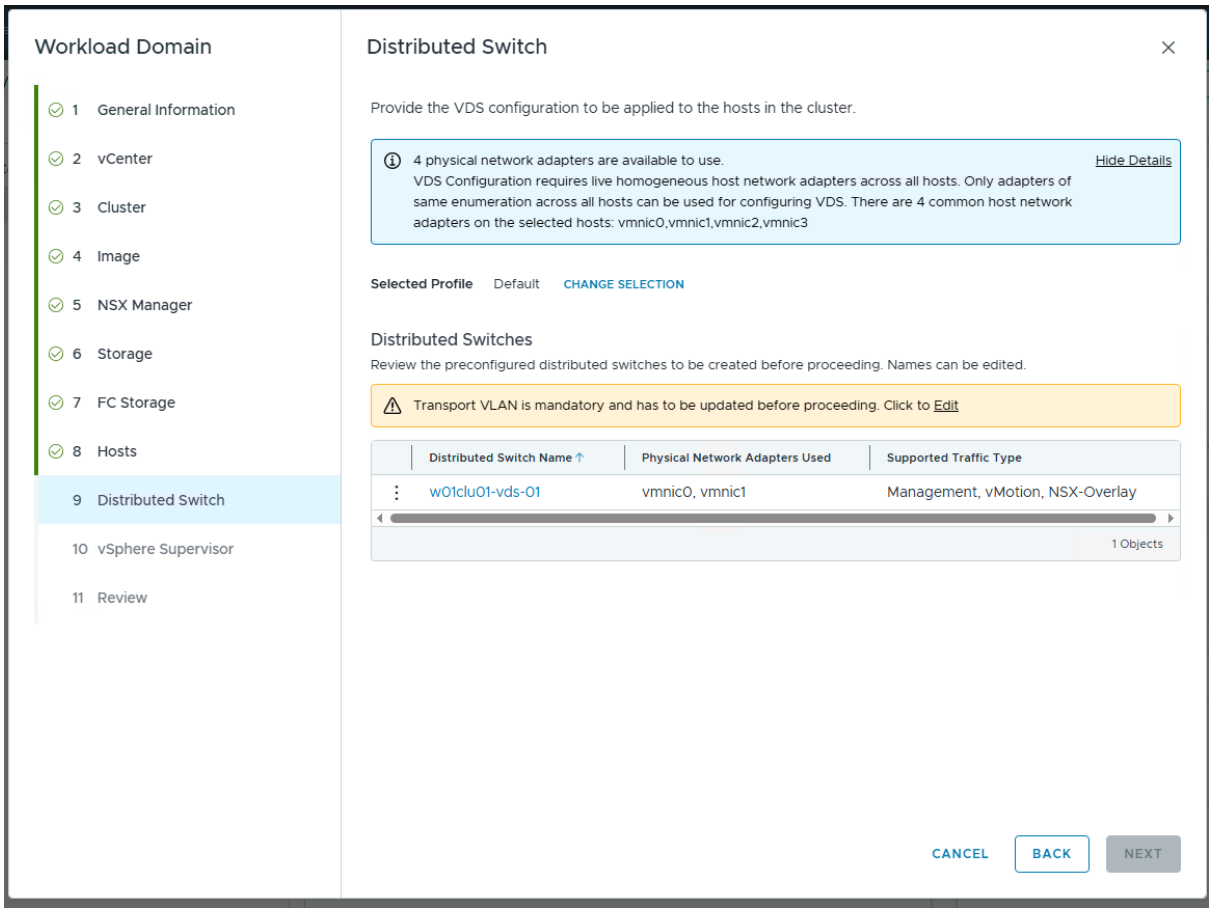

Figure 68. Distributed switch configuration for single 2port NIC in FC external storage configurations

Note

The **NEXT** button will be enabled when all the parameters entered and acknowledged.

16. Enter the vSphere Supervisor details and click **Next**.

Note

The Transit Gateway simplifies network connectivity between VPCs and external networks, acting as a central hub. Private CIDR blocks, within the VPC connectivity profile, define the IP address ranges used for workloads within a VPC, enabling communication within that VPC or potentially with other VPCs connected to the same Transit Gateway. For more information, refer to Requirements for Supervisor Deployment with NSX VPC.

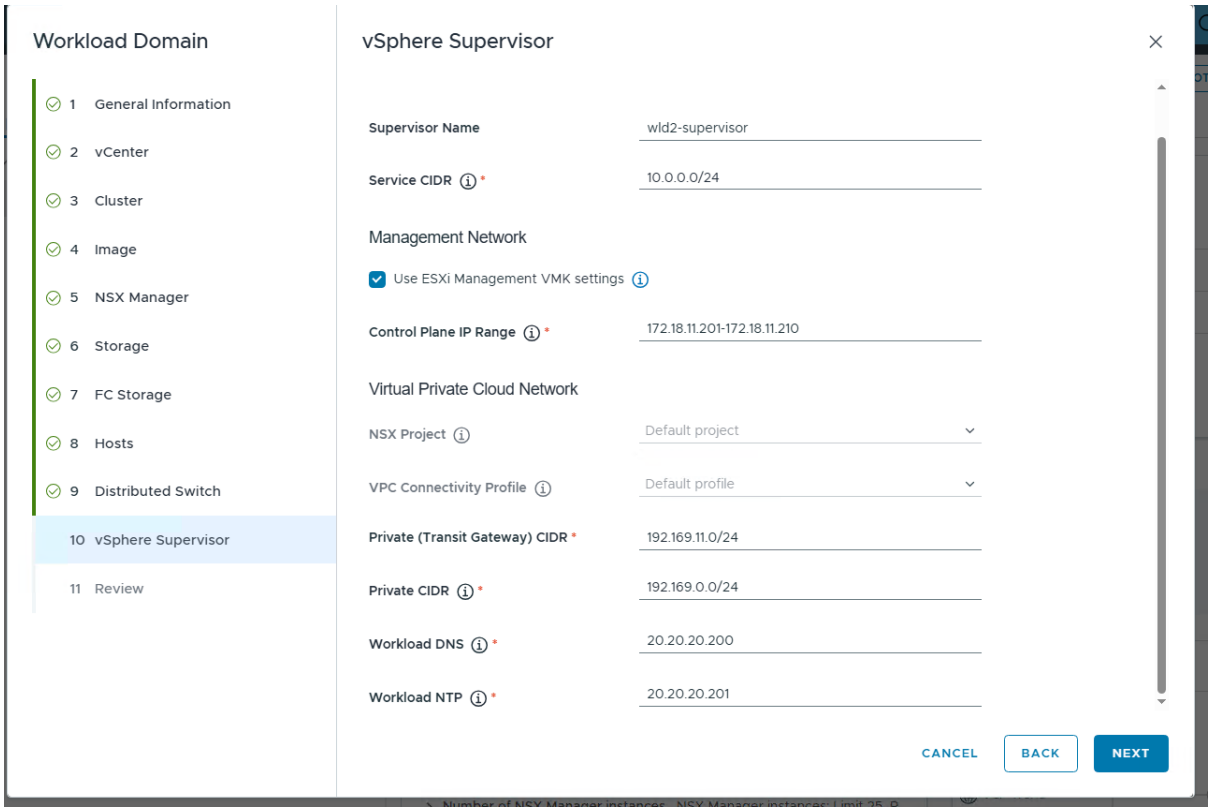

Figure 69. vSphere Supervisor

17. Review page, validate all the details and click **FINISH**.
18. Progress of the deployment can be viewed in VCF Operations, select **Inventory > Fleet Management > Tasks**.
19. After successful workload deployment a banner pop-up window appears with the next steps.

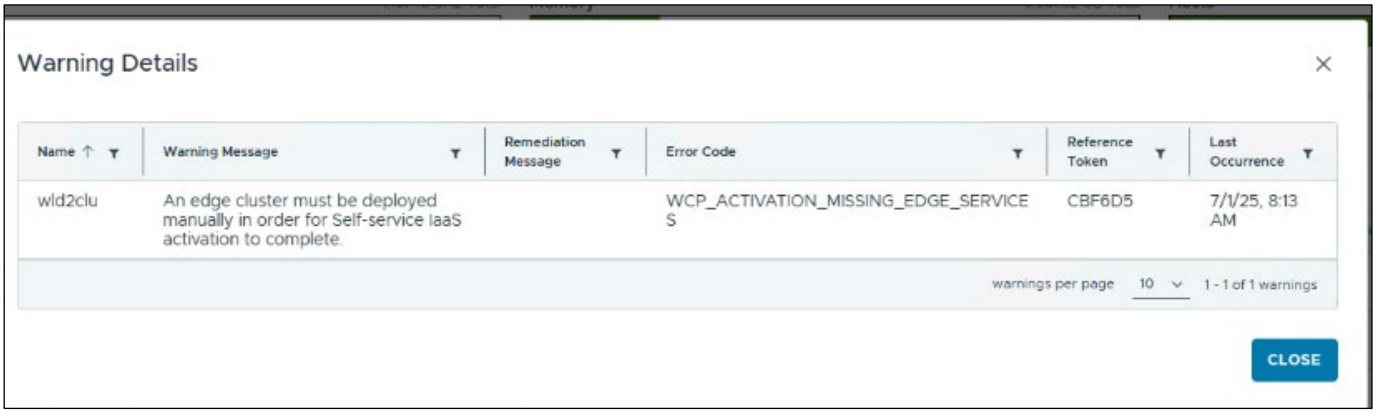

Figure 70. Warning message to deploy edge cluster

Define TEP IP Pool Range in Workload NSX-Manager :

Note

This step is required only when we need to configure NSX TEP IP statically as the UI method of Workload Deployment, doesn't support static TEP IP configuration.

After Workload Domain Deployment is complete, log in to Workload NSX manager and do the below changes to make TEP IP assignment from the defined Static IP pool range instead of using DHCP.

If we have DHCP, Supervisor configuration takes a hit and ends us in configuring state.

Hence, it is suggested to go with IP Pool range. Perform the following mentioned steps :

1. Login into Workload NSX manager.
2. Navigate to **Networking --> IP Management Section --> IP Address Pools**.

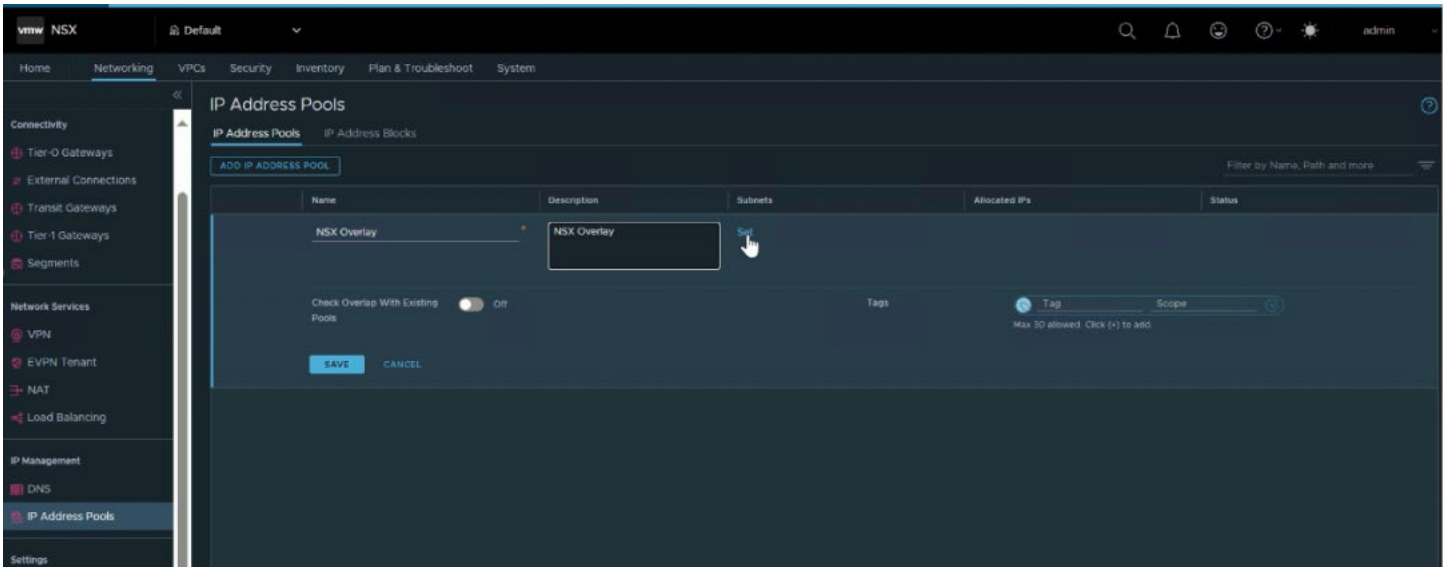

Figure 71. IP address Pools in workload NSX Manager

3. Click **Add IP Address Pool --> Enter a Name --> Click Set**.

4. Now Enter the Range of the IP Address Pool for TEP purpose (NSX Overlay), CIDR, Gateway IP.

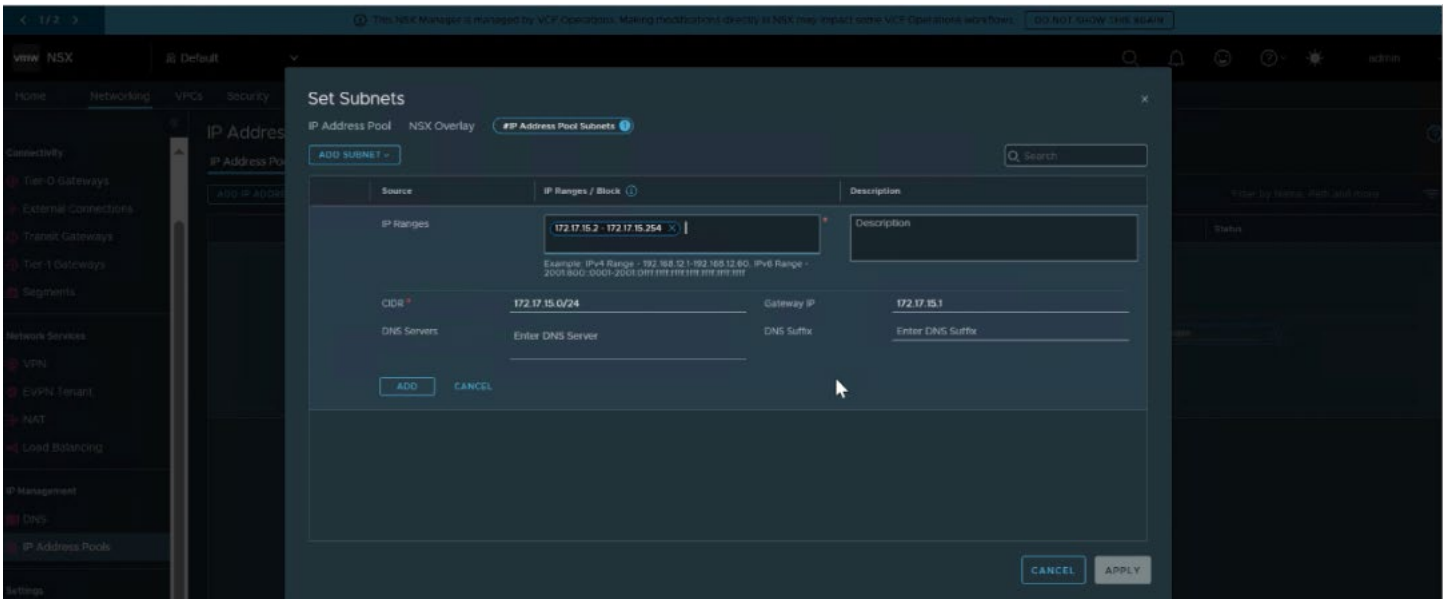

Figure 72. Define IP Pool Range and Gateway

5. Click **Apply--> Save**.

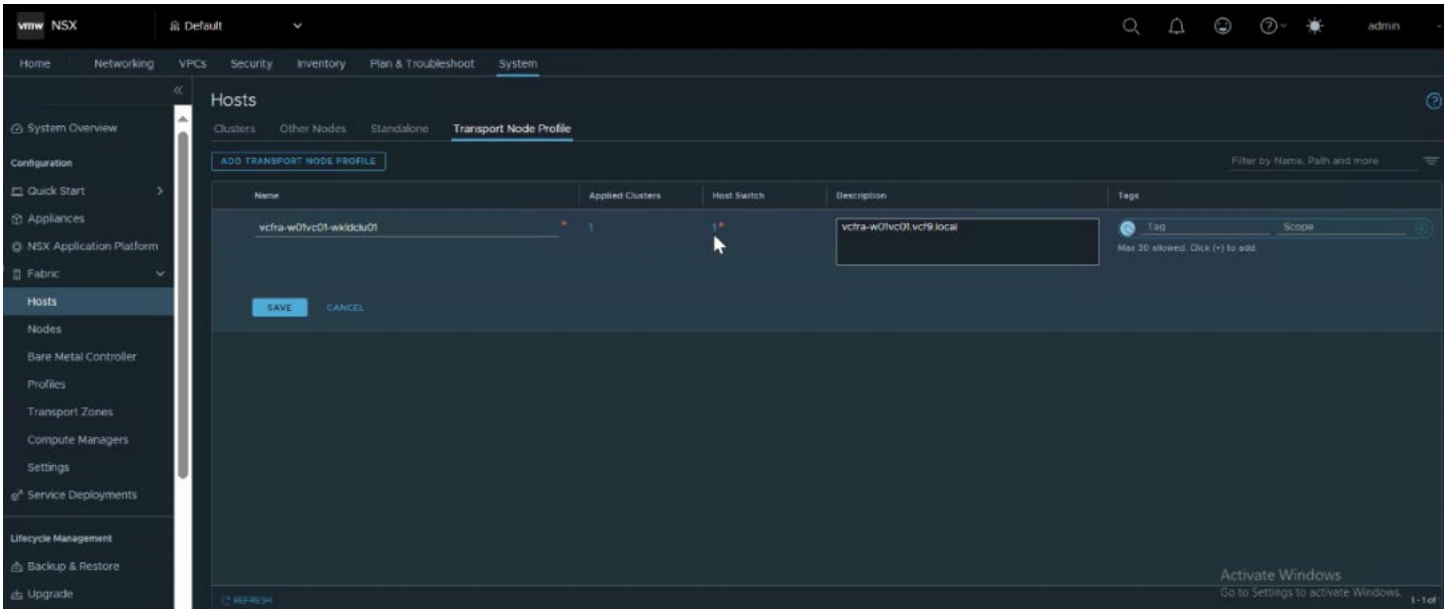

Figure 73. Edit Transport Node profile

6. In NSX **Manager --> Go to System --> Fabric --> Hosts -- Transport Node Profile.**
7. You will find the **workload Profile --> Click on 3 Dots --> Click Edit**.
8. Now Click **Host Switch** and can now see the properties on Host Switch.

