Hewlett Packard Enterprise

Check if the document is available in the language of your choice.

VMWARE CLOUD FOUNDATION CERTIFICATION ON HPE PROLIANT DL360

Best practices and general build information for deploying and using VMware Cloud Foundation on HPE ProLiant DL360 platform

CONTENTS

INTRODUCTION AND EXECUTIVE SUMMARY

Applications are moving to the cloud, and most companies have some combination of cloud and on-premises applications. With more applications being used, typically from various vendors, the need for integration has never been greater. Technology must work together, and happen faster, to meet the increasing demand for information and services. There is a need for greater optimization and efficiency in how software and solutions that power data centers are deployed and managed. These trends are pushing IT departments to find better ways to integrate, provision, deploy, and manage systems at a faster pace without straining already burdened budgets.

To meet the growing demands for an integrated cloud environment, HPE ProLiant DL360 Gen10 Server and VMware Cloud Foundation™ partner to provide an integrated cloud platform. The benefits include:

- HPE ProLiant is the intelligent compute foundation for hybrid cloud delivering unmatched workload optimization, security, and automation, all available as a service.

- Integrated cloud infrastructure (compute, storage, networking, and security) and cloud management services to run enterprise applications in both private and public environments.

- A common cloud operating model that works seamlessly on-premises, at the edge or in public cloud.

- Built on a hyperconverged architecture (VMware vSAN™) that offers all-flash performance and enterprise-class storage services including deduplication, compression, and erasure coding. vSAN implements hyperconverged storage architecture that delivers elastic storage and drastically simplifies storage management.

- Provide end-to-end security for all applications by delivering micro-segmentation, distributed firewalls, VPN (VMware NSX®), VM, hypervisor, VMware vMotion encryption, and AI-powered workload security and visibility (VMware vSphere®). In addition, VMware Cloud Foundation includes data at rest, cluster, and storage encryption (vSAN).

- Integrated lifecycle management by simplifying and automating patching and upgrading the full private cloud stack with workload domain-level lifecycle management.

Target audience—The intended users for this content are Hewlett Packard Enterprise, VMware®, channel partners, and customers who are interested in setting up a lab or performing service implementations. This document is not intended to be a training guide for HPE ProLiant DL360 server series or VMware Cloud Foundation. Prior knowledge of the applications and hardware is required to execute this implementation.

Document purpose: This document is a guide for VMware Cloud Foundation installations on the HPE ProLiant DL hardware platform.

PHYSICAL AND LOGICAL LAYOUT

Solution components

Hardware components
Initial configuration, as tested.

TABLE 1. Solution hardware components

Hardware	Details
Compute	8 x HPE DL360 Gen10 8SFF CTO Server—(four for management/VMware Cloud Foundation stack, four for workloads)
	8 x HPE DL360 Gen10 Intel® Xeon® Silver 4114 (2.2 GHz/10-core/85W) FIO Processor Kit
	8 x HPE DL360 Gen10 Intel Xeon Silver 4114 (2.2 GHz/10-core/85W) Processor Kit
	32 x HPE 32GB (1 x 32 GB) Dual Rank x4 DDR4-2666 CAS-19-19-19 Registered Smart Memory Kit
Network	2 x HPE Composable Fabric 3180 25G switch
	16 x HPE Composable Fabric SFP28 DAC cable
Storage	8 x HPE Smart Array P408i-a SR Gen10 (8 Internal Lanes/2 GB Cache) 12G SAS Modular Controller
	8 x HPE 400GB SAS 12G Write Intensive SFF (2.5in) SC SSD—(Caching tier)
	32 x HPE 1.6TB SAS 12G Mixed Use SFF (2.5in) SC SSD—(Storage tier)
	8 x HPE 8 GB Dual microSD Flash USB Drive

Note: The vSAN configuration specified here is one of the many supported vSAN configurations on HPE servers and is selected for this white paper. To view a complete list of supported vSAN Configurations, refer to the VMware Compatibility Guide for vSAN.

HPE ProLiant DL360 Gen10 Servers

HPE ProLiant DL360 Gen10 Server is a secure, performance-driven dense server that can be confidently deployed for virtualization, database, or high-performance computing. It supports the Intel® Xeon® scalable processor with considerable performance gains and an increase in the number cores, along with 2933 MT/s HPE DDR4 SmartMemory supporting capacities of up to 3.0 TB which provides a significant increase in performance.

With the added performance that HPE Persistent Memory, NVDIMMs, and 10 NVMe bring, the HPE ProLiant DL360 Gen10 Server means business. Deploy, update, monitor, and maintain with ease by automating essential server lifecycle management tasks with HPE OneView and HPE Integrated Lights Out 5 (iLO 5). Deploy this 2P secure platform for diverse workloads in space-constrained environments.

FIGURE 1. HPE ProLiant DL360 Gen10 Server

HPE iLO 5

HPE iLO is embedded in HPE ProLiant platforms. It provides server management that enables faster deployment, simplified lifecycle operations while maintaining end-to-end security thus increasing productivity.

