



NetApp Verified Architecture

# NetApp HCI for VMware Private Cloud

## NVA Deployment

Andy Banta, James Bradshaw, Eric Lozano, Chris Reno  
April 2019 | NVA-1122-DEPLOY | Version 1.0

### Abstract

This document describes the detailed deployment steps of a NetApp® Verified Architecture that uses VMware cloud-enablement products with NetApp HCI.



## TABLE OF CONTENTS

<b>1</b>	<b>NetApp HCI and Private Cloud Architectures.....</b>	<b>4</b>
<b>2</b>	<b>Solution Overview .....</b>	<b>4</b>
2.1	Solution Technology .....	5
2.2	NetApp HCI.....	5
2.3	VMware vRealize Suite.....	6
2.4	Use Case Summary.....	6
<b>3</b>	<b>Primary Use Case .....</b>	<b>6</b>
<b>4</b>	<b>NetApp HCI with VMware Private Cloud Technical Overview.....</b>	<b>7</b>
<b>5</b>	<b>Technology Requirements .....</b>	<b>7</b>
5.1	Hardware Requirements .....	7
5.2	Software Requirements .....	7
<b>6</b>	<b>Deployment Procedures .....</b>	<b>8</b>
6.1	Virtual Infrastructure Implementation with NetApp Deployment Engine.....	9
6.2	Operations and Cloud Management Implementation.....	37
6.3	vRealize Suite Configuration.....	50
<b>7</b>	<b>Solution Verification.....</b>	<b>63</b>
7.1	NetApp HCI and SPBM.....	63
7.2	NetApp HCI and vRealize Automation .....	64
7.3	NetApp HCI and vRealize Operations Manager.....	65
7.4	NetApp HCI and vRealize Log Insight.....	67
<b>8</b>	<b>Conclusion .....</b>	<b>69</b>
<b>Appendix.....</b>		<b>69</b>
	Sample Storage Node Switch Configuration .....	69
	Sample Compute Node Switch Configuration.....	70
	Modification to Standard vCenter Cluster in Preparation for VMware Private Cloud .....	70
	NSX Configuration.....	71
	<b>Where to Find Additional Information .....</b>	<b>75</b>

## LIST OF TABLES

Table 1)	Hardware requirements.....	7
Table 2)	Software requirements. ....	8
Table 3)	Required VLANs.....	11

Table 4) NSX required IP addresses. ....	11
Table 5) Required VMware private cloud IP addresses.....	12
Table 6) Service accounts in Active Directory. ....	22

## LIST OF FIGURES

Figure 1) NetApp HCI and VMware private cloud components. ....	5
Figure 2) NetApp HCI with VMware private cloud network topology. ....	10
Figure 3) NDE Network Settings Easy Form. ....	15
Figure 4) Export NDE setup information. ....	16
Figure 5) VMware vCenter cluster configuration. ....	24
Figure 6) VVols implementation on Element. ....	63
Figure 7) VVols implementation on Element. ....	63
Figure 8) VMware private cloud catalog. ....	64
Figure 9) VMware private cloud catalog. ....	65
Figure 10) NetApp HCI cluster overview. ....	66
Figure 11) NetApp HCI Health Investigation.....	67
Figure 12) NetApp HCI VVols details. ....	68
Figure 13) vRLI details. ....	68
Figure 14) vRLI details. ....	68

## 1 NetApp HCI and Private Cloud Architectures

NetApp® HCI provides compute and storage resources for a data center that can scale in a predictable and easy-to-manage manner. Modular components are combined to meet CPU, memory, capacity, and IOPS requirements for any environment.

VMware provides a hypervisor and management console to abstractly provision virtual machines (VMs) for practically any purpose. VMware also offers a suite of products to provide cloudlike provisioning and oversight of VMs, allowing customer self-service, centralized operations, debugging capabilities, and departmental or customer bill-back accounting. VMware defines the construct of the software-defined data center (SDDC), which enables private cloud models.

By combining NetApp HCI and VMware private cloud products, an IT department can quickly build out hardware resources at exactly the required capacity, without unused excesses. It further enables an IT department to conduct, troubleshoot, and monitor the environment from several utilities available from a single console. The combination also allows you to deploy VMs, either transiently or long term, using exactly the resources needed for the application. If your requirements change, you can alter the resource allocation dynamically to suit your needs without intervention by the IT staff. Finally, the combination allows detailed accounting of how the infrastructure is being used, both in provisioning and in actual use. Discrepancies between requirements and demands are easily identified, and separate departments and consumers can be accurately assessed for their use of the HCI environment.

## 2 Solution Overview

The combination of technologies from NetApp and VMware positions customers to take advantage of the benefits of a private cloud ecosystem. This NetApp Verified Architecture (NVA) details the deployment steps to construct a VMware private cloud architecture on NetApp HCI.

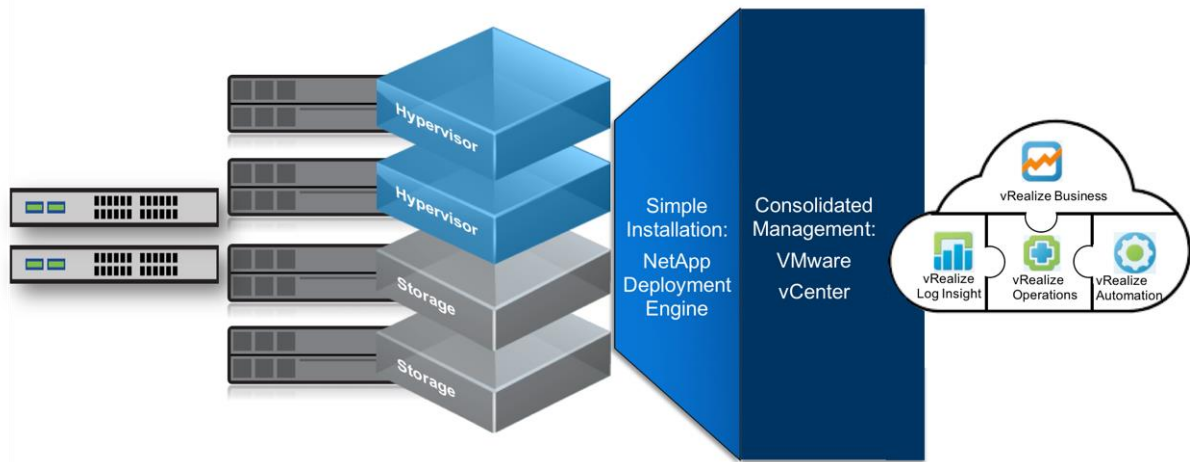
For information about the design considerations of this validation, see the [VMware Private Cloud on NetApp HCI NVA Design Guide](#).

NetApp HCI is a hybrid cloud infrastructure solution that is capable of transforming and empowering organizations to move faster, drive operational efficiencies, and reduce costs. NetApp HCI is the foundation of a private cloud strategy, running multiple applications with the predictable performance that enterprises and customers demand. NetApp HCI with VMware private cloud can be deployed in minutes with a turnkey cloud infrastructure, which eliminates the complex management of traditional three-tier architectures. Integration into the NetApp Data Fabric means that you can unleash the full power of your applications, with the data services they require, across any infrastructure or cloud.

VMware private cloud, consisting of multiple components of the vRealize Suite, VMware NSX, and NetApp HCI, allows customers to deploy VMs using the resources required on an infrastructure that can be deployed quickly and scale as needs change.

Figure 1 shows NetApp HCI and VMware private cloud suite of products.

Figure 1) NetApp HCI and VMware private cloud components.



## 2.1 Solution Technology

NetApp HCI and VMware private cloud products form an integrated system that offers all the benefits of VMware private cloud and the scalability and granularity of NetApp HCI.

## 2.2 NetApp HCI

The underlying NetApp HCI platform allows expanding or resizing a data center according to CPU, memory, storage capacity, and storage IOPS requirements. NetApp HCI also lets you add and repurpose compute and storage nodes of various capacities to expand or contract any of the compute or storage parameters according to the data center's needs. This scaling is managed through vCenter and the NetApp Deployment Engine (NDE). NDE manages the hardware configuration and deployment of the NetApp HCI environment. This means that compute and NetApp HCI storage nodes can be added or deleted easily in any configuration. Compute nodes can easily be added to the VMware cloud configuration by adding them to the vCenter data center and compute clusters. Storage nodes are added to the NetApp HCI cluster transparently to the VMware cloud management. Capacity and throughput are added or managed this way, and they simply become available to the VMware private cloud.

VMware management tools are used to add compute nodes to available data centers and compute clusters, and compute resources can be dynamically applied by using VMware Distributed Resource Scheduling (DRS).

The NetApp SolidFire® Plug-In for VMware vCenter Server can be used to perform configuration and management actions of the underlying NetApp Element® storage cluster, all within vCenter. This simplifies the management and configuration by allowing you to use the integrated plug-ins to add and manage clusters, datastores, and quality of service (QoS) policies, enable virtual volumes, and monitor events throughout the deployed cluster. to here

Use of VMware Virtual Volumes (VVOs) allows more flexible VM allocation, with capacities matching the capacities of the NetApp HCI cluster. You can manage the VM throughput and latency requirements with virtual-disk granularity by using VMware Storage Policy-Based Management (SPBM).

Multitenancy is a core capability of NetApp HCI. Guaranteed QoS enables control over performance in large-scale environments of multiple, high-demand workloads. By setting the QoS levels on the volumes in a multitenant environment, you can guarantee individual SLAs. NetApp HCI allows setting SLAs on varied, disparate workloads on the same system, ensuring that the different workloads don't interfere with each other, while each receives the required performance. These are the underpinnings of multitenancy

on NetApp HCI, which means that a single NetApp HCI system can prevent numerous siloed data centers for an enterprise or service provider.

For more information about NetApp HCI, see the [NetApp HCI product page](#).

## 2.3 VMware vRealize Suite

In addition to virtualized infrastructure components such as vSphere and vCenter, VMware provides the VMware vRealize Suite of products to aid in the construction of an SDDC. Multiple components comprise the vRealize Suite, allowing you to build an SDDC that meets the needs of your organization. These products include:

- vRealize Suite Lifecycle Manager (vRLCM)
- vRealize Automation (vRA)
- vRealize Operations Manager (vROps)
- vRealize Log Insight (vRLI)
- vRealize Business for Cloud

The VMware vRealize Suite is a comprehensive management framework for private cloud deployments. It accelerates adoption and delivery of new workloads and VMs through task automation, simultaneously providing insight and monitoring of the infrastructure.

For more information about the vRealize Suite, see <https://www.vmware.com/products/vrealize-suite.html>.

## 2.4 Use Case Summary

In addition to the benefits just described, NetApp HCI is architected to deliver exceptional value for the following use cases:

- Private cloud deployments
- Virtual desktop infrastructure for end-user computing environments
- Workload consolidation

# 3 Primary Use Case

NetApp HCI targets three use cases. The deployment documented in this guide focuses primarily on the private cloud use cases, specifically with VMware vRealize Suite elements.

NetApp HCI is an optimal foundation for an enterprise or service provider private cloud model. This is because NetApp HCI uses the capabilities of native NetApp Element software to provide on-demand provisioning of workloads through storage drivers and management plug-ins.

As an example, NetApp HCI integrates with VMware VVols, enabling VMware administrators to achieve granular control over storage performance on a per-VM basis. This means that you can set minimum, maximum, and burst IOPS levels, specifying service levels and performance for even the most sensitive VMs. And you can change capacity and performance dynamically without migrating data or affecting system performance.

VMware private cloud also incorporates the vRealize Suite, which includes management operations automation, business accounting, and more in-depth log analysis. The vRealize Suite provides more thorough operations management, including integration with management packs available from NetApp specifically for providing more information about NetApp HCI. It also directly links to vRLI, which provides elaborate integration to logs from various products and tools. vRA gives role-based access to any automation processes you can create, either for administrative use or for the end consumers.

These additions from the vRealize Suite convert NetApp HCI from a commonplace virtualization platform to an enterprise-wide environment for numerous consumers, without a lot of administrator oversight.

## 4 NetApp HCI with VMware Private Cloud Technical Overview

Hyperconverged infrastructure has promised the industry simplicity of deployment, ease of operation, and scale. However, the inherent design of most modern HCI systems limits the ability to deliver on one or more of these promises. NetApp HCI is a hybrid cloud infrastructure that brings together simplicity of configuration, efficiency of operation, and elasticity of scale, in a single product.

Similarly, the term *private cloud* has many definitions and interpretations. Virtualization is the first step toward a software-defined data center. Combining virtualization, software defined networking, and components of the vRealize suite yields a true private cloud, enabling you to self-provision resources from a service catalog, manage chargeback, and maintain SLAs across business units and customers can be achieved.

When NetApp HCI is combined with VMware components that define an SDDC, customers realize the benefits of a private cloud.

For a technical overview of NetApp HCI, see the [NetApp HCI Theory of Operations](#).

For a technical overview of SDDC and VMware private cloud, see the [Software-Defined Data Center – In-Depth](#) solution page.

## 5 Technology Requirements

This section covers the technology requirements for the VMware private cloud with NetApp HCI solution.

### 5.1 Hardware Requirements

Table 1 lists the hardware components that are required to implement the validated solution. The components that are used in any particular implementation of the solution might vary according to customer requirements.

**Note:** Because several deployment options are available, the hardware requirements do not include specific switch infrastructure. For details about these requirements, see the section “Network and Switch Requirements.”

Table 1) Hardware requirements.

Hardware	Minimum Quantity
Compute node: NetApp H500E*	4
Storage node: NetApp H500S*	4

\*The H500E and H500S have been updated with a midcycle refresh to enable more configuration options. These nodes are currently listed as H410C and H410S and are completely interoperable with the previous nodes and chassis.

### 5.2 Software Requirements

Table 2 lists the software components that are required to implement the solution. Because of the layering aspect of VMware private cloud, the components that are used in any implementation of the solution might vary according to customer requirements.

**Table 2) Software requirements.**

Product Family	Product Name	Product Version
VMware vSphere Enterprise Plus	ESXi*	6.5 U1
	vCenter Server Appliance*	6.5 U1
VMware NSX for vSphere Enterprise	NSX for vSphere*	6.4.1
VMware vRealize Automation (Advanced or higher)	vRealize Orchestrator (vRO)	7.4
	vRealize Suite Lifecycle Manager	2.0
	vRealize Automation*	7.5
VMware vRealize Operations Manager (Advanced or higher)	vRealize Operations Manager*	6.7.0
	vRealize Operations Management Pack for NSX for vSphere	3.5.1
	vRealize Operations Management Pack for Storage Devices	6.0.5
	vRealize Operations Management Pack for VMware Site Recovery Manager	6.5.1.1
VMware vRealize Log Insight	vRealize Log Insight*	4.7.0
	vRealize Log Insight Content Pack for NSX for vSphere	3.6
NetApp	NetApp Element software	10.3.0.157
	NDE	1.4
	NetApp ONTAP® Select (file services) *	9.3P2

**Note:** \* Denotes licensed product.

## 6 Deployment Procedures

This section describes the steps required to deploy a VMware private cloud aligned with several SDDC tenants including primary storage, software defined storage (SDS), software defined networking (SDN), and components of the vRealize Suite. These steps include review of the prerequisites, deployment of the physical infrastructure, and configuration of the NetApp HCI system with VMware vCenter 6.5u1, VMware NSX, vRLCM, vROps, vRA, and vRLI.

Where appropriate, sample automation or manual steps are provided to reconfigure and deploy VMware components. Automation is provided using pyVmommi, VMware's Python SDK for the vSphere API and detailed manual steps are referenced in the appendix where relevant.

The sample automation is free to use and available at <https://github.com/solidfire/pyNSXdeploy>.

**Note:** NetApp does not support sample scripts used in this document.

For more information about the NetApp and VMware's SDK toolkit, see <https://vmware.github.io/vsphere-automation-sdk/>.



The steps to deploy the NetApp HCI with VMware private cloud solution include:

Implementation of virtual infrastructure with NetApp Deployment Engine

---

Implementation of operations and cloud management

---

Configuration of VMware vRealize Suite

---

**Note:** The variables used in this validation are covered for the initial system setup. However, detailed guidance for deploying the NetApp HCI system is beyond the scope of this document.

## 6.1 Virtual Infrastructure Implementation with NetApp Deployment Engine

NetApp Deployment Engine (NDE) simplifies day 0 operations by reducing the number of manual steps from over 400 to less than 30. This document assumes a successful completion of NDE followed by virtual infrastructure modifications to support VMware private cloud.

The implementation of the virtual Infrastructure with NDE includes the following steps:

NDE execution prerequisites

---

NDE execution

---

Post NDE configuration

---

### NDE Execution Prerequisites

Consult the [NetApp HCI Prerequisites Checklist](#) to see the requirements and recommendations for NetApp HCI before you begin deployment.

The following are high-level requirements for NDE:

Network and switch requirements

---

Preparation of the required VLAN IDs

---

Network requirements for NSX

---

Switch configuration

---

IP address requirements for NetApp HCI and VMware

---

DNS and timekeeping requirements

---

Final preparations

---

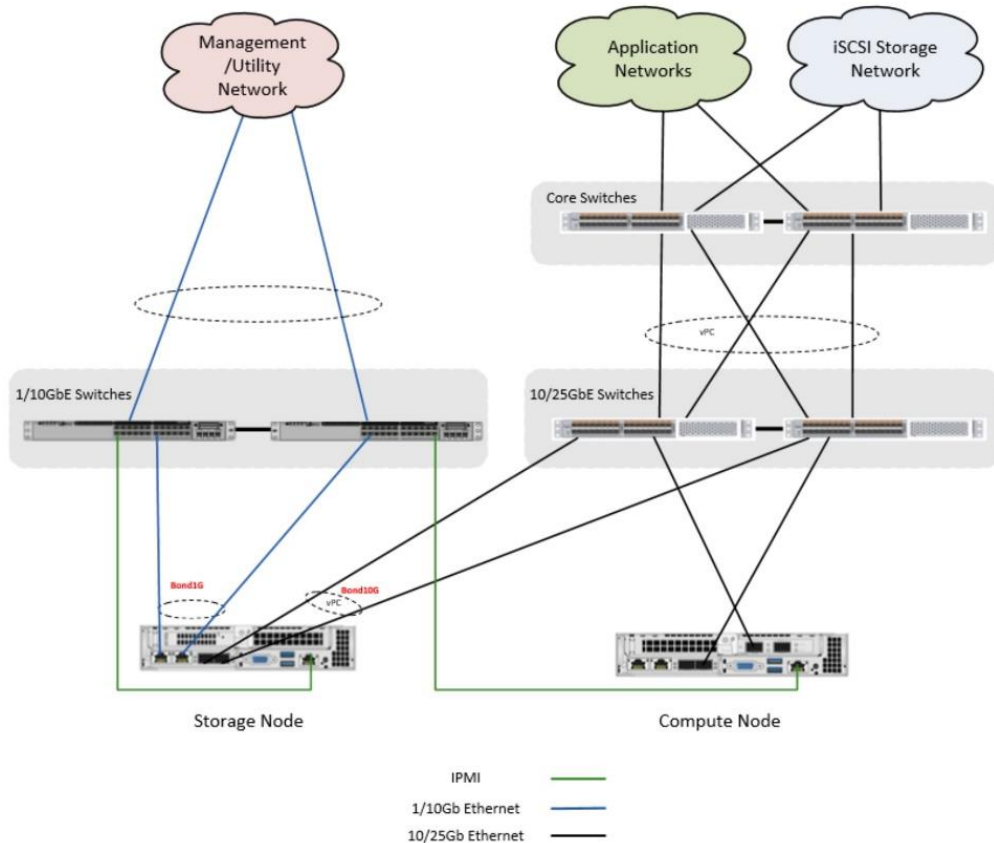
### Network and Switch Requirements

The switches used to transfer NetApp HCI traffic require a specific configuration for successful deployment.

See the [NetApp HCI Network Setup Guide](#) for the physical cabling and switch details. This NVA uses a two-cable design for compute nodes. Optionally, compute nodes can be configured in a six-node cable design affording options for deployment of compute nodes.

Figure 2 depicts the network topology of this NetApp HCI with VMware private cloud architecture with a two-cable design for compute nodes.

Figure 2) NetApp HCI with VMware private cloud network topology.



NetApp HCI has the following switch requirements:

- All switch ports connected to NetApp HCI nodes must be configured to allow the Spanning Tree Protocol (STP) to enter the forwarding state immediately; on Cisco switches, this functionality is known as PortFast. Ports connected to NetApp HCI nodes should not receive STP Bridge Protocol Data Units (BPDUs).
- The switches handling storage, virtual machine, and vMotion traffic must support speeds of at least 10GbE per port (up to 25GbE per port is supported).
- The switches handling management traffic must support speeds of at least 1GbE per port.
- The MTU size on the switches handling storage traffic must be 9216 bytes end-to-end for a successful installation (MTU size is configured on the storage node interfaces automatically).
- Cisco Virtual PortChannel (vPC), Multi-chassis Link Aggregation (MLAG), or the equivalent switch stacking technology for your switches must be configured on the switches handling the storage network for NetApp HCI. Switch stacking technology eases configuration of Link Aggregation Control Protocol (LACP) and port channels. It provides a loop-free topology between switches and the 10/25GbE ports on the storage nodes.
- The switch ports connected to the 10/25GbE interfaces on NetApp HCI storage nodes must be configured as an LACP port channel.