9. If IPv4 Assignment shows DHCP for TEP, click 3 dots, **edit**.

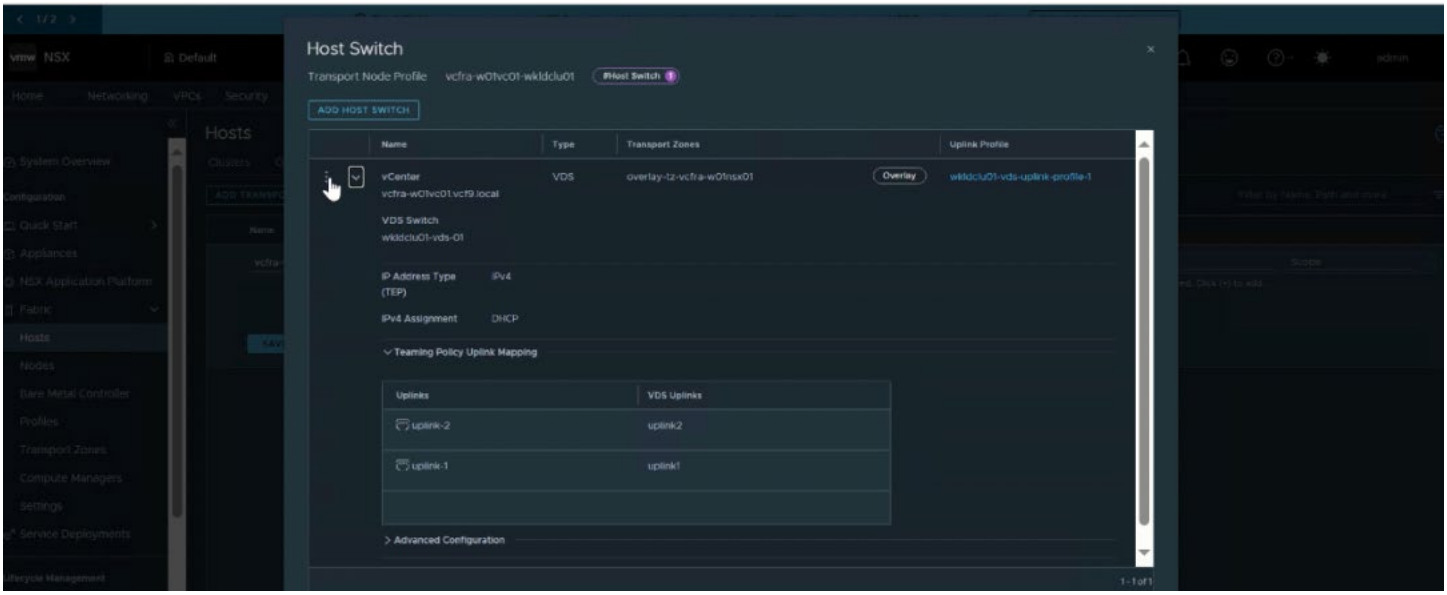

Figure 74. Update Host Switch .

10. Now, in the field, select Use IP Pool.
11. After IP Pool is selected, we have option to select IPv4 Pool which was created earlier in step.
12. Click **Add**.
13. Then Click **Apply** and **Save**.

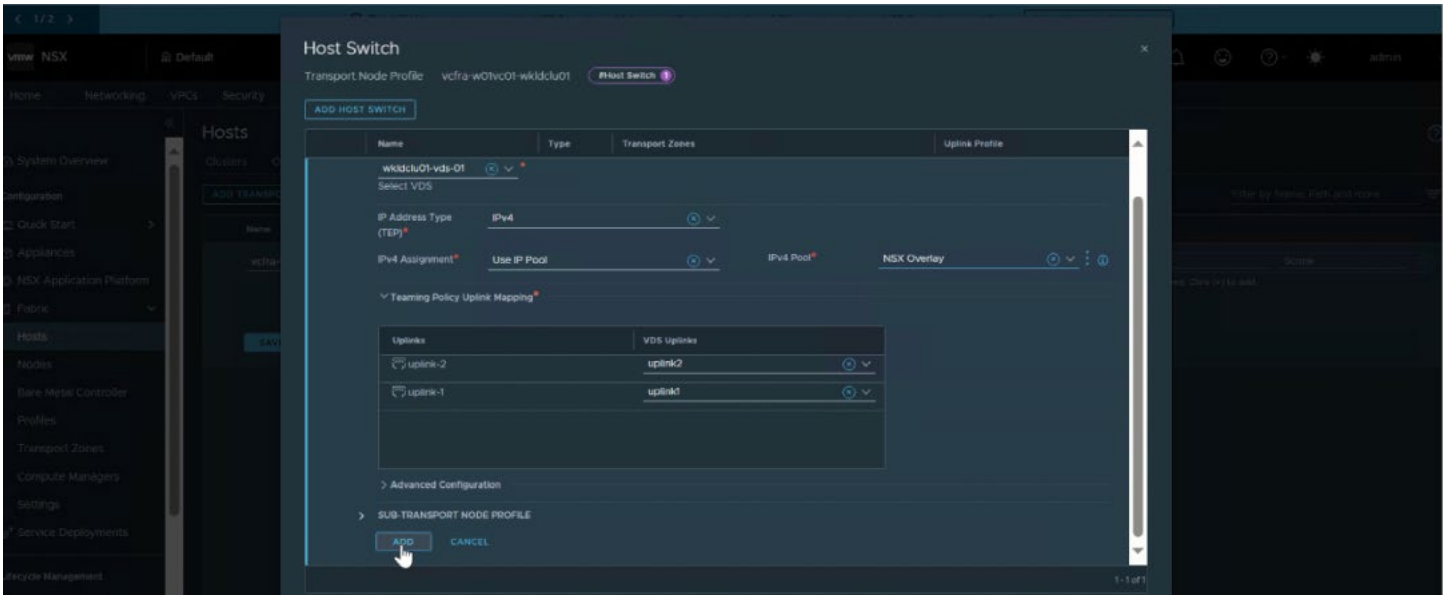

Figure 75. Select Use IP Pool and Range

14. Go to **Workload NSX Manager -->System--> Fabric --> Hosts**.

15. Select the Workload Cluster and Click **Configure NSX** to apply the changes.

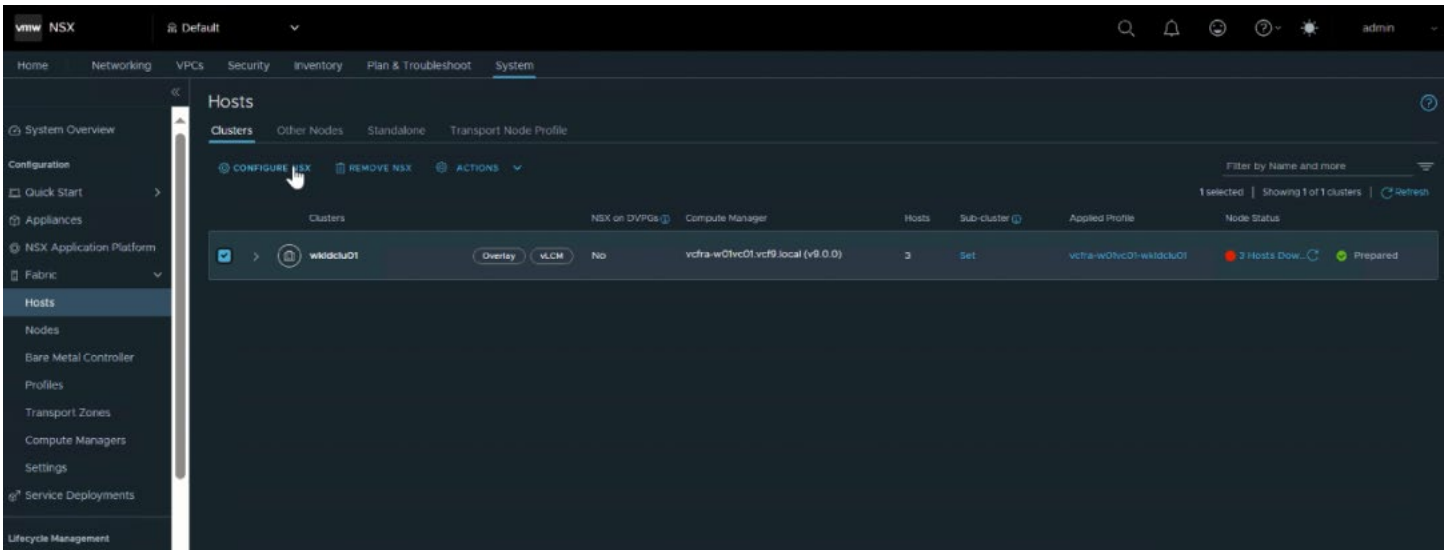

Figure 76. Configure NSX

16. Select the Correct workload Domain name and **SAVE**.

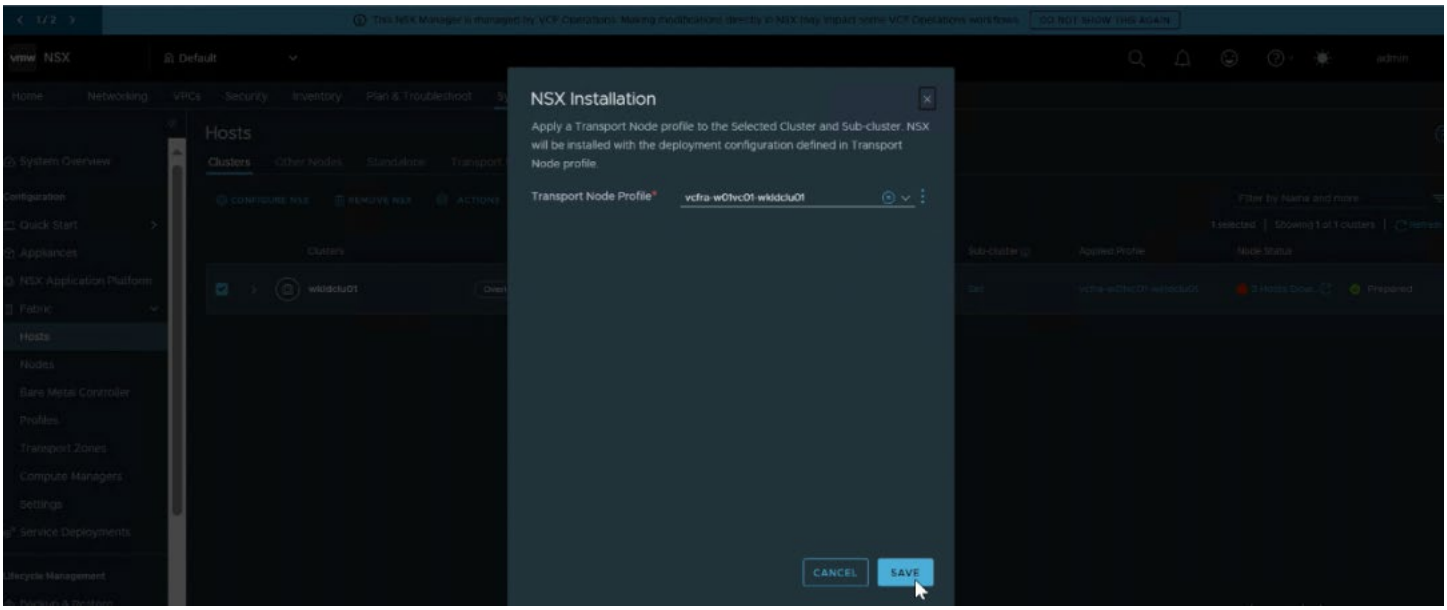

Figure 77. Select Transport Node profile for Workload Cluster

17. On the same page, wait for some time and node Status for all the Hosts in the respective workload Domain must show Green as show in below picture with Status as up. Depending on the number of Hosts in the workload Domain, this can take time.

18. After this is complete, we can proceed to the next stage.

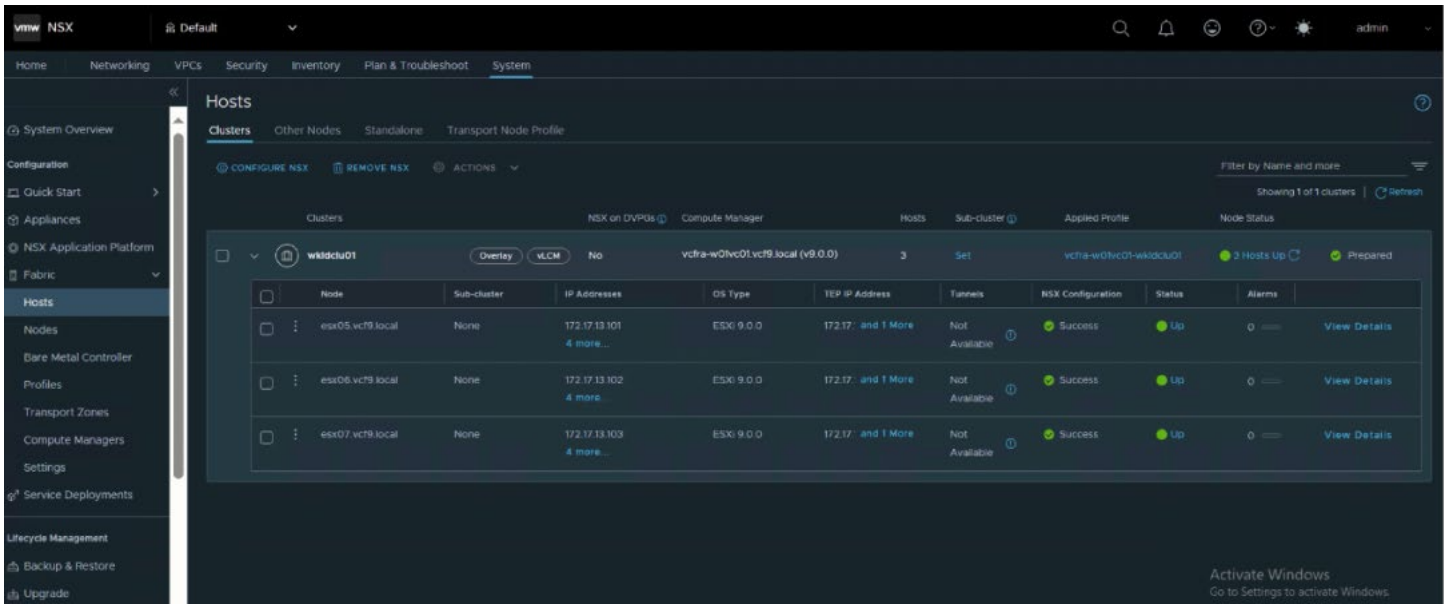

Figure 78. Check Node Status

Configure workload domain to be VPC-ready with a Centralized Transit Gateway

This section illustrates the configuration of a Centralized Transit Gateway to make the workload domain VPC-ready. The setup involves deploying NSX Edge clusters, which are required for centralized connectivity, and configuring BGP (Border Gateway Protocol) on the Top-of-Rack (ToR) network switches to establish routing between the physical and virtual infrastructure.

Note

Centralized Transit Gateway is required for deployment with a supervisor, and it is demonstrated in this reference architecture. If you intend to deploy a Distributed Transit Gateway instead, refer to the Configuring Network Connectivity with Distributed Gateway.

The following are the pre-requisites for configuring centralized transit gateway:

1. Two additional VLANs need to be configured on the TOR switches for NSX edge cluster deployment. The VLANs are configured as 'Uplinks' for VMware NSX edge nodes in the VMware Cloud Foundation workload domain. These uplinks will represent the NSX Edge VM uplinks to the physical ToR switch for North-South communication.
2. One extra VLAN for Edge Tunnel Endpoint (TEP) connectivity must be configured if NSX on DVPG is not activated on workload hosts.
3. VLANs configured as Edge uplinks do not have an active gateway configured since BGP Peering is not supported on Aruba active gateway interfaces. Instead, switch virtual interface IP is used for BGP peering in case of edge uplink VLANs.
4. The Autonomous System ID of the BGP instance on the Aruba switch is mentioned as <65001>. The edge cluster deployed as part of NSX deployment in the VMware Cloud Foundation workload domain has the BGP Autonomous System ID as <65010>. Both these BGP Autonomous Systems need to establish peering for North-South communication.

Note

Here sample ASN numbers are provided, but customers need to enter according to their BGP ASN numbering scheme.

Figure 79 shows the BGP peering between VMware Cloud Foundation edge VMs and Aruba top of rack switches. Diagram represents the edge VM to Aruba ToR peering with 2 NICs on the ESX host.

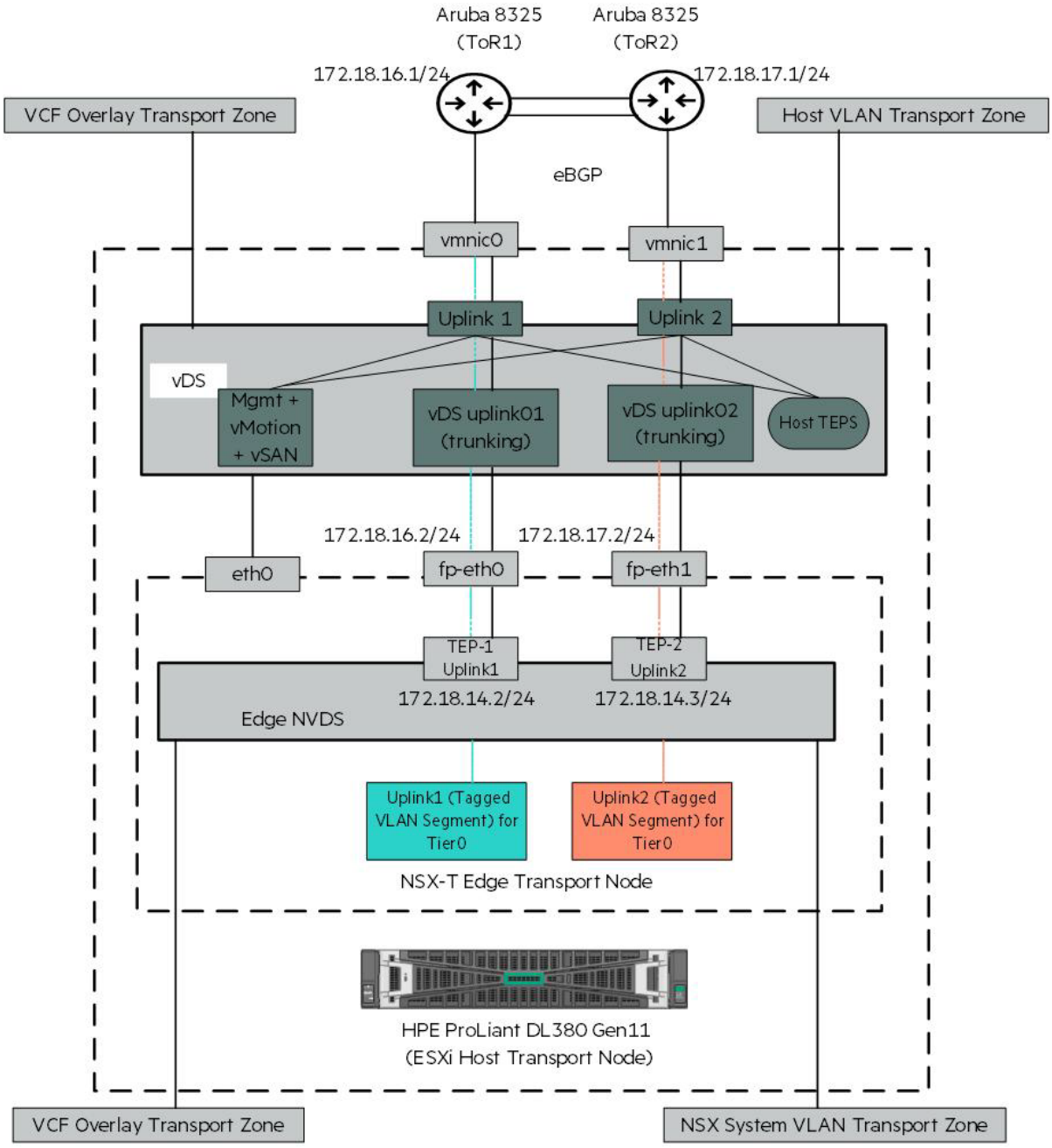

Figure 79. BGP peering between VMware Cloud Foundation edge VMs and Aruba top of rack switches.

Aruba Fabric Composer is used to configure the NSX Edge uplinks as BGP neighbors on the ToRs with Autonomous System ID 65001. Figure 80 shows the BGP configuration for VMware Cloud Foundation workload domain NSX edge cluster peering with 2 ToR Aruba CX 8325 Switches. After the edge cluster is successfully

deployed, the connectivity status of peers on Aruba CX 8325 TORs and NSX edge virtual machines will show as established.