HPE Composable Fabric FM 3180

HPE Composable Fabric FM 3180 is a top-of-rack (TOR) connectivity module that delivers the next generation of innovative networking solutions designed to meet the growing needs of today's virtual and highly dynamic data center and cloud environments. Specifically designed to support scale-out applications with high-performance east/west traffic needs, HPE Composable Fabric provides an easily scalable and automated fabric solution for diverse application workloads.

HPE Composable Fabric FM 3180 provides a cost-effective 1U solution for intensive Big Data or agile IT workload environments. The HPE Composable Fabric FM 3180 industry-standard architecture uses Ethernet switching to create a high-performance, resilient, low-latency, and scalable data center network fabric. HPE Composable Fabric connectivity modules can be deployed as a single tier, eliminating cost and complexity while vastly reducing operational overhead and creating true fabric agility to support dynamic workload needs. In conjunction with HPE Composable Fabric Manager—a centralized management, visualization, and control platform, the solution streamlines operations and dynamically aligns network resources to the demanding workload and data requirements of the modern data center.

FIGURE 2. HPE Composable Fabric FM 3180

HPE Smart Array Controller

HPE Smart Array P408i-a SR Gen10 Controller, supporting 12 Gb/s SAS and PCIe 3.0, provides enterprise-class storage performance, reliability, security, and efficiency needed to address your evolving data storage needs. This controller has eight internal SAS lanes, allowing connection to SAS or SATA drives, supports mixed-mode operations of RAID and HBA simultaneously, and it offers encryption for data-at-rest on any drive. The HPE Smart Array P408i-a SR Gen10 Controller is ideal for maximizing performance while supporting advanced RAID levels with 2 GB Flash-Backed Write Cache (FBWC). This type A modular controller occupies a dedicated storage slot without occupying a PCIe expansion slot. The HPE Smart Storage Battery supports the Gen10 controllers.

FIGURE 3. The HPE Smart Array P408i-a SR Gen10 Controller

Software components

Starting reference during publication, refer to <u>VMware Cloud Foundation release notes</u> for current list:

TABLE 2. Solution software components

Software	Version
VMware Cloud Foundation	3.9.0
VMware ESXi™ Server	6.7 U3 (August 2019 HPE Custom ISO)

VMware Cloud Foundation 3.9.0

VMware Cloud Foundation is an integrated hybrid cloud platform that delivers a complete set of software-defined services for compute, storage, networking, security, and cloud management for the private and public cloud. VMware Cloud Foundation drastically simplifies data center operations by deploying a standardized and validated architecture with built-in lifecycle automation of the cloud stack. It can also be flexibly consumed as a service in the public cloud (VMware Cloud™ on AWS, IBM, Rackspace, and so on), enabling a true hybrid cloud that is based on a consistent infrastructure and operational model using common tools and processes. A typical VMware Cloud Foundation deployment consists of a management domain with a minimum of four hosts and one or more workload domains. The management domain is where the VMware Cloud Foundation stack is deployed and is responsible for infrastructure and management tasks. Workload domains are a logical entity consisting of a group of hosts that can be used for a specific task.

VMware ESXi server

VMware ESXi server is a computer virtualization software developed by VMware. The ESXi server is an advanced, smaller-footprint version of the VMware ESX® server, VMware's enterprise-level computer virtualization software product. Implemented within the VMware infrastructure, ESXi can be used to facilitate centralized management for enterprise desktops and data center applications.

Virtualization components

A virtual rack is a set of physical racks combined into and managed as a single logical entity. A virtual rack domain is a resource group with specific availability and performance attributes.

TABLE 3. Solution virtualization components

Component	Description
VMware ESXi	A foundation for creating SDDC architecture by using the hypervisor to run VMs in workload clusters as well as the management domain clusters.
VMware vCenter Server®	Provides a single point of management of a VMware virtualized environment with one or more VMware ESXi instances.
	The management domain cluster on each physical rack includes a VMware vCenter Server® Appliance™ deployed as two VMs, one for the Platform Services Controller™ division, and one for the VMware vCenter® division. All other virtual rack domains include the vCenter divisions (deployed from a vCenter Server Appliance), logically connected to the management domain cluster's Platform Services Controller VM.
VMware Cloud Foundation Manager	It provisions, manages, and monitors the logical and physical resources. Use the VMware Cloud Foundation Manager for configuration, operations, and management functions.
Hardware Management Service (HMS)	Performs auto-discovery of hardware, inventorying, monitoring for hardware failures and low-level patches.
VMware Virtual SAN	Allows you to create a virtual SAN from the local datastores on clustered VMware ESXi instances. The resulting virtual SAN becomes a shared datastore for the VMware ESXi instances contributing to storage.
	Each virtual rack domain contains one or more clusters. The VMware Cloud Foundation Manager creates a single virtual SAN volume spanning all the hosts within each cluster. This means that each cluster must have a minimum of three hosts.