- The LACP timers on the switches handling storage traffic must be set to “fast mode (1s)” for optimal failover detection time. During deployment, the Bond1G interface on all NetApp HCI storage nodes are automatically configured for active-passive mode.
- Round-trip network latency between all storage and compute nodes should not exceed 2ms.

You must implement the following best practices to prepare your network for NetApp HCI deployment:

- You should install as many switches as is needed to meet high-availability requirements.
- You should balance 1/10GbE port traffic between at least two 1/10GbE capable management switches.
- You should balance 10/25GbE port traffic between two 10GbE capable switches.

## Prepare Required VLAN IDs

NetApp HCI deployment requires multiple logical network segments, one for each of the following types of traffic:

- Management
- VMware network
- vMotion
- Storage

Table 3 lists the necessary VLANs for deployment, as outlined in this validation. NetApp recommends configuring these VLANs on the network switches before executing the NDE.

**Table 3) Required VLANs.**

Network Segment	Details	VLAN ID
Out-of-band management network	Network for HCI terminal user interface (TUI)	16
In-band management network	Network for accessing management interfaces of nodes, hosts, and guests	3496
VMware vMotion	Network for live migration of VMs	3495
SAN storage	Network for iSCSI storage traffic	3494
NAS storage	Network for NFS storage traffic	3493
VM network	Network for VM traffic	3490
NSX VLAN for VTEPs	Network for VXLAN VTEPs	3492

## Network Requirements for VMware NSX

VMware NSX requires multiple IP addresses. Table 4 lists number of IP addresses required for NSX. Unless otherwise indicated, addresses are assigned automatically with NDE.

**Table 4) NSX required IP addresses.**

IP Address Qty	Details	VLAN ID/ VNI
1 per interface	External tenant connectivity	186
2 per host	NSX VXLAN VTEPs	3492
1 per host	VXLAN (transit)	3491

IP Address Qty	Details	VLAN ID/ VNI
1 per VM	VXLAN (app 1)	5000
1 per VM	VXLAN (app 2)	5001
1 per VM	VXLAN (app 3)	5002

## Switch Configuration

NetApp HCI has specific physical and network requirements for an enterprise-grade data center deployment. As a part of prerequisites to run NDE, it is assumed that the switches are deployed and have corresponding relevant configuration for the compute and storage ports.

This solution uses Cisco Nexus switches and provides relevant configuration for compute and storage ports on NetApp HCI. The complete switch configuration is beyond the scope of this document.

It is assumed that the switches have been installed, cabled, and the initial configuration such as NTP, default gateway, management IP, port descriptions, and other relevant global configurations are completed. Switch features such as LACP, vPC, defined in section “Network and Switch Requirements” should be enabled on the switches.

Detailed description about the switch configuration is beyond the scope of this document. Sample switch port configurations for storage and compute nodes are included in the appendix.

## IP Address Requirements for NetApp HCI and VMware Components

NetApp HCI deployment and VMware private cloud require multiple IP addresses to be allocated. Table 5 lists the number of IP addresses required. Unless otherwise indicated, addresses are assigned automatically with NDE.

**Table 5) Required VMware private cloud IP addresses.**

IP Address Qty	Details	VLAN ID
1 per storage and compute node*	HCI terminal user interface (TUI) addresses	16
1 per vCenter Server (VM)	vCenter Server management address	3496
1 per management node (VM)	Management node IP Address	
1 for file services (VM)	NFS / ONTAP appliance node and cluster management addresses	
1 per ESXi host	ESXi compute management addresses	
1 per storage node	NetApp HCI storage node management addresses	
1 per storage cluster	Storage cluster management address	
10 total for vRealize Suite**	vRealize Suite VMs management addresses	
1 per ESXi host**	NSX VXLAN VTEPs	
1 per ESXi host	VMware vMotion address	3495
2 per ESXi host	ESXi host initiator address for iSCSI storage traffic	3494
2 per storage node	Storage node target address for iSCSI storage traffic	

IP Address Qty	Details	VLAN ID
1 per storage cluster	Storage cluster target address for iSCSI storage traffic	
1 per ESXi host**	ESXi host VMkernel interface for NFS storage traffic	3493
1 per storage virtual machine (SVM)**	Storage LIF for NFS storage traffic	
1+ per guest VM**	IP address for VM network; assigned based on use case	3490

\*This validation requires the initial setup of the first storage node TUI address. NDE automatically assigns the TUI address for subsequent nodes.

\*\*Addresses are assigned after NDE completes.

## DNS and Timekeeping Requirements

Depending on your deployment, you might need to prepare DNS records for your NetApp HCI system. NetApp HCI requires a valid NTP server for timekeeping; you can use a publicly available time server if you do not have one in your environment.

This validation involves deploying NetApp HCI with a new VMware vCenter Server instance using a fully qualified domain name (FQDN). Before deployment, you must have one pointer (PTR) record and one address (A) record created on the DNS server.

## Final Preparations

For instructions on deploying NetApp H-Series system, see the [Installation and Setup Instructions Guide](#). This document covers:

- Preparation for installation: gathering all relevant information about your network, current or planned VMware Infrastructure, and planned user credentials.
- Preparation of hardware: installing, cabling, and powering on the NetApp HCI system.
- Configuration of NetApp HCI using the NDE.

For more information about the rack setup of your NetApp HCI system, see the [NetApp HCI Rail Kit Installation Flyer](#).

For detailed deployment steps of HCI System, see the [NetApp HCI Deployment Guide Version 1.4](#).

Before executing the NDE, do as follows:

Review the installation and setup instructions guide

---

Review the HCI rail kit installation flyer

---

Install the HCI system

---

Cable the HCI system

---

Prepare to execute the NDE

---

## NDE Execution

Before you execute the NDE, you must complete the rack and stack of all components, configuration of the network switches, and verification of all prerequisites. You can execute NDE by connecting to the management address of a single storage node if you plan to allow NDE to automatically configure all addresses.

NDE performs the following tasks to bring an HCI system online:

1. Installs the storage node (NetApp Element software) on a minimum of four storage nodes.
2. Installs the VMware hypervisor on a minimum of two compute nodes.
3. Installs VMware vCenter to manage the entire NetApp HCI stack.
4. Installs and configures the NetApp storage management node and NetApp Monitoring Agent.
5. Installs and configures for management access an ONTAP Select appliance.

**Note:** This validation uses NDE to automatically configure all addresses. You can also set up DHCP in your environment or manually assign IP addresses for each storage node and compute node. These steps are not covered in this guide.

**Note:** As mentioned previously, this validation uses a two-cable configuration for compute nodes.

**Note:** Detailed steps for the NDE are not covered in this document.

To execute NDE, do as follows:

Launch NDE

---

Export the configuration after NDE completion

---

### Launch NDE

To execute NDE, complete the following steps:

1. Navigate to the management address of the first storage node.

**Note:** <http://172.21.240.221:442/nde> is the example address used for this validation where the NodeMIP is the management IP address of the first storage node, configured in the TUI.

2. Complete the installation wizard.

Figure 3 shows the Network Settings Easy form for this validation, which is completed during NDE.

Figure 3) NDE Network Settings Easy Form.

### Network Settings Easy Form

Enter values on this easy form to define Network Settings, or overwrite existing Network Settings.  
Note, empty form fields will not overwrite existing values.

Naming Prefix ?  ✓

Will you assign VLAN IDs? ☒ Yes ☐ No

Your network topology selection requires VLAN IDs for certain networks.

#### Management Network

	VLAN ID	Subnet <span>?</span>	Default Gateway	Starting IP	
vCenter Server Apply to 1 IP address	<input type="text" value="3496"/> <span>✓</span>	<input type="text" value="172.21.240.0/24"/> <span>✓</span>	<input type="text" value="172.21.240.1"/> <span>✓</span>	<input type="text" value="172.21.240.20"/> <span>✓</span>	<input type="button" value="Clear"/>
Management Node Apply to 1 IP address	<input type="text" value="3496"/> <span>✓</span>	<input type="text" value="172.21.240.0/24"/> <span>✓</span>	<input type="text" value="172.21.240.1"/> <span>✓</span>	<input type="text" value="172.21.240.21"/> <span>✓</span>	<input type="button" value="Clear"/>
File Services Apply to 2 IP addresses	<input type="text" value="3496"/> <span>✓</span>	<input type="text" value="172.21.240.0/24"/> <span>✓</span>	<input type="text" value="172.21.240.1"/> <span>✓</span>	<input type="text" value="172.21.240.22"/> <span>✓</span>	<input type="button" value="Clear"/>
Compute Management Apply to 2 IP addresses	<input type="text" value="3496"/> <span>✓</span>	<input type="text" value="172.21.240.0/24"/> <span>✓</span>	<input type="text" value="172.21.240.1"/> <span>✓</span>	<input type="text" value="172.21.240.24"/> <span>✓</span>	<input type="button" value="Clear"/>
Storage Management Apply to 5 IP addresses	<input type="text" value="3496"/> <span>✓</span>	<input type="text" value="172.21.240.0/24"/> <span>✓</span>	<input type="text" value="172.21.240.1"/> <span>✓</span>	<input type="text" value="172.21.240.26"/> <span>✓</span>	<input type="button" value="Clear"/>

#### vMotion Network

	VLAN ID	Subnet	Default Gateway	Starting IP	
Compute vMotion Apply to 2 IP addresses	<input type="text" value="3495"/> <span>✓</span>	<input type="text" value="172.21.238.0/24"/> <span>✓</span>	<input type="text" value="172.21.238.1"/> <span>✓</span>	<input type="text" value="172.21.238.20"/> <span>✓</span>	<input type="button" value="Clear"/>

#### iSCSI Network

	VLAN ID	Subnet	Default Gateway	Starting IP	
iSCSI Network Apply to 9 IP addresses	<input type="text" value="3494"/> <span>✓</span>	<input type="text" value="172.21.238.0/24"/> <span>✓</span>	<input type="text" value="172.21.238.1"/> <span>✓</span>	<input type="text" value="172.21.238.20"/> <span>✓</span>	<input type="button" value="Clear"/>

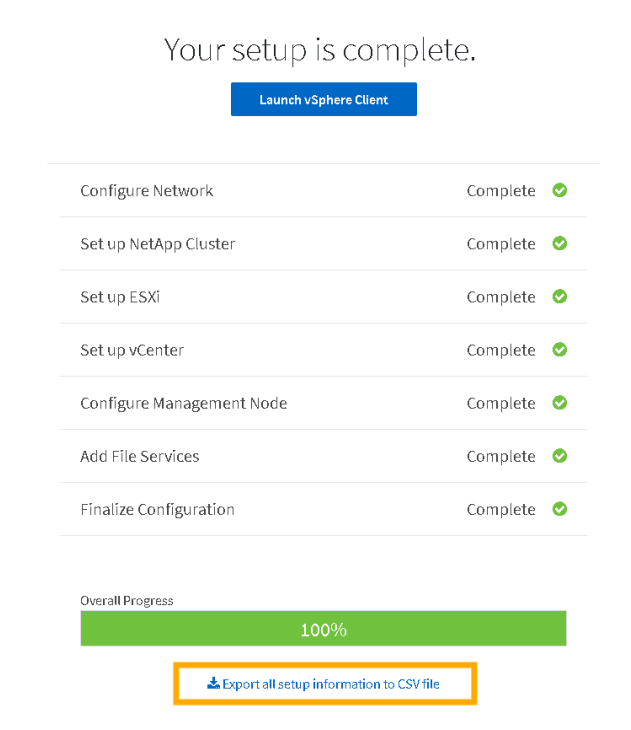
## Export Configuration After NDE Completion

After the successful deployment of NDE, export the HCI configuration from the Progress dialog box (Figure 4). This information is valuable for future automation exercises.

To export the configuration settings, complete the following step.

1. In the Your Setup is Complete dialog box, click “Export all setup information to CSV file.”  
The setup information about the installation will download in the CSV format.

**Figure 4) Export NDE setup information.**



## Post NDE Configuration

After the successful deployment of the HCI system using the NDE, there are various preparations that must be completed before configuring SDS through file services with ONTAP Select, tenant SDN with NSX, and VMware private cloud components.

Before deploying NetApp ONTAP Select, VMware NSX, and vRealize Suite, complete the following steps:

Deploy VMware NSX

Active Directory considerations

Enable service accounts privileges

Configure management cluster, shared edge and compute cluster

VMware licensing

Modify VMware Distributed Switch (vDS) (optional)

Configure VMware configuration for file services

Configure file services with ONTAP Select

Enable VVols and create storage container

Create SPBM policy



## Deploy VMware NSX

After deploying the HCI system through NDE and preparing the environment, you are ready to deploy tenant software-defined networking and VMware private cloud components.

NetApp has provided a sample Python script for deploying NSX. The manual steps to deploy NSX, are included in section “NSX Configuration.” You can find the sample script at <https://github.com/solidfire/pyNSXdeploy>.

The sample NSX deployment script configures NSX as follows:

1. Deploys NSX Manager.
2. Registers NSX Manager with vCenter.
3. Deploys NSX controllers.
4. Prepares hosts and cluster for NSX.
5. Prepares and configure logical networking.

The steps in this section details how to:

- Prepare environment for sample script
- Deploy the NSX Manager
- Configure the NSX Manager
- Confirm the NSX deployment

### Prepare Environment for Sample Script

To prepare your environment to execute the sample script, complete the following steps.

1. Install Python 3.6.6 on a system with access to the management network of the HCI environment.
2. Install the required packages.

```
pip3 install --upgrade pyvim requests vcrpy pyvmomi suds-jurko lxml ipaddress
```

3. Install Git with the Windows or Linux installer. Add the Git binary location to PATH (if not completed by the installer).
4. Download the pyVmomi community samples from GitHub.

```
git clone https://github.com/vmware/pyvmomi-community-samples.git
```

5. Install the pyVmomi community samples from the directory.

```
setup.py install
```

6. Clone the pyNSXdeploy scripts from the NetApp GitHub site to a local directory.

```
git clone https://github.com/solidfire/pyNSXdeploy/blob/master/deploy_nsx_manager.py
```

7. Copy the "tools" directory to the pyNSXdeploy directory under pyvmomi-community-samples/samples/tools.

### Deploy the NSX Manager

After you have prepared to run the script, complete the following step to deploy NSX Manager.

1. Modify and execute the sample script to deploy NSX Manager.

```
python ./deploy_nsx_manager.py -s vmpr-rtp-vc.sddc.netapp.com -u administrator@vsphere.local -p NetApp!23 -S -ds NetApp-HCI-Datastore-02 --ova-path "E:\Software\VMware\NSX\VMware-NSX-Manager-6.4.1-8599035.ova" -vsm_cli_passwd_0 NetApp!23NetApp!23 -vsm_cli_en_passwd_0 NetApp!23NetApp!23 -vsm_hostname vmpr-rtp-nsx-01 -vsm_ip_0 172.21.240.121 -vsm_netmask_0 255.255.255.0 -vsm_gateway_0 172.21.240.4 -vsm_ntp_0 172.21.240.7 -vsm_dns1_0 10.61.186.231 -map_eth0_to_network "Management Network" -cluster Management
```

**Note:** Wait 5-10 minutes before configuring NSX Manager.

## Configure the NSX Manager

After deploying the NSX Manager, complete the following step to configure the NSX Manager.

1. Modify and execute the sample script to configure the NSX Manager.

```
Python ./configure_nsx_manager.py -nsx_manager_address nsxmanager1.vmwpc.local -
nsx_manager_username admin -nsx_manager_password NetApp123!NetApp123! -s vmwpc-vcsa1.vmwpc.local
-u administrator@vsphere.local -p NetApp123! -S -VTEP_IP_Range 10.193.138.104-10.193.138.113 -
VTEP_Mask /24 -VTEP_Gateway 10.193.138.1 -VTEP_DNS 10.193.138.39 -VTEP_domain vmwpc.local -
lookup_service_address vmwpc-vcsa1.vmwpc.local -VTEP_VLAN_ID 20 -Controller_IP_Range
10.193.138.101-10.193.138.103 -Controller_Mask /24 -Controller_Gateway 10.193.138.1 -
Controller_Cluster Management -Controller_DNS 10.193.138.39 -Controller_domain vmwpc.local -
Controller_Datastores
Management_Cluster_Datastore_1,Management_Cluster_Datastore_2,Management_Cluster_Datastore_3 -
Controller_Network_Management_VMs -Controller_Password NetApp123!NetApp123! -DVS Compute_DVS -
cluster_prep_list Compute -key <insert NSX license key>
```

**Note:** Insert NSX license key for “Compute -key”.

## Confirm NSX Deployment

To confirm the NSX deployment, complete the following steps:

1. Navigate to the [https://<ip\\_address\\_NSX\\_Manager>](https://<ip_address_NSX_Manager>).
2. Enter the admin credentials.
3. Click Manage.
4. Click NSX Management Service and verify vCenter connectivity.

**vCenter Server** Edit

Connecting to a vCenter server enables NSX Management Service to display the VMware Infrastructure inventory. HTTPS port (443) needs to be opened for communication between NSX Management Service, ESX and VC. For a full list of ports required, see section 'Client and User Access' of Chapter 'Preparing for Installation' in the 'NSX Installation Guide'.

If your vCenter server is hosted by a vCenter Server Appliance, please ensure that appropriate CPU and memory reservation is given to this appliance VM. After successful configuration of vCenter on NSX Manager, you need to log out of any active client sessions on vSphere Web Client and log back in to enable NSX user interface components.

vCenter Server:	172.21.240.201
vCenter User Name:	administrator@vsphere.local
Status:	<span style="color: green;">●</span> Connected - Last successful inventory update was on Wednesday, September 19, 2018, 3:21:48 PM EDT

## Active Directory Considerations

Organizations that use Windows Active Directory, should add the vCenter instance to their environment. This addition simplifies user management and improves auditing.

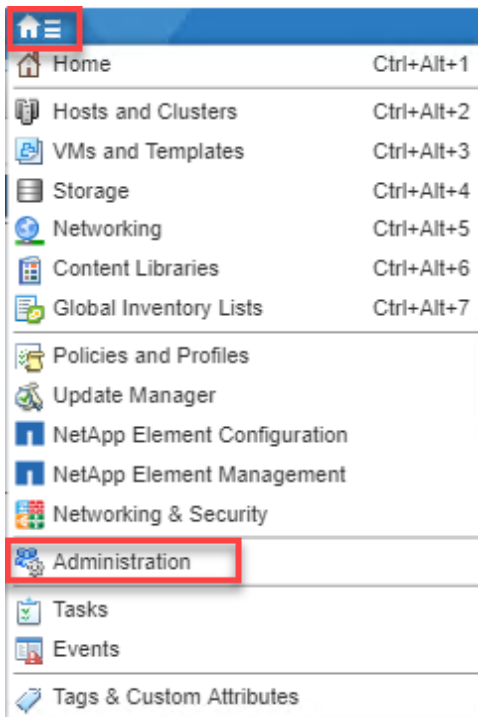
The steps in this section detail how to:

- Join vCenter instance to Active Directory
- Add Active Directory Authentication in vCenter

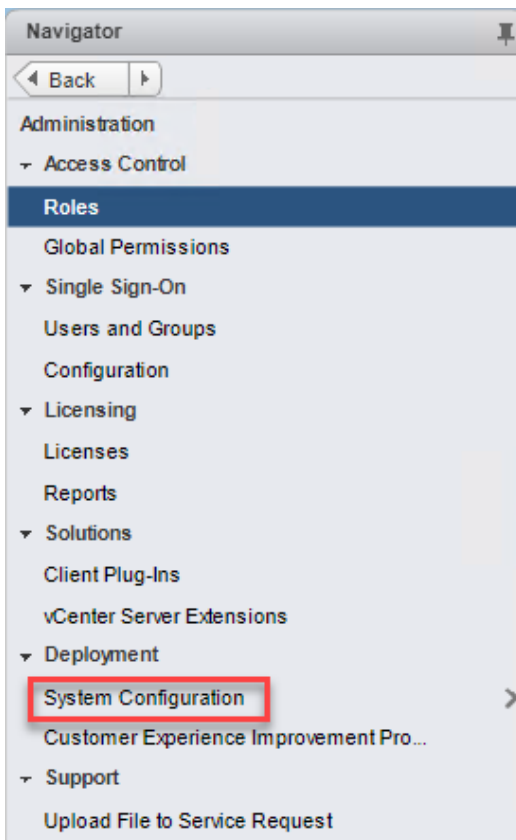
## Join vCenter Instance to Active Directory

To join the vCenter instance to Active Directory, complete the following steps:

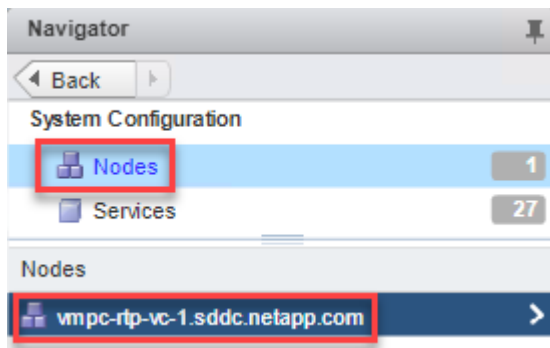
1. Log in to vSphere Web Client.
2. Navigate to Home > Administration.