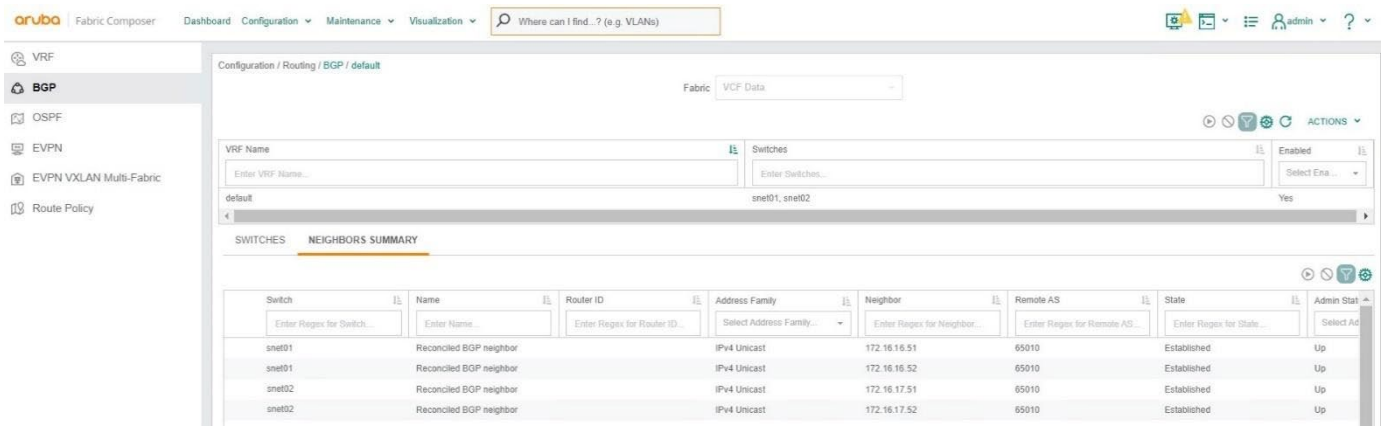

Figure 80. BGP peering configured between VMware Cloud Foundation workload domain edge VMs and Aruba top of rack switches through Aruba Fabric Composer

Activate NSX on DVPGs in NSX Manager

With VMware Cloud Foundation 9.0, Host TEP VLAN can be the same as Edge TEP by '[Activating NSX on DVPG]' on NSX Manager.

1. Log into workload NSX Manager UI for this workload domain.
2. Navigate to **System > Fabric > Hosts > Clusters** and select the cluster where the ESX are deployed.
3. Click **Actions** and select 'Activate NSX on DVPG'.
4. Click **YES** to continue.

Centralized transit gateway for the workload domain

The [centralized transit gateway] for the workload domain can be configured on the workload vCenter by the following steps:

1. Login to vSphere client and navigate to **Inventory > Network** view, select the vCenter for the workload domain.
2. Under the **Networks tab > Network Connectivity > Configure Network Connectivity**. Gateway configuration wizard will start.
   a. On the Gateway type page, select Centralized Connectivity.
   b. Check Select All network prerequisites page, click **Continue**.
   c. On the Edge Cluster page, Enter Name and Select Edge form factor as Large.
   d. Click **'Add'**, to deploy the first Edge node, Configure Edge Node wizard starts. Enter the configuration as needed and click **Apply**.
   e. Click **Add** to deploy the second Edge node. Configure Edge Node wizard starts. Enter the configuration as needed to establish peering and edge overlays and click **Apply**.

Figure 81 and 82 show the Edge node configuration details.

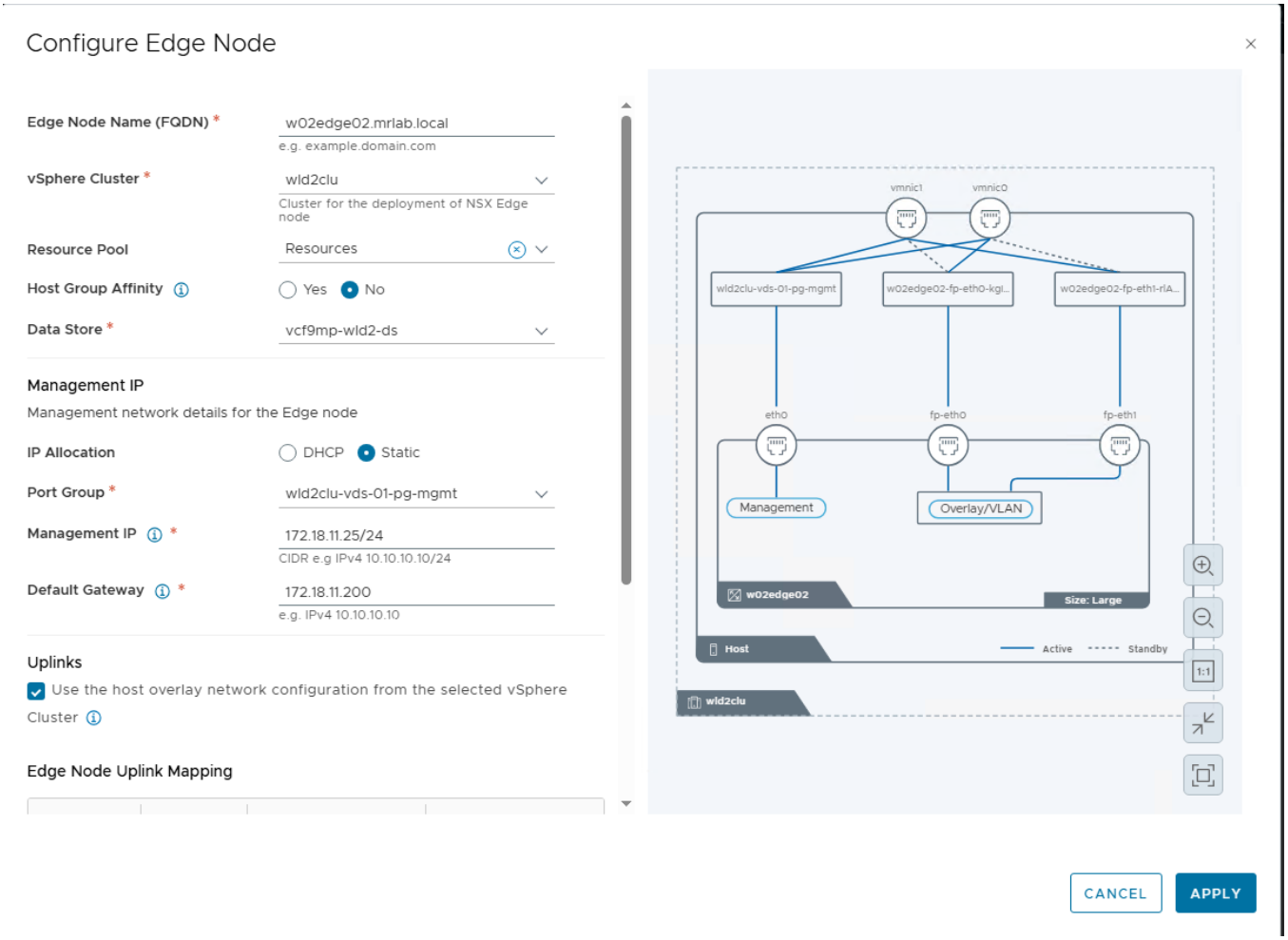

Figure 81. Edge node

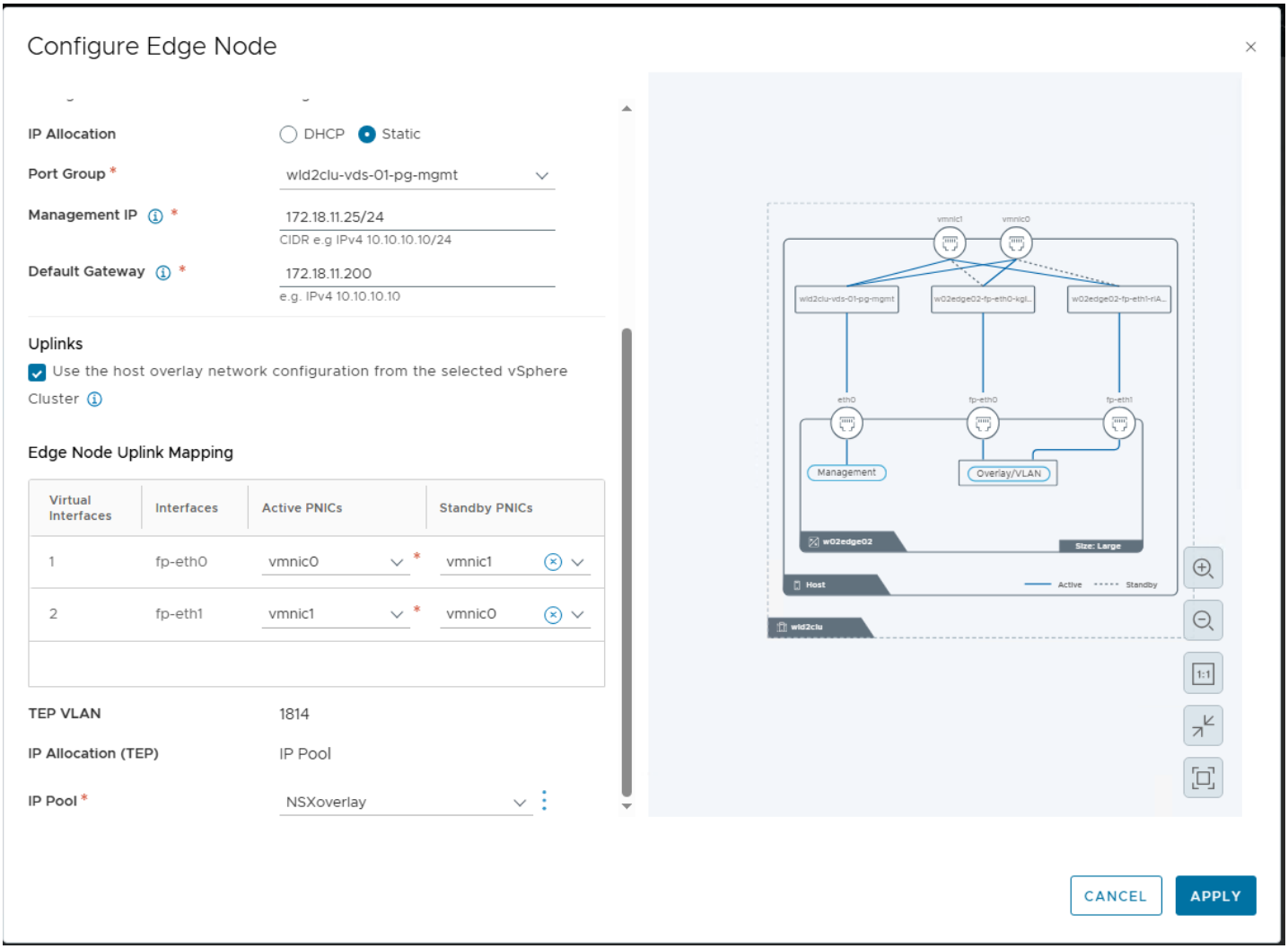

Figure 82. Edge node Uplink mapping

Workload Domain Connectivity configuration

1. Click **Apply.**
2. In the Workload Domain Connectivity configuration.
3. Enter Gateway Name.
4. Enter the Tier-0 Gateway Routing Configuration as needed for your deployment. BGP configuration is recommended.

Note

The Tier-0 gateway must be in active/standby HA mode to be used with supervisor Cluster and VCF Automation.

---

5. Click "**Set**" to configure each Edge Gateway Uplinks.
6. Configure Gateway Uplink - Enter the configuration for each Edge node first uplink and second uplink as required by the deployment.
7. Enter VPC External IP Blocks and Private - Transit Gateway IP Blocks, and then click **Next**.

Note

External IP blocks are used to create public subnets in the VPC, and private IP blocks are used to create private subnets in the VPC.

Figure 83 shows Tier0 gateway configuration details.

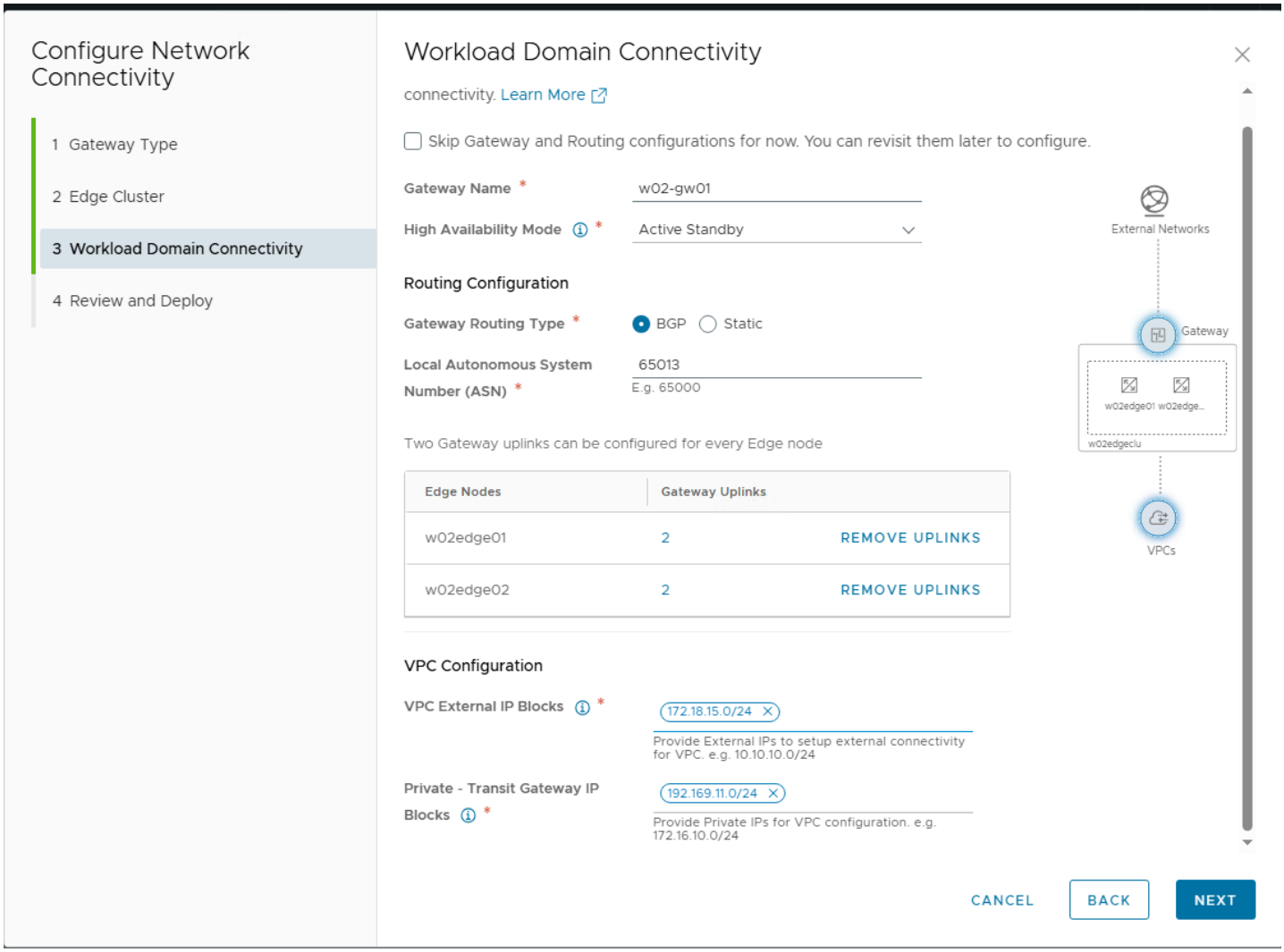

Figure 83. Tier0 gateway configuration

8. Review the configuration and deploy as shown in the following figure:

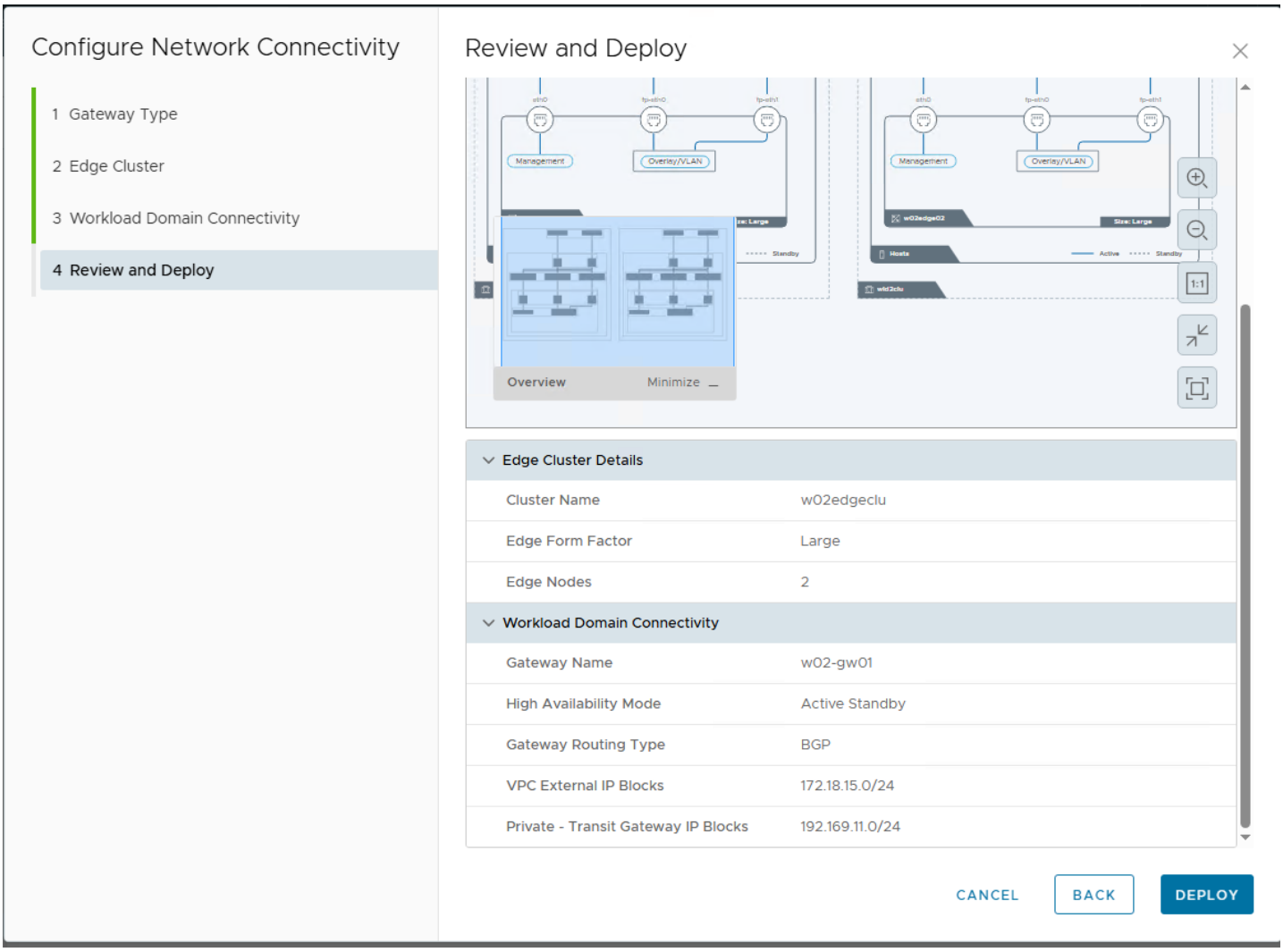

Figure 84. Tier0 Gateway configuration

9. The progress of the deployment of the Edge nodes and gateway can be tracked in the vCenter Tasks panel.
10. After the deployment is completed make sure that BGP neighbor state is shown as Established in NSX Manager Tier0 Gateway.

Note

Refer the Configuring Network Connectivity with Centralized Gateway to know more about the configuration.

Firmware update of workload domain using HPE OneView for VMware vCenter

With vLCM-based functionality enabled in VCF domains, firmware and driver updates are managed using a combination of HPE OneView, HPE OneView for VMware vCenter (OV4vC) and VMware vSphere Lifecycle Manager (vLCM). vLCM handles ESX upgrades and patching including hardware vendor drivers and value-add software, while OV4vC - through the integrated HPE OneView Hardware Support Manager (HSM) plug-in enables coordinated firmware updates during the same maintenance window, often with a single reboot. The HSM service is embedded within HPE OneView for VMware vCenter enabled by the OV4vC plugin integrated into the vCenter UI, streamlining server lifecycle operations across compute infrastructure.

Deploy and configure OneView

HPE OneView assists in compliance of the server hardware configuration in addition to applying firmware updates to the server utilizing HPE Smart Update Tools (SUT) included within the HPE Custom image and the vLCM HPE Addon depot. HPE OneView is deployed on the VMware Cloud Foundation management domain as a virtual machine. Once the networking configuration is set up on HPE OneView VM, import HPE ProLiant DL Servers of VCF management and workload domains to the HPE OneView using the server iLO IP address and credentials.