Resources for sizing and use of VMware Cloud Foundation on HPE ProLiant Servers

Compute, memory, and storage must be vSAN certified and a part of the HPE vSAN ReadyNodes. You can work with your HPE sales representative to build the order and follow the prescribed configurations in the ReadyNodes document from the VMware hardware compatibility list. For more information, follow these links for easy to use compatibility and sizing tools:

- VMware Compatibility Guide for vSAN
- vSAN ReadyNode Sizer
- VMware vSAN Design and Sizing Guide 6.7

KEY CONSIDERATIONS AND PREREQUISITES

Considerations

Observe the following considerations to avoid errors:

1. The VMware Compatibility Guide for vSAN must be used as a reference for required driver and firmware versions.
    a. Check the driver/firmware combinations against what is currently being used in the latest HPE ProLiant SPP.
    b. If the firmware version required isn't available in the latest SPP, download the required version from the HPE support page and install.
2. Cache and data drive sizes are dictated by VM sizing done prior to purchasing. Refer to the vSAN ReadyNode Sizer resource.
3. All nodes must have equivalent configurations of memory and vSAN sizing in the same cluster.

Prerequisites

Ensure the following prerequisites are met for a smooth deployment process:

1. A DNS/DHCP/NTP server for the network on which VMware Cloud Foundation will be deployed.
2. A platform for VMware Cloud Builder VM deployment, it is responsible for the bringing up the VMware Cloud Foundation SDDC Manager. Ensure that this platform has access to the servers on which VMware Cloud Foundation will be deployed in the private network. Supported platforms include:
    a. A dedicated ESXi host.
    b. A laptop or workstation running VMware Fusion® or VMware Workstation.
3. License keys for the following VMware products (quantity of licenses required will depend on the desired size of deployment):
    a. VMware ESXi
    b. VMware vSAN Enterprise
    c. VMware vCenter Server® Standard™ (or higher)
    d. VMware NSX Data Center for vSphere
    e. VMware Cloud Foundation SDDC Manager appliance
    f. VMware vRealize® Suite Enterprise

NETWORK CONFIGURATION

VMware Cloud Foundation requires all constituent components to be on separate subnets and VLANs. For instance, an example configuration could look like:
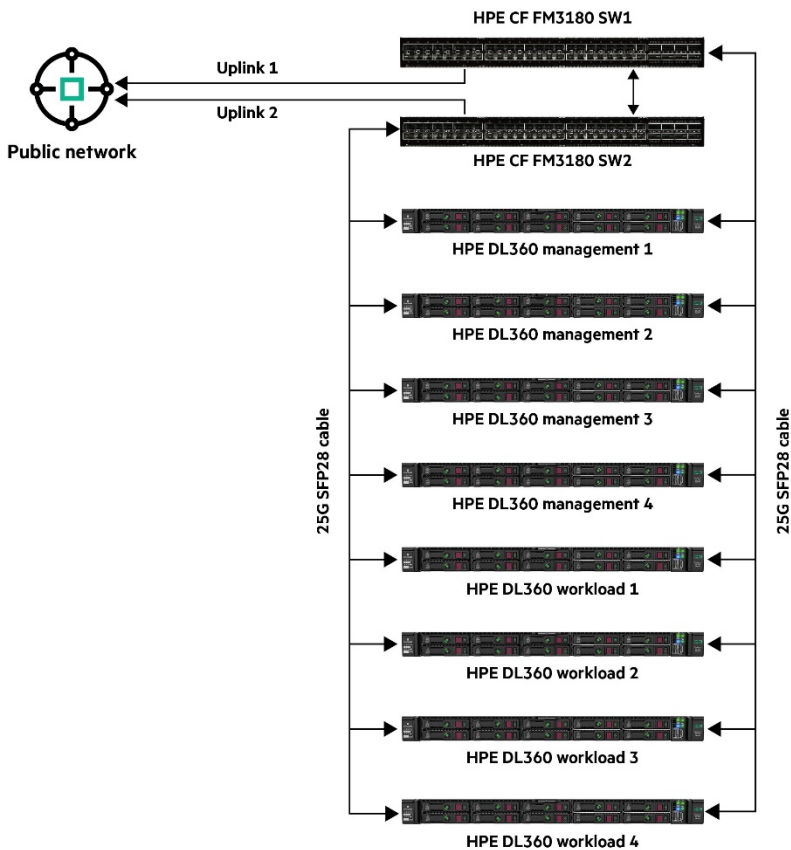
TABLE 4. Solution network configuration

Function	VLAN ID	Subnet (CIDR)	Gateway
Management	50	172.20.50.0/24	172.20.50.1
VMware vSphere® vMotion®	51	172.20.51.0/24	172.20.51.1
vSAN	52	172.20.52.0/24	172.20.52.1
VXLAN (NSX VTEP)	53	172.20.53.0/24	172.20.53.1
VMware vRealize® Suite	54	172.20.54.0/24	172.20.54.1
Uplink 1	1011	172.10.11.0/24	172.10.11.1
Uplink 2	1012	172.10.12.0/24	172.10.12.1

To configure subnets and VLANs on the HPE Composable Fabric, download the HPE Composable Fabric Manager ISO or HPE OVA and deploy it on an ESXi host (it can be installed and executed on the same host as the DNS/DHCP server). Refer to underline:installation guide for instructions on how to get it up and running. For more information on HPE Composable Fabric Manager for VMware Cloud Foundation, refer to this underline:white paper.