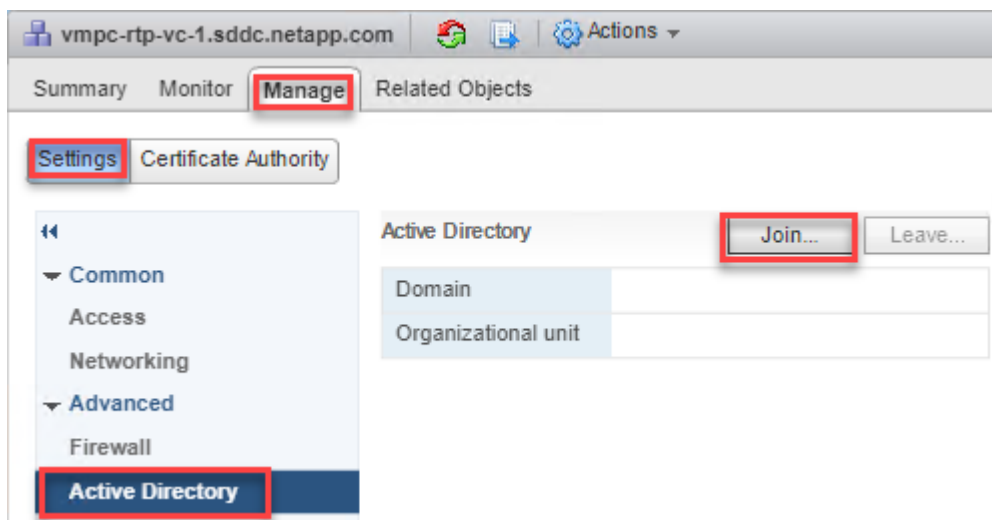
3. Under Deployment, select System Configuration.



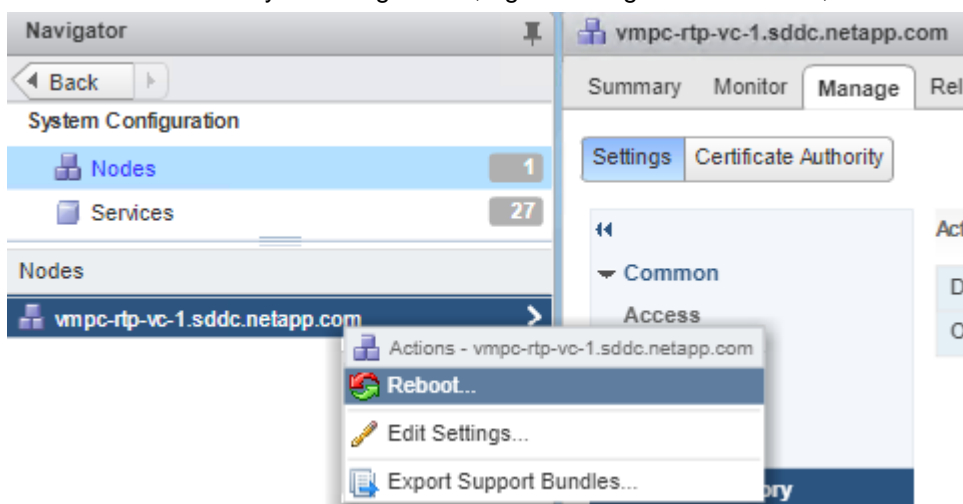
4. Navigate to Nodes and select the vCenter FQDN.



5. Go to Manage > Settings > Advanced > Active Directory and then click Join.



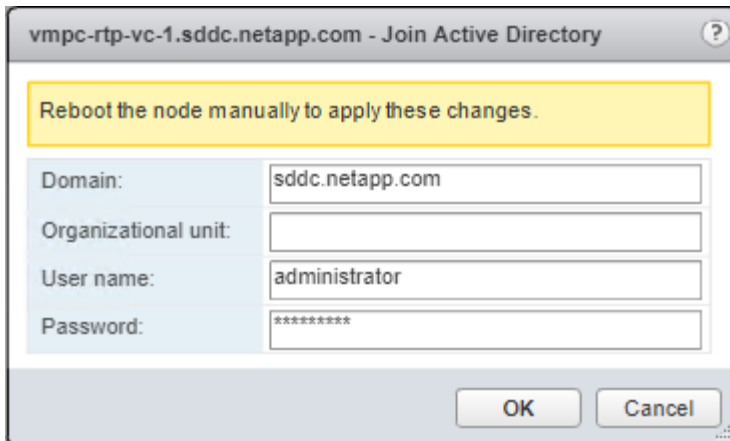
6. Enter domain, OU, user name and password. Click OK.
7. Reboot vCenter by selecting Nodes, right-clicking vCenter FQDN, and then selecting Reboot.



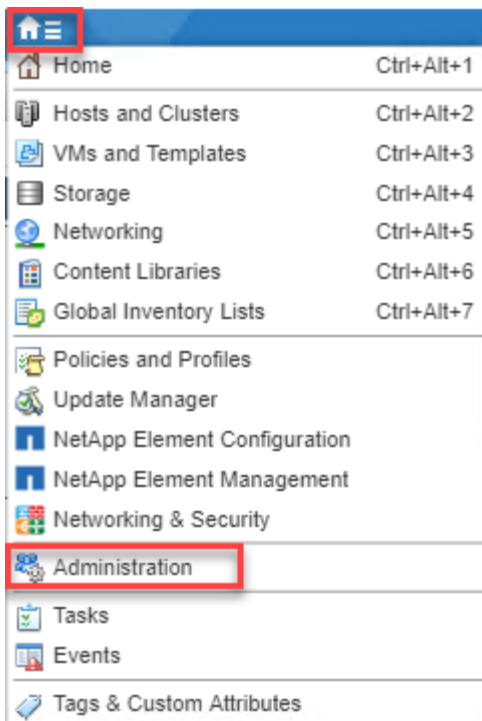
## Add Active Directory Authentication in vCenter

To add Active Directory authentication in vCenter, complete the following steps:

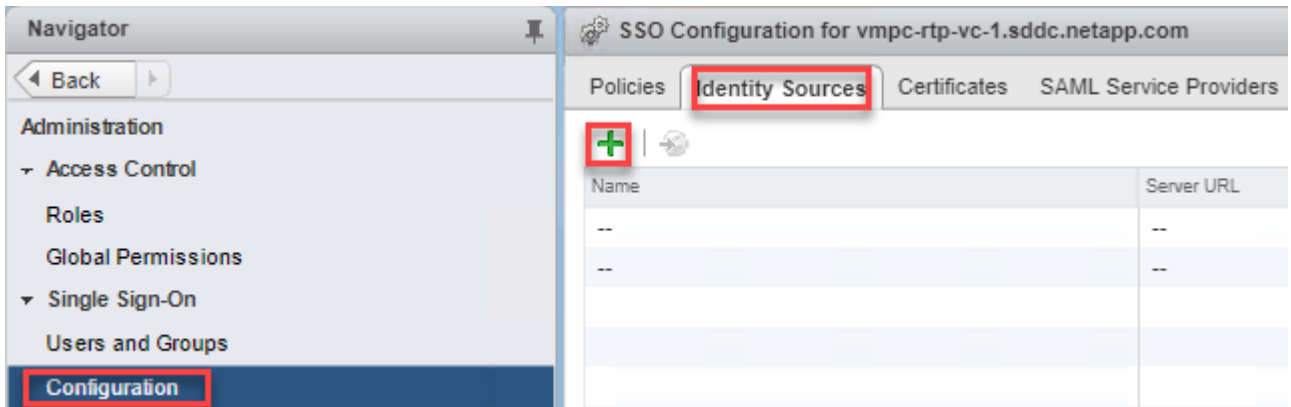
1. Log in to vSphere Web Client as a single sign-on administrator.



2. Navigate to Home > Administration.



3. Under Single Sign-On, click Configuration > Identity Sources > Add.



4. Select Active Directory (Integrated Windows Authentication), and then click Next.

5. Click Finish.

## Enable Service Accounts Privileges

Table 6 shows the service accounts created in Active Directory with the allocated permissions. We will apply permissions to the service accounts for their respective products.

The steps in this section detail how to:

- Add account privileges to vCenter
- Add account privileges to NSX

**Table 6) Service accounts in Active Directory.**

Product	Service Account Name	Permissions
Microsoft SQL Server 2016	svc-sql	Local Administrator in operating system and Active Directory Sysadmin role in Microsoft SQL Server
vRealize Automation	svc-vra	Service Account Privileges for vCenter
vRealize Operations Manager	svc-vro	Service Account Privileges for NSX

### Add Account Privileges to vCenter


To add account privileges to vCenter, complete the following steps:

1. Configure administrator privileges for the svc-vra and svc-vro users on the compute vCenter Server.
2. Log in to the compute vCenter Server.
3. From the Navigator pane, go to Global Inventory Lists > vCenter Servers.
4. Right-click the vCenter FQDN instance and select Add Permission.
5. In the Add Permission dialog box, click Add.  
The Select Users/Groups dialog box appears.
6. From the Domain options, select sddc.netapp.com. Enter `svc` in the Show Users First field to filter user and group names.
7. Select svc-vra and svc-vro from the User/Group list, click Add, and then click OK.
8. In the Add Permission dialog box, select Administrator from the Assigned Role options, and click OK.

The svc-vra and svc-vro users now have administrator privilege on the vCenter Server.

### Add Account Privileges to NSX

To account privileges to NSX, complete the following steps:

1. Log in to the Compute vCenter Server.
2. From the Home menu, select Networking & Security.
3. From the Navigator pane, select Users and Domains.
4. Under the Users tab, select the Compute NSX Manager 172.16.11.66 from the drop-down menu.
5. Click the Add (  ) icon.  
The Assign Role wizard appears.
6. In the Identify User section, click Specify a vCenter User.
7. Enter svc-vra@sddc.netapp.com in the User field and click Next.
8. In the Select Roles section, click Enterprise Administrator, and click Finish.

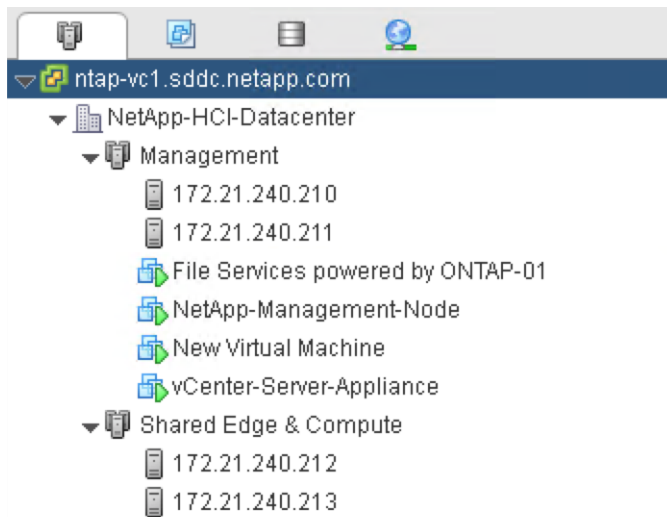
The svc-vra user now has enterprise permission in NSX.

### Configure Management Cluster, Shared Edge and Compute Cluster

The SDDC differentiates between types of clusters; for example, it differentiates management cluster from shared edge and compute cluster. You must divide resources into these separate clusters after NDE. You can accomplish this separation by simply creating a cluster dedicated to either compute clusters, edge clusters, or shared edge.

This validation uses a management cluster and a shared edge and compute cluster. You can modify your vCenter cluster to reflect the configuration shown in Figure 5. For the detailed procedure, see the appendix.

Figure 5) VMware vCenter cluster configuration.



## VMware Licensing

NetApp HCI makes use of VMware vCenter Server to manage and monitor the VMware ESXi hypervisor installed on each compute node. In this validation, a new vCenter was deployed during the installation process.

The vCenter Server license used during NDE is a temporary evaluation license. For continued operation after the evaluation period, you must obtain a new license key from VMware and add it to the vCenter Server license inventory. Navigate to licensing pane within vCenter and add the Enterprise Plus license.

## (Optional) VMware vSphere Distributed Switch Modification

The SDDC requires VMware's software-defined networking offering, NSX. The NDE deploys a single vDS as part of the initial configuration. In preparation for NSX, the two-cable configuration takes advantage of this single VMware vSphere Distributed Switch (vDS).

Optionally, for six-cable configurations, the detailed steps to modify the vDS are provided in Github site: <https://github.com/solidfire/pyNSXdeploy>.

## VMware Configuration for File Services

VMware describes SDS as part of the SDDC solution. File services are used for user and tenant shares. NFS is the protocol chosen for this validation using a NetApp ONTAP Select instance.

The steps in this section detail how to:

- Create an NFS port group for file services
- Create VMkernel adapters for file services

### Create an NFS Port Group for File Services

To create an NFS port group for file services, complete the following steps:

1. Open a web browser.
2. Enter the IP address for the vCenter previously configured through NDE.
3. Enter credentials for the admin account entered during NDE.
4. Select the Networking tab on the left.



5. Right-click the vDS used for compute resources and select Distributed Port Group > New Distributed Port Group.
6. In the Select Name and Location section, enter the name of the new distributed port group: HCI\_OTS\_NFS.
7. In the Configure Settings section, enter the following details and click Next.

Setting	Value
Port binding	Static binding
Port allocation	Elastic
Number of ports	Choose the correct quantity based on environment
Network resource pool	Default
VLAN type	VLAN
VLAN ID	Enter the ID for NFS in your environment

8. In the Review to Complete section, review the details of the new distributed port group.

**New Distributed Port Group**

1 Select name and location  
2 Configure settings  
**3 Ready to complete**

Ready to complete  
Review the changes before proceeding.

Distributed port group name: HCI\_OTS\_NFS  
Port binding: Static binding  
Number of ports: 8  
Port allocation: Elastic  
Network resource pool: (default)  
VLAN ID: 3492

9. Click Finish.
10. Review the Recent Tasks pane and confirm task completion.

## Create VMkernel Adapters for File Services

To create VMkernel adapters for file services, complete the following steps:

1. Select the Networking tab on the left.
2. Right-click the vDS deployed with NDE and select Add and Manage Host networking.
3. In the Select Task dialog box, select Manage Host Networking. Click Next.
4. Click the + Attached hosts icon. The Select Member Hosts page appears.
5. Select All Hosts and click OK.
6. Click Next.
7. In the Select Network Adapter Tasks section, clear the Manage Physical Adapter option. Select the Manage VMkernel adapters checkbox. Click Next.
8. Click the (+) New adapter icon. The Add Networking wizard opens.

**Note:** You will create a new adapter for all hosts

9. In the Select Target Device section, click Browse to select an existing network.
10. Select the newly created HCI\_OTS\_NFS port group and click OK.
11. Click Next.
12. In the Connection Settings: 2a Port Properties section, enter the following settings and click Next.

Setting	Value
Network label	HCI_OTS_NFS
IP Settings	IPv4
Available services	Do not select the option to enable additional services.

13. In the Connection settings: 2b IPv4 Settings section, enter the following details and click Next:

- IPv4 address
- Subnet mask
- (Optional) override default gateway

14. In the Review to Complete section, review the details of the new VMkernel interface.

The screenshot shows the '172.21.240.210 - Add Networking' wizard. The left sidebar shows a progress list with steps 1 through 3, where step 3 'Ready to complete' is highlighted. The main area is titled 'Ready to complete' and contains a table of settings.

Ready to complete	
Review your settings selections before finishing the wizard.	
Distributed port group:	HCI_OTS_NFS
Distributed switch:	NetApp HCI Compute
TCP/IP stack:	Default
vmotion:	Disabled
Provisioning:	Disabled
Fault Tolerance logging:	Disabled
Management:	Disabled
vSphere Replication:	Disabled
vSphere Replication NFC:	Disabled
vSAN:	Disabled
<b>IPv4 settings</b>	
IPv4 address:	172.21.235.5 (static)
Subnet mask:	255.255.255.0

15. Click Finish.

**Note:** Repeat steps 8-15 for all hosts.

16. Click Next.

17. In the Analyze Impact section, confirm that the overall impact status displays as *No impact*. Click Next.

18. In the Ready to Complete section, confirm that the overall impact status displays as *No impact*. Click Next.

19. In the Ready to Complete section, review the settings.

The screenshot shows the 'Add and Manage Hosts' wizard. The left sidebar shows a progress list with steps 1 through 7, where step 7 'Ready to complete' is highlighted. The main area is titled 'Ready to complete' and contains summary information.

Ready to complete	
Review your settings selections before finishing the wizard.	
<b>Number of managed hosts</b>	
Hosts to update:	4
<b>Number of network adapters for update</b>	
New VMkernel network adapters:	4

20. Click Finish.

21. Review the Recent Tasks pane and confirm task completion.

## File Services Configuration with ONTAP Select

ONTAP Select is used for file services for user and tenant shares with the VMware private cloud with NetApp HCI solution. NetApp ONTAP Select offers robust enterprise storage services that are deployed within a virtualized infrastructure. It combines the best of the cloud, in terms of agility and granular capacity scaling, with the flexibility, resilience, and locality of on-premises storage. ONTAP Select builds on the familiar tools and capabilities found with traditional NetApp FAS and AFF systems.

For more information about ONTAP Select's capabilities, see the [NetApp ONTAP Select Datasheet](#).

The ONTAP Select instance is provisioned as part of the NDE process. The default configuration with NDE is to deploy the ONTAP Select instance using the management subnet. This section demonstrates how to modify the network and configure the ONTAP Select instance to enable file services.

For more information about how to administer and configure ONTAP Select, see: [TR-4517: ONTAP Select Product Architecture and Best Practices](#).

Highlights of the deployment steps to configure file service with NetApp ONTAP Select include:

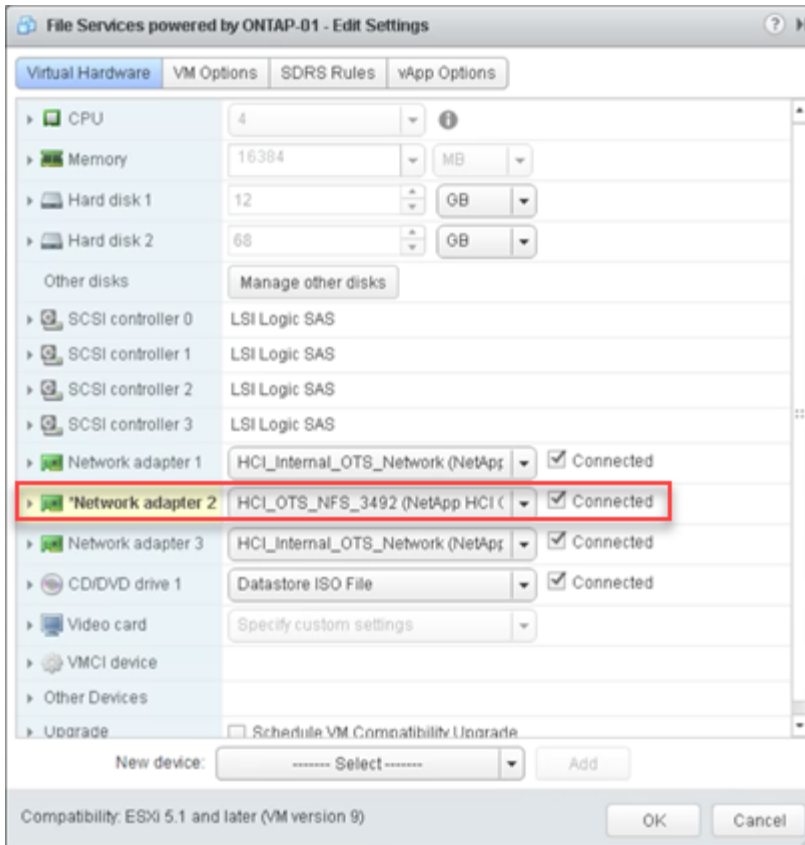
- Modifications to ONTAP Select VM networking
- NetApp OnCommand System Manager dashboard review
- Storage pool creation
- NFS service configuration and access
- NFS share mount

### Modifications to ONTAP Select VM Networking

File services are used for user and tenant shares. NFS is the protocol chosen for this validation using a NetApp ONTAP Select instance.

To modify the networking of the ONTAP Select VM, complete the following steps.