Create an associated server profile to apply consistency in server hardware configuration and the baseline firmware bundle based upon the Service Pack for ProLiant (SPP) as noted in the software and firmware matrix document.

The following are the steps to deploy HPE OneView appliance software:

The HPE OneView 10.0 appliance ova can be downloaded from My HPE Software Center. (Sign-in credentials using HPE Passport account is required).

1. Select the HPE_OneView_10.00.00_ESXi_Z7550-97956.ova from the list of possible downloadable files and download it.
2. Log in to vCenter Server in the VMware vSphere Foundation and right-click the Resource Pool and select Deploy OVF template to start the deployment wizard for deploying the appliance.

Installation	Action Needed
Select an OVF template	Select “local files” and point to folder. Select the “HPE_OneView_10.00.00_ESXi_Z7550-97956.ova” within the folder to deploy
Select a name and folder	Provide the HPE OneView Virtual Machine name: HPEOneView-10.00.00-0507518
Select a compute resource	Select the VMware vSphere Foundation cluster as a destination compute resource for this virtual machine
Review details	Check details of the appliance
Select Storage	Select VM storage policy as “vSAN default Storage policy”. Select VMware vSphere Foundation vSAN storage in the list of storage
Select network	From the destination network drop down select the VM network for OneView.

Installation	Action Needed
Ready to Complete	Review the details for the installation and click Finish to start the installation

3. After the HPE OneView appliance deployment is completed, from the vCenter Server start the OneView Appliance, launch the HPE OneView web console and enter the username as Administrator, password as Admin, and verify the HPE OneView UI opens successfully. Change the password when prompted.
4. Assign host name, IP address, Subnet Mask, gateway and DNS server details.
5. Open a browser connect to the OneView by typing the FQDN.
6. After the HPE OneView UI opens successfully, use the **Server > Server Hardware > Add server hardware option** to add all the HPE ProLiant Servers designated as VCG management domain and Workload domain cluster nodes. On the Add server hardware page provide HPE iLO IP address, iLO credentials, select HPE OneView Advanced, click Add.
7. Upload the firmware bundle listed in the FWSW matrix to OneView. To add the Firmware, on the Appliance click **OneView > Firmware > Firmware Bundle**. Click the **Add Firmware Bundle**. Browse and select the SPP ISO file and click **OK**. The SPP gets added and shows up under Firmware Bundles.

Note

Server hardware must be added as 'Managed' to HPE OneView using the HPE OneView Advanced license, enabling consistent hardware configuration through server profiles that standardize settings, firmware, and compliance across your infrastructure for enhanced reliability and scalability. For more information, refer to the HPE OneView User Guide. For more information refer to the HPE OneView User guide.

Deploying HPE OneView for VMware vCenter

HPE OneView for VMware vCenter provides server hardware management capabilities, including comprehensive monitoring, firmware update, vSphere/ESX image deployment, remote control, end-to-end monitoring for Virtual Connect, and power optimization for HPE servers in the VMware environment.

HPE OneView for VMware vCenter version 11.7 supports staging updates on the server. The staging process downloads the components from vSphere Lifecycle Manager to the ESX hosts without immediately applying the software and firmware. This process reduces the time that ESX hosts spend in maintenance mode during the schedule maintenance window.

VMware vLCM remediation requires a Hardware Support Manager (HSM) service to facilitate firmware updates on the servers. For HPE servers, the HSM service bundled with HPE OneView for VMware vCenter (OV4vC) leverages the firmware repository hosted on HPE OneView. The combination of these software components facilitates the firmware upgrade on all the hosts in the cluster.

The following steps outline the deployment of HPE OneView for vCenter 11.7 on VMware Cloud Foundation Management Domain:

1. HPE OneView for vCenter 11.7 appliance ova can be downloaded from https://myenterpriselicense.hpe.com/cwp-ui/product-download-info/Z7500-63235/-/sw_free?& (Sign-in credentials using HPE Passport account is required).
2. Select HPE_OneView_for_VMware_vCenter_11.7_June_2025_Z7550-04009 from the list of possible downloadable files and download it.

3. Extract the zip file to the folder as HPE_OneView_for_VMware_vCenter_11.7_June_2025_Z7550-04009.
4. Log in to vCenter Server in the VMware Cloud Foundation management domain and right-click the cluster and select Deploy OVF template to start the deployment wizard for deploying the appliance.

Table 10 shows the details of each screen and performs the required action.

Table 10. Deployment wizard actions for each screen

Installation	Action Needed
Select an OVF template	Select “local files” and point to folder “HPE_OneView_for_VMware_vCenter_11.7_June_2025_Z7550-04009” extracted. Select the “ov4vc-11.7.0.508437” within the folder to deploy
Select a name and folder	Provide the HPE OneView for vCenter Virtual Machine name
Select a compute resource	Select the VMware Cloud Foundation Management Domain cluster as a destination compute resource for this virtual machine
Review details	Check details of the appliance
License agreement	Accept the license agreement
Select Storage	Select VM storage policy as “vSAN default Storage policy”. Select VMware Cloud Foundation Management Domain vSAN storage in the list of storage
Select network	HPE OneView for VMware vCenter allows you to configure up to three networks. At least one network needs to be configured during deployment. Configure “Network 1” to the VMware Cloud Foundation management network during deployment. You may configure additional networks for redundancy or if the storage network is on a private network and vCenter on a public network. Configure additional networks from the Administrator Console post-deployment as needed. Refer to the Figure 64 for the networking configuration
Customize template	Provide IP Address, Subnet Mask, Default gateway, DNS server, and Fully Qualified Domain Name for the “Network Settings”
Ready to Complete	Review the details for the installation and click Finish to start the installation

Figure 85 shows the network configuration for HPE OneView for the VMware vCenter appliance.

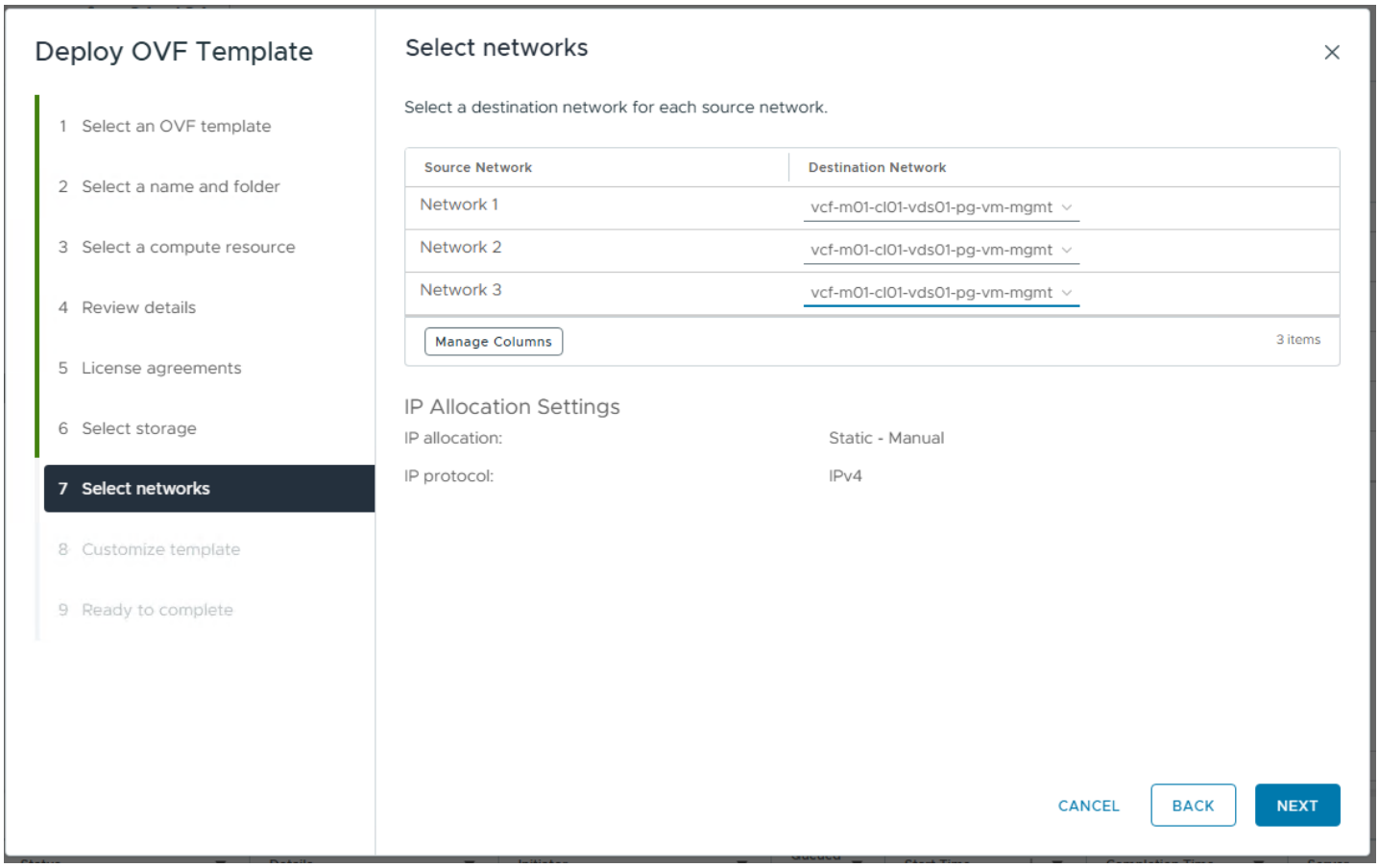

Figure 85. Network configuration for HPE OneView for VMware vCenter appliance

5. After the HPE OneView for vCenter appliance is deployed, power on the appliance and connect to the Administrator console using the appliance's fully qualified domain name (FQDN) or IP address as https://<<ApplianceHostnameIpaddress>>.
6. Click **Setup**. Enter a New Password and Confirm password and click **OK**.

7. Add VCF management domain vCenter to HPE OneView for vCenter. **Click Main menu -> Managers -> vCenters**. This will open the Add vCenter windows. Provide details of vCenter Fully Qualified Domain Namep(FQDN) and credentials.

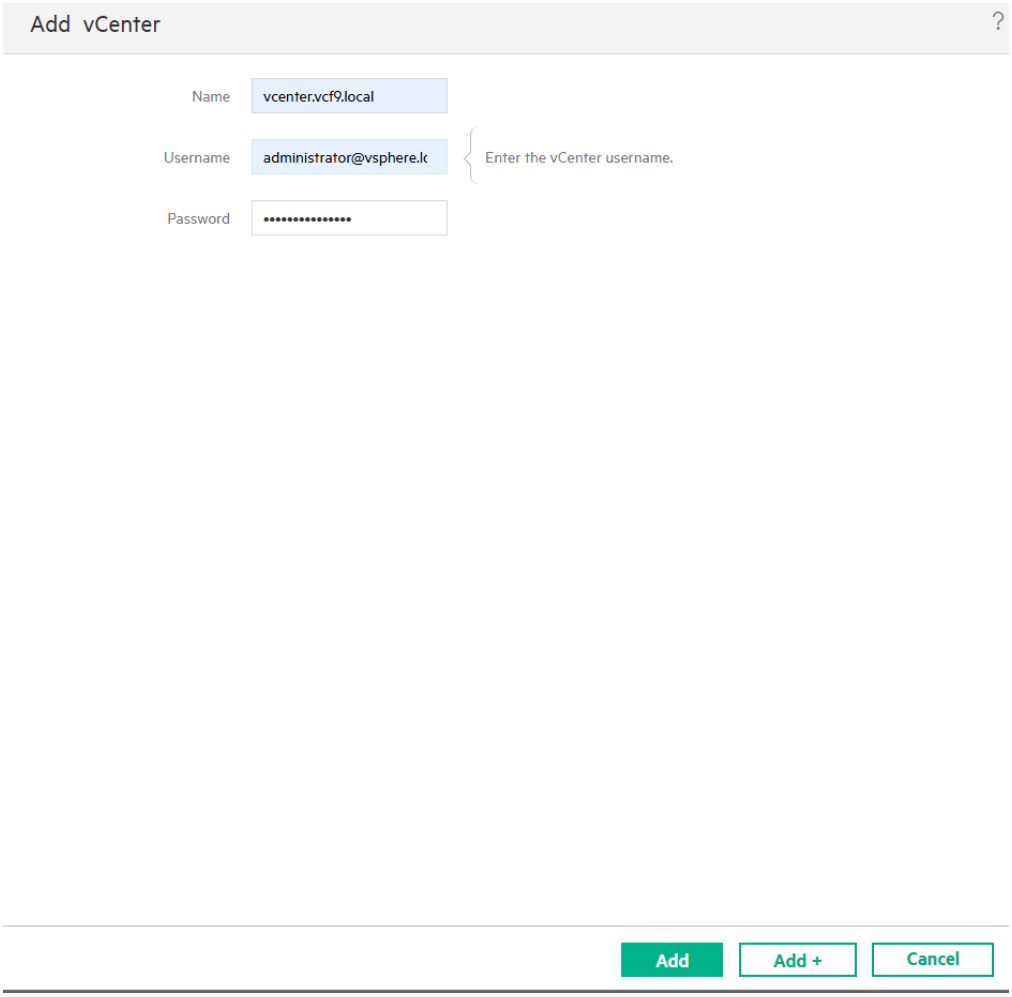

Figure 86. Add vCenter through HPE OneView

This task will install a plug-in into the vCenter UI. Refresh the vCenter UI browser tab if open while the plugin was being installed.

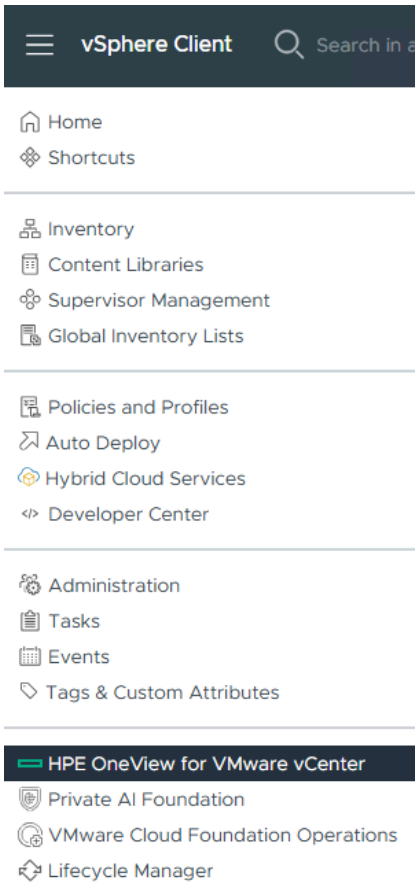

Figure 87. HPE OneView for VMware vCenter plugin

8. Register HPE OneView IP and Credentials within HPE OneView for the vCenter plug-in on the VCF Management domain vCenter.
9. Login to VCF Management domain vCenter and select the HPE OneView for VMware vCenter as shown in Fig xx. Click **HPE OneView Credentials** to provide FQDN and Credentials for HPE OneView. Click **TEST**. On the credential test Success screen, click **SAVE**.

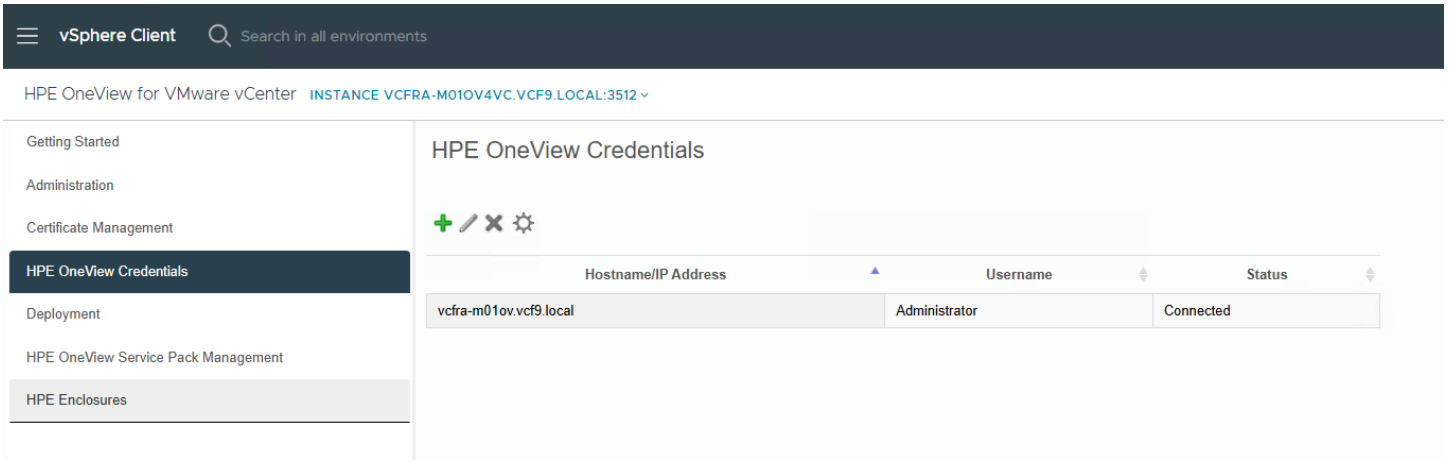

Figure 88. HPE OneView Credential through HPE OneView for vCenter plugin

10. Add the HPE OneView for VMware vCenter certificate to VMware Cloud Foundation management domain vCenter, **vSphere Client > HPE OneView for VMware vCenter > HPE OneView Service Pack Management > Add Certificate**. After Certificate is added click **REGISTER** tab to register the HPE SPP software through HPE OneView Service Pack Management plugin.

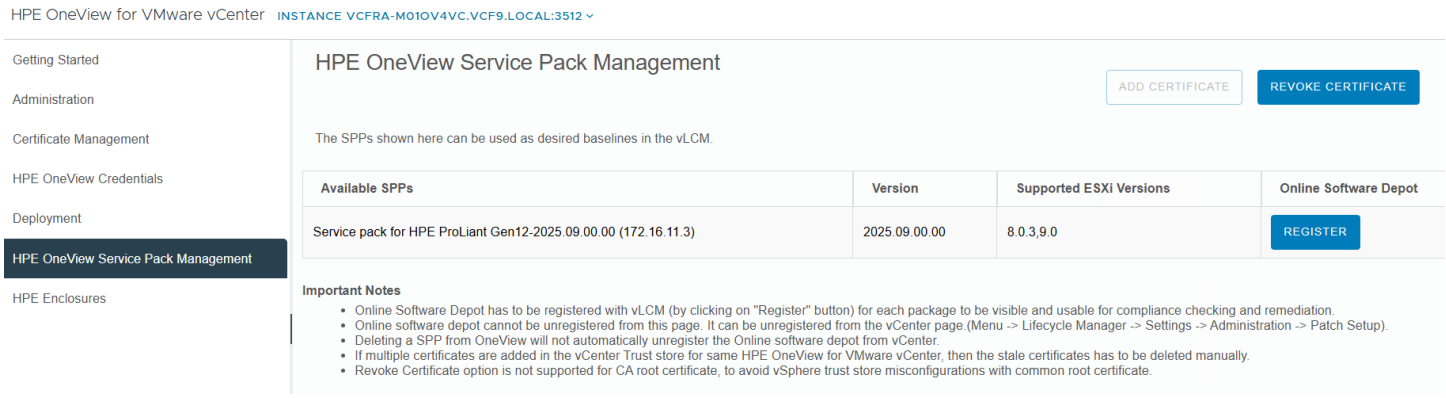

Figure 89. Add Center and REGISTER SPP

11. Configure the management domain vCenter certificate in the HPE OneView, **OneView > Settings >Security> Manage Certificates > Add certificates**.