Ensure that an instance of a firewall/router software is deployed and configured for routing between the subnets and to act as a firewall/gateway. Ensure that the platform on which the Cloud Builder VM is deployed has access to the management VLAN.

A sample network configuration diagram is provided in Figure 4:

FIGURE 4. Sample Network Configuration

Figure 4 shows eight HPE ProLiant DL360 Gen10 servers split into two groups of four servers each, one for the management domain and one for a workload domain. The servers are connected to the HPE Composable Fabric switches via 25G SFP28 cables for high speed connectivity.

DEPLOYMENT

The first step in deployment is to install ESXi on the host servers. Download and install the HPE custom ESXi ISO image from the HPE website, on all servers where VMware Cloud Foundation will be deployed. Ensure the following configuration requirements are met on all ESXi hosts:

1. Static IP address assigned to the management interface.
2. Management network portgroup configured with the correct VLAN ID.
3. VM network portgroup configured with the same VLAN ID as the management network.
4. TSM-SSH service is enabled and policy set to Start and Stop with Host.
5. NTP service is enabled, configured, and policy set to Start and Stop with Host.

Once the ESXi hosts have been configured, add entries for static IP addresses in the DNS server for the following components:

1. Cloud Builder VM

2. Platform Services Controller x 2

3. vCenter Server

4. VMware NSX® Manager™

5. VMware vRealize® Log Insight™

    a. Master node x 1

    b. Worker nodes x 2

    c. Load balancer node x 1

6. SDDC Manager

Cloud Builder

To deploy the Cloud Builder VM:

1. Download the Cloud Builder OVA and the vcf_ems_deployment_parameters excel workbook from your MyVMware account.

2. Deploy the Cloud Builder OVA as a VM on the platform selected for the Cloud Builder VM in the prerequisites mentioned previously.

    a. Select the option to deploy a VM from an OVF/OVF file.

    b. Enter a name for the virtual machine and select the VMware Cloud Builder OVA file.

    c. Select the datastore where the virtual machine will be deployed.

    d. Accept the end-user license agreement.

    e. In deployment options, select the portgroup designated to the management network as Network 1. Leave the other options on their default values.

    f. In the additional settings tab, input an administrator username and password, a root password, and specify the hostname/DNS server/NTP server/Gateway and other information as required.

    g. Verify the information entered in the next step and click Finish to proceed with deploying the VM.

SDDC Manager

To deploy the SDDC Manager:

1. Fill all the sheets in the downloaded Excel workbook with the required information:

    a. Ensure all prerequisites in the **Prerequisite Checklist** sheet are met and change the status of each prerequisite to **Verified**.

    b. Fill in the respective license keys for each component in the **Management Workloads** sheet.

    c. In the **Users and Groups** sheet, fill the respective passwords for each of the components that will be deployed.

    d. In the **Hosts and Networks** sheet, provide the CIDR notation of management domain networks. VMware recommends an MTU value of 9000 for the management networks. Next, specify the hostnames and IP addresses of the ESXi hosts that will be a part of the management domain. Also, specify the vMotion and vSAN IP address ranges.

    e. In the **Deploy Parameters** sheet, start by specifying the DNS and NTP servers. Next, enter a single sign on-site name for the SDDC along with information related to virtual networking, depending on your network configuration. Subsequently, enter the hostnames and static IP addresses for each VMware Cloud Foundation component created earlier.

2. Navigate to the Cloud Builder VM and log in using credentials specified when deploying the VM. Upload the configuration Excel workbook when prompted.

FIGURE 5. Cloud Builder landing page

3. Wait for the Cloud Builder to validate the information entered in the configuration Excel workbook. The configuration file validation should take about 10 minutes. If validation fails due to an error, download the validation report, diagnose, and resolve the issue and re-upload the file for validation.

FIGURE 6. Configuration File Validation

4. Once validation is successful, click **Next** to start bringing up SDDC Manager. This will start deploying the constituent components of the SDDC, create a vSAN datastore, and apply the license keys specified in the configuration file. The entire deployment process should take about two hours. If any step fails, refer to the troubleshooting section for common pitfalls and the location of the deployment log file.
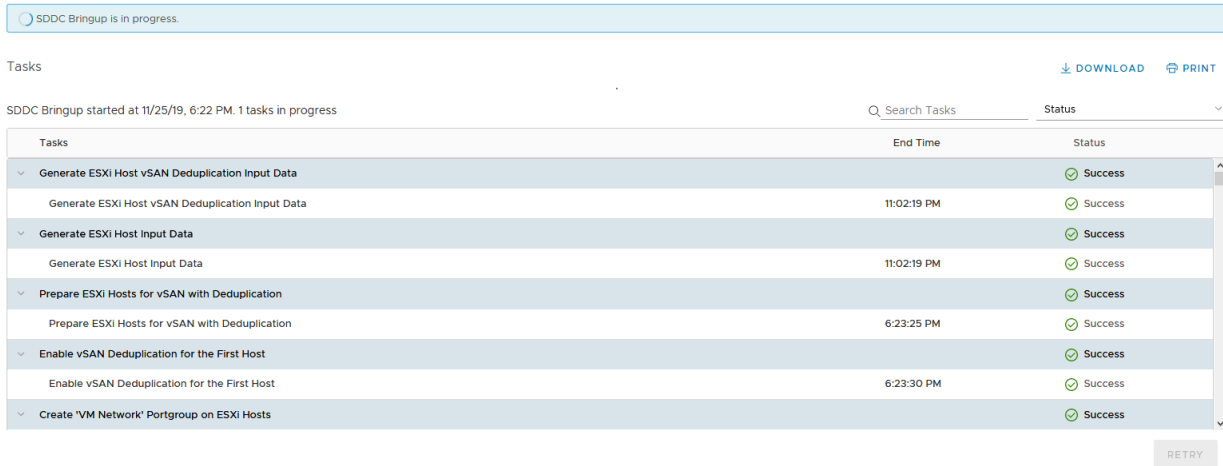
FIGURE 7. Bringing up SDDC Manager