1. Open a web browser and enter the IP address for the vCenter previously configured through NDE.
2. Enter credentials for the admin account entered during NDE.
3. Select the Hosts and Cluster tab on the left.
4. Expand the NetApp-HCI data center.
5. Expand the mgmt cluster.
6. Right-click the File Services powered by ONTAP-01 VM and select Edit Settings.
7. Click the Virtual Hardware tab.
8. From the options, select the network adapter 2.
9. Click Show more network.
10. Select the HCI\_OTS\_NFS port group.
11. Click OK.
12. Click OK.



13. Review the Recent Tasks pane and confirm task completion.

### NetApp OnCommand System Manager Dashboard Review

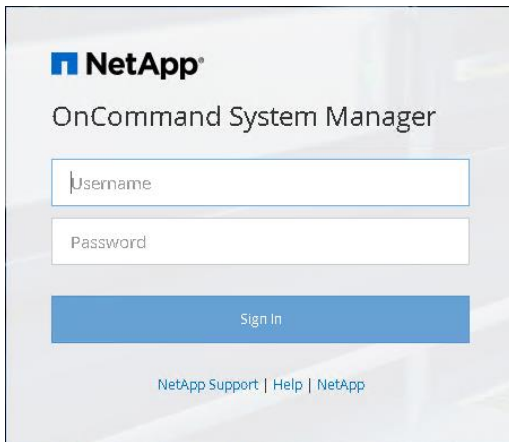
ONTAP Select is a virtual instance of the NetApp ONTAP software. OnCommand System Manager is the tool used for initial configuration. The steps in this section detail how to:

- Connect to OnCommand System Manager
- Review the ONTAP Select Dashboard

To connect to the OnCommand System Manager and review the dashboard, complete the following steps.

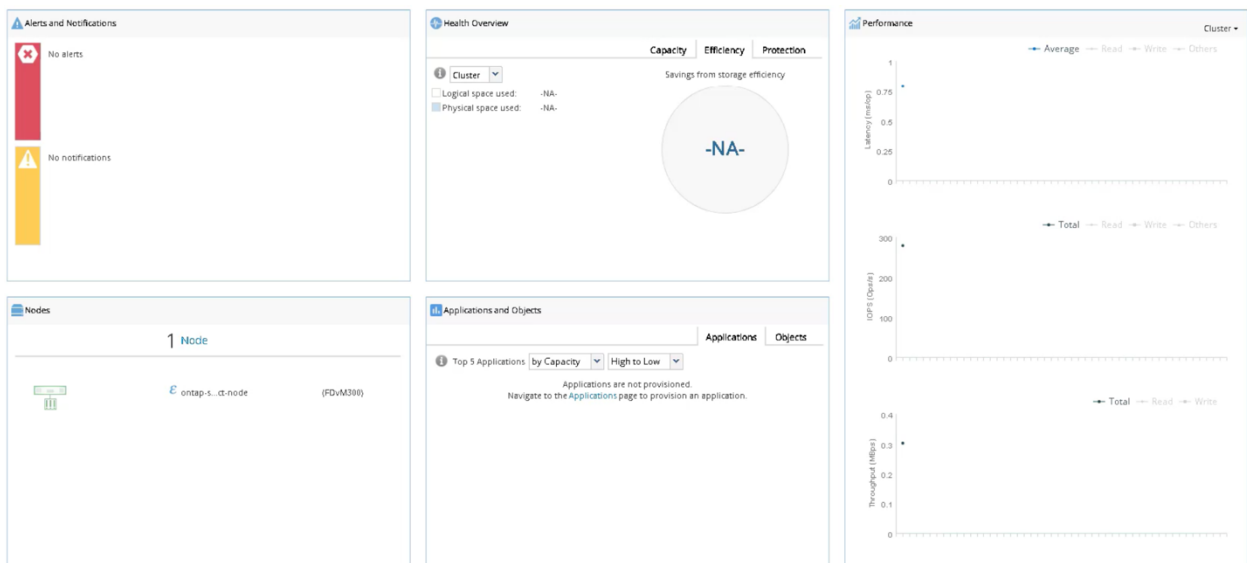
1. Open a web browser.
2. Enter the IP address previously defined during NDE for file services to log in to OnCommand System Manager.

**Note:** This is defined as the ONTAP Select (OTS) Cluster Management address.



3. Log in using the admin credentials.
4. In the OnCommand System Manager, review the initial dashboard. The panels that are available by default include:
  - Alerts and Notifications
  - Health Overview
  - Performance
  - Nodes
  - Applications and Objects

**Note:** If a notification to configure Advanced Cluster Features appears, it is because of file services with HCI being deployment as a single node ONTAP Select Cluster. Close the page and set up Cluster Peering later.



## Storage Pool Creation

To create a storage pool, complete the following steps:

1. In OnCommand System Manager, expand Storage on the left.
2. Expand Aggregates & Disks.
3. Select Aggregates.

4. Click the (+) Create icon to launch the Create Aggregate wizard.
5. Enter the name of the new aggregate for file services.
6. Retain the defaults for Disk Type.
7. Retain the defaults for Number of Disks.
8. Retain the defaults for RAID Configuration.
9. Leave the Mirror This Aggregate checkbox cleared.
10. Click Submit.

Aggregates

✓ SUCCESS: The aggregate has been created.

	Status	Name	Node	Type	Used (%)	Available Space	Used Space	Total Space	Volumes	Disk C.	Flash Pool
+	✓	hd_agg_1	ontap-select-node	VMDISK	0	6.74 TB	232 KB	6.74 TB	0	4	-NA-
+	✓	agg0	ontap-select-node	VMDISK	95	2.92 GB	57.3 GB	60.22 GB	1	1	-NA-

## NFS Service Configuration and Access

After the creation of an aggregate for file services, an SVM with storage and associated networking must be created. The steps in this section detail how to:

- Create an SVM for NFS
- Create a flexible volume for NFS
- Create an NFS export policy

To configure the NFS service and access, complete the following steps.

1. In the OnCommand System Manager, expand Storage on the left.
2. Select SVMs.
3. Click the (+) Create icon to launch the Storage Virtual Machine (SVM) Setup wizard.
4. Enter a name for the SVM for file services.
5. Select the default IPspace.
6. Select the NFS checkbox.
7. Retain the default Language.
8. Retain the default Security Style.
9. Select the newly created data aggregate

**Note:** Do not use agg0.

10. Click Submit and Continue.
11. In the Assign IP Address field, select Without a Subnet.
12. In the Add Details section, enter the following details, and click OK.
  - IPv4 address
  - Subnet mask
  - (Optional) Gateway
  - (Optional) Destination

13. In the Port section, click Browse.

14. Expand the ontap-select-node, select e0b as the network port or adapters, and click OK.

**Note:** Interface e0b corresponds to the VM adapter that was previously joined to the NFS port group.

15. (Optional) Enter the NIS domain name details:
  - a. Configure NIS domain on the SVM to authorize NFS users.

- b. Enter the domain names.
  - c. Enter the IP address of the NIS domain.
16. Configure the volume details:
  - a. Enter the Export Name.
  - b. Enter the size.
  - c. Enter Permission list of clients.
17. Click Submit & Continue.
18. (Optional) Enter Administrator Details for the new SVM.
19. (Optional) Create a LIF for SVM management by selecting the checkbox.
20. (Optional) Enter the following information by selecting the “Without a Subnet In the Assign IP Address” checkbox and click OK:
  - IPv4 address
  - Subnet mask
  - (Optional) Gateway
  - Destination
21. (Optional) In the Port section, click Browse.
  - a. Expand ontap-select-node and select e0b as the network port or adapters. Click OK.
  - b. Click Submit and Continue.
  - c. Click OK.

## Mount NFS Share

The final step in setting up file services is to mount a share to test connectivity. This share could be used for user file shares, log files, and so on. There are various operating systems that can be used. This example demonstrates a basic Linux VM.

To mount the newly created NFS share, complete the following steps:

1. Log in to the host or guest that you will use for NFS connectivity to the HCI system.
2. Mount to the junction path of the SVM for NFS. The following example is for Linux:

```
root@linux-new:/home/user# mount -t nfs 172.21.236.20:/hci_vol_1 /mnt/hci/nfs
```

See the Linux and ONTAP documentation for security hardening and administrative tasks.

**Note:** NetApp does not recommend using this ONTAP Select instance for an NFS datastore for VMs.

## VVols Enablement and Storage Container Creation

This section describes the creation of VVols on SolidFire storage. All actions are performed in vCenter using the NetApp HCI plug-in. The NetApp HCI-integrated plug-in for vCenter enables you to conveniently create VVols for your VMware environment.

**Note:** When the VVols functionality is enabled, the SolidFire cluster starts the VASA provider, opens port 8444 for VASA traffic, and creates protocol endpoints (PEs) that can be discovered by vCenter and all ESXi hosts.

**Caution:** Do not register a SolidFire VASA provider to more than one vCenter instance. The SolidFire VASA provider can only be registered to a single vCenter due to limitations with how vCenter handles SSL. A single vCenter can have multiple SolidFire clusters, but a SolidFire cluster cannot be shared between two instances of vCenter.

The steps in this section detail how to:

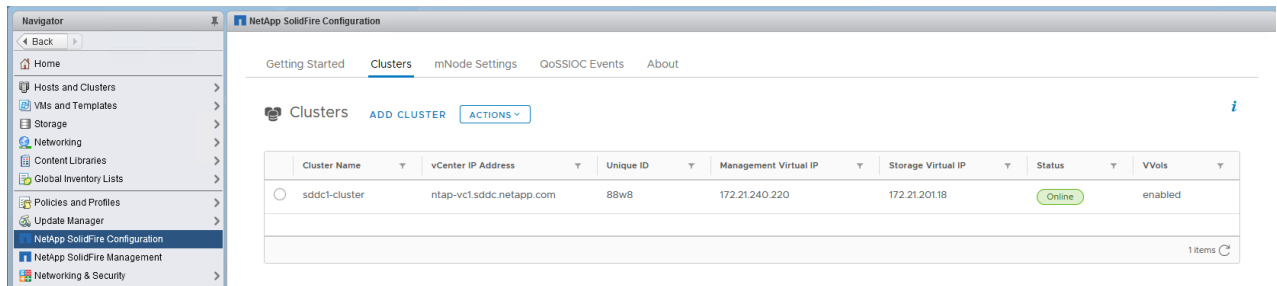
- Enable VVols on the Element cluster
- Register the SolidFire VASA Provider
- Create a storage container and discover a VVols Datastore

### Enable VVols on the Element Cluster

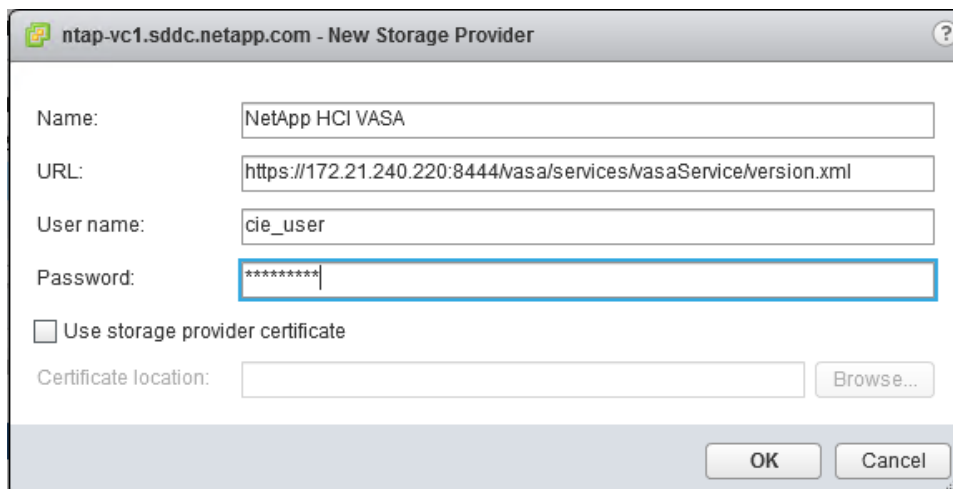
For more information, about VVols, see [TR-4642: VMware vSphere Virtual Volumes for SolidFire Storage Configuration Guide](#).

To enable VVols on the SolidFire storage, complete the following steps.

1. From the Navigator pane, select NetApp SolidFire Configuration.
2. Click the Clusters tab.
3. Select vSphere environment listed in the Cluster section.
4. From the Actions options, select Enable VVols.
5. Click Yes to confirm the vSphere VVols configuration change.
6. Select Actions and Details.



7. Copy the VASA Provider URL. We will use this URL to register the VASA provider in vCenter in the next section.



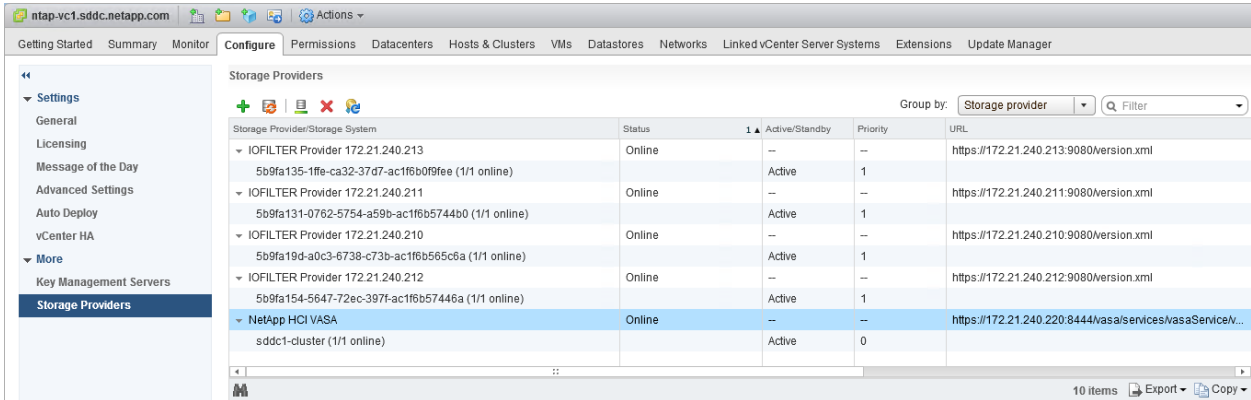
### Register the SolidFire VASA Provider

To register the SolidFire VASA Provider, complete the following steps.

1. In vCenter, open the vCenter inventory list.
2. Browse to vCenter Server in the vSphere Web Client navigator.



- Click the Configure tab and then click Storage Providers.
- From Storage Providers, click the Add (+) icon. The New Storage Provider dialog box appears.
- Enter the following information and click OK to add the VASA provider.
  - VASA provider name
  - VASA provider URL
  - Administrative account user name for the SolidFire cluster
  - Administrative account password for the SolidFire cluster
- Click Yes to install the SolidFire SSL certificate when prompted. The SolidFire VASA provider should now be registered and show the status as Connected.



## Create a Storage Container and Discover a VVols Datastore

In this section, we create the storage containers, verify protocol endpoints, and discover a VVols datastore. All actions are completed within the integrated NetApp SolidFire Plug-in for vCenter.

To create a storage container and discover a VVols datastore, complete the following steps.

- From the Navigator pane, select NetApp SolidFire Management.
- Select VVols and then click Storage Containers.
- Click Create Storage Containers and then enter the following information:
  - Storage Container Name
  - Initiator Secret
  - Target Secret

**Create Storage Container**

Storage Container Name \*

Initiator Secret

Target Secret

☒ Create a datastore

Datastore Name \*

Select the hosts to access this datastore

- ☒ vmppc-rtp-vc-1.sddc.netapp.com

**OK** **CANCEL**

4. In the same dialog box, click Protocol Endpoints.
5. Verify that a Protocol Endpoint has been created for each node in the cluster.

Cluster

SDDC1-CLUSTER

MVIP: 172.21.240.220

SVIP: 172.21.201.18

vCenter: ntap-vc1.sddc.netapp.com

Getting Started

Reporting

Management

Protection

Cluster

VVols

VIRTUAL VOLUMES

STORAGE CONTAINERS

PROTOCOL ENDPOINTS

ACTIONS

	Primary Provider	Secondary Provider	Protocol Endpoint ID	Status	Provider Type	SCSI NAA Device ID
<input type="radio"/>	1	2	cd5e2bb5-af68-499f-b1e5-cd863a158a1f	Active	Primary	6f47acc2000000013838773800000000
<input type="radio"/>	2	3	b786b9a1-ce35-4302-98b6-28ea46044989	Active	Primary	6f47acc2000000023838773800000000
<input type="radio"/>	3	4	e0b30ad5-4d12-4360-bda0-2d3f3ca0c611	Active	Primary	6f47acc2000000033838773800000000
<input type="radio"/>	4	1	e8daee87-222f-4578-ac20-a45a1a8a6445	Active	Primary	6f47acc2000000043838773800000000

1 - 4 of 4 items

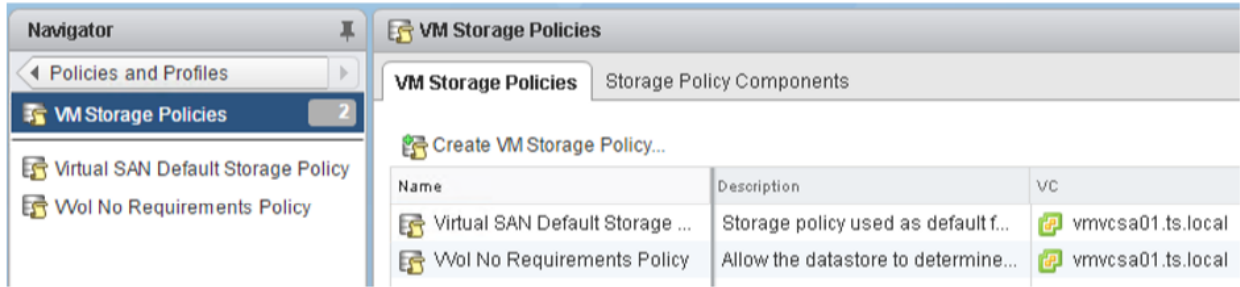
## Create SPBM Policy

In this section, we will Create SPBM policies to set QoS metrics for VVols. Storage Policy-Based Management (SPBM) is a storage policy framework that provides a single unified control pane across a broad range of data services and storage solutions.

For more information, see section Storage Policy-Based Management in the [vSphere Storage - VMware vSphere 6.5 Guide](#).

To create an SPBM policy, complete the following steps.

1. In vCenter, click Home icon and go to Policies and Profiles.



2. Click VM Storage Policies.
3. Click Create VM Storage Policy.
4. In the Create New VM Storage Policy section, enter the following information, and click Next:
  - a. Select a vCenter.
  - b. Enter a name for the policy.
  - c. Enter a description of the policy.
5. Click Next to move through the Policy Structure section.
6. Click Next to move through the Common Rules section.
7. In the Rule-Set 1 section, complete the following steps:
  - a. Select Use Rule-Sets for the Storage Policy.
  - b. Select com.solidfire.vasa.capabilities from the Storage Type list.
  - c. Set a guaranteed minimum IOPS value for VMDKs using this policy in the Data VVol Minimum IOPS field.
  - d. Set the maximum IOPS value for VMDKs using this policy in the Data VVol Maximum IOPS field.
  - e. Set the burst IOPS value for VMDKs using this policy in the Data VVol Burst IOPS field.
  - f. Use the default values for the following fields: (Recommended)
    - Config VVol Minimum IOPS
    - Config VVol Maximum IOPS
    - Config VVol Burst IOPS

**Caution:** Specifying a higher value for Config VVols Minimum IOPS unnecessarily consumes a portion of the cluster IOPS budget for each VM created.



## 6.2 Operations and Cloud Management Implementation

After the successful deployment of the NetApp HCI virtual infrastructure, you are ready to deploy VMware Operations and Cloud Management products.

There are many methods to deploy vRLCM, vROps, vRA, and vRLI to add features and capabilities to your SDDC.

You can install vRealize products to support minimal, proof-of-concept environments, or in different sizes of distributed, enterprise configurations that are capable of handling production workloads. In this validation, vRLCM is used to deploy vRA, vRLI, and vROps.

Consult vRealize Suite product documentation for more information about design considerations, deployment options, system requirements that fits the need in your SDDC deployment. See the following resources to learn more about VMware Validated Designs and vRealize products.

- VMware Validated Designs:
  - <https://docs.vmware.com/en/VMware-Validated-Design/index.html>
  - [NetApp VMware Validated Design for NetApp HCI VVD 4.2 Architecture Design](#)
  - <https://www.netapp.com/us/media/nva-1128-design.pdf>
- Configuring vRA 7.5
  - <https://docs.vmware.com/en/vRealize-Automation/7.5/vrealize-automation-7.5-configuration.pdf>
- vRLCM product page
  - <https://www.vmware.com/products/vrealize-lifecycle-manager.html>.
- vRA product page
  - <https://www.vmware.com/products/vrealize-automation.html>
- vROps product page
  - <https://www.vmware.com/products/vrealize-operations.html>
- vRLI product page
  - <https://www.vmware.com/products/vrealize-log-insight.html>

The high-level steps to deploy vRLCM and vRealize Suite components include:

Environment preparation for vRLCM and vRealize components

---

vRLCM deployment

---

vRealize Suite deployment with VMware vRLCM

### Environment Preparation for vRealize Suite Lifecycle Manager and vRealize Components

To prepare the environment for vRLCM and vRealize components, do as follows:

DNS and NTP requirements

---

Create the Windows IaaS servers

---

Install MS SQL Server

---

Create snapshot of IaaS and MS SQL servers

---

Create blueprint VM used by vRA

Create snapshot of blueprint VM and convert to template

## DNS and NTP Requirements

There are multiple user accounts and corresponding credentials that should be considered before installing vRA.