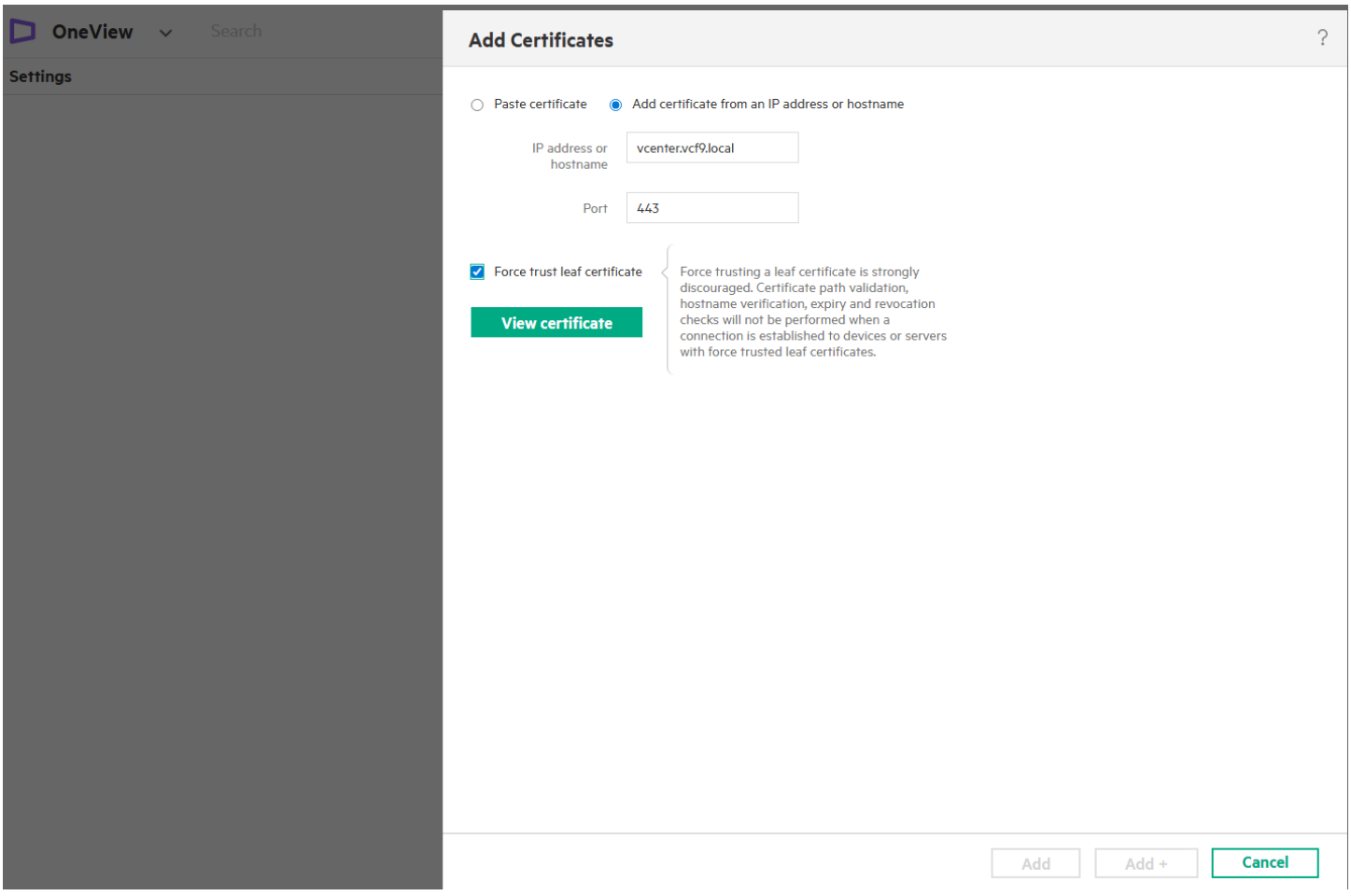

Figure 90. Add vCenter Certificate through HPE OneView

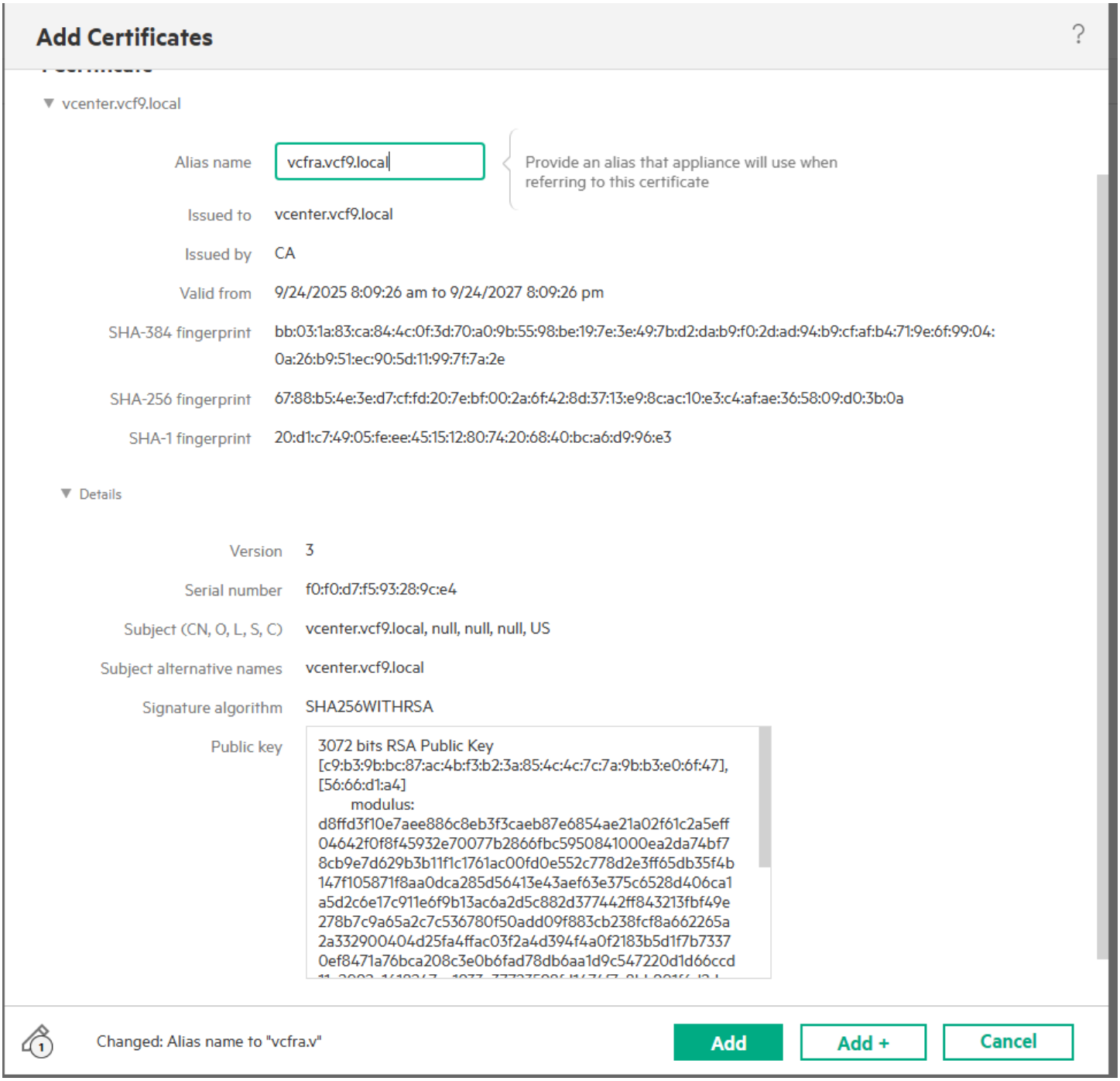

Figure 91. vCenter certificates details

Set-up Intelligent System Update Tool and Agentless Management Service accounts to enable vSphere Lifecycle Manager -based firmware updates on HPE Gen12 servers.

HPE Gen12 servers introduce enhanced security by supporting only High Security modes (SecureStandard, CNSA, FIPS). This impacts how you configure Intelligent System Update Tool (iSUT) and Agentless Management Service (AMS) for vSphere Lifecycle Manager (vLCM) based firmware updates.

Following are the pre-requisites to create iSUT and AMS accounts

— Access to server CLI or DCUI.

— ILO Virtual NIC should be enabled

Please refer Configuring the Virtual NIC feature (iLO 7 Web Interface) in this document for enabling ILO Virtual NIC. After ILO Virtual NIC is enabled ILO reset and Server reboot is needed so that ILO Virtual NIC is discovered with ESXi Host.

The following steps describe how to create iSUT and AMS accounts to enable vLCM-based firmware updates on HPE Gen12 servers:

1. Open the **iLO GUI > HPE iLO 7 HTML5 IRC > ESXi DCUI. > press F2 > Troubleshooting Options** and press Enter > Highlight Enable ESXi Shell and press **Enter** to enable it > Press Esc to return to the main DCUI menu.
2. Press Alt + F1 to switch to the ESXi Shell command line, log in as root user and run the following command to configure Application and Agentless Management Service (AMS) accounts.
   a. Run the following command to create an application account on iLO7 using CLI. Application accounts are used by host applications (like iSUT and AMS) to securely authenticate and communicate with iLO.

      ```
      sut appaccount create -u <ilo_username> -p <ilo_password>
      ```

   b. Set the iSUT mode to AutoDeploy to enable automated firmware updates:

      ```
      sut -set mode=AutoDeploy
      ```

   c. Configure AMS Application Account (for VMware)

      ```
      /opt/amsdv/bin/amsdCli appaccount create -u <iLO_username> -p <iLO_password>
      ```

5. Log out of the root user account, and to return to the DCUI, press Alt + F2. Post configuration Disable ESXi Shell (optional).
6. Verify Application Account in iLO. Open the iLO GUI >Navigate to iLO Settings > User Management > Users > Under Application Account Confirm the application account details are present.
7. Check AMS status in iLO GUI. Open the iLO GUI > Dashboard >Host Overview > Ensure AMS status is reported as Available.
8. Verify iSUT and AMS status in vCenter. Log in to **VMware vSphere > select the required cluster > configure tab > HPE Server Hardware > from the drop-down menu select vLCM Pre-Check > under vSphere LifeCycle Manager Pre-Check > click the gear icon > on the Configure Hosts page**, under Common Hosts Password > provide the ESX credentials > Click **Submit** and wait for the task to complete.

9. The status of iSUT state and AMS state should be compliant (green).

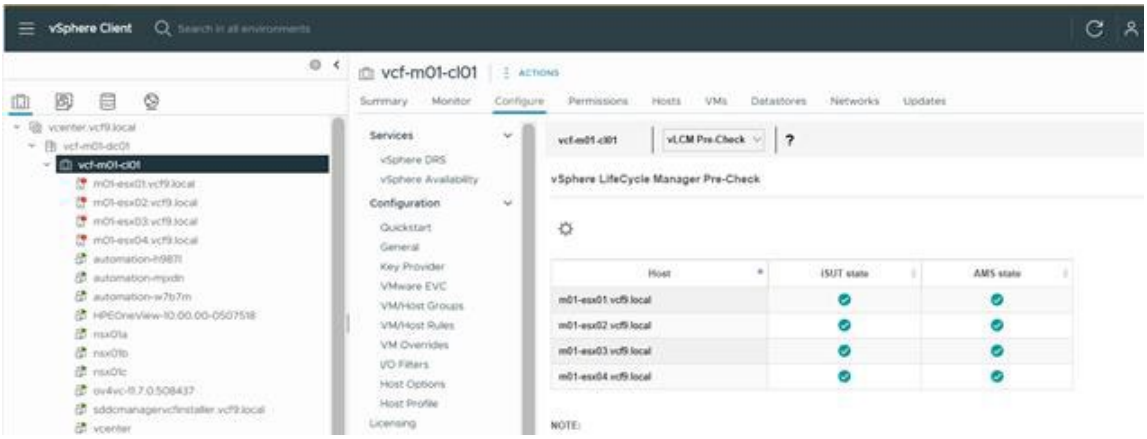

Figure 92. vLCM Pre-check through vCenter

vLCM Cluster image

A vLCM desired image definition is a specification of the software, components, vendor add-on, and firmware to be applied on all hosts in vSphere clusters in VMware Cloud Foundation Workload Domains.

vLCM Cluster image components for HPE ProLiant DL server-based workload domain as shown in Figure 64 consist of the following files as mentioned in Table 11. It is important to note the versions detailed are relevant to VMware Cloud Foundation 9.0 and will change depending upon the VMware Cloud Foundation build versions. For detailed software and firmware versions, refer to the software and firmware matrix documentation at HPE Firmware and Software Compatibility Matrix for VMware Cloud Foundation 9.0. To view a list of recommended combinations, refer to vLCM Desired Image Definitions for ProLiant.

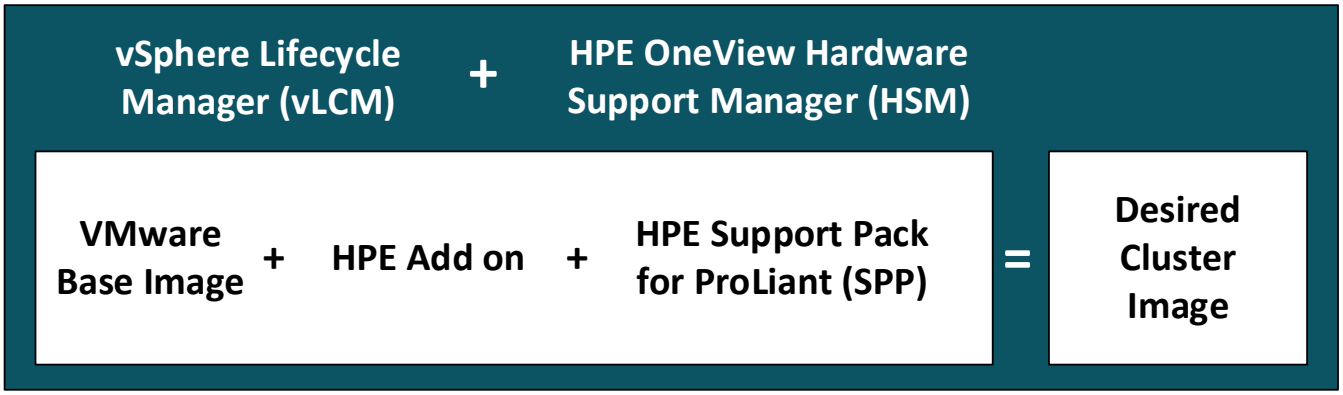

Figure 93. vLCM Cluster Image components

Table 11. vLCM image components

Name	Image file
VMware Base Image	VMware-ESXi-9.0.0-24813472-depot.zip
HPE Add-On	HPE-900.0.0.12.2.0.0.4-oct2025-Addon-depot.zip
HPE Service Pack for ProLiant (SPP)	P87830_001_gen12spp-2025.09.00.00-Gen12SPP2025090000.2025_0924.18.iso

Workflow for remediating the cluster

During DayN operations, opportunities arise to update the vSphere base image, vendor drivers and/or firmware. Updating all the hosts in the cluster using a single desired state specification of a vLCM cluster image and firmware maintains a homogeneous cluster environment and updates occur to software and firmware in a single remediation workflow and thus reducing downtime.

Figure 94 shows the approach for remediating a VMware Cloud Foundation cluster with the vLCM desired cluster image initiated by an updated release of the SPP.

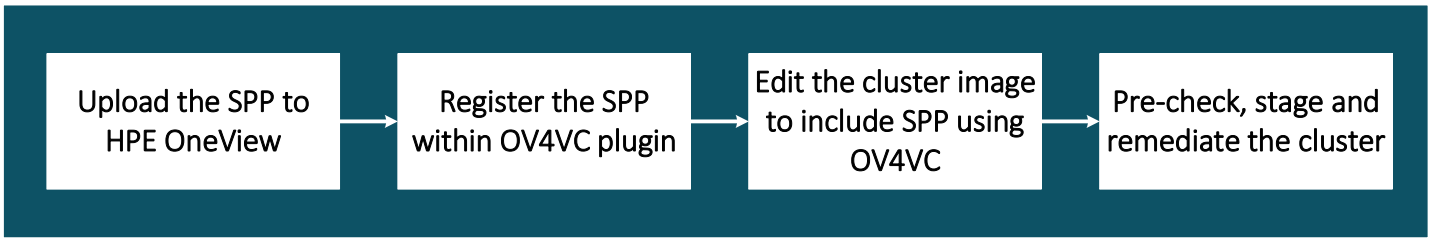

Figure 94. Flow diagram for vLCM based VMware Cloud Foundation workload domain remediation

The following are the overview steps to remediate the cluster with the desired cluster image. The same steps can be followed for both management and workload domain clusters:

1. Upload the Support Pack for ProLiant (SPP) package to HPE OneView main menu > Firmware > Firmware Bundles > Add Firmware Bundle.
2. Register the uploaded package using HPE OneView for VMware vCenter plug-in in vCenter and wait for the "Sync Updates" task to complete. vSphere Client > HPE OneView for VMware vCenter > HPE OneView Service Pack Management >. The "Sync Updates" task is populating the vCenter database with the metadata of the SPP updates for the supported vSphere versions. Select the cluster to be updated and open the Updates submenu.
3. Provide a unique name to identify this image definition in the image library.
4. Update the cluster image with desired components for ESX version, Vendor Addon, Firmware, and Drivers Addon leveraging the recommended vLCM combinations document as needed.

5. Validate the image components are available in the vCenter updates library and save the image.

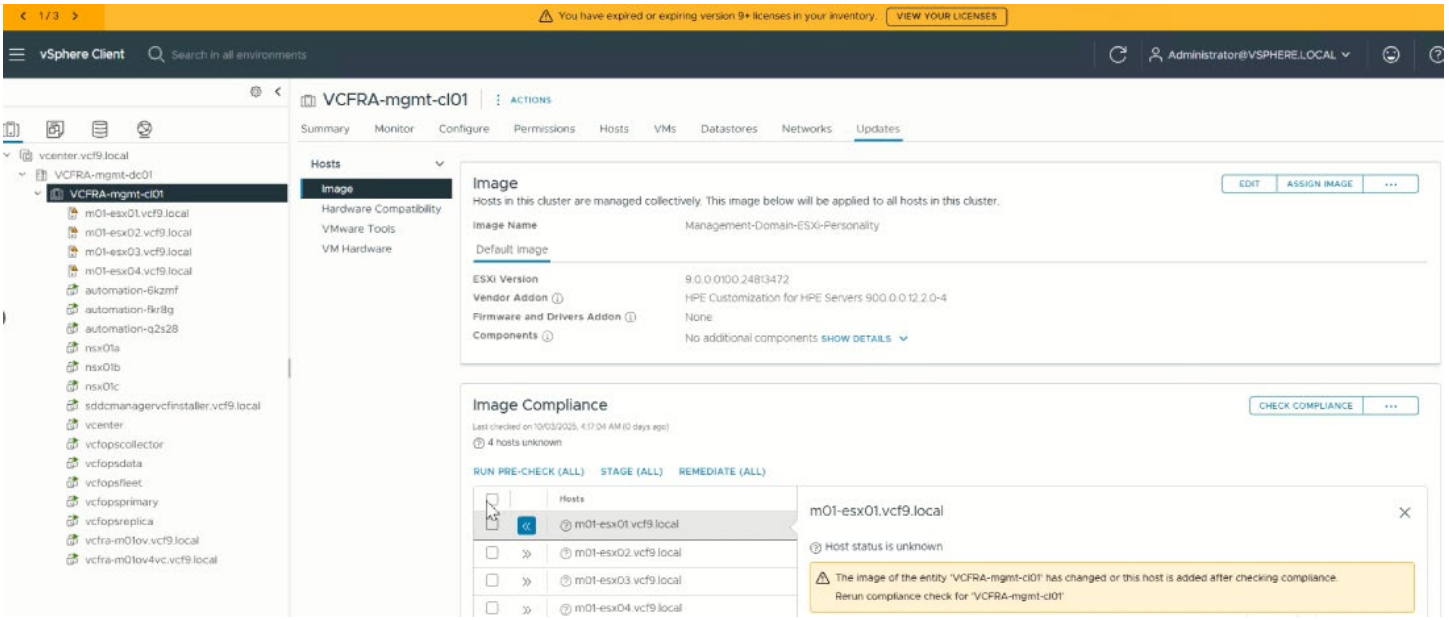

Figure 95. vLCM Cluster Image components chosen in vCenter when remediating cluster

6. After the image is saved, the Image Compliance check should automatically initiate to determine if the hosts in the cluster are compliant with the newly defined desired state image. If any of the hosts are not compliant, additional options for PRE-CHECK, STAGE and REMEDIATE the VMware Cloud Foundation cluster with new image will appear.