5. Once the deployment succeeds, navigate to the SDDC Manager hostname or IP address to access the SDDC Manager.

COMMISSIONING ADDITIONAL HOSTS

Use the credentials from the configuration file to log in to the SDDC Manager. Once logged in to the SDDC Manager UI, a dashboard highlighting the number of deployed workload domains, information about the hosts being managed by the SDDC Manager, and resource utilization will be displayed.
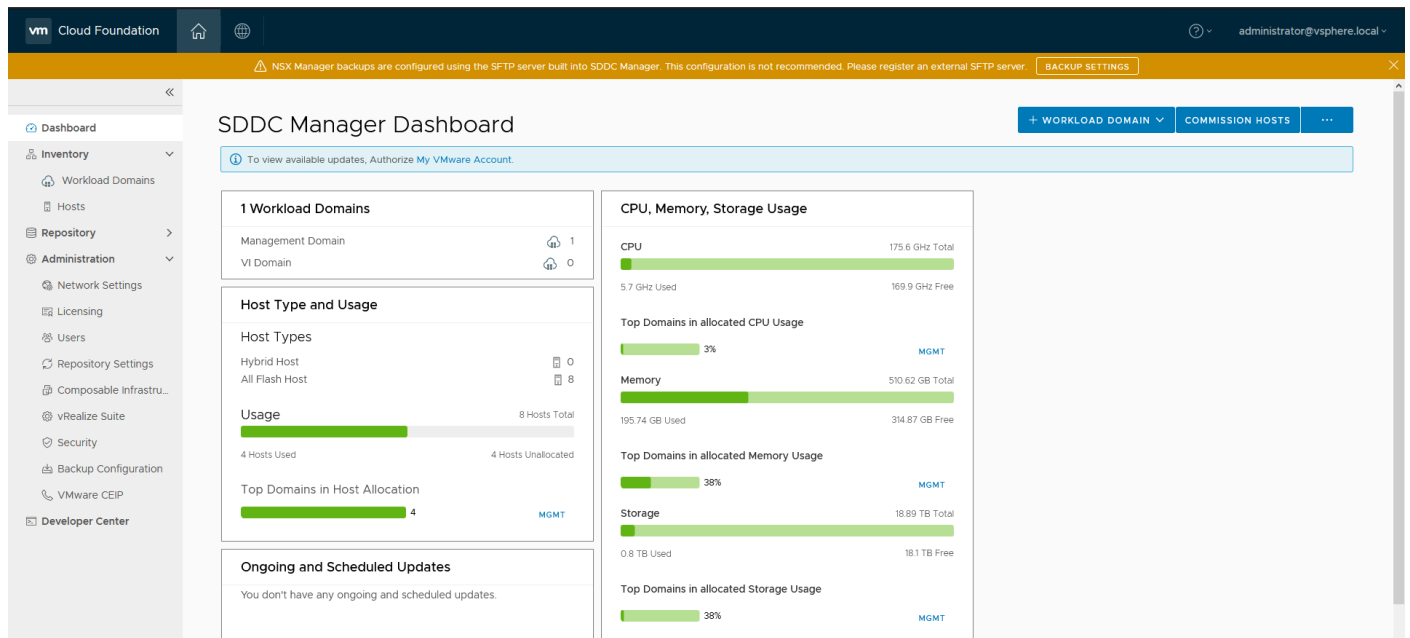
FIGURE 8. SDDC Manager Dashboard

To create a new workload domain, additional hosts apart from the ones being used by the management domain need to be commissioned. To commission additional hosts:

1. Click on the **Commission Hosts** button on the top right-hand corner of the SDDC Manager UI. This will open a new window, which contains a checklist of the prerequisites for adding a new host to the SDDC. After ensuring all prerequisites are met, check **Select All** and proceed.

Checklist

Commissioning a host adds it to the VMware Cloud Foundation inventory. The host you want to commission must meet the checklist criterion below.

☐ **Select All**

☐ Host for vSAN workload domain should be vSAN compliant and certified per the VMware Hardware Compatibility Guide. BIOS, HBA, SSD, HDD, etc. must match the VMware Hardware Compatibility Guide.

☐ Host has a standard switch with two NIC ports with a minimum 10 Gbps speed.

☐ Host has the drivers and firmware versions specified in the VMware Compatibility Guide.