- **DNS:** All vRA appliances should be resolvable by short and long FQDN. It is recommended to plan the host name and IPs that will be used and prepopulate the DNS.

**Note:** While performing the installation, always enter the complete FQDN when identifying or selecting a vRA machine.

- **NTP:** Make sure that your NTP server is deployed, accessible, and enabled in the virtual infrastructure.
- **Email Server** (optional): vRA provides the option to use an email server.

## Create the Windows IaaS Servers

IaaS server are used to host Infrastructure as a Service (IaaS) components for vRA. Create two virtual machines with Windows Server 2016 with the following minimum settings and resources:

- IaaS Server 1

Settings	Value
VM Name	Vmpc-iaas-01
Operating System	Windows Server 2016
CPU	2
Memory	8GB
Network	Management
Hard Disk Size	40GB
Datastore	NetApp VVol 01

- IaaS SQL Server 1

Settings	Value
VM Name	Vmpc-sql-01
Operating System	Windows Server 2016
Network	Management
CPU	2
Memory	8GB
Network	Management
Hard Disk Size	40GB 100GB
Datastore	NetApp VVol 01

For detailed information about the requirements of Windows IaaS, see section “Preparing for vRealize Automation Installation” in the [Installing vRealize Installation and Configuration Documentation](#).

**Note:** For this validation, vRLCM deploys Windows IaaS components during the installation of vRA.

## Install MS SQL Server

After preparing the Windows IaaS servers, you must install SQL Server on the designated IaaS SQL Server VM.

For information about the SQL Server installation, see the [Install SQL Server from the Installation Wizard \(Setup\)](#) document.

**Note:** During installation, do as follows:

- Install SQL with sddc\svc-vra service account.
- Use the database instance name `vra` when prompted for instance ID.
- Select Windows Authentication for Security Mode.
- Add sddc\svc-vra as an authenticated user.

## Create Snapshot of IaaS and MS SQL Servers VMs

After configuring the IaaS and MS SQL Servers, shut down the VM and create a VM-level snapshot of each VM. This is done in the event of a failure during the deployment of vRealize products. If installation fails, you can use the snapshot to revert to the last known good configuration and try to install again.

## Create Blueprint Virtual Machine Used by vRealize Automation

An Ubuntu VM is used to create a blueprint in vRA as the last step of vRA configuration. Create a virtual machine with Ubuntu with the following minimum settings and resources:

- Ubuntu VM 1

Settings	Value
VM Name	vra-ubuntu-temp
Operating System	Ubuntu 18.04.1
CPU	2
Memory	4GB
Network	Internet_3491
Hard Disk Size	20GB
Datastore	NetApp VVol 01

## Create Snapshot of Blueprint VM and Convert to Template

After creating the Ubuntu VM, shut down the VM and create a VM-level snapshot. Then, convert this VM to a template that can be used during vRA blueprint configuration.

## vRealize Suite Lifecycle Manager Deployment

To deploy vRLCM, do as follows:

Deploy the vRLCM appliance

Configure the vRLCM appliance

## Deploy vRealize Suite Lifecycle Manager Appliance

In this section, we will deploy the vRLCM appliance. This appliance will be used to deploy subsequent components of the vRealize Suite.

To deploy the vRLCM appliance, complete the following steps.

1. Log in to vCenter Server by using the vSphere Web Client.
2. From the Home menu, go to Global Inventory Lists > vCenter Servers.
3. Right-click vmopc-rtp-vc.sddc.netapp.com and select Deploy OVF Template.
4. In the Select Template section, select Local file, browse to the location of the vRLCM OVA file, and click Next.
5. In the Select Name and Location section, enter the name of the new VM, and select the data center to which to deploy. Click Next.
6. In the Select a Resource section, select the management cluster, and click Next.
7. In the Review Details section, review the details of the new template, and click Next.
8. In the Accept License Agreements section, review the terms and click Accept. Click Next.
9. In the Select Configuration section, disable Content Management (optional). Click Next.
10. In the Select Storage section, select Thin Provision as the disk format, leave the VM storage policy as none, and select NetApp-HCI-Datastore-01. Click Next.
11. In the Select Networks section, select the management network, and click Next.
12. In the Customize Template section, enter the following and click Next.

Settings	Value
Hostname	nva-vrlcm.sddc.com
Join the VMware Customer Experience	Selected
Common Name	nva-vrlcm.sddc.com
Country Code	US
Organization Name	NetApp
Organization Unit	NetApp
Default Gateway	172.21.240.4
Domain Name	sddc.netapp.com
Domain Name Servers	10.61.186.231
Domain Search Path	sddc.netapp.com
Network 1 IP Address	172.21.240.60
Network 1 Netmask	255.255.255.0

13. In the Ready to Complete section, click Finish.
14. See the Recent Task section to confirm that OVA deployment has started. Wait for the process to complete.
15. Power on the vRLCM appliance.

## Configure the vRealize Suite Lifecycle Manager Appliance

After deploying the vRLCM appliance, you must log in and configure the common system settings such as the appliance passwords, the configuration drift interval, enablement of SSH, and joining the VMware Customer Experience Improvement Program.

To configure the vRLCM appliance, do as follows:

- Perform initial configuration of the vRLCM appliance
- Generate and replace certificate for vRLCM environments
- Configure NTP servers for deploying products in environments
- Configure NTP on the vRLCM appliance
- Register vRLCM with My VMware

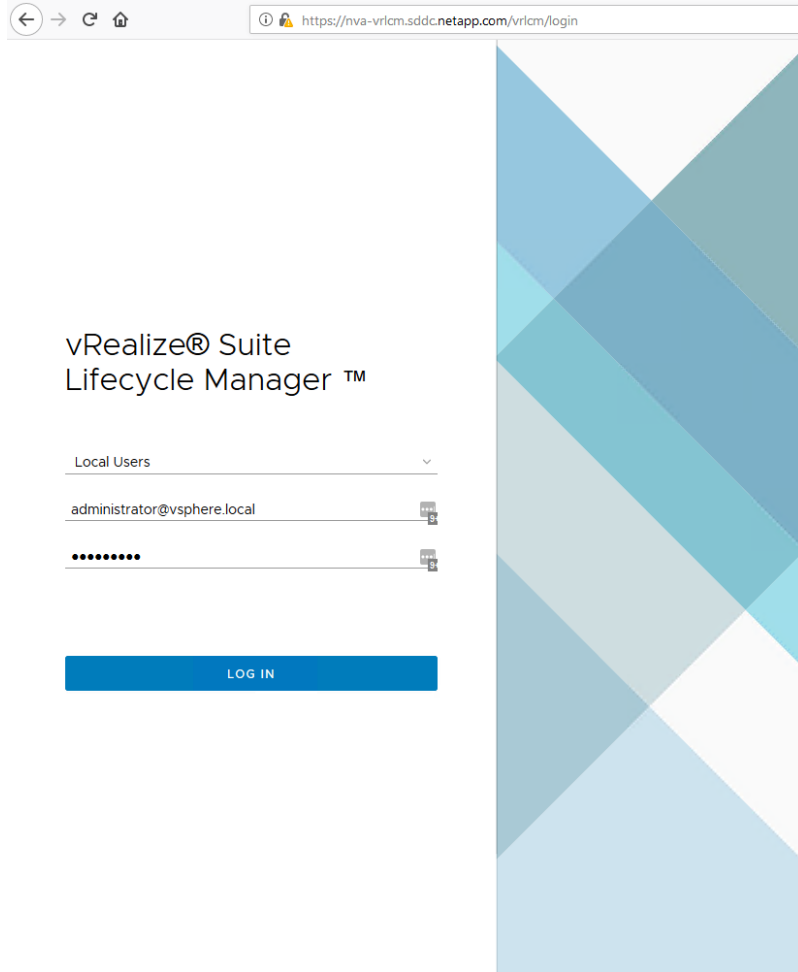


- Download product binaries

### Initial Configuration of the vRealize Suite Lifecycle Manager Appliance

To complete the initial configuration of the vRLCM appliance, complete the following steps.

1. Open a web browser and navigate to the <https://vmprc-lcm-01.sddc.com/vrlcm/login>.



2. Enter the following first-time credentials.

Setting	Value
User name	admin@localhost
Password (default)	vmware

3. Click Manager vCenter Registration.
4. In the Choose a new LCM Password section, provide the following values to set a new root password and click Update Password.
5. Close the Welcome page.
6. In the Navigator Pane, click Settings.

Note: ~5% space is used by the internal file system.

### Common Settings of vRealize Suite Lifecycle Manager

☒ SSH Service (Enable/Disable SSH service of vRealize Suite Lifecycle Manager)

Root Password

Confirm Root Password

Admin Password

Confirm Admin Password

Configuration Drift Interval  Hours

Server

Current status: Running RESTART SERVER

Schedule a restart ☐

Every  at

This product participates in VMware's Customer Experience Improvement Program ("CEIP"). The CEIP provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As part of the CEIP, VMware collects technical information about your organization's use of VMware products and services on a regular basis in association with your organization's VMware license key(s). This information does not personally identify any individual. For additional information regarding the CEIP, please see the Trust & Assurance Center at <http://www.vmware.com/trustvmware/ceip.html>. You can select your participation preferences below.

☒ Join the VMware Customer Experience Improvement Program

SAVE

7. Click the Common Configuration tab and enter the following details:

Settings	Value
Password (default)	Selected
User name	vrslcm_root_password
Password (default)	vrslcm_root_password
User name	vrslcm_admin_password
Password (default)	vrslcm_admin_password
User name	24 hours
Password (default)	Deselected (default)
User name	Deselected (default)
Password (default)	Selected (default)

8. Click Save, and in the Confirm Logout dialog box, click OK.  
vRCLM logs you out back to the vRCLM login page.

## Generate and Replace Certificate for vRealize Suite Lifecycle Manager Environments

Before deploying a product with vRCLM, you must a self-signed certificate that is used during product path, solution path, or configuration file deployment.

**Note:** Use your data center Active Directory domain controller as a certificate authority for your environment. See section "Certificate Replacement" in the VMware Validated Design Planning and Preparation documentation.

**Note:** In this validation, we use a self-signed certificate.

To generate and replace certificate for vRCLM environments, complete the following steps.

1. Select Settings and then click the Generate Certificate tab.
2. In the Generate CSR tab, enter the following information, and click Generate.

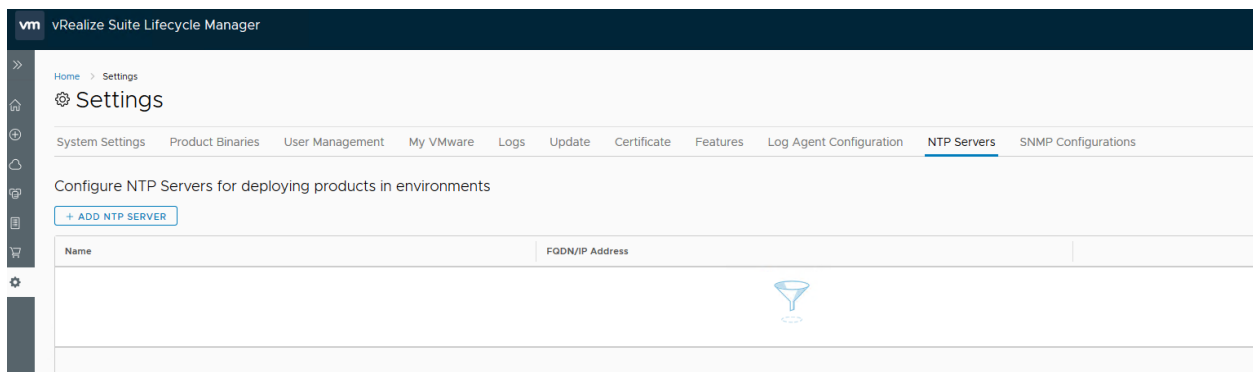
Settings	Value
Certificate Name	VMPC Cert
Common Name	NetApp
Organization Name	CIE
Organizational Unit	VMPC
Country Code	US
Locality	RTP
State	NC
Domain Name	*.sddc.netapp.com
IP Address	None

3. Click Save.

### Configure NTP Servers for Deploying Products in Environments

To configure NTP servers for deploying products in environments, complete the following steps.

1. From the Settings, click NTP Servers.
2. Click Add NTP server.
3. Enter NTP server name.
4. Enter NTP server IP 172.21.240.7.
5. Click Add.



### Configure NTP on the vRealize Suite Lifecycle Manager Appliance

NTP must be configured on the vRLCM appliance to keep vRLCM synchronized with the other SDDC components.

Before you perform the following steps, verify that the SSH service on the vRLCM appliance is enabled.

To configure NTP on the vRLCM appliance, complete the following steps.

1. Log in to vRLCM appliance using **username: root** by using Secure Shell (SSH) client.
2. Configure the NTP source for the vRLCM appliance.
3. Open the `/etc/systemd/timesyncd.conf` file for editing using a text editor such as `vi`.

```
vi /etc/systemd/timesyncd.conf
```

4. Remove the comment for the #NTP configuration and add the following NTP settings.

```
NTP=172.21.240.7
```

5. Run the following command to enable the network time synchronization.

```
timedatectl set-ntp true
```

6. Run the following command to enable the NTP synchronization.

```
systemctl restart systemd-timesyncd
```

7. Run the following command to verify the status of the service.

```
timedatectl status
```

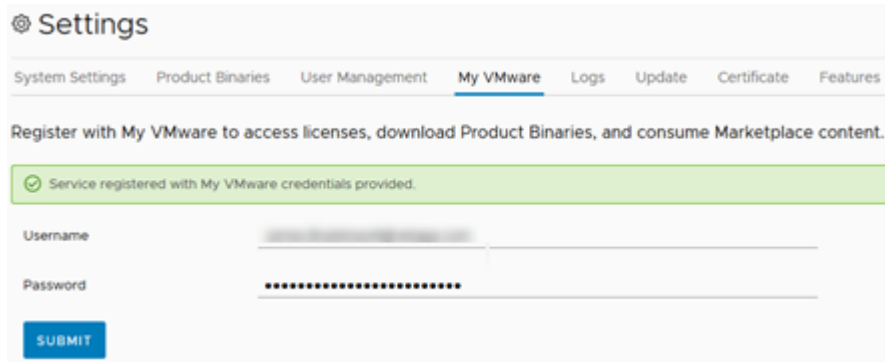
## Register vRealize Suite Lifecycle Manager with My VMware

Integrate vRLCM directly with a My VMware account to access vRealize Suite licenses within an entitlement account and manage the download of product OVAs for install, patches, and upgrades.

Before registering vRLCM with My VMware, verify that you have created a My VMware account with permissions to view licenses and download products from your entitlement account.

To register vRLCM with My VMware, complete the following steps.

1. Log in to vRLCM UI.
2. In the Navigator pane, click the Settings icon.
3. Register vRLCM with My VMware.
  - a. In the Settings dialog box, click the My VMware tab, enter your My VMware credentials, and click Submit.
  - b. In the Download OVA dialog box that prompts you to start a content download, click No.
4. After vRLCM is registered with My VMware, you see a message *Service registered with My VMware credentials provided*.
5. Allow some time for products to download before proceeding to next section.



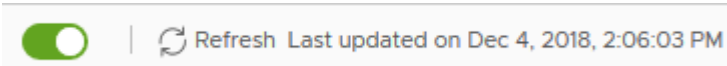
## Download Product Binaries

Product binaries must be downloaded so that vRLCM can deploy environments with relevant software.

To download product binaries, complete the following steps.

1. Log in to vRLCM and click My VMware.
2. Scroll down to My VMware Products and download the following products:
  - vRealize Automation 7.5
  - vRealize Operations Manager 6.7.0

- vRealize Log Insight 4.6.1
- 3. From the Settings, click Product Binaries.
- 4. Click the Add Product Binaries button.
- 5. Click My VMware Downloads.
- 6. Click Discover.
- 7. Select to import and add the following OVAs:
  - vRealize Automation 7.5
  - vRealize Operations Manager 6.7.0
  - vRealize Log Insight 4.6.1
- 8. At the bottom of the My VMware page, enable Auto Refresh.



- 9. Monitor the Download Status column as each product transitions from `INPROGRESS` to `COMPLETED`.

**Note:** Based on the size of each product download for install and upgrade, the process can take some time to complete.

## vRealize Suite Deployment with vRealize Suite Lifecycle Manager

After the configuring the vRLCM appliance, you will deploy a new environment that includes vRA, vROps, and vRLI.

To deploy vRLCM and vRealize Suite components, do as follows:

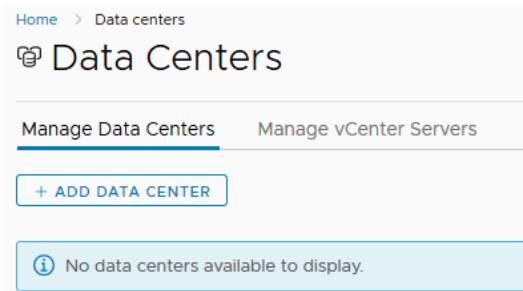
Add data centers and vCenter Server instance

Deploy vRA, vROps, and vRLI

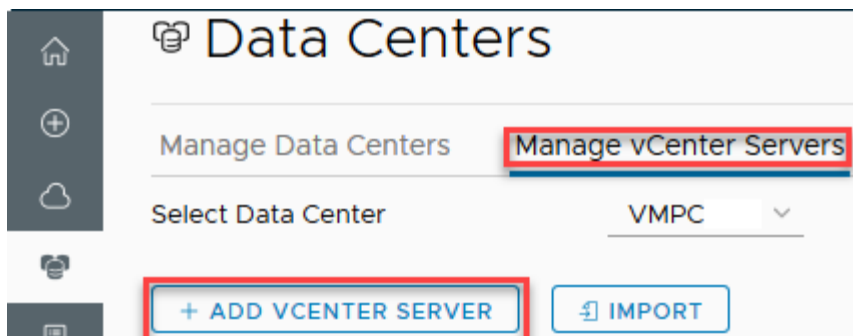
### Add Data Center and vCenter Server Instance

To add a data center and vCenter Server instance, complete the following steps.

1. Log in to vRLCM.
2. In the Navigator, click Data Centers.



3. Click Add Datacenter.
4. Enter the name of the data center: VMPC-RTP.
5. Click Add.
6. Click the Manage vCenter Servers tab.



7. Click Add vCenter Server, enter the following information:

Settings	Value
Host Name	vmnpc-rtp-vc.sddc.netapp.com
User Name	<vCenter Username>
Password	<vCenter password>

8. For vCenter Server Type, select either (Management, Workload, or Consolidated Management and Workload).
9. Click Submit.
10. Select Requests from the Navigator pane and wait momentarily until the request is complete.

## Deploy vRealize Automation, vRealize Operations Manager, and vRealize Log Insight

To deploy vRA, vROps, and vRLI, complete the following steps.

**Note:** Before proceeding, make sure that you have added the vRealize application and IaaS server Reverse and Forward entries in DNS.

1. Log in to vRLCM.
2. In the Navigator Pane, click Create Environment.
3. Enter the following settings and click Next.

Settings	Value
Data Center	VMPC-RTP
Environment Type	Development
Environment Name	VMPC RTP
Administrator Email	administrator@sddc.netapp.com
Default Password	<default password>
Confirm Default Password	<default password>
Join the VMware customer Experience Improvement Program	Selected

4. Select the checkbox to install vRA.
  - a. Click the New Install button.
  - b. Select Version 7.5.0.
  - c. Select the size as Small.
5. Select the checkbox to install vRealize Log Insight.
  - a. Click the New Install button.
  - b. vRealize Log Insight 4.7.0

- c. Select the size as Small.
6. Select the checkbox to install vRealize Operations.
  - a. Click the New Install button.
  - b. vRealize Operations 6.7.0
  - c. Select the size as Small.
7. Click Next.
8. Accept the license agreement and click Next.
9. Enter the license information and click Next.
10. Enter the following for Infrastructure Details and click Next.