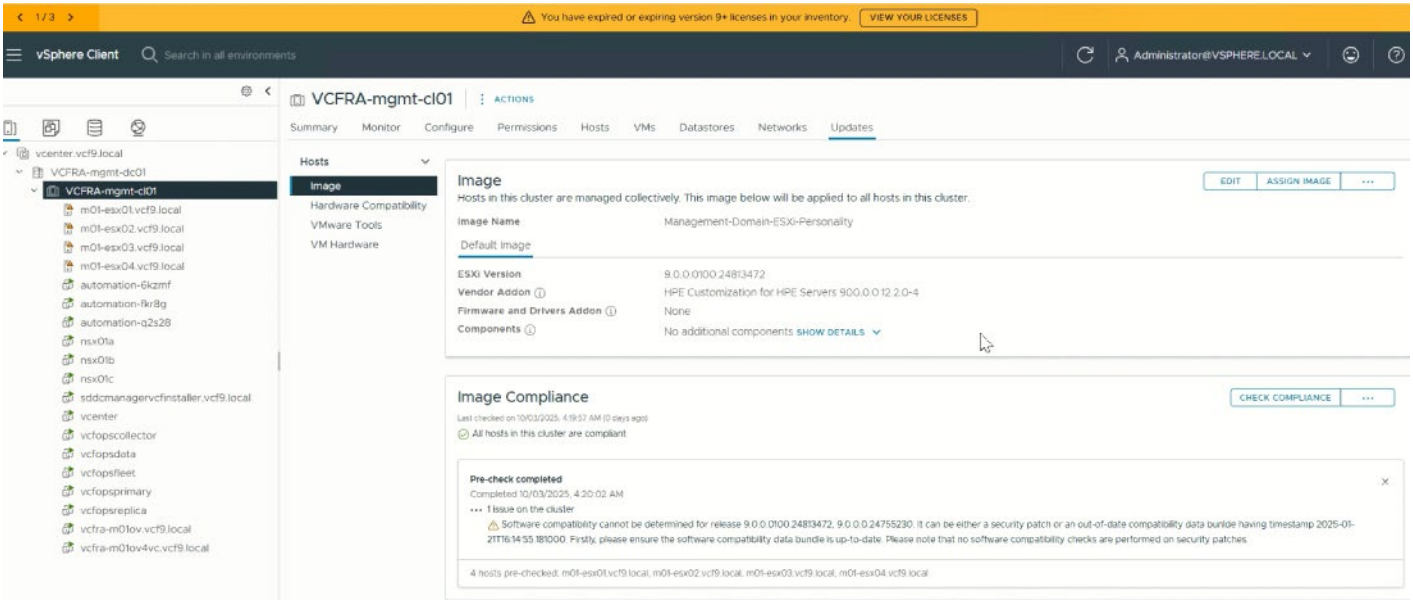

Figure 96. Host compliance check

Note

When updating the Vendor Addon or Firmware bundle in this environment, the remediation would be initiated by either the stage and/or remediate options. Refer to Remediating a Cluster or a Standalone Host Against an Image documentation for more information.

In a VCF environment, the remediation is initiated by the VCF Operations Fleet Management Lifecycle if there is an updated vSphere base image. For more information, refer to the Lifecycle Management chapter of the VCF documentation specifically Managing vSphere Lifecycle Manager Images for VMware Cloud Foundation.

Cluster Remediation using VCF Operations

To provide a consistent view of available resources in the VCF environment, utilize the VCF Operations Fleet Management Lifecycle subsystem to make the updated cluster image available to multiple domains. In this example, the remediation is necessary due to a vSphere ESX patch in a VCF environment utilizing the online VMware depot. The patch is included in a new cluster image definition which includes the appropriate vendor Addon components.

1. In VCF Operations UI, browse to Fleet Management > Lifecycle.
2. Expand VCF Instances and select the VCF instance.
3. Select Binary Management.

   Verify the VCF version and select Patch Binaries and verify the vSphere ESX patch has been downloaded. If the patch is not in the list, click **SYNCHRONIZE NOW** in the ESX Components subsection. Once the patch appears in the table with a Download Status of Pending, select the patch and click **DOWNLOAD**.

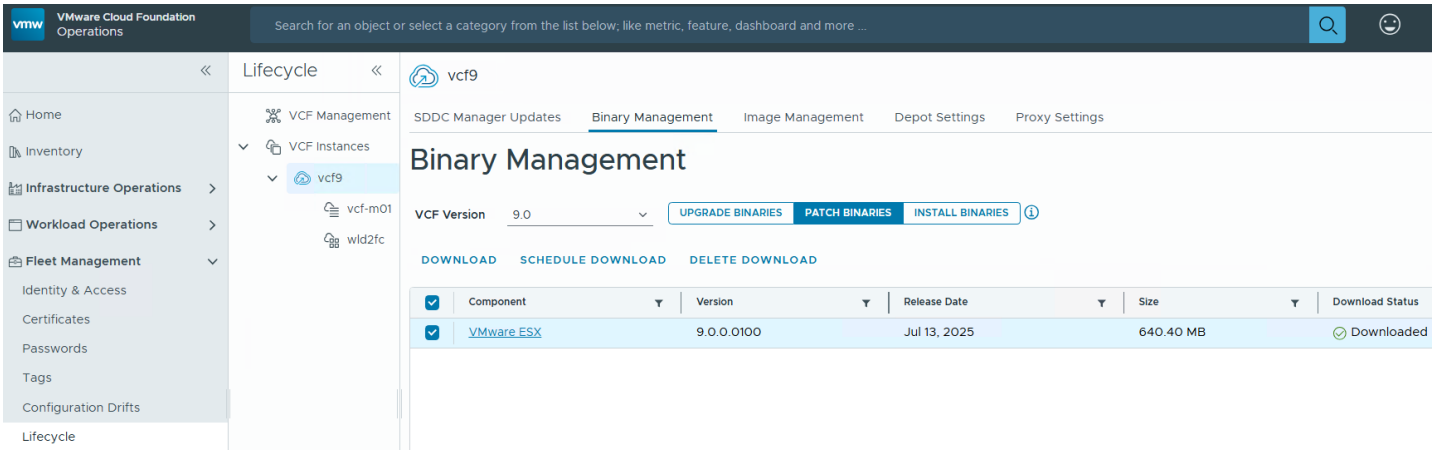

Figure 97. New patch binary

4. Select **Image Management > Import Image**.

5. Select Import from a vCenter and choose the vCenter which contains the newly defined cluster image.

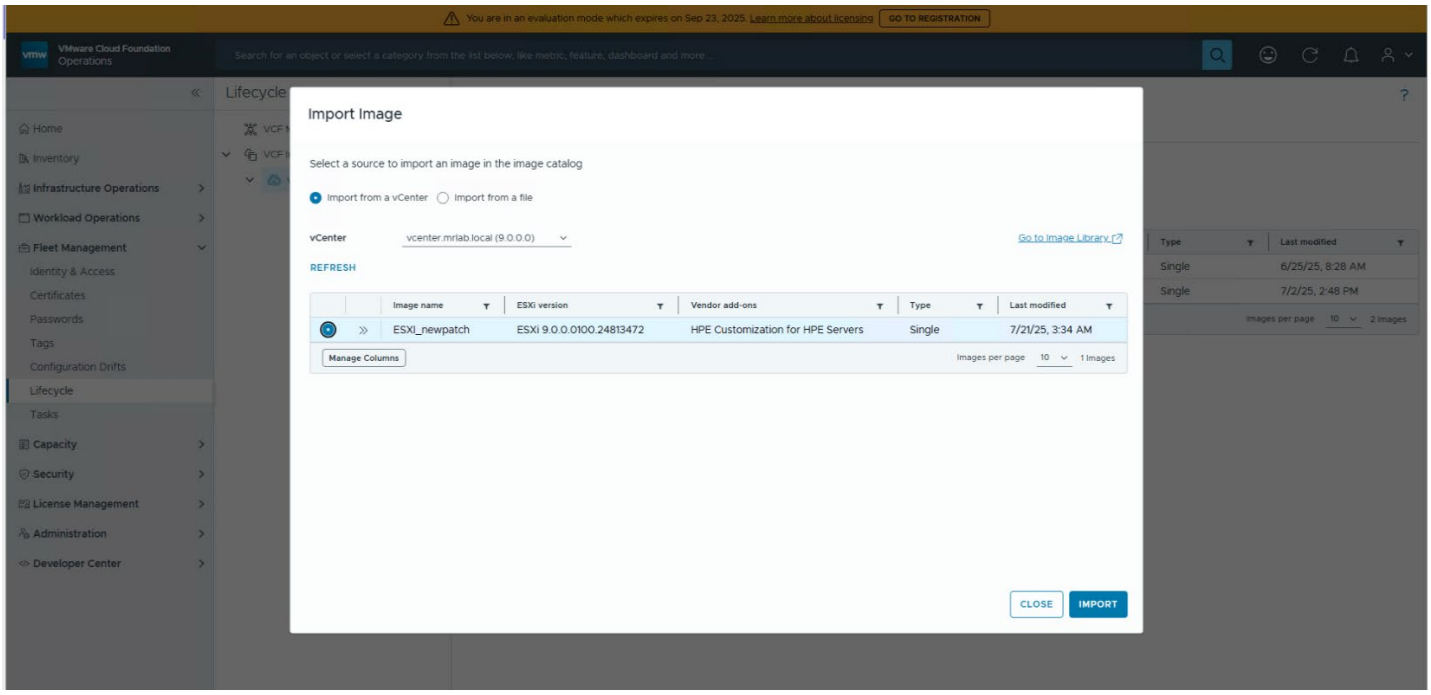

Figure 98. New Cluster image with HPE Add on

6. Select the image and click **IMPORT**. Wait for the completion of the import task. Monitor the import task via the **Fleet Management > Tasks**. If the updated cluster image has not yet been defined, click **Go** to Image Library to define the new image in the vCenter UI.
7. Select the domain to be updated from the expanded **VCF Instances > VCF Instance listing**.
8. Run the Precheck to ensure the domain has a general upgrade readiness. Review any warnings and errors to be resolved before proceeding.

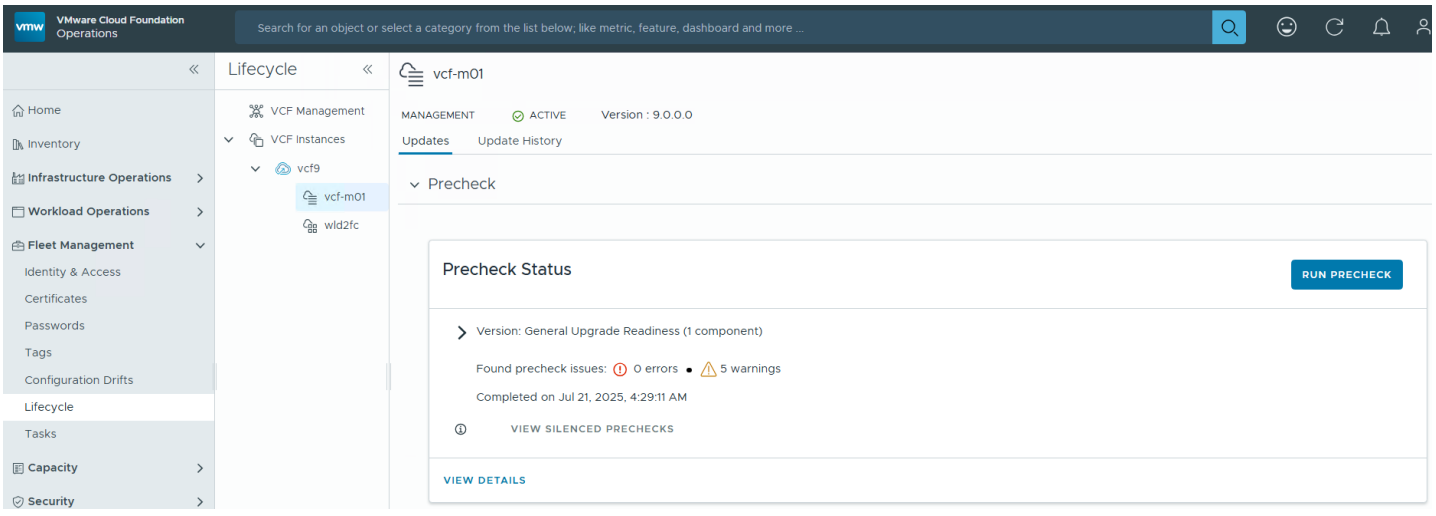

Figure 99. check Update Readiness of the cluster

9. Select **PLAN PATCHING** in the Available Updates section.

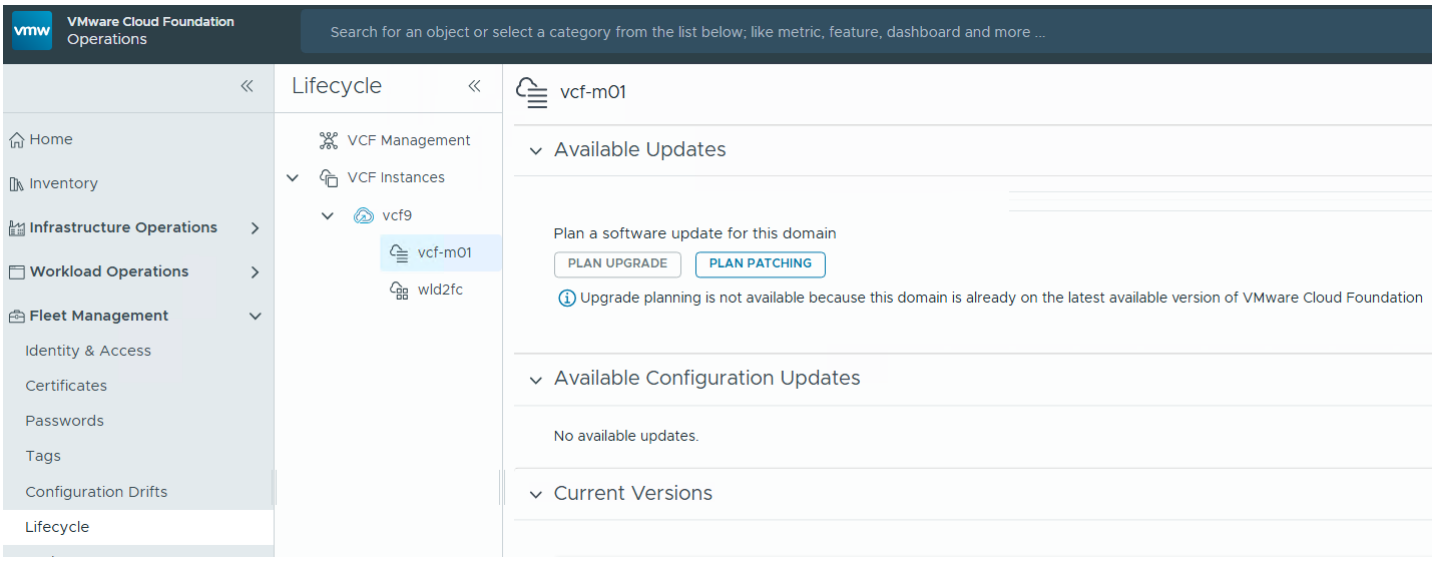

Figure 100. Plan patching

10. Select the vSphere ESX patch which was downloaded previously and is the base image of the defined cluster image and click **CONFIRM.**