☐ Host has ESXi installed on it. The host must be preinstalled with supported versions (6.7.0-14320388)

☐ SSH and syslog are enabled on the host.

☐ Host is configured with DNS server for forward and reverse lookup and FQDN.

☐ Hostname should be same as the FQDN.

☐ Management IP is configured to first NIC port.

☐ Ensure that the host has a standard switch and the default uplinks with 10Gb speed are configured starting with traditional numbering (e.g., vmnic0) and increasing sequentially.

☐ Host hardware health status is healthy without any errors.

☐ All disk partitions on HDD / SSD are deleted.

☐ Ensure required network pool is created and available before host commissioning.

☐ Ensure hosts to be used for VSAN workload domain are associated with VSAN enabled network pool.

☐ Ensure hosts to be used for NFS workload domain are associated with NFS enabled network pool.

☐ Ensure hosts to be used for VMFS on FC workload domain are associated with NFS or VMOTION only enabled network pool.

                                                                    CANCEL   PROCEED

FIGURE 9. Checklist for Commissioning Hosts

2. On the next screen, add a new host by specifying an FQDN. For storage type, select **VSAN**. Next, choose the default network pool from the drop-down list. Subsequently, specify a User Name and a Password and click **Add**.

FIGURE 10. Adding a new host

3. Similarly, add as many hosts as required. Once all hosts are added, click on the tick mark next to the **Confirm fingerprint** column and click on Validate All. This will start the validation process on the new hosts. Wait for the validation to complete.

FIGURE 11. Host validation

4. Once the hosts are validated successfully, click **Next**, review the information, and proceed. The new hosts will now be commissioned and will be available in the SDDC.

ADDING A WORKLOAD DOMAIN

Once additional hosts have been commissioned, a new workload domain can be added. A workload domain requires a separate instance of vCenter and VMware NSX Manager. It is advised to add new static IP entries for the same in the DNS server at this stage. Additionally, make sure that the appropriate quantity of licenses for VMware vSphere, VMware vSAN, and NSX-V for vSphere (or NSX-T, depending on the choice of network virtualization) is available before proceeding.

1. Click on the **Workload Domain** button next to the **Commission Hosts** button on the SDDC Manager UI and select **Virtual Infrastructure** Domain. This will open a new window asking for the type of storage to be used. Select **vSAN** and click **Begin**.

FIGURE 12. Storage Selection for Workload Domain

2. On the **Name** screen, enter a Virtual Infrastructure Name, Cluster Name, and Organization Name pertinent to the workload this domain is being deployed for and click **Next**.

FIGURE 13. Adding a workload domain—Name

3. On the Compute screen, enter relevant details pertaining to the vCenter instance for the workload domain and click **Next**.

FIGURE 14. Adding a workload domain—Compute

4. On the Networking screen, start by selecting an NSX platform. (Note: NSX-T may require a separate license and additional downloads). Thereafter, specify the VLAN ID, NSX Manager IP Address, FQDN, and related information.

FIGURE 15. Adding a workload domain—Networking

5. On the **vSAN Storage** screen, specify the vSAN Parameters—Failure to tolerate (a higher number would require more redundancy and, therefore, more hosts) and the option to enable vSAN deduplication and compression.
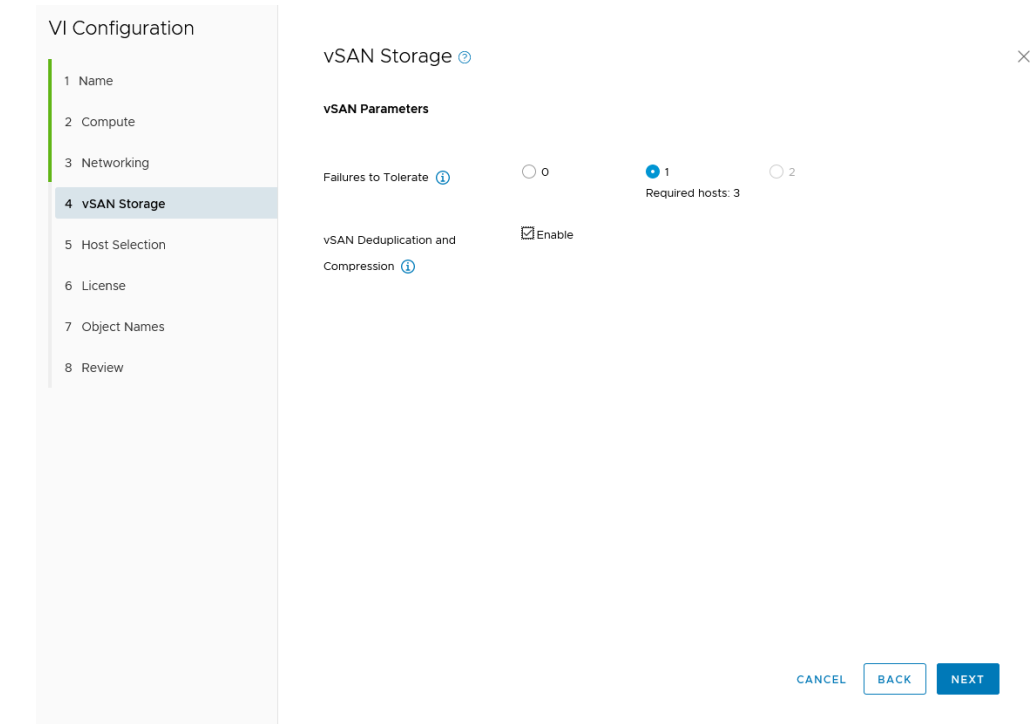