Select vCenter Server	vmpc-rtp-vc.sddc.netapp.com	▼						
Select Cluster	Management (NetApp-HCI-Datacenter)	▼						
Select Network	Management Network	▼						
Select Datastore	NetApp-HCI-Datastore-02	▼						
Select Disk Format	Thick	▼						
Applicable Time Sync Mode	<input checked="" type="radio"/> Use Time Server (NTP) <input type="radio"/> Use Host Time							
Time Servers (NTP)	<table> <thead> <tr> <th>Priority</th> <th>Server</th> <th>IP Address</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>SDDC NTP</td> <td>172.21.240.7</td> </tr> </tbody> </table>		Priority	Server	IP Address	1	SDDC NTP	172.21.240.7
Priority	Server	IP Address						
1	SDDC NTP	172.21.240.7						
	<div> <a href="#">EDIT SERVERS</a> <a href="#">ADD NTP SERVERS</a> </div>							

11. Enter the following for Network Details and click Next.

Default Gateway	172.21.240.4
Domain Name	sddc.netapp.com
Domain Search Path	sddc.netapp.com
Domain Name Servers	10.61.186.231
Netmask	255.255.255.0

12. For Certificate, select VMPC Cert and click Next.
13. Enter the product details for vRLI.

Settings	Value
Node Size	Medium
Configure Virtual IPS	Uncheck

14. Enter the component details for vRLI and click Next.

Settings	Value
VM Name	(vmopc-vrli-01)
Hostname	(vmopc-vrli-01.sddc.netapp.com)
IP Address	(172.21.240.142)

15. Enter the product details for vROps and click Next.

Settings	Value
Node Size	Medium
Add NTP servers	

16. Enter the component details for vROps and click Next.

Settings	Value
VM Name	(vmopc-vrops-01)
Hostname	(vmopc-vrops-01.sddc.netapp.com)
IP Address	(172.21.240.143)

17. Enter the product details for vRA and click Next.

Settings	Value
Check	Monitor with vROPS
Check Workload Placement and Reclamation	
Windows Username	(sddc\svc-vra)
Windows Password	(Windows Password)
Add NTP servers	(172.21.240.7)
Leave Configure Cluster Virtual IPs and Configure Windows Box	Cleared

18. Enter the primary vRA server details for vROps.

Settings	Value
vRA VM Name	(vmopc-vra-01)
vRA Hostname	(vmopc-vra-01.sddc.netapp.com)
vRA IP Address	(172.21.240.141)

19. Enter the database details for vROps.

Settings	Value
Database Hostname	(vmopc-sql-01.sddc.netapp.com)
Database IP Address	(172.21.240.136)
Windows VM Name	(vmopc-sql-001)

20. Enter the IaaS Web details for vROps.

Settings	Value
Windows Web Hostname	(vmopc-iaas-01.sddc.netapp.com)
IP Address	(172.21.240.137)
Windows VM Name	(vmopc-iaas-001)



21. Enter the IaaS Manager active details for vROps.

Settings	Value
Windows MS Hostname	(vmopc-iaas-02.sddc.netapp.com)
DEM Orchestrator Name	(Demorchestrator-01)
IP Address	(172.21.240.138)
Windows VM Name	(vmopc-iaas-002)

22. Enter the IaaS DEM worker details for vROps.

Settings	Value
Windows DEM Hostname	(vmopc-iaas-03.sddc.netapp.com)
IP Address	(172.21.240.139)
Windows VM Name	(vmopc-iaas-003)

23. Enter the vSphere Proxy Agent details for vROps.

Settings	Value
Windows Agent Hostname	(vmopc-iaas-03.sddc.netapp.com)
IP Address	(172.21.240.139)
Windows VM Name	(vmopc-iaas-003)

**Note:** The value `proxy-agent-vsphere` is used as the endpoint name for connecting vCenter as an endpoint in the section “Configuration of vRealize Automation.”

24. Click Next.

25. Click Run PreCheck. Allow the precheck to run and then click Next.

26. Review Request Summary. Click Download Configuration and click Next.

27. Click Request in the navigation pane to track progress of environment deployment.

28. After the deployment is complete, log in to vCenter and remove the snapshot from the IaaS VMs.

<b>Step 1/13</b> <table> <tr><td>Deploy vRA.</td><td>100 %</td></tr> <tr><td>Deploy vRLI master.</td><td>100 %</td></tr> <tr><td>Install master node for vROPS.</td><td>100 %</td></tr> </table>	Deploy vRA.	100 %	Deploy vRLI master.	100 %	Install master node for vROPS.	100 %	<b>Step 6/13</b> <table> <tr><td>Install IaaS Web.</td><td>100 %</td></tr> <tr><td>Add vROPS License.</td><td>100 %</td></tr> </table>	Install IaaS Web.	100 %	Add vROPS License.	100 %
Deploy vRA.	100 %										
Deploy vRLI master.	100 %										
Install master node for vROPS.	100 %										
Install IaaS Web.	100 %										
Add vROPS License.	100 %										
<b>Step 2/13</b> <table> <tr><td>Deploy vRLI worker.</td><td>100 %</td></tr> <tr><td>Deploy vRLI worker.</td><td>100 %</td></tr> <tr><td>Install replica node for vROPS.</td><td>100 %</td></tr> </table>	Deploy vRLI worker.	100 %	Deploy vRLI worker.	100 %	Install replica node for vROPS.	100 %	<b>Step 7/13</b> <table> <tr><td>Install Manager Service.</td><td>100 %</td></tr> </table>	Install Manager Service.	100 %		
Deploy vRLI worker.	100 %										
Deploy vRLI worker.	100 %										
Install replica node for vROPS.	100 %										
Install Manager Service.	100 %										
<b>Step 3/13</b> <table> <tr><td>Install data node for vROPS.</td><td>100 %</td></tr> <tr><td>Install data node for vROPS.</td><td>100 %</td></tr> <tr><td>Install collector node for vROPS.</td><td>100 %</td></tr> </table>	Install data node for vROPS.	100 %	Install data node for vROPS.	100 %	Install collector node for vROPS.	100 %	<b>Step 8/13</b> <table> <tr><td>Install Manager Service.</td><td>100 %</td></tr> </table>	Install Manager Service.	100 %		
Install data node for vROPS.	100 %										
Install data node for vROPS.	100 %										
Install collector node for vROPS.	100 %										
Install Manager Service.	100 %										
<b>Step 4/13</b> <table> <tr><td>Deploy secondary vRA.</td><td>100 %</td></tr> <tr><td>Add vRLI license.</td><td>100 %</td></tr> <tr><td>Initialize Cluster</td><td>100 %</td></tr> </table>	Deploy secondary vRA.	100 %	Add vRLI license.	100 %	Initialize Cluster	100 %	<b>Step 9/13</b> <table> <tr><td>Install Dem.</td><td>100 %</td></tr> <tr><td>Configure vRA license.</td><td>100 %</td></tr> </table>	Install Dem.	100 %	Configure vRA license.	100 %
Deploy secondary vRA.	100 %										
Add vRLI license.	100 %										
Initialize Cluster	100 %										
Install Dem.	100 %										
Configure vRA license.	100 %										
<b>Step 5/13</b> <table> <tr><td>Install IaaS Web.</td><td>100 %</td></tr> <tr><td>vRLI Clustering and vIDM Registration.</td><td>100 %</td></tr> </table>	Install IaaS Web.	100 %	vRLI Clustering and vIDM Registration.	100 %	<b>Step 10/13</b> <table> <tr><td>Install Dem.</td><td>100 %</td></tr> <tr><td>Initial content on Cafe.</td><td>100 %</td></tr> </table>	Install Dem.	100 %	Initial content on Cafe.	100 %		
Install IaaS Web.	100 %										
vRLI Clustering and vIDM Registration.	100 %										
Install Dem.	100 %										
Initial content on Cafe.	100 %										
	<b>Step 11/13</b> <table> <tr><td>Install IaaS Agent.</td><td>100 %</td></tr> </table>	Install IaaS Agent.	100 %								
Install IaaS Agent.	100 %										
	<b>Step 12/13</b> <table> <tr><td>Install IaaS Agent.</td><td>100 %</td></tr> </table>	Install IaaS Agent.	100 %								
Install IaaS Agent.	100 %										
	<b>Step 13/13</b> <table> <tr><td>Notifications Schedules</td><td>100 %</td></tr> </table>	Notifications Schedules	100 %								
Notifications Schedules	100 %										
<b>COMPLETED</b> Last updated on 4:16:08 PM											

**Note:** In the event of failure during precheck validation, validate that the vRLCM appliance can resolve all IaaS servers, vROps, and vRLI appliances with short name and FQDN. For more information about vRLCM, see [Troubleshooting VMware vRealize Suite Lifecycle Manager from VMware](#).

## 6.3 vRealize Suite Configuration

This section details the configuration of VMware vRA, vRLI, and vROps.

An overview of the steps to configure vRealize Suite include:

Configuration of vRLI

---

Configuration of vROps

---

Configuration of vRA

## Configuration of vRealize Log Insight

In this section, we will perform the initial configuration of the vRLI. This includes integrating vRLI with vCenter and vROps.

For more information about vRLI product documentation, see <https://docs.vmware.com/en/vRealize-Log-Insight/index.html>.

To perform the initial configuration of vRLI, complete the following steps.

1. Using a web browser, navigate to <https://vmpr-vrli-01.sddc.netapp.com>, and log in to vRLI.
2. In the Ready to Ingest Data section, click Configure vSphere integration.
3. Enter the host name, user name, password for your vCenter.
4. Click Test Connection.
5. Click Save.
6. In the Integration section, click vRealize Operations.
7. Repeat steps 3 through 5.

## Configuration of vRealize Operations Manager

To perform the initial configuration of vROps, do as follows:

Add Blue Medora NetApp HCI Plug-In

---

Integrate vROps with vCenter

---


Integrate vROps with vRLI

---

Integrate vROps with the Blue Medora NetApp HCI Plug-in

### Add Blue Medora HCI Plug-in

To add the Blue Medora HCI Plug-in, complete the following steps.


1. Using web browser, navigate to <https://vmpr-vrops-001.sddc.netapp.com> and log into vROps.
2. (Optional) Set your currency by going to Actions > Global settings, and then selecting your currency.
3. From the Navigator pane, select Administration.
4. Under Solutions, click the  button.
5. Click Browse.
6. Select the NetAppHCI-6.6\_1.0.0\_b20180511.165636.pak file and then click Upload.
7. Wait for the package to upload and then click Next.
8. Accept the license agreement and click Next.  
The NetApp HCI plug-in installs.
9. After the solution is installed, click Finish.

### Integrate vRealize Operation Manager with vCenter

To integrate vROps with vCenter, complete the following steps.

1. Under Solutions, select VMware vSphere.
2. Click Configure.
3. Under Instance Settings enter the following information:

Settings	Value
Display Name	VMPC VC
Description	(Optional)
vCenter Server	https://vmc-rtp-vc.sddc.netapp.com

4. To set credentials, click the  button and enter the following credentials for your vCenter. Click OK.

Settings	Value
Credential name	VMPC VC Creds
User Name	<vcenter username>
Password	<vcenter password>

- Click Test Connection.
- Click Save Settings.
- Click Close.

### Integrate vRealize Operation Manager with vRealize Log Insight

To integrate vROps with vRLI, complete the following steps.

- Under Instance Settings, enter the following information:

Settings	Value
Display Name	VMPC Log Insight
Description	(Optional).
Log Insite server	vmc-vrli-001.sddc.netapp.com.

- Click Test Connection.
- Click Save Settings.
- Click Close.

### Integrate vRealize Operation Manager with the Blue Medora NetApp HCI Plug-in

To integrate vROps with the Blue Medora HCI Plug-in, complete the following steps.

- Under Instance Settings, enter the following information:

Settings	Value
Display name	VMPC Blue Medora
Description	(optional).
NetApp HCI host FQDN or IP	vmc-rtp-esx-01 vmc-rtp-esx-02 vmc-rtp-esx-03 vmc-rtp-esx-04 vmc-rtp-esx-05 vmc-rtp-esx-06

- To set credentials, click the  button and enter your vCenter details.

Settings	Value
Credential name	VMPC VC Host Creds
User Name	<vcenter username>
Password	<vcenter password>

3. Click OK.
4. Click Test Connection.
5. Click Save Settings.
6. Click Close.

## Configuration of vRealize Automation

In this section, we will create and configure a new tenant, IaaS Fabric, which is a collection of infrastructure components that are used to provision virtual machines and applications. This is followed by creating a blueprint and catalog, and configuring the SPBM plug-in.

To configure vRA, do as follows:

Configure a new tenant

---

Configure Active Directory for a tenant

---

Configure the Embedded vRO Server

---

Configure vCenter endpoints

---

Configure vRO endpoints

---

Create a fabric group

---

Create a custom group

---

Configure machine prefixes

---

Create a business group

---

Create a network profile

---

Create a reservation

---

Create an example blueprint

---

Configure catalog management

---

Install and configure SPBM plug-in

---

Install and configure SPBM plug-in

---

Configure the endpoint

---

Create a new workflow subscription

---

Enable the Set Storage Policy for virtual machine provisioning

---

Enable the storage policy in a blueprint

Change storage policy for storage migration

## Configure a New Tenant

To configure a new tenant, complete the following steps.

1. Log in to the vRA console (<https://vmprc-vra01.sddc.netapp.com/vcac>) as an administrator.
2. Go to Administration > Tenants. Click the New button.
3. For Name, enter Development. For URL Name, enter Development.
4. Click Submit and then click Next.
5. For Local Users click the New icon. Enter the following information, click OK, and then click Next.

Settings	Value
First name	Dev
Last Name	Admin
Email	administrator@sddc.netapp.com
User Name	devadmin
Password	<devadmin password>ls "
Confirm Password	<devadmin password>

6. Enter and assign Devadmin user account for Tenant Administrator and IaaS Administrator.
7. Click Finish and log out.

## Configure Active Directory for a Tenant

To configure Active Directory for a tenant, complete the following steps.

1. Log in to newly created tenant: <https://vmprc-vra01.sddc.netapp.com/vcac/org/development> with devadmin account.
2. Navigate to Administration > Directories Management > Directories.
3. Click Add Directory and select Add Active Directory over LDAP/IWA.
4. Enter the following information and click Save & Next.

Settings	Value
Directory Name	SDDC AD
	Select the Active Directory over LDAP button
Base DN	cn=Users,dc=sddc,dc=netapp,dc=com
Bind DN	cn=administrator,cn=Users,dc=sddc,dc=netapp,dc=com
Bind DN Password	<Password>

5. Click Test Connection to test the connection to the configured directory.
6. Click Save & Next.
7. Review Select the Domain and click Next.
8. Review Map User Attributes and click Next.
9. Click Add and enter cn=Users,dc=sddc,dc=netapp,dc=com. Click Select and select the domain admins and domain users. Click Save and click Next.
10. Review the groups and users and click Sync Directory.
11. Wait for synchronization to complete and then log out.

## Configure the Embedded vRealize Orchestrator Server

To configure the embedded vRO server, complete the following steps.

1. Log in to the vRA console as devadmin.
2. Navigate to Administration > VRO Configuration > Server Configuration.
3. Click Use the Default Orchestrator Server.

## Configure vCenter Endpoints

To configure vCenter endpoints, complete the following steps.

1. Navigate to Infrastructure > Endpoints > Endpoints.
2. Click the (+) New > Virtual > vSphere(vCenter).
3. Enter the following information:

Settings	Value
Name	vCenter
Address	https://vmpr-rtp-vc.sddc.netapp.com/sdk
User name	administrator@vsphere.local
Password	<administrator password>

4. Click OK.

## Configure vRealize Orchestrator Endpoints

To configure vRO endpoints, complete the following steps.

1. Click the (+) New > Orchestration > vRealize Orchestrator.
2. Enter the following information:

Settings	Value
Name	vCenter
Address	https://vmpr-rtp-vc.sddc.netapp.com/sdk
User name	administrator@vsphere.local
Password	<administrator password>

3. Click OK.


## Create a Fabric Group

To create a fabric group, complete the following steps.

1. Click Infrastructure > Fabric Groups.
2. Click (+) New.
3. Enter `Development FG` in the Name field.
4. Enter `devadmin@vsphere.local` in the Fabric Administrators field and press Enter.
5. In the Compute Resources section, select Compute-Edge.
6. Click OK.

## Create a Custom Group

To create a custom group, complete the following steps.

1. Navigate to Administration > Users & Groups > Custom Groups.
2. Click the Add (  ) icon.
3. Enter `Development Architects` in the New Group Name field.
4. Select All Roles from the Add Roles to this Group list. Click Next.
5. Enter `devadmin` user or group name in the Search box and press Enter.
6. Click Finish.


## Configure Machine Prefixes

To create machine prefixes, complete the following steps.

1. Log in to vRA.
2. Navigate to Infrastructure > Administration > Machine Prefixes.
3. Click + New.
4. Enter `Dev-` in the Name field.
5. Specify if the machine prefix is displayed in all tenants or only in the current tenant in the Visibility column.
6. Select 3 for Number of Digits.
7. Select 1 for Next Number.
8. Click the Check button.


## Create a Business Group

To create a business group, complete the following steps.

1. Navigate to Administration > Users & Groups > Business Groups.
2. Click the Add (  ) icon.
3. Enter `Development BG` in the Name field.
4. Enter `administrator@sddc.netapp.com` for Send Capacity Alert Emails.
5. Click Next.
6. Enter `devadmin` for the Group manager role and click Next.
7. Enter `devauser1` for the user role and click Next.
8. Select `dev-` for Default Machine Prefix.
9. (Optional) Enter `CN=Computers,DC=sddc,DC=netapp,DC=com` for the Active Directory container.
10. Click Finish.
11. Log out of vRA.

## Create a Network Profile

To create a network profile, complete the following steps.

1. Log in to vRA.
2. Navigate to Infrastructure > Reservations > Network Profiles.
3. Click the Add (  ) icon.
4. Enter `Dev IP Pool` in the Name field.



5. Leave the IPAM endpoint and Subnet Mask as default.
6. Enter 172.21.235.4 in the Gateway field.
7. Click DNS and enter the following information:

Settings	Value
Primary DNS	10.61.186.231
Secondary DNS	10.61.186.232
DNS Suffix	sddc.netapp.com
DNS search suffixes	sddc.netapp.com

8. Click Network Ranges and select + New button, enter the following information.

Settings	Value
Name	VLAN_3491_prod
Start IP	172.21.235.100
End IP	172.21.235.149

9. Click OK.

## Create a Reservation

To create a reservation, complete the following steps.

1. Navigate to Infrastructure > Reservations > Reservations.
2. Click the New icon and select vSphere.
3. In the General page, enter the following information:

Settings	Value
Name	Development Reservation
Tenant	Development
Business groups	Development BG
Priority	1

4. Click Resources and enter the following information:

Settings	Value
Compute resource	Compute-Edge
Machine Quota	Unlimited
Memory	200
Storage	NetApp VVol 01
Reservation reserved	10000
<b>Priority:</b>	1

5. Click Network, select the following information, and click OK.

Settings	Value
Network Adapter	Internet_3491
Network Profile	Dev IP Pool

## Create an Example Blueprint

To create an example blueprint, complete the following steps.

1. Log in to vRA.
2. Navigate to Infrastructure > Compute-Edge > Data Collection.
3. Under Inventory, click Request Now.
4. Monitor the collection by clicking Refresh at the bottom left of the screen.
5. After the collection is refreshed, navigate to the Design tab > Blueprints.
6. Click + New, enter the following information, and click OK.

Settings	Value
Name	Ubuntu 18.04.1
Deployment Limit	30
Lease (Min / Max)	1 / 90
Archive	30

7. At the bottom left of the page, click and drag vSphere (vCenter) machine into the Design Canvas.
8. Enter the following information in the General page:

Settings	Value
ID	Ubuntu_Base
Machine Prefix	Dev-
Instances (Min / Max)	1 / 15

9. Enter the following information for build information:

Settings	Value
Blueprint type	Ubuntu_Base
Action	Dev-
Provisioning workflow	CloneWorkflow
Clone from	Ubuntu-Template
Clone from snapshot	Use current snapshot
Customization Specs	vRA Linux Cust (Optional)

10. Enter the following information for Machine Resources.

Settings	Value
CPU (Min / Max)	2 / 8
Memory (Min / Max)	4096 / 40960
Storage (Min / Max)	20 / 200

11. Under Categories, click Network & Security.
12. Click and drag Existing Network into the Design Canvas.
13. Click Network Profile and select Dev IP Pool.
14. Click the Ubuntu\_Base icon in the Design Canvas.
15. Click the Network tab, select first network ID, and select Edit.
16. From the Network options, select DevIPPool.
17. Click Assignment Type and select DHCP.
18. Click OK.


19. Click Finish.
20. Click Ubuntu 18.04.1, select Publish.

**Note:** Create additional blueprints as needed.


## Configure Catalog Management

To configure catalog management, complete the following steps.

1. Navigate to Administration tab > Services.
2. Click the + New button.
3. Configure the following information for New Services:

Settings	Value
Name	Development Catalog
Description	Service Catalog for Development resources
Icon	 (Optional)
Status	Active

4. Under Catalog Management, click Catalog Items.
5. Select Ubuntu 18.04.1 and configure the following information:

Settings	Value
Icon	 (Optional)
Status	Active
Quota	Unlimited
Service	Development Catalog

6. Click OK.
7. Under Catalog Management, select Entitlements.
8. Click + New.
9. Enter `Development Entitlements` for Name.
10. Change the status to Active and click Next.
11. For Items & Approvals, select the following, and click Finish.