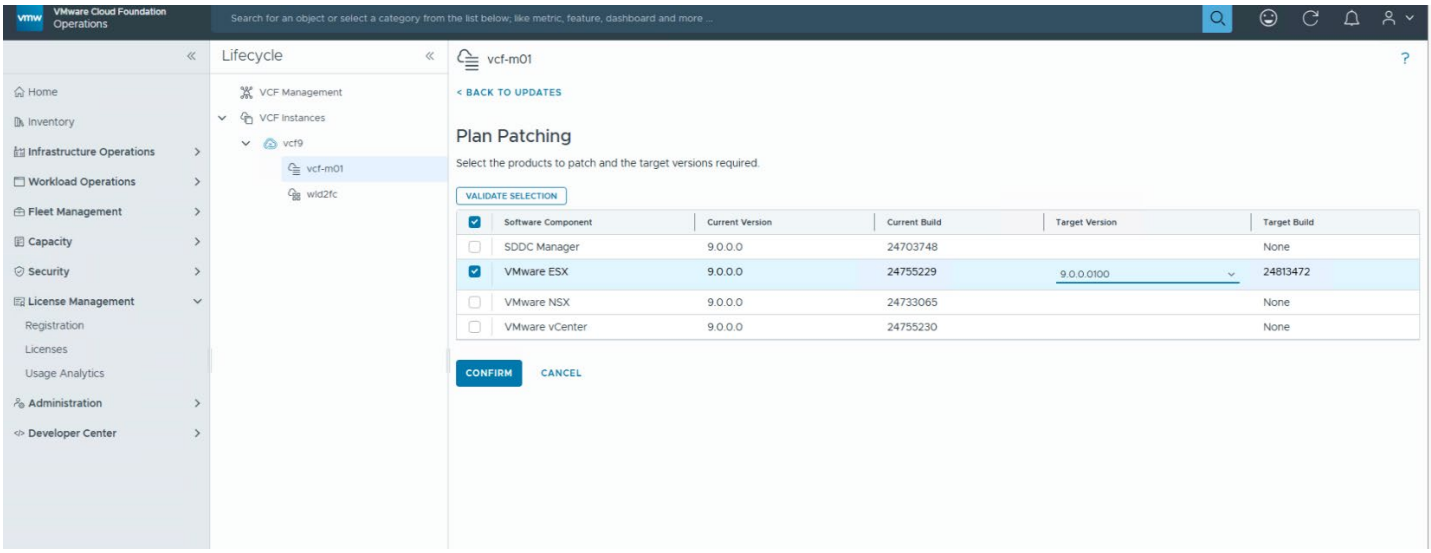

Figure 101. Plat patching confirmation

11. Click **configure update** under Available Updates section.

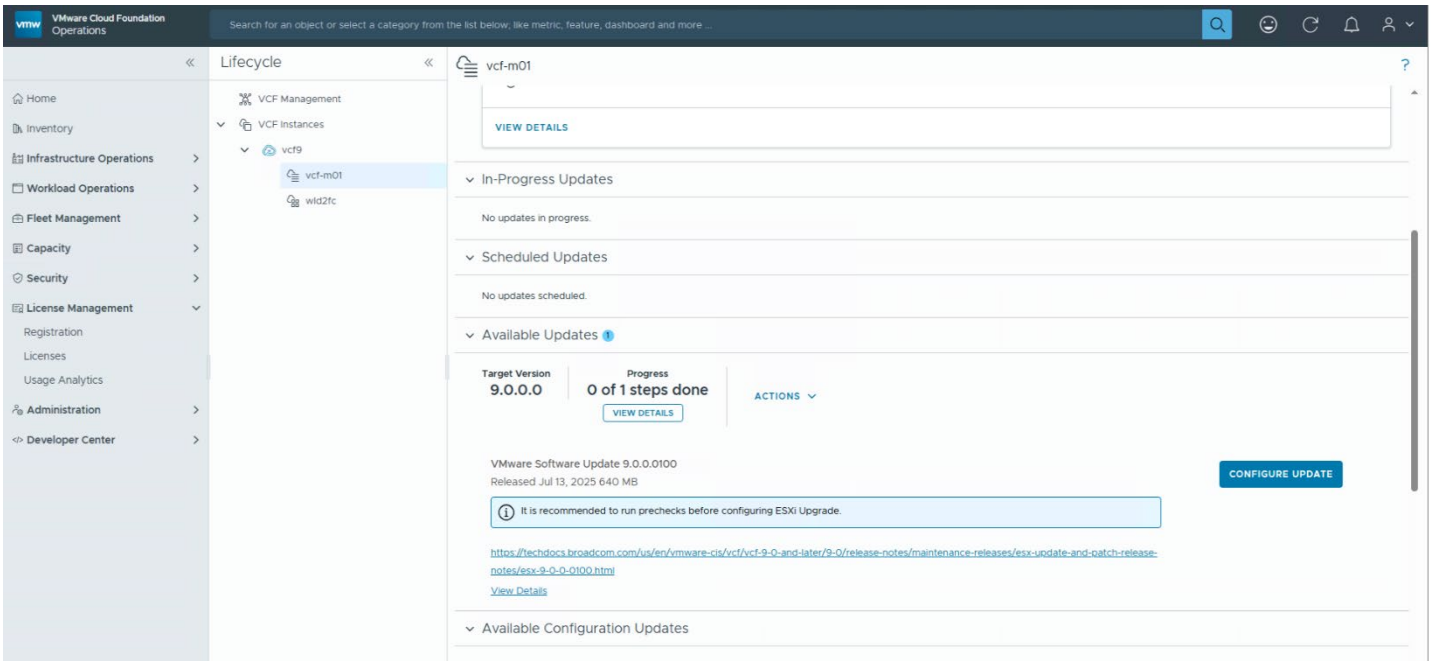

Figure 102. Configure Update

12. Provide all the details to Configure Update workflow and click **RUN PRECHECK**.

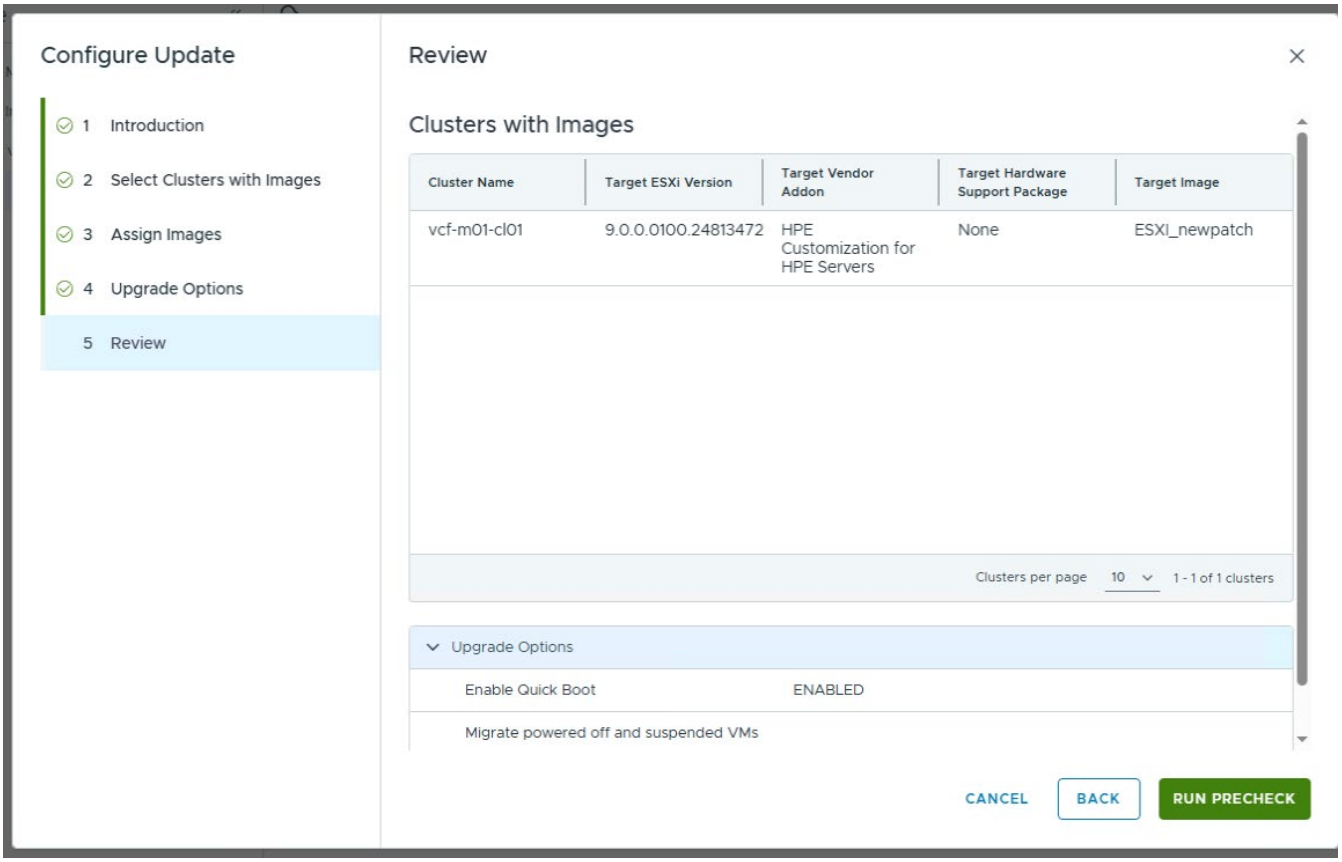

Figure 103. Configure Update workflow

13. Precheck is in progress as follows:

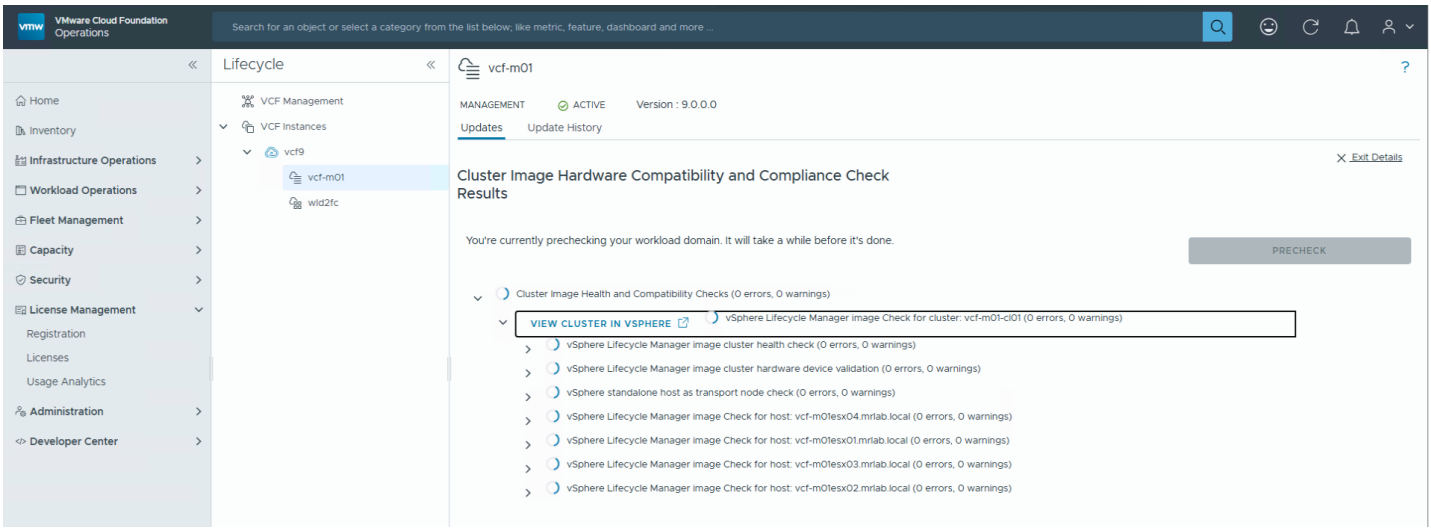

Figure 104. Precheck is in progress

14. Schedule update, shown as follows:

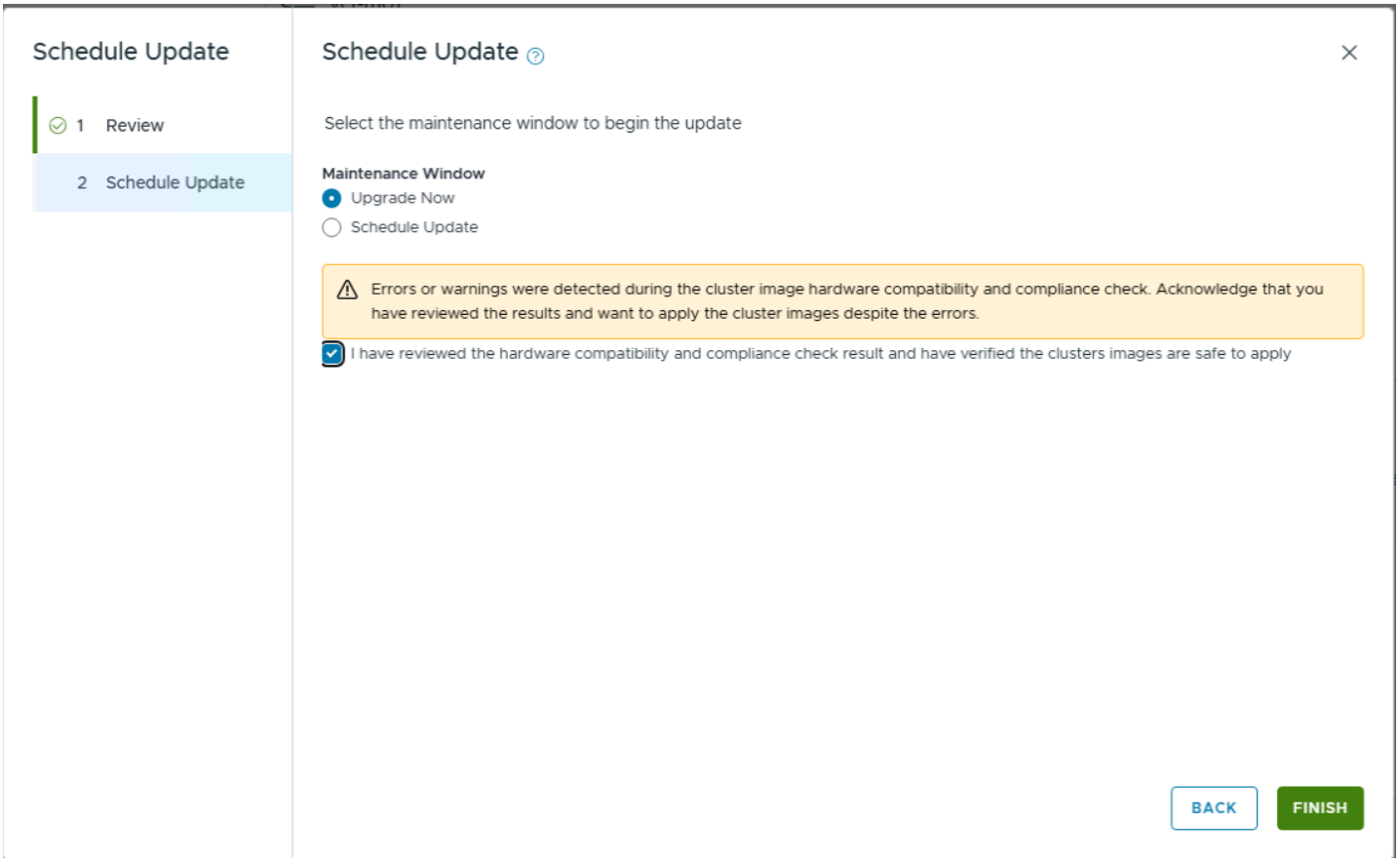

Figure 105. Schedule update

15. Verify patching and remediation was successfully completed as follows:

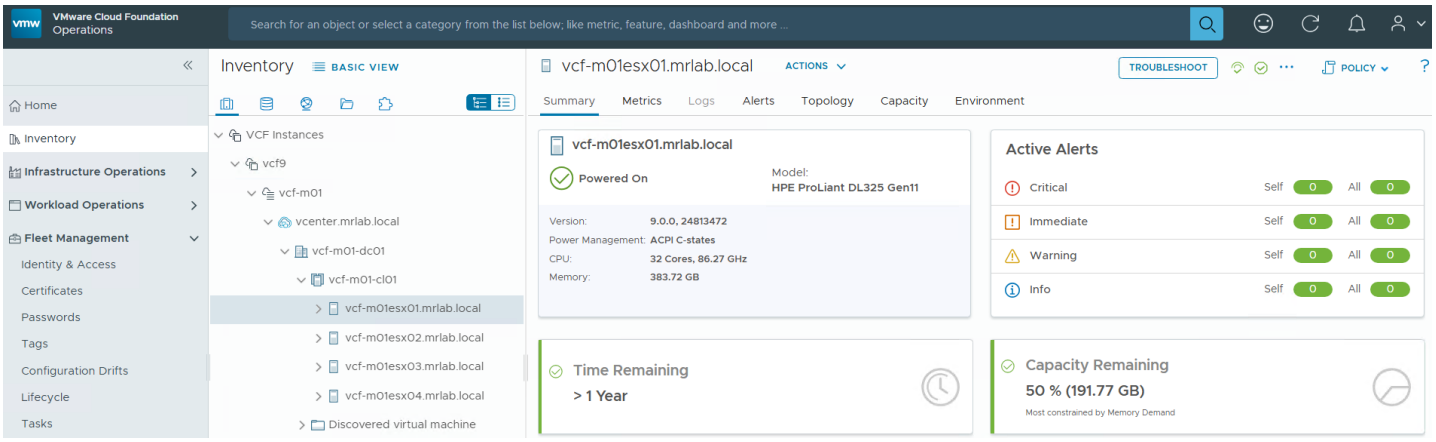

Figure 106. ESX version showing new build number

Summary

This reference architecture validates the deployment of VMware Cloud Foundation (VCF) 9.0 on HPE ProLiant Gen12 servers using two supported storage configurations—vSAN Express Storage Architecture (ESA) for hyperconverged deployments and HPE Alletra Storage MP B10000 over Fibre Channel (FC) for external storage. It outlines a complete, enterprise-ready hybrid cloud solution, detailing design choices, implementation steps, and operational guidance across compute, storage, and networking layers.

Key highlights include:

— Flexible Storage Architecture: Choose between high-performance NVMe-based vSAN ESA or Fibre Channel–attached HPE Alletra MP B10000 storage depending on business needs and existing infrastructure.

— Lifecycle Automation: Integration of vSphere Lifecycle Manager (vLCM) with HPE OneView for VMware vCenter (OV4vC) via Hardware Support Manager (HSM) enables coordinated patching of firmware, drivers, and ESX during a single maintenance window.

— Network Orchestration: Aruba Fabric Composer (AFC) automates and visualizes the deployment of Aruba CX 8325 (data) and 6300M (OOB) switches, simplifying VLAN, VSX, and MC-LAG configuration.

— Workload Domain Support: Includes detailed steps for bringing up workload domains with vSphere Supervisor, NSX, and centralized gateway configurations using BGP peering for VPC-ready connectivity.

The design was tested and validated in September 2025, offering a proven configuration baseline for the fresh install of hybrid cloud deployments. This architecture ensures a scalable, automated, and operationally consistent hybrid cloud platform—optimized for both traditional enterprise IT and modern cloud-native workloads.

Appendix A: Bill of materials – vSAN ESA

Table A1 lists the hardware utilized for testing and developing this Reference Architecture.

Note

Part numbers are at the time of publication and subject to change. The bill of materials does not include complete support options or complete rack and power requirements. For questions regarding ordering, consult with your Hewlett Packard Enterprise Reseller or Hewlett Packard Enterprise Sales Representative for more details. http://www.hpe.com/us/en/services/consulting.html.

Table A1. Bill of materials

Product	Quantity	Product description
		Rack and Power
P9K40A	1	HPE 42U 600mmx1200mm G2 Enterprise Shock Rack
P59419-B21	2	Enlogic by nVent G3 Metered Switched 3-phase 22kVA/Outlets (24) C13 (24) Combo C13/C19 PDU for HPE
P9L11A	1	HPE G2 Rack Grounding Kit
P9L12A	1	HPE G2 Rack Baying Kit
P9L12A B01	1	HPE G2 Rack Baying Kit
P9L16A	1	HPE G2 Rack 42U 1200mm Side Panel Kit
P9T01A	1	HPE G2 PDU Environmental Temperature and Humidity Sensor
P9T02A	1	HPE G2 PDU Environmental 3 Temperature and 1 Humidity Sensor
P9T03A	1	HPE G2 PDU Open Door Sensor
120672-B21	1	HPE Rack Ballast Kit
BW930A	1	HPE Air Flow Optimization Kit
BW930A B01	1	Include with complete system
BW932A	1	HPE 600mm Rack Stabilizer Kit
BW932A B01	1	HPE 600mm Rack include with Complete System Stabilizer Kit
		Management hosts
P73282-B21	4	HPE ProLiant Compute DL380 Gen12 SFF NC Configure-to-order Server
P73282-B21 ABA	4	HPE DL380 Gen12 8SFF NC CTO Svr
HA454A1-001	4	HPE FE ProLiant Svr Pkg 4 SVC
P74573-B21	8	Intel Xeon 6730P 2.5GHz 32-core 250W Processor for HPE
P69727-B21	128	HPE 32GB (1x32GB) Dual Rank x8 DDR5-6400 CAS-52-52-52 EC8 Registered Smart Memory Kit
P75740-B21	4	HPE ProLiant Compute DL3XX Gen12 8SFF x1 U.3 Tri-Mode Drive Cage Kit
P63871-B21	8	HPE 1.6TB SAS Mixed Use SFF BC Self-encrypting FIPS 140-2 PM7 SSD
P75741-B21	8	HPE ProLiant Compute DL3XX Gen12 8SFF x4 U.3 Tri-Mode Drive Cage Kit

Product	Quantity	Product description
P50230-B21	32	HPE 3.2TB NVMe Gen4 High Performance Mixed Use SFF BC U.3 PM1735a SSD
P48802-B21	4	HPE ProLiant DL380 Gen11 2U x8/x16/x8 Secondary Riser Kit
P48803-B21	4	HPE ProLiant DL380 Gen11 2U x16/x16/x16 Primary Riser Kit
P47785-B21	4	HPE MR216i-p Gen11 x16 Lanes without Cache PCI SPDM Plug-in Storage Controller
P42041-B21	8	Mellanox MCX631432AS-ADAI Ethernet 10/25Gb 2-port SFP28 OCP3 Adapter for HPE
P44712-B21	8	HPE 1800W-2200W Flex Slot Titanium Hot Plug Power Supply Kit
P78145-B21	8	HPE C13 - C14 250V 10Amp 2m FIO Power Cord
E5Y43A	4	HPE OneView for ProLiant DL Server including 3yr 24x7 Support FIO Bundle Physical 1-server LTU
P72205-B21	4	HPE ProLiant Compute DL3XX/ML350 Gen12 CPU2 to Rear OCP SlotB x8 Cable Kit
P76453-B21	4	HPE ProLiant Compute DL380 Gen12 8SFF SFF x4 UMB PCIe Box 1/2 Cable Kit
P76461-B21	4	HPE ProLiant Compute DL380 Gen12 8SFF x4 Direct Attach Box 1 for 2 Processors Cable Kit
P77489-B21	4	HPE ProLiant Compute DL380 Gen12 8SFF x4 Direct Attach Box 2/3 for 1P Cable Kit
P48820-B21	4	HPE ProLiant DL380/DL560 Gen11 2U High Performance Fan Kit
P48922-B21	4	HPE ProLiant DL3XX Gen11 Intrusion Cable Kit
P08040-B21	4	HPE iLO Common Password FIO Setting
P42104-B21	4	HPE ProLiant Platform Certificate and IDevID iLO FIO Setting
P52341-B21	4	HPE ProLiant DL3XX Gen11 Easy Install Rail 3 Kit
P73325-B21	4	HPE ProLiant Compute Localization FIO Kit
P74792-B21	8	HPE ProLiant Compute DL380 Gen12 Performance Heat Sink Kit
P77931-B21	4	HPE ProLiant Compute DL380 Gen12 16SFF x4 Direct Attach Balanced FIO Bundle Kit
P79552-B21	4	HPE ProLiant Compute 30C System Inlet Ambient Operating Temperature Configuration Tracking
C7536A	4	HPE 4.3m/14ft CAT5 RJ45 M/M Ethernet Cable
845420-B21	4	HPE QSFP28 to 4x25Gb SFP28 7m Active Optical Cable
		Workload hosts
P73282-B21	4	HPE ProLiant Compute DL380 Gen12 SFF NC Configure-to-order Server
P73282-B21 ABA	4	HPE DL380 Gen12 8SFF NC CTO Svr
HA454A1-001	4	HPE FE ProLiant Svr Pkg 4 SVC
P74573-B21	8	Intel Xeon 6730P 2.5GHz 32-core 250W Processor for HPE