FIGURE 16. Adding a workload domain—vSAN storage

6. On the **Host Selection** screen, select the commissioned hosts that will be dedicated to this workload domain and click **Next**.
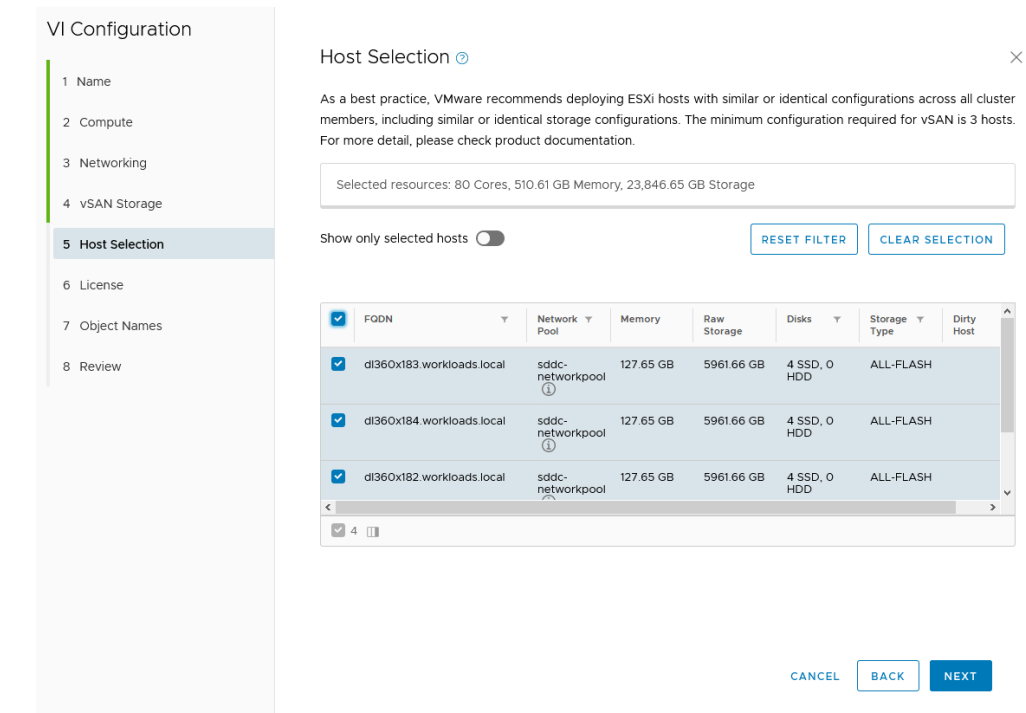

FIGURE 17. Adding a workload domain—Host Selection

7. On the **License** screen, select the appropriate licenses for NSX-V for vSphere, VMware vSAN, and VMware vSphere from the respective drop-down lists. If there are insufficient licenses for a product, additional license keys can be added from SDDC Manager UI under the License tab.
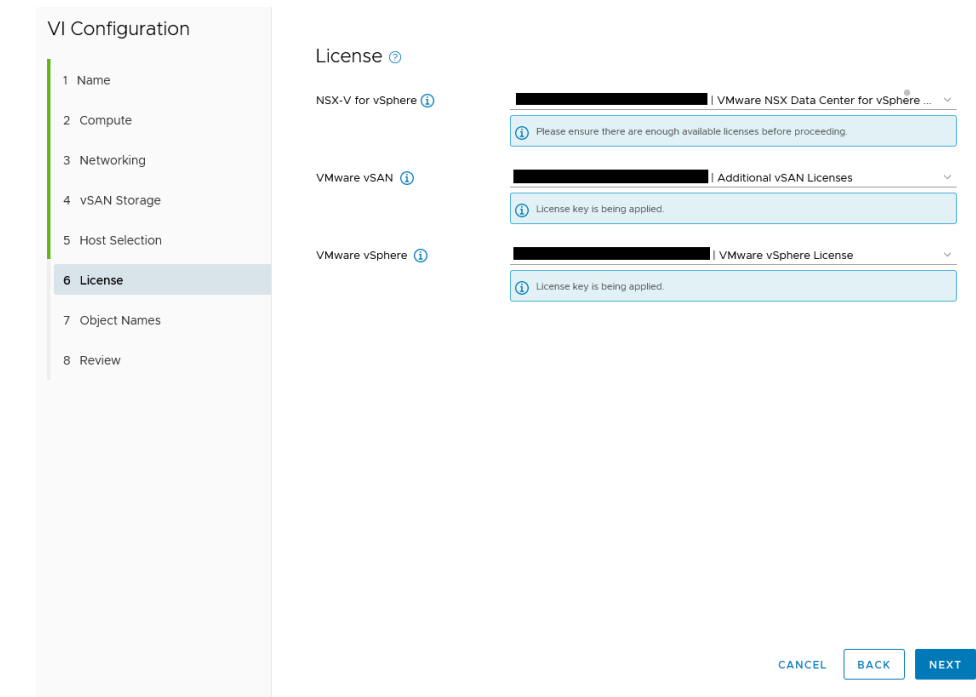