Settings	Value
Entitled Services, click +	Development Catalog
Entitled Items, click +	Ubuntu 18.04.1
Entitled Actions, click +	All Actions

## Install and Configure SPBM Plug-In

To install and configure the SPBM, complete the following steps.

1. Download the SPBM plug-in from the [VMware Marketplace](#).
2. Log in as an administrator to vRO Java Client: <https://vmprc-vra01.sddc.netapp.com/vco/client/client.jnlp>.
3. Select Import and navigate to SPBM plug-in package `com.vmware.library.spbm_2.1.4`.
4. Select Import and Trust Provider.
5. Select the required elements to be imported.

**Note:** For more information, see [Configuring vRealize Automation with VMware Storage Policy-Based Management and SolidFire Virtual Volumes](#).

## Configure the Endpoint

To configure the endpoint, complete the following steps.

1. Navigate to Infrastructure > Endpoints > Endpoints, and edit the endpoint being used or the blueprints for which you want to enable the storage policy.
2. Add the following properties:
  - `spbmvvc_username` and set the value to `administrator@vsphere.local`.
  - `spbmvvc_password` and set the value to your vCenter password.
  - `spbmvvc_sslthumbprint` and set the value to vCenter SSL thumbprint.

**Note:** See the article [Obtain the SSL Certificate Thumbprint](#) to get the vCenter SSL thumbprint.

## Create a Workflow Subscription

To create a workflow subscription, complete the following steps.

1. Navigate to Administration > Events > Subscriptions. Click the New button.
2. Select Machine Provisioning and click Next.
3. Select Run Based On Conditions and from the drop-down menu select all the following:
  - a. Add expression  
Data > Lifecycle state > Lifecycle state name  
Equals  
Constant: VMPSMasterWorkflow32.MachineProvisioned
  - b. Add expression  
Data > Lifecycle state > State phase  
Equals  
Constant: PRE
  - c. Add expression  
Data > Blueprint name  
Contains  
Constant: SPBM


**Note:** This is just a sample. You can define the conditions based on your requirements. In this case, the blueprints must have the keyword “SPBM” in their name.

4. In the Workflow, go to Orchestrator > Library > SPBM. Click Set Storage Policy.
5. In the Details tab, select Blocking.

6. Click Finish.
7. Click Set Storage Policy and click Publish.

## Enable the Set Storage Policy for Virtual Machine Provisioning

To enable the set storage policy for virtual machine provisioning, complete the following steps.

1. Navigate to Administration > Property Dictionary > Property Definitions, and add following definitions using the Add (  ) icon:
  - VM.StoragePolicy.Home
  - VM.StoragePolicy.Disk0
  - VM.StoragePolicy.Disk1
  - VM.StoragePolicy.Disk2

**Note:** The plug-in searches for these definitions. The spellings must match the definitions.

2. Enter the following information for each newly created property definitions:
  - a. Set the Data Type to String.
  - b. Set the Display As option to Dropdown.
  - c. Select the External values option. Select `com.vmware.library.spbm > getStoragePoliciesBasedOnEndpointName`. Click OK.
  - d. Click Edit `endpointName`, enter `proxy-agent-vsphere`. Click OK.
  - e. Click Edit for VMHome.
    - Set VM.StoragePolicy.Home to true
    - Set VM.StoragePolicy.Disk0 to false
    - Set VM.StoragePolicy.Disk1 to false
    - Set VM.StoragePolicy.Disk2 to false

**Note:** Values represent each respective storage policy.

3. Navigate to the Administration > Property Dictionary > Property Groups and add the following definitions:
  - SPBM VM 1 Disk
  - SPBM VM 2 Disk
  - SPBM VM 3 Disk
4. Enter the following information in the group definition:
  - a. Extensibility.Lifecycle.Properties.VMPSMasterWorkflow32.MachineProvisioned with a value of \* and leave Show in Request to no.
  - b. VM.StoragePolicy.Home
    - Set Value to Datastore Default
    - Set Show in Request to yes
  - c. VM.StoragePolicy.Disk0
    - Set Value to Use VM Home Storage Policy
    - Set Show in Request to yes
  - d. VM.StoragePolicy.Disk1
    - Set Value to Use VM Home Storage Policy
    - Set Show in Request to yes
  - e. VM.StoragePolicy.Disk2

- Set Value to Use VM Home Storage Policy
- Set Show in Request to yes

**Note:** The plug-in looks for these values; make sure to use the exact spellings.

## Enable the Storage Policy in a Blueprint

To enable the storage policy in a blueprint, complete the following steps.

1. Navigate to Design > Blueprints.
2. Open the Ubuntu-template-vra blueprint.
3. Select the VM and navigate to Properties > Property Groups.
4. Add the appropriate group based on the number of disks to configure in the VM. For example, a VM with a single disk would use “SPBM VM 1 Disk”. A VM with two disks would use “SPBM VM 2 Disk”.
5. Click Save and Finish.

## Change Storage Policy for Storage Migration

To change the storage policy for storage migration, complete the following steps.

1. Navigate to Design > Xaas > Resource Actions and create a new resource action.
2. In Workflow, navigate to Orchestrator > Library > SPBM. Select Change Storage Policy for Storage Migration.
3. In the Input Resource page, select the following and click Next.
  - IaaS VC VirtualMachine for Resource type.
  - vcVM for Input Parameter.
4. Under Details, clear the Hide Catalog Request Information Page option.
5. Under the Forms tab, select Storage Policy.
  - a. On the right side of screen under Details > Label, enter `Change Storage Policy for Storage Migration`.
  - b. On the right side of screen under Details, click Type and select Drop-down.
  - c. On the right side of screen under Values, select External Values and then click `com.vmware.library.spbm > getStoragePoliciesBasedOnVM`.
  - d. Click Submit.
  - e. For vCenterVM, select Field, and select vcVM.
  - f. For IAASServer, select Field, and select IAASServer.
  - g. Click Apply.
6. Under the Forms tab, select IAASServer.
  - a. On the right side of screen under Constraints, select Value > Constant, and then select the IAAS entity.
7. After you submit the action, publish it and add it to entitlement.

## 7 Solution Verification

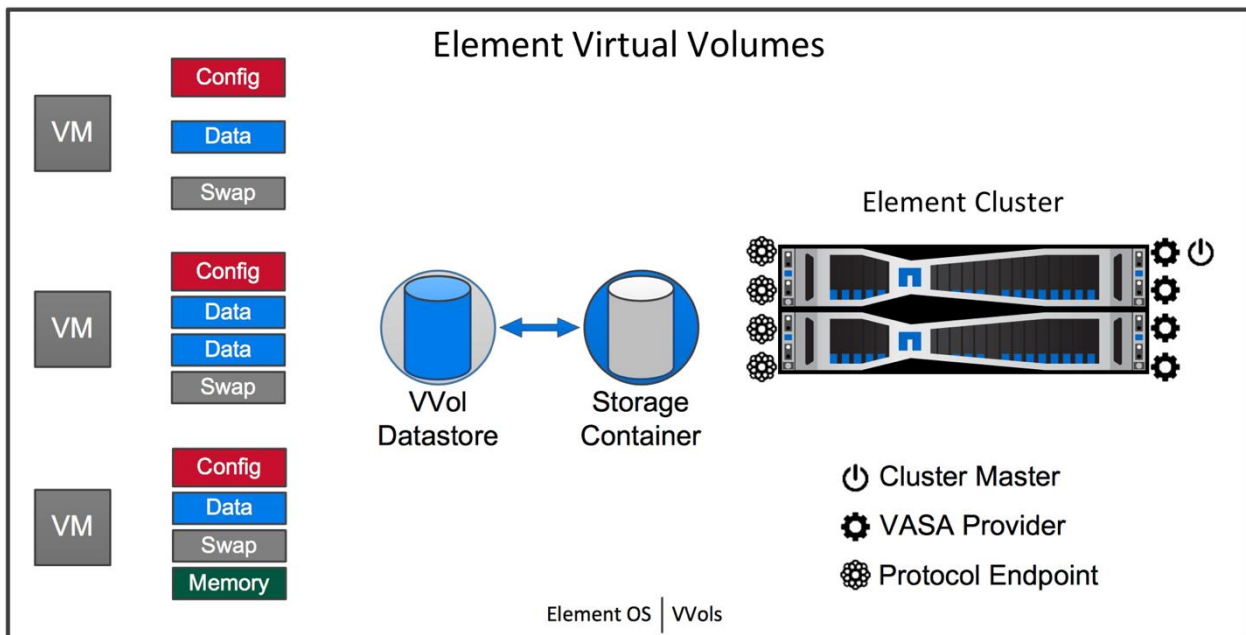
In addition to the deployment guidance provided in this document, the engineering team conducted multiple verifications of features and capabilities of the VMware private cloud on NetApp HCI solution. These verifications focus on:

- NetApp HCI and SPBM
- NetApp HCI and vRA
- NetApp HCI and vROps
- NetApp HCI and vRLI
- NSX tenant considerations

### 7.1 NetApp HCI and SPBM

As mentioned previously, NetApp has integrations with VMware SPBM. See section “Create SPBM Policy” for details about how to create a new storage policy. Element exposes QoS profiles through the Virtual Machine API for Storage Awareness (VASA) provider, which can be used to provide a per virtual disk level of guaranteed performance for the volume’s minimum, maximum, and burst IOPS settings. Figure 6 illustrates the implementation of VVols on Element.

Figure 6) VVols implementation on Element.



For this validation, the integration of Element with VMware through SPBM is demonstrated through the creation of storage policies for new VMs, datastores, or tenants, by using the Element VASA provider.

Figure 7 highlights the use of storage profiles for tenants that require low, medium, and high QoS settings from the Element cluster.

Figure 7) VVols implementation on Element.

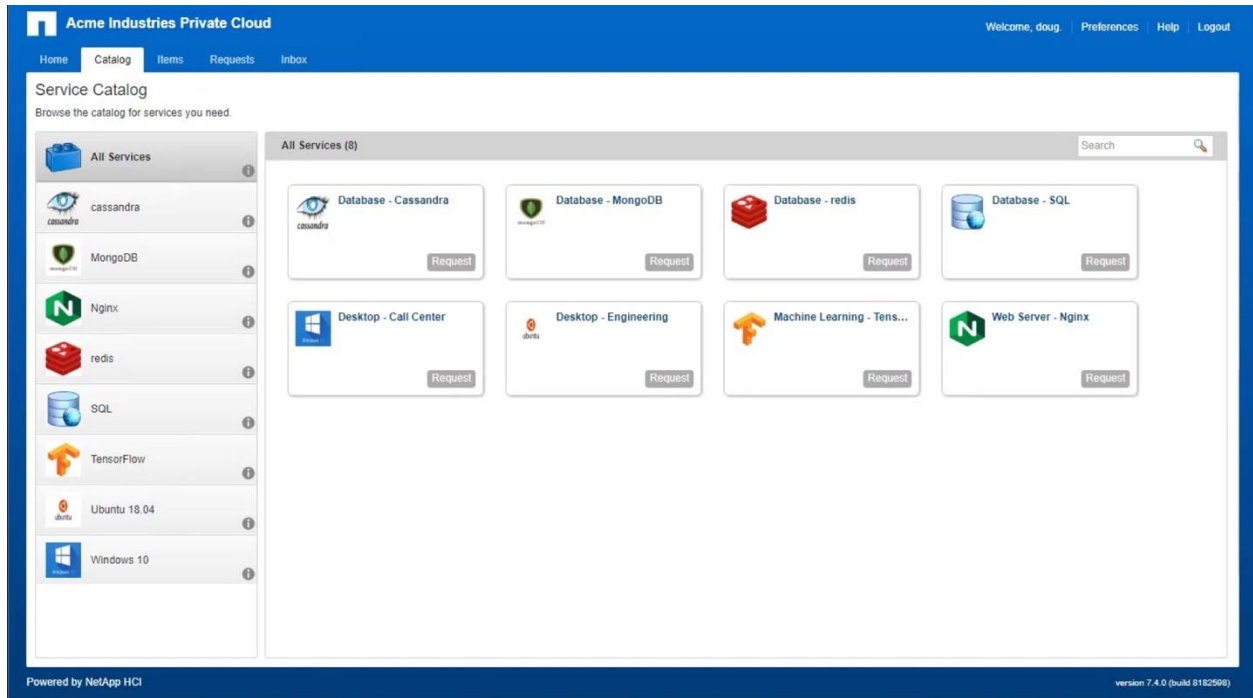
low	Storage policy with low QoS settings	vmpc-rtp-vc.sddc.netapp.com
medium	Storage policy with medium QoS settings	vmpc-rtp-vc.sddc.netapp.com
high	Storage policy with high QoS settings	vmpc-rtp-vc.sddc.netapp.com

## 7.2 NetApp HCI and vRealize Automation

Blueprints represent a very important aspect of vRA as they describe parameters of a given service, resource, or software components. The development of blueprints for a variety of administrative tasks, enables a customizable catalog of services that are available to tenants of the VMware private cloud. The integration of Element with SPBM enables the self-provisioning of predefined services that take advantage of storage features and capabilities.

Figure 8 shows the use of a catalog consisting of a variety of services that can be deployed through a customized portal and dashboard.

Figure 8) VMware private cloud catalog.

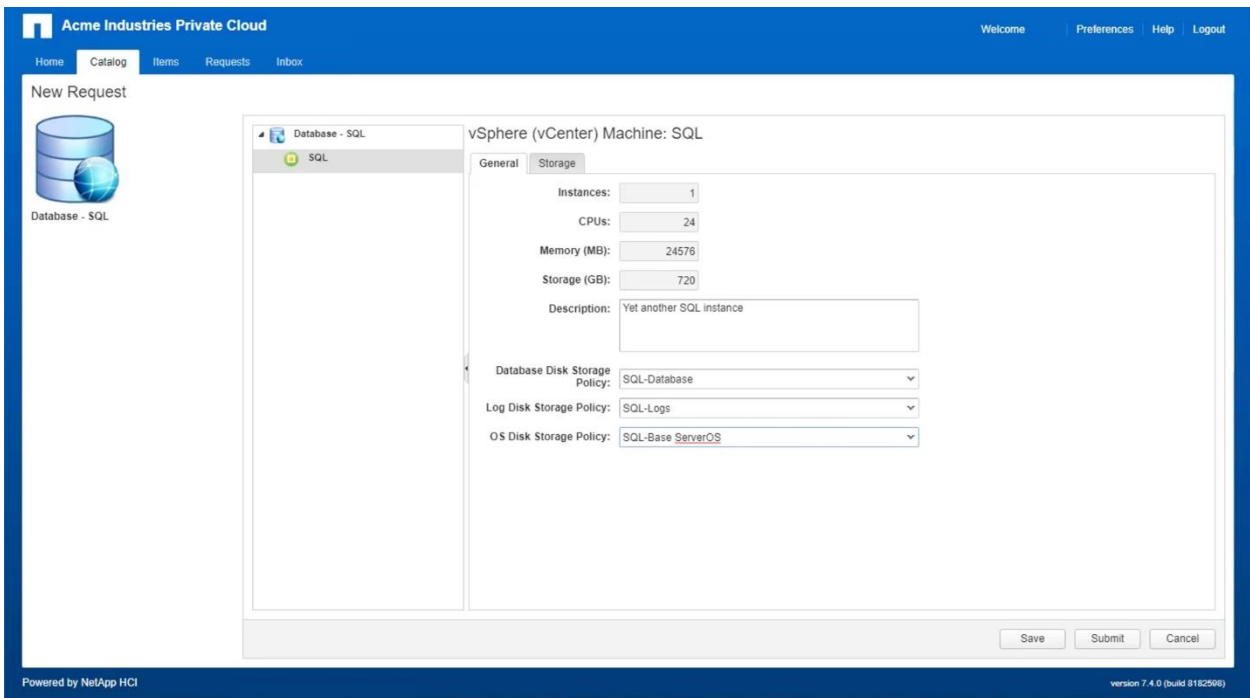


For this validation, the tenants take advantage of Element features by self-provisioning of resources predefined with Element characteristics. New resources are provisioned by making a request from the catalog. After a service is selected, values are specified for the predefined variables.

Figure 9 highlights a new request of a SQL instance. This instance has predefined general parameters and by selecting the correct database, log and OS disk storage policies, the provisioning of new SQL instance is consistent and time to value is reduced.



Figure 9) VMware private cloud catalog.



### 7.3 NetApp HCI and vRealize Operations Manager

NetApp has partnered with Blue Medora to deliver a comprehensive management pack for systems that are based on Element. The VMware vRealize Operations Management Pack for NetApp HCI and SolidFire provides visibility into storage systems and workloads from within vOps. The visibility provided by this management pack helps to optimize performance and eliminate potential resource constraints.

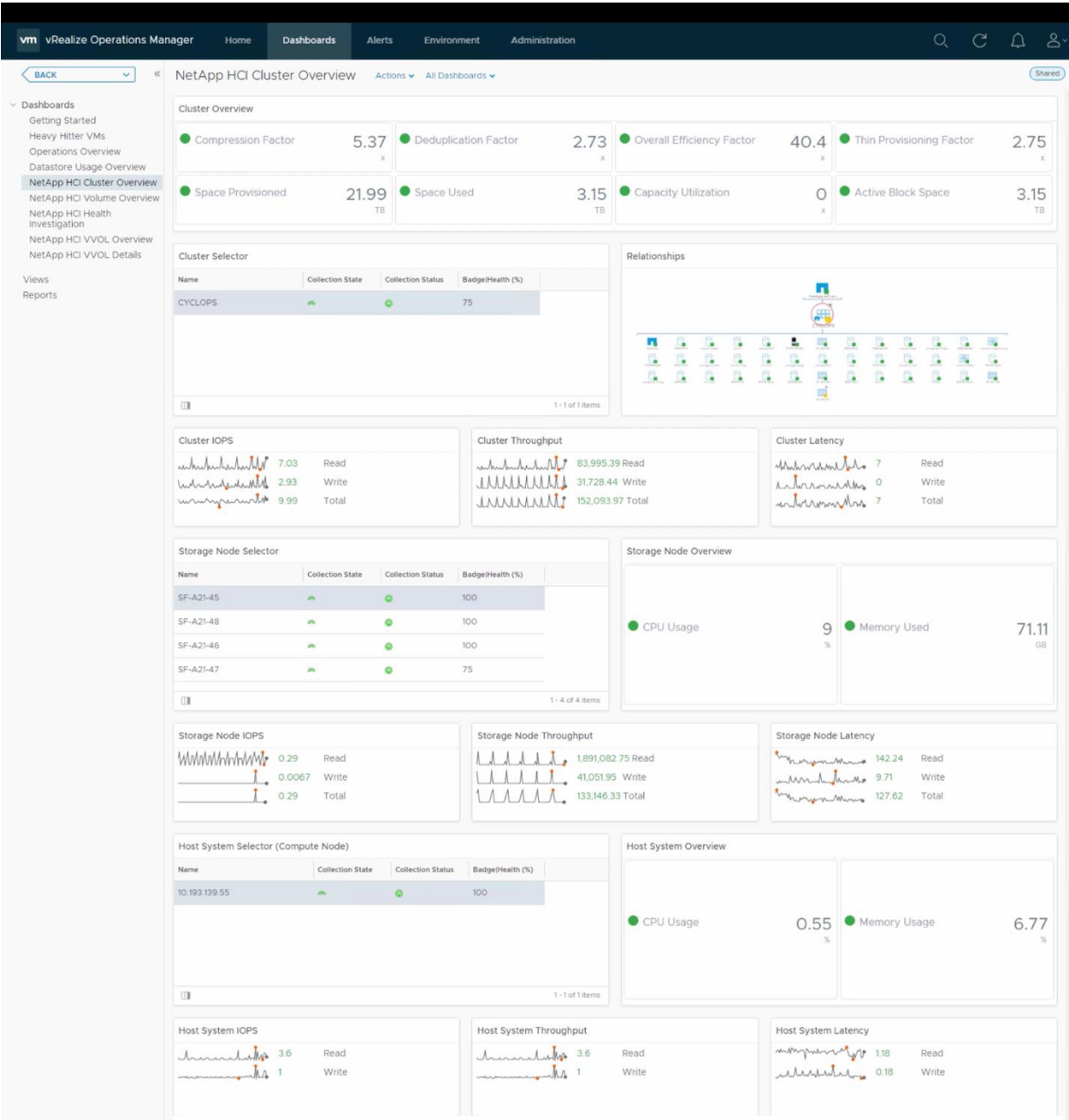
For more information about the Element integration with vOps, see the [VMware vRealize Operations Management Pack for NetApp HCI and SolidFire](#) from Blue Medora.