Product	Quantity	Product description
P69727-B21	128	HPE 32GB (1x32GB) Dual Rank x8 DDR5-6400 CAS-52-52-52 EC8 Registered Smart Memory Kit
P75740-B21	4	HPE ProLiant Compute DL3XX Gen12 8SFF x1 U.3 Tri-Mode Drive Cage Kit
P63871-B21	8	HPE 1.6TB SAS Mixed Use SFF BC Self-encrypting FIPS 140-2 PM7 SSD
P75741-B21	8	HPE ProLiant Compute DL3XX Gen12 8SFF x4 U.3 Tri-Mode Drive Cage Kit
P50230-B21	64	HPE 3.2TB NVMe Gen4 High Performance Mixed Use SFF BC U.3 PM1735a SSD
P48802-B21	4	HPE ProLiant DL380 Gen11 2U x8/x16/x8 Secondary Riser Kit
P48803-B21	4	HPE ProLiant DL380 Gen11 2U x16/x16/x16 Primary Riser Kit
P47785-B21	4	HPE MR216i-p Gen11 x16 Lanes without Cache PCI SPDM Plug-in Storage Controller
P42041-B21	8	Mellanox MCX631432AS-ADAI Ethernet 10/25Gb 2-port SFP28 OCP3 Adapter for HPE
P44712-B21	8	HPE 1800W-2200W Flex Slot Titanium Hot Plug Power Supply Kit
P78145-B21	8	HPE C13 - C14 250V 10Amp 2m FIO Power Cord
E5Y43A	4	HPE OneView for ProLiant DL Server including 3yr 24x7 Support FIO Bundle Physical 1-server LTU
P72205-B21	4	HPE ProLiant Compute DL3XX/ML350 Gen12 CPU2 to Rear OCP SlotB x8 Cable Kit
P76453-B21	4	HPE ProLiant Compute DL380 Gen12 8SFF SFF x4 UMB PCIe Box 1/2 Cable Kit
P76461-B21	4	HPE ProLiant Compute DL380 Gen12 8SFF x4 Direct Attach Box 1 for 2 Processors Cable Kit
P77489-B21	4	HPE ProLiant Compute DL380 Gen12 8SFF x4 Direct Attach Box 2/3 for 1P Cable Kit
P48820-B21	4	HPE ProLiant DL380/DL560 Gen11 2U High Performance Fan Kit
P48922-B21	4	HPE ProLiant DL3XX Gen11 Intrusion Cable Kit
P08040-B21	4	HPE iLO Common Password FIO Setting
P42104-B21	4	HPE ProLiant Platform Certificate and IDevID iLO FIO Setting
P52341-B21	4	HPE ProLiant DL3XX Gen11 Easy Install Rail 3 Kit
P73325-B21	4	HPE ProLiant Compute Localization FIO Kit
P74792-B21	8	HPE ProLiant Compute DL380 Gen12 Performance Heat Sink Kit
P77931-B21	4	HPE ProLiant Compute DL380 Gen12 16SFF x4 Direct Attach Balanced FIO Bundle Kit
P79552-B21	4	HPE ProLiant Compute 30C System Inlet Ambient Operating Temperature Configuration Tracking
C7536A	4	HPE 4.3m/14ft CAT5 RJ45 M/M Ethernet Cable
845420-B21	4	HPE QSFP28 to 4x25Gb SFP28 7m Active Optical Cable

Product	Quantity	Product description
		Aruba switches
R9F63A	2	HPE Aruba Networking CX 6300M 48G Power-to-Port Airflow 2 Fans 1 Power Supply Unit Bundle
R9F63A B2B	2	HPE Aruba Networking CX 6300M 48G Power-to-Port Airflow 2 Fans 1 Power Supply Unit Bundle PDU
HA454A1-021	2	HPE FE Strg and Ntwking Pkg 4 SVC
R9G06A	2	HPE Aruba Networking 50G SFP56 to SFP56 0.65m Direct Attach Copper Cable
R9G06A B01	2	HPE Aruba Networking 50G SFP56 to SFP56 0.65m Direct Attach Copper Cable
R9F61A	2	HPE Aruba Networking CX 6300M 12VDC 250W 100-240VAC Power-to-Port Airflow Power Supply Unit
R9F61A B2B	2	HPE Aruba Networking CX 6300M 12VDC 250W 100-240VAC Power-to-Port Airflow Power Supply Unit PDU
R9F57A	2	HPE Aruba Networking 1U Universal 4-post Rack Mount Kit
R9F59A	2	HPE Aruba Networking 4-post Rack Kit
R9F67A	2	HPE Aruba Networking CX 8325-32C Power-to-Port Airflow 6 Fans 2 Power Supply Units Bundle
R9F67A B2B	2	HPE Aruba Networking CX 8325-32C Power-to-Port Airflow 6 Fans 2 Power Supply Units Bundle PDU
HA454A1-021	2	HPE FE Strg and Ntwking Pkg 4 SVC
845416-B21	8	HPE 100Gb QSFP28 to 4x25Gb SFP28 3m Direct Attach Copper Cable
845420-B21	4	HPE QSFP28 to 4x25Gb SFP28 7m Active Optical Cable
R9F77A	4	HPE Aruba Networking 100G QSFP28 to QSFP28 1m Direct Attach Copper Cable
R9F77A B01	4	HPE Aruba Networking 100G QSFP28 to QSFP28 1m Direct Attach Copper Cable
C7533A	3	HPE 1.2m/4ft CAT5 RJ45 M/M Ethernet Cable
C7535A	6	HPE RJ45 to RJ45 Cat5e Black M/M 7.6ft 1-pack Data Cable
C7536A	4	HPE 4.3m/14ft CAT5 RJ45 M/M Ethernet Cable

Note

The above BOM contains US localization (ABA is for the US); Customers must choose localization options based on the deployment location.

Appendix B: Bill of materials – Fibre Channel based External Storage

Table B1. Bill of materials

Product	Quantity	Product description
		Rack and Power
P9K40A	1	HPE 42U 600mmx1200mm G2 Enterprise Shock Rack
P59419-B21	2	Enlogic by nVent G3 Metered Switched 3-phase 22kVA/Outlets (24) C13 (24) Combo C13/C19 PDU for HPE
P9L11A	1	HPE G2 Rack Grounding Kit
P9L12A	1	HPE G2 Rack Baying Kit
P9L12A B01	1	HPE G2 Rack Baying Kit
P9L16A	1	HPE G2 Rack 42U 1200mm Side Panel Kit
P9T01A	1	HPE G2 PDU Environmental Temperature and Humidity Sensor
P9T02A	1	HPE G2 PDU Environmental 3 Temperature and 1 Humidity Sensor
P9T03A	1	HPE G2 PDU Open Door Sensor
120672-B21	1	HPE Rack Ballast Kit
BW930A	1	HPE Air Flow Optimization Kit
BW930A B01	1	Include with complete system
BW932A	1	HPE 600mm Rack Stabilizer Kit
BW932A B01	1	HPE 600mm Rack include with Complete System Stabilizer Kit
		Workload hosts
P72176-B21	3	HPE ProLiant Compute DL360 Gen12 10SFF/20EDSFF Hybrid NC Configure-to-order Server
P72176-B21 ABA	3	HPE DL360 G12 10SFF/20EDSFF Hyb CTO Svr
P74573-B21	6	Intel Xeon 6730P 2.5GHz 32-core 250W Processor for HPE
P69726-B21	48	HPE 16GB (1x16GB) Single Rank x8 DDR5-6400 CAS-52-52-52 EC8 Registered Smart Memory Kit
P72223-B21	3	HPE ProLiant Compute DL3XX Gen12 1U 2SFF x4 Tri-Mode U.3 Stacking Backplane Kit
P63871-B21	6	HPE 1.6TB SAS Mixed Use SFF BC Self-encrypting FIPS 140-2 PM7 SSD
P65333-B21	3	HPE InfiniBand NDR200/Ethernet 200GbE 2-port QSFP112 PCIe5 x16 MCX755106AC-HEAT Adapter
R2E09A	3	HPE SN1610Q 32Gb 2-port Fibre Channel Host Bus Adapter
P47789-B21	3	HPE MR216i-o Gen11 x16 Lanes without Cache OCP SPDM Storage Controller
P48908-B21	3	HPE ProLiant DL3X0 Gen11 1U High Performance Fan Kit
P03178-B21	6	HPE 1000W Flex Slot Titanium Hot Plug Power Supply Kit

Product	Quantity	Product description
P78145-B21	6	HPE C13 - C14 250V 10Amp 2m FIO Power Cord
E5Y43A	3	HPE OneView for ProLiant DL Server including 3yr 24x7 Support FIO Bundle Physical 1-server LTU
P72600-B21	3	HPE ProLiant Compute DL360 Gen12 2SFF Stacking x2 Box1 Box2 Rear OCP SlotA Controller Cable Kit
P48922-B21	3	HPE ProLiant DL3XX Gen11 Intrusion Cable Kit
P07818-B21	3	HPE DDR4 DIMM Blank Kit
P08040-B21	3	HPE iLO Common Password FIO Setting
P52343-B21	3	HPE Easy Install Rail 5 Kit
P72209-B21	3	HPE ProLiant Compute DL360 Gen12 10SFF/20EDSFF Hybrid Backplane Power Cable Kit
P73325-B21	3	HPE ProLiant Compute Localization FIO Kit
P74787-B21	6	HPE ProLiant DL3XX Gen12 High Performance Heat Sink Kit
P79555-B21	3	HPE ProLiant Compute 27C System Inlet Ambient Operating Temperature Configuration Tracking
P79633-B21	3	HPE ProLiant Compute DAC ACC Networking Cable Operating Configuration Tracking
R9F78A	6	HPE Aruba Networking 100G QSFP28 to QSFP28 5m Direct Attach Copper Cable
C7536A	3	HPE 4.3m/14ft CAT5 RJ45 M/M Ethernet Cable
		HPE Alletra Storage MP B10000
R6B05A	2	HPE SN6700B 64Gb 56/24 24-port 32Gb Short Wave SFP28 Integrated Fibre Channel Switch
R6B09A	6	HPE SN6700B 8-port POD Upgrade License with 32Gb SFP28 Short Wave Transceiver Kit
S1R06A	1	HPE Alletra Storage MP B10000 Base Cluster Configuration
R7C75A	1	HPE Alletra Storage MP 10000 2U Chassis
R7C76A	4	HPE Alletra Storage MP C14 1600W AC Power Supply
R9R52A	2	HPE C13 - C14 250V 10Amp Black 1.4m WW Power Cord
R9S00A	2	HPE C13 - C14 250V 10Amp Gray 1.4m WW Power Cord
R7D03A	2	HPE Alletra Storage MP B10240 Controller Node
S2A68A	6	HPE Alletra Storage MP 100GbE 2-port OCP Host Bus Adapter
R9F76A	12	Aruba 100G QSFP28 to QSFP28 2m Active Optical Cable for HPE
S2S64A	4	HPE Alletra Storage MP 32Gb 4-port Fibre Channel OCP LPm37004 Host Bus Adapter
S3N85A	8	HPE 32Gb SFP28 Short Wave 1-pack Pull Tab Optical Transceiver
S1R08A	2	HPE Alletra STG MP 32-port 100GbE Switch Bundle
S3L68A	2	HPE C13 - C14 250V Blk 2m WW Pwr Cord
S3L69A	2	HPE C13 - C14 250V Gry 2m WW Pwr Cord

Product	Quantity	Product description
S0A95A	1	HPE Switch Pair Installation Kit
S1J10A	1	HPE Alletra Storage MP 10001 NVMe Configure-to-order Expansion Shelf
S1R28A	2	HPE Alletra Storage MP 10010 Expansion Shelf Node
R9H67A	24	HPE Alletra Storage MP 3.84TB NVMe SFF Self-encrypting SSD
S0A98A	1	HPE Storage Data Encryption LTU
S3Q00A	1	HPE Alletra Storage MP B10000 OS per TB 3-year LTU
S3Q00AAE	92	HPE Alletra Storage MP B10000 OS per TB 3-year Software and Support SaaS
		Management hosts
P72176-B21	4	HPE ProLiant Compute DL360 Gen12 10SFF/20EDSFF Hybrid NC Configure-to-order Server
P72176-B21 ABA	4	HPE DL360 G12 10SFF/20EDSFF Hyb CTO Svr
HA454A1-001	4	HPE FE ProLiant Svr Pkg 4 SVC
P74576-B21	8	Intel Xeon 6737P 2.9GHz 32-core 270W Processor for HPE
P69727-B21	128	HPE 32GB (1x32GB) Dual Rank x8 DDR5-6400 CAS-52-52-52 EC8 Registered Smart Memory Kit
P72223-B21	4	HPE ProLiant Compute DL3XX Gen12 1U 2SFF x4 Tri-Mode U.3 Stacking Backplane Kit
P63871-B21	8	HPE 1.6TB SAS Mixed Use SFF BC Self-encrypting FIPS 140-2 PM7 SSD
P65333-B21	4	HPE InfiniBand NDR200/Ethernet 200GbE 2-port QSFP112 PCIe5 x16 MCX755106AC-HEAT Adapter
R2E09A	4	HPE SN1610Q 32Gb 2-port Fibre Channel Host Bus Adapter
P47789-B21	4	HPE MR216i-o Gen11 x16 Lanes without Cache OCP SPDM Storage Controller
P48908-B21	4	HPE ProLiant DL3X0 Gen11 1U High Performance Fan Kit
P03178-B21	4	HPE 1000W Flex Slot Titanium Hot Plug Power Supply Kit
P78145-B21	8	HPE C13 - C14 250V 10Amp 2m FIO Power Cord
E5Y43A	4	HPE OneView for ProLiant DL Server including 3yr 24x7 Support FIO Bundle Physical 1-server LTU
P72600-B21	4	HPE ProLiant Compute DL360 Gen12 2SFF Stacking x2 Box1 Box2 Rear OCP SlotA Controller Cable Kit
P48922-B21	4	HPE ProLiant DL3XX Gen11 Intrusion Cable Kit
P08040-B21	4	HPE iLO Common Password FIO Setting
P52343-B21	4	HPE Easy Install Rail 5 Kit
P72209-B21	4	HPE ProLiant Compute DL360 Gen12 10SFF/20EDSFF Hybrid Backplane Power Cable Kit
P73325-B21	4	HPE ProLiant Compute Localization FIO Kit
P74787-B21	8	HPE ProLiant DL3XX Gen12 High Performance Heat Sink Kit
P79633-B21	4	HPE ProLiant Compute DAC ACC Networking Cable Operating Configuration Tracking

Product	Quantity	Product description
P79558-B21	4	HPE ProLiant Compute 25C System Inlet Ambient Operating Temperature Configuration Tracking
		Aruba Switches
R9F63A	2	HPE Aruba Networking CX 6300M 48G Power-to-Port Airflow 2 Fans 1 Power Supply Unit Bundle
R9F63A B2B	2	HPE Aruba Networking CX 6300M 48G Power-to-Port Airflow 2 Fans 1 Power Supply Unit Bundle PDU
HA454A1-021	2	HPE FE Strg and Ntwking Pkg 4 SVC
R9G06A	2	HPE Aruba Networking 50G SFP56 to SFP56 0.65m Direct Attach Copper Cable
R9G06A B01	2	HPE Aruba Networking 50G SFP56 to SFP56 0.65m Direct Attach Copper Cable
R9F61A	2	HPE Aruba Networking CX 6300M 12VDC 250W 100-240VAC Power-to-Port Airflow Power Supply Unit
R9F61A B2B	2	HPE Aruba Networking CX 6300M 12VDC 250W 100-240VAC Power-to-Port Airflow Power Supply Unit PDU
R9F57A	2	HPE Aruba Networking 1U Universal 4-post Rack Mount Kit
R9F59A	2	HPE Aruba Networking 4-post Rack Kit
R9F67A	2	HPE Aruba Networking CX 8325-32C Power-to-Port Airflow 6 Fans 2 Power Supply Units Bundle
R9F67A B2B	2	HPE Aruba Networking CX 8325-32C Power-to-Port Airflow 6 Fans 2 Power Supply Units Bundle PDU
HA454A1-021	2	HPE FE Strg and Ntwking Pkg 4 SVC
845416-B21	8	HPE 100Gb QSFP28 to 4x25Gb SFP28 3m Direct Attach Copper Cable
845420-B21	4	HPE QSFP28 to 4x25Gb SFP28 7m Active Optical Cable
R9F77A	4	HPE Aruba Networking 100G QSFP28 to QSFP28 1m Direct Attach Copper Cable
R9F77A B01	4	HPE Aruba Networking 100G QSFP28 to QSFP28 1m Direct Attach Copper Cable
C7533A	3	HPE 1.2m/4ft CAT5 RJ45 M/M Ethernet Cable
C7535A	6	HPE RJ45 to RJ45 Cat5e Black M/M 7.6ft 1-pack Data Cable
C7536A	4	HPE 4.3m/14ft CAT5 RJ45 M/M Ethernet Cable

URLs for firmware, software, and documentation

Rack and power links

HPE G3 Metered and Switched Power Distribution Unit, https://www.hpe.com/psnow/doc/a50009202enw.

HPE Rack and Power Infrastructure, https://www.hpe.com/us/en/integrated-systems/rack-power-cooling.html.

HPE Network links

Networking documentation, https://networkingsupport.hpe.com/home

HPE Aruba Networking CX 6300 Switch Series (R9F63A), https://www.arubanetworks.com/products/switches/6300-series/

HPE Aruba Networking CX 8325 Switch Series (R9F67A), https://www.arubanetworks.com/products/switches/core-and-data-center/8325-series/

HPE Alletra Storage

HPE Alletra Storage, https://www.hpe.com/us/en/hpe-alletra.html

HPE Servers

HPE ProLiant Servers, https://www.hpe.com/us/en/servers/proliant-dl-servers.html

Service Pack for ProLiant (SPP) Software, http://www.hpe.com/info/spp/download

Service Pack for ProLiant (SPP) Documentation: http://www.hpe.com/info/spp/documentation

Software

HPE OneView

Software: https://myenterpriselicense.hpe.com/cwp-ui/software

Documentation: http://www.hpe.com/info/oneview/docs

Partner Integrations: http://www.hpe.com/info/ovpartners

Broadcom links

VMware Cloud Foundation 9.0 guides, https://techdocs.broadcom.com/us/en/vmware-cis/vcf/vcf-9-0-and-later/9-0/deployment.html.

VMware Cloud Foundation 9.0 release notes, https://techdocs.broadcom.com/us/en/vmware-cis/vcf/vcf-9-0-and-later/9-0/release-notes/vmware-cloud-foundation-90-release-notes.html.

Build numbers and versions of VMware ESXi/ESX, https://knowledge.broadcom.com/external/article/316595/build-numbers-and-versions-of-vmware-esx.html.

Resources and additional links

HPE Reference Architectures
https://www.hpe.com/docs/reference-architecture

HPE Servers
hpe.com/servers

HPE Storage
hpe.com/storage

HPE Networking
hpe.com/networking

HPE ProLiant DX380 Gen11 Server User Guide,
https://support.hpe.com/hpesc/public/docDisplay?docId=sd00002997en_us

Aruba Fabric Composer (AFC)
https://www.arubanetworks.com/en-in/products/switches/core-and-data-center/fabric-composer/

HPE GreenLake Advisory and Professional Services
hpe.com/us/en/services/consulting.html

HPE and VMware
hpe.com/partners/vmware

HPE Enterprise Support Center
https://support.hpe.com/hpesc/public/home

HPE OneView for VMware vCenter Release Notes,
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=sd00003083en_us

To help us improve our documents, please provide feedback at hpe.com/contact/feedback.

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, use the Feedback button and icons (located at the bottom of an opened document) on the Hewlett Packard Enterprise Support Center portal (hpe.com/support/hpesc) to send any errors, suggestions, or comments. All document information is captured by the process.

.

Visit HPE.com

a50014174enw

HEWLETT PACKARD ENTERPRISE

HPE.com