FIGURE 18. Adding a workload domain—License

8. The **Object Names** screen will display the auto-generated vSphere Object Names based on the user input in previous fields.
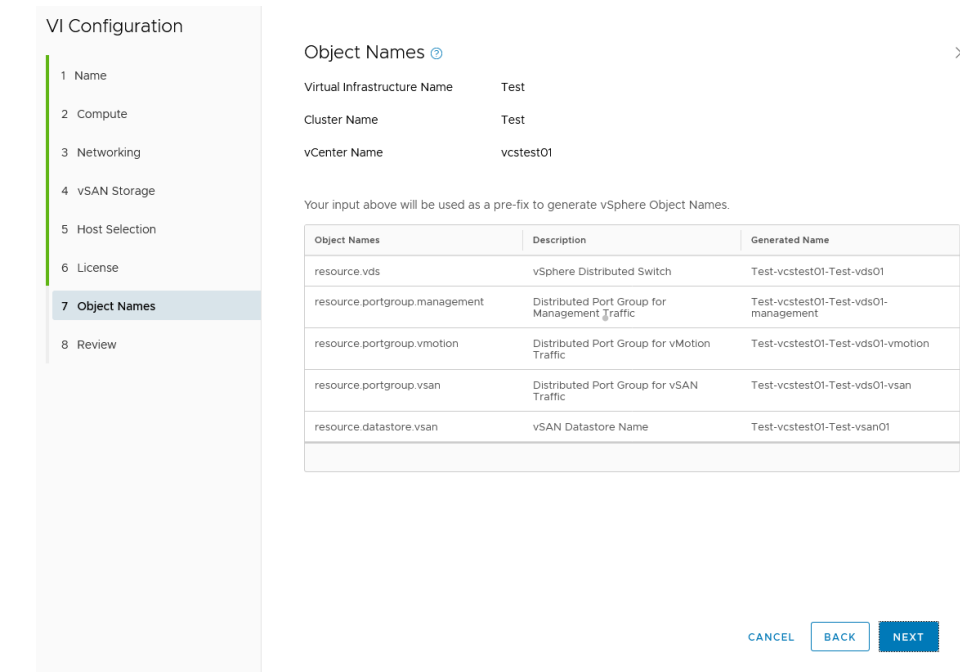

FIGURE 19. Adding a workload domain—Object Names

9. The final screen displays all the information entered for review. If satisfied, click **Finish** and the workload domain will be created.

VI Configuration

1 Name

2 Compute

3 Networking

4 vSAN Storage

5 Host Selection

6 License

7 Object Names

8 Review

Review ⓘ   ✕

∨ General

Virtual Infrastructure Name	Test
Cluster Name	Test
Organization Name	HPE

∨ Compute

vCenter IP Address	172.20.50.160
vCenter DNS Name	vcstest01.workloaads.local
vCenter Subnet Mask	255.255.255.0
vCenter Default Gateway	172.20.50.1

∨ Networking

VxLAN Networking VLAN ID	50
NSX Manager IP Address	172.20.50.162
NSX Manager DNS Name	nsxvtest01.workloads.local
NSX Manager Subnet Mask	255.255.255.0
NSX Manager Default Gateway	172.20.50.1
NSX Controller IP Address	172.20.50.163, 172.20.50.164, 172.20.50.165
NSX Controller Subnet Mask	255.255.255.0
NSX Controller Default Gateway	172.20.50.1

CANCEL   BACK   FINISH

FIGURE 20. Adding a workload domain—Review

TROUBLESHOOTING

1. The deployment logs for the Cloud Builder VM are located at: /opt/vmware/bringup/logs/vcf-bringup.log. If at any step the deployment of SDDC Manager fails and the logs provided in the UI are not descriptive enough, SSH into the Cloud Builder VM and access the logs stored at this location to find out the root cause of failure.

2. If an SSO connection timed out error is encountered during the bring-up process, ensure that the time is synchronized across all hosts and VMs that have been deployed thus far.

3. If a Platform Services Controller becomes unresponsive while using the SDDC Manager, go to the ESXi host on which the VM is deployed and reboot.

4. Workload domain creation may fail on the Deploy vCenter Server Appliance task and the retry option may be unsuccessful. This is a known issue with VMware Cloud Foundation 3.x. Refer to the workaround here: kb.vmware.com/s/article/67064.

Resources and additional links

- VMware Cloud Foundation Planning and Preparation Guide

- VMware Cloud Foundation Architecture and Deployment Guide

- VMware Cloud Foundation Operations and Administration Guide

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

**Make the right purchase decision.
Contact our presales specialists.**

Chat   **Email**   **Call**

→ **Share now**

🖥 **Get updates**

a50000778ENW, January 2020

**Hewlett Packard
Enterprise**