When you are logged into vOps, various dashboards are visible. The VMware vRealize Operations Management Pack for NetApp HCI and SolidFire offers additional insight into the HCI system with dashboards for:

- NetApp HCI Cluster Overview
- NetApp HCI Volume Overview
- NetApp HCI Health Investigation
- NetApp HCI VVols Overview
- NetApp HCI VVols Details

Figure 10 shows the HCI Cluster Overview dashboard in vOps, which provides insights such as storage efficiency results, cluster performance, node memory, and CPU usage.

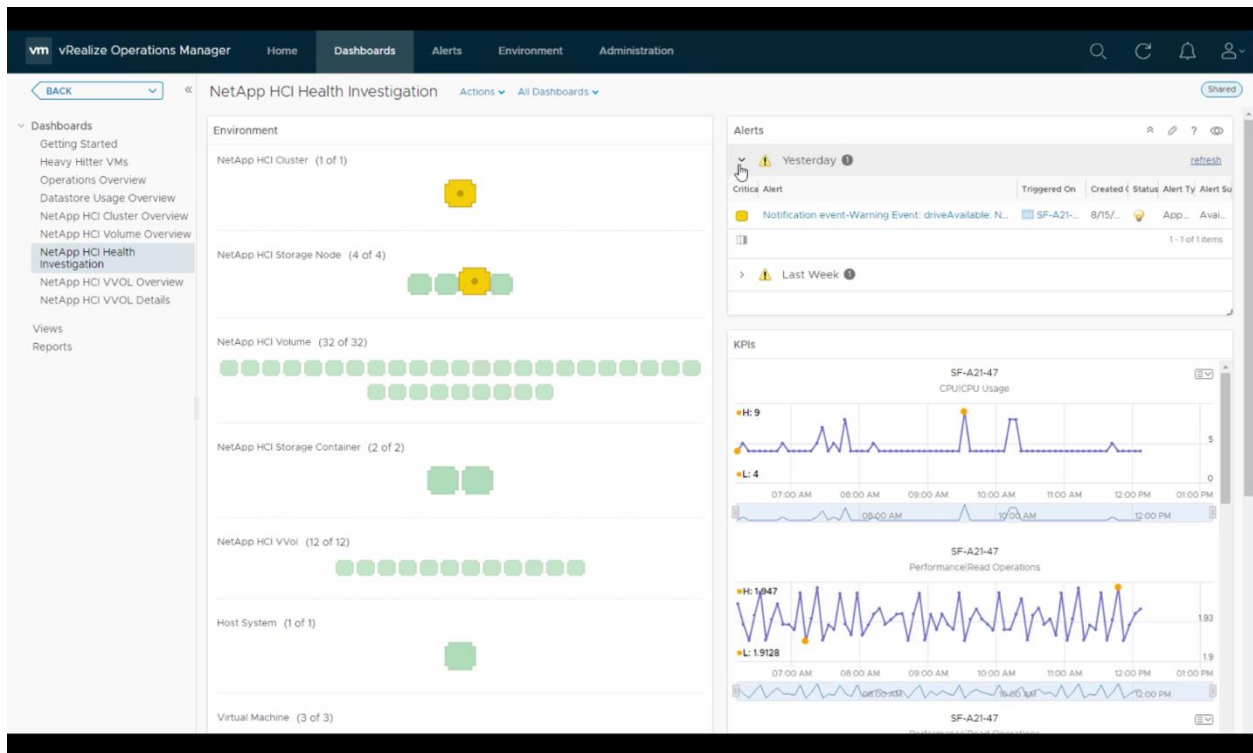
Figure 10) NetApp HCI cluster overview.



The NetApp HCI Health Investigation dashboard provides details about the overall cluster health, as well as alerts for physical, CPU usage, and performance-related activities.

Figure 11 shows the health of the HCI system and the capability to drill into alerts and errors.

Figure 11) NetApp HCI Health Investigation.

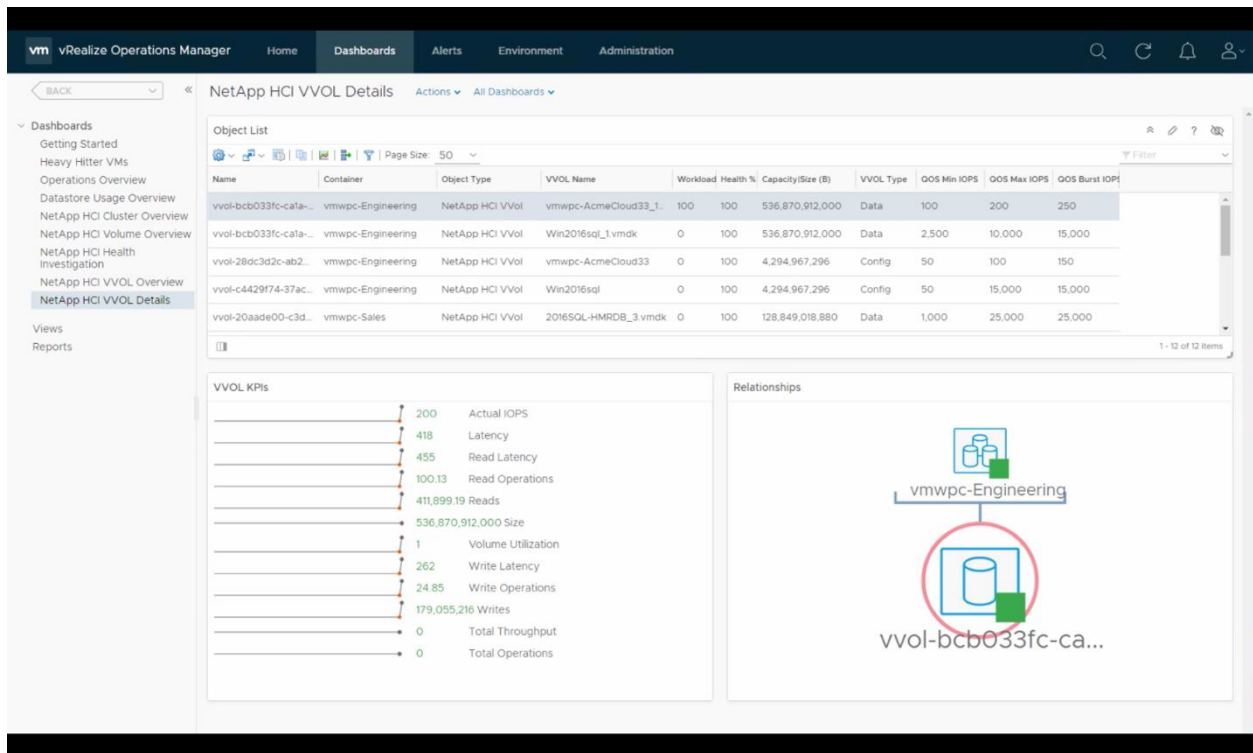


## 7.4 NetApp HCI and vRealize Log Insight

In addition to general visibility into storage systems and workloads, you can identify performance metrics and bottlenecks through vROps. By using the VVols Details dashboard, you can troubleshoot problematic workloads. With vRLI and by using interactive analytics, you can identify workloads that need remediation to improve performance.

Figure 12 shows a workload that has high utilization as visible from the VVols Details dashboard.

Figure 12) NetApp HCI VVols details.



In vRLI, you can identify problems on the identified workload by clicking the Object Detail icon and then the Logs tab. A number of dashboards are available to explore. You can explore the recent logs by clicking the Storage – SCSI Latency / Errors dashboard and Interactive Analytics of the required VVols.

Figure 13 shows the increase in latency of a VVol during a test case. Figure 14 demonstrates the reduction in latency after the review and remediation of the VM storage policy.

Figure 13) vRLI details.

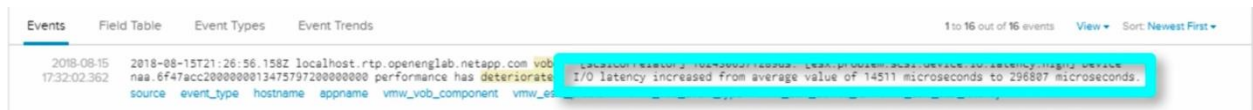
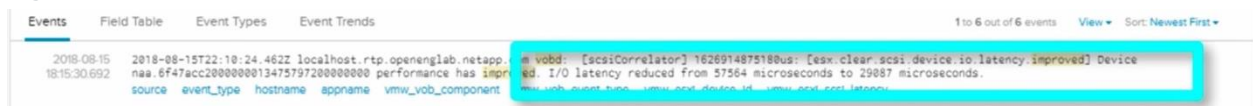


Figure 14) vRLI details.



The combination of the Blue Medora plug-in and SPBM policies enables great visibility into the health of the HCI system. Furthermore, performance issues can be investigated and resolved without ever having to leave the VMware environment.

## 8 Conclusion

By delivering compute and storage resources in an efficient form factor, NetApp HCI scales in a predictable and easy-to-manage manner. VMware vSphere and vCenter use NetApp Element software plug-ins to enable provisioning of VMs for several use cases, with granular control. VMware also provides a suite of products to provide cloudlike provisioning and oversight of these VMs. By combining NetApp HCI and VMware private cloud products, this solution enables self-serviced, centralized operations and debugging capabilities. Additionally, departmental or customer bill-back accounting is achieved with a resilient and easily scalable hyperconverged system. This solution enables an IT department to quickly scale hardware resources to match the dynamic needs of the business. The VMware private cloud on NetApp HCI NVA enables a single console from which an IT department can conduct, troubleshoot, and monitor an environment that includes data from several utilities.

## Appendix

The following sections provide additional details where appropriate or insight for items that were covered through automation previously in the document.

### Sample Storage Node Switch Configuration

#### Storage node switch port example configuration commands

Use the following commands to configure the 1/10GbE (Bond1G) switch ports used for storage node NetApp HCI management traffic:

```
interface GigabitEthernet1/0/1
description HCI-Mgmt-StorageNode01:eth2
switchport access vlan 16
```

Use the following commands to configure the 10/25GbE (Bond10G) switch port channel used for storage node iSCSI traffic:

```
interface Port-channel1
description HCI-Data-StorageNode01-Bond10G
switchport mode trunk
switchport trunk native vlan 2
switchport trunk allowed vlan 3495
spanning-tree port type edge trunk
vpc 102
```

Use the following commands to configure the 10/25GbE (Bond10G) switch ports used for storage node iSCSI traffic:

```
interface Ethernet1/1
description HCI-Data-StorageNode01:eth0
switchport mode trunk
switchport trunk native vlan 3495
spanning-tree port type edge trunk
channel-group 1 mode active
```

## Sample Compute Node Switch Configuration

### Compute node switch port example configuration commands for 2 cable design

Use the following commands to configure the compute node 1/10GbE switch ports used for compute node NetApp HCI management traffic:

```
interface GigabitEthernet1/0/10
description HCI-Mgmt-ComputeNode01:eth0
switchport access vlan 16
```

Use the following commands to configure the 10/25GbE switch ports used for compute node virtual machine and vMotion traffic in a two-cable configuration:

```
interface Ethernet1/10
description HCI-ComputeNode01:eth3
switchport mode trunk
switchport trunk native vlan 2
switchport trunk allowed vlan 3490,3493-3496
spanning-tree port type edge trunk
```

## Modification to Standard vCenter Cluster in Preparation for VMware Private Cloud

In preparation for cluster modification, migrate all VMs using vMotion from hosts destined to be removed from the default HCI cluster. By following these steps, you will have a management cluster and a shared edge and compute cluster.

1. Open a web browser, enter the IP address for the vCenter previously configured through NDE.
2. Enter credentials for the admin account entered during NDE.
3. Select Hosts and Clusters tab on the left.
4. Expand the vCenter for the HCI system.
5. Expand the NetApp HCI Datacenter.
6. Right-click the NetApp HCI Cluster and select Rename.
7. Enter a name to reflect a management cluster and click OK.
8. Right-click the Management Cluster and select New Cluster.
  - a. Enter a cluster name to reflect a shared edge & compute cluster.
  - b. Select the DRS checkbox.
  - c. Select the vSphere HA checkbox.
  - d. Keep the other options at its defaults.
  - e. Click OK.
9. Select a host to be moved to the new cluster:
  - a. Right-click the host, expand Maintenance Mode, and select Enter Maintenance Mode.
  - b. Click OK.

**Note:** Repeat step 9 for all hosts that are to be moved to new cluster.

10. Right-click the newly created cluster and select Move Hosts into New Cluster.
  - a. Select checkboxes for the hosts to be moved.
  - b. Click OK.
11. Select a host moved to the new cluster:
  - a. Right-click the host, expand Maintenance Mode, and select Exit Maintenance Mode.
  - b. Click OK.

**Note:** Repeat step 11 for all hosts that are moved to the new cluster.

## NSX Configuration

To configure and deploy NSX for your environment, complete the following steps.


### Deploy an OVF Template

1. Open a web browser and enter the IP address for the vCenter previously configured through NDE.
2. Log in using the credentials for the admin account entered during NDE.
3. In the Navigation pane, right-click the vCenter and select Deploy OVF Template.
4. In the Select Template section, select the location where you have your NSX Manager OVA file and click Next.
5. In the Select Name and Location section, enter the name of the new VM and select the data center to deploy into. Click Next.
6. In the Select a Resource section, select the Management cluster and click Next.
7. In the Review Details section, review the details of the new template and click Next.
8. In the License Agreements section, review the details and click Accept. Click Next.
9. In the Select Storage section, select the disk format, retain the VM storage policy as none, and select NetApp-HCI-Datastore-01. Click Next.
10. In the Select Networks section, select the management network and click Next.
11. In the Customize Template section, enter the following details and click Next:
  - The DNS Server List information.
  - The Domain Search List information.
  - Network properties including gateway, host name, network 1 IP address, and network 1 netmask.
  - Do not select the checkbox to enable SSH and enter the NTP server information.
  - Enter the CLI “admin” user password and the CLI privilege mode password.
  - Select whether to join the VMware Customer Experience Improvement Program.
12. In the Ready to Complete section, review the settings and click Finish.
13. Review the Recent Tasks section and confirm task completion.

### Register vCenter Server with NSX Manager


1. Open a web browser and navigate to the [https://<ip\\_address\\_NSX\\_Manager>](https://<ip_address_NSX_Manager>). Log in using the admin credentials.
2. Click Manage vCenter Registration.
3. Click Manage and then click NSX Management Service.
4. Under vCenter Server, click Edit.
5. Enter the IP address or FQDN of the vCenter Server.
6. Enter the vCenter user name and password. Click OK.
7. Click Yes to trust the certificate.
8. Return to your vCenter Web Client.













### Add and Assign a License

1. Click Home tab and click Licensing.
2. In the Licenses pane, click the Add (  ) icon to add a license.
3. In the Enter License Key dialog box, enter your licenses and click Next.
4. In the Edit license Names dialog box, optionally modify the license name and click Next.

5. Review the licenses to be added and click Finish.
6. In the Licenses tab, review the licenses that are added.
7. Navigate to the Assets tab and click Solutions.
8. Click Assign License.
9. In the Assign License Wizard, select the NSX for vSphere – Enterprise license and click OK.



## Add NSX Manager to vCenter


1. In vCenter, go to Home and select Networking & Security.
2. Select Installation and Upgrade.
3. Click the NSX controller node tab.
4. Click the Add (+) icon.
5. Select the NSX Manager.
6. In the Password Settings section, enter the credentials for the NSX Manager and click Next.
7. In the Deployment and Connectivity section, select the following:
  - a. The first NSX controller
  - b. HCI data center
  - c. Management cluster
  - d. NetApp-HCI-Datastore-01
  - e. Host
  - f. Management network
  - g. From the IP Pool options, select New IP Pool and enter the following details.
    - The name of the IP pool
    - The gateway
    - The prefix length
    - The primary DNS
    - The secondary DNS
    - The DNS suffix
  - h. Click the Add (+) icon to add an IP address range.
  - i. Enter the IP address range.
  - j. Click Add.
8. Select the newly created IP Pool.
9. Click OK.
10. Click Finish.
11. Review the Status column of hci-nsx-controller-1 and wait until  Connected is shown.
12. Repeat steps 7-10 for the remaining two controller nodes.

	Name	Controller Node	NSX Manager	Managed By	Status	Peers	Upgrade Status	Software Version
<input type="radio"/>	hci-nsx-controller-3	172.21.240.242 controller-3	 172.21.240.207	 172.21.240.207	 Connected		Version up-to-date	6.4.1.8409915
<input type="radio"/>	hci-nsx-controller-2	172.21.240.241 controller-2	 172.21.240.207	 172.21.240.207	 Connected		Version up-to-date	6.4.1.8409915
<input type="radio"/>	hci-nsx-controller-1	172.21.240.240 controller-1	 172.21.240.207	 172.21.240.207	 Connected		Version up-to-date	6.4.1.8409915







## Host Preparation

1. Click the Host Preparation tab.
2. Select the Management cluster.
3. Click the Install NSX button.
4. Click Yes.
5. Click the Configure VXLAN button.
6. Select the HCI Compute switch.
7. Enter the VLAN ID for the VM Network.
8. Keep the default value for the MTU.
9. Select the IP Pool Radial button.
10. Select the IP Pools icon and in the Create a New IP Pool dialog box:
  - a. Enter the name of the IP Pool.
  - b. Enter the Gateway.
  - c. Enter the Prefix Length.
  - d. Enter the Primary DNS.
  - e. Enter the Secondary DNS.
  - f. Enter the DNS suffix.
  - g. Click the Add (  ) icon to add an IP address range.
  - h. Enter the IP address range.
  - i. Click Add.
11. Set vmkNIC Teaming Policy to Load Balance – SRCID.
12. Click Save.
13. Select the Shared Edge & Compute cluster.
14. Click the Install NSX icon.
15. Click Yes
16. Click the Configure VXLAN icon.
17. Select the HCI Compute switch.
18. Enter the VLAN ID for the VM Network.
19. Keep the default for the MTU.
20. Select the IP Pool Radial.
21. Set vmkNIC Teaming Policy to Load Balance – SRCID.
22. Click Save.
23. Select the Logical Network Settings.
24. Under the VXLAN Settings, click Edit under Segment IDs.
25. Specify the range of available ID in the ID pool.
26. Click Save.
27. Select the Transport Zone icon.
28. Click the Add (  ) icon.
29. Enter the name VXLAN-Global-Transport.
30. Select Unicast as the Replication Mode.
31. Select all clusters.

32. Click Add.
33. Select Logical Switches from the Navigator pane.
34. Click the Add (  ) icon to add a New Logical Switch.
35. Enter the Name of the new logical switch.
36. Enter the description of the new logical switch.
37. Enter the VXLAN-Global-Transport zone.
38. Select Unicast as the Replication Mode.
39. Click OK.

**Note:** Repeat as needed for additional VXLANs.

## Configure NSX Edges

1. Select NSX Edges from the navigator pane.
2. Click Add (  ) icon.
3. In the Name and Description section:
  - a. Select Edge Services Gateway for the Install Type.
  - b. Enter the name of the gateway.
  - c. (Optional) enter a host name.
  - d. (Optional) enter a description and tenant.
  - e. Leave the Deploy NSX Edge checkbox selected.
  - f. Click Next.
4. In the Settings section:
  - a. Enter and confirm the admin password.
  - b. Leave the Enable auto rule generation checkbox selected.
  - c. Click Next.
5. In the Configure Deployment section:
  - a. Select the HCI Datacenter.
  - b. Select the appropriate appliance size.
  - c. Click the  icon.
  - d. Select the Shared Edge & Compute Pool.
  - e. Select HCI Datastore 02.
  - f. Click OK.
  - g. Click Next.
6. In the Configure Interfaces section:
  - a. Click the  icon
  - b. Enter the name of the NSX Edge interface
  - c. Select Type: Uplink
  - d. Click select to connect the NSX Edge to a network.
  - e. Select the appropriate logical switch for this connection.
  - f. Click OK.
  - g. Click the  icon.
  - h. Enter the primary IP address.

- i. Enter the subnet prefix length.
  - j. Click OK.
  - k. Click Next.
7. In the Default Gateway Settings section:
  - a. Leave the Configure Default Gateway checkbox selected.
  - b. Select the appropriate vNIC.
  - c. Enter the Gateway IP.
  - d. Click Next.
8. In the Firewall and HA section, retain the default settings and click Next.
9. In the Ready to Complete section, review the settings and click Finish.

## Where to Find Additional Information

To learn more about the information described in this document, refer to the following documents and/or websites:

- NVA-1122-DESIGN: NetApp HCI for VMware Private Cloud  
<https://www.netapp.com/us/media/nva-1122-design.pdf>
- NetApp Product Documentation  
[docs.netapp.com](https://docs.netapp.com)
- HCI Resources page  
<https://mysupport.netapp.com/info/web/ECMLP2831412.html>
- NetApp HCI  
<https://www.netapp.com/us/products/converged-systems/hyper-converged-infrastructure.aspx>

Refer to the [Interoperability Matrix Tool \(IMT\)](#) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

### **Copyright Information**

Copyright © 2019 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

### **Trademark Information**

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

NVA-1122-DEPLOY-0419