NetApp Verified Architecture

FlexPod Express with VMware vSphere 6.0: Large Configuration

NVA Deployment Guide

Karthick Radhakrishnan, Arvind Ramakrishnan, NetApp
Chris O'Brien, Cisco

September 2015 | NVA-0017-DEPLOY | Version 1.0

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Program Summary

1.1 NetApp Verified Architecture Program

The NetApp Verified Architecture (NVA) program offers customers a validated architecture for NetApp® solutions. NVAs provide customers with a NetApp solution architecture that:

- Is thoroughly tested
- Is prescriptive in nature
- Minimizes deployment risks
- Accelerates customers' time to market

This document is for NetApp and partner solution engineers and customer strategic decision makers. The document describes the architecture design considerations used to determine the specific equipment, cabling, and configuration required in a particular environment.

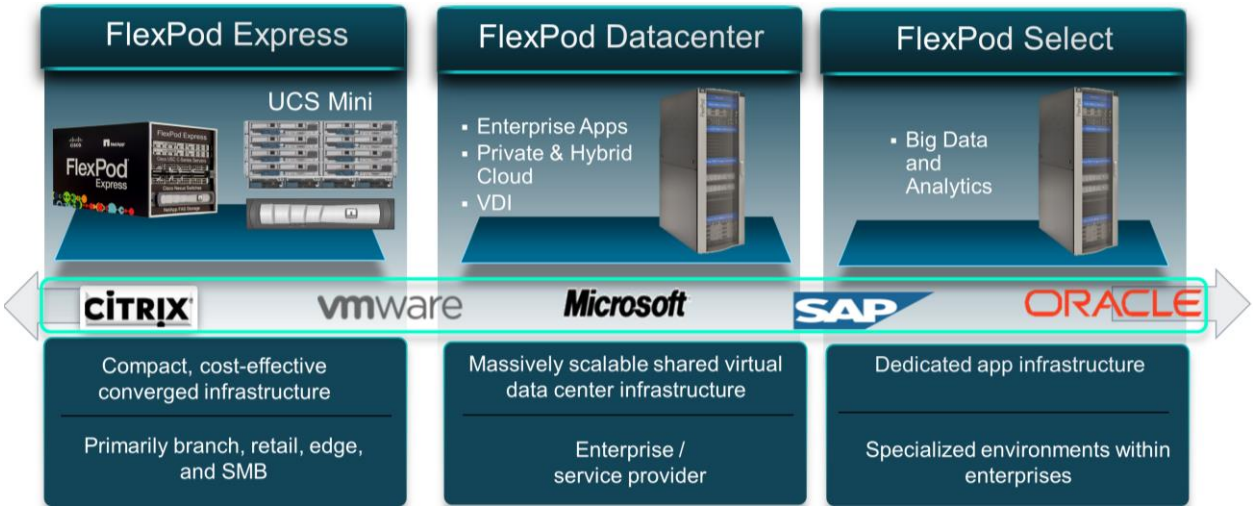
1.2 FlexPod Converged Infrastructure Program

The FlexPod® data center platform delivers key technologies from Cisco and NetApp. FlexPod reference architectures are often delivered as Cisco Validated Designs (CVDs) or NetApp Verified Architectures (NVAs). Deviations because of customer requirements from a given CVD or NVA are encouraged, provided that variations do not result in the deployment of unsupported configurations.

As depicted in Figure 1, the FlexPod program includes three solutions: FlexPod Express, FlexPod Datacenter, and FlexPod Select.

- **FlexPod Express** offers customers an entry-level solution consisting of technologies from Cisco and NetApp.
- **FlexPod Datacenter** delivers an ideal multipurpose foundation for a variety of workloads and applications.
- **FlexPod Select** incorporates the best aspects of FlexPod Datacenter and tailors the infrastructure to a given application.

Figure 1) FlexPod portfolio.



The solution discussed in this design guide is part of the FlexPod Select family. Optimizing Oracle databases can include changes in the compute, network, and storage layer. As such, the design outlined in this document dives into architecture tied to specific performance criteria

2 Solution Overview

FlexPod Express is a suitable platform for running a variety of virtualization hypervisors as well as bare-metal operating systems and enterprise workloads. FlexPod Express delivers not only a baseline configuration, but also the flexibility to be sized and optimized to accommodate many different use cases and requirements. The large FlexPod Express configuration is a low-cost, standardized infrastructure solution developed to meet the needs of small and midsize businesses. Each configuration provides a standardized base platform capable of running a number of business-critical applications while providing scalability options to enable infrastructure augmentation with increasing business demands.

FlexPod Express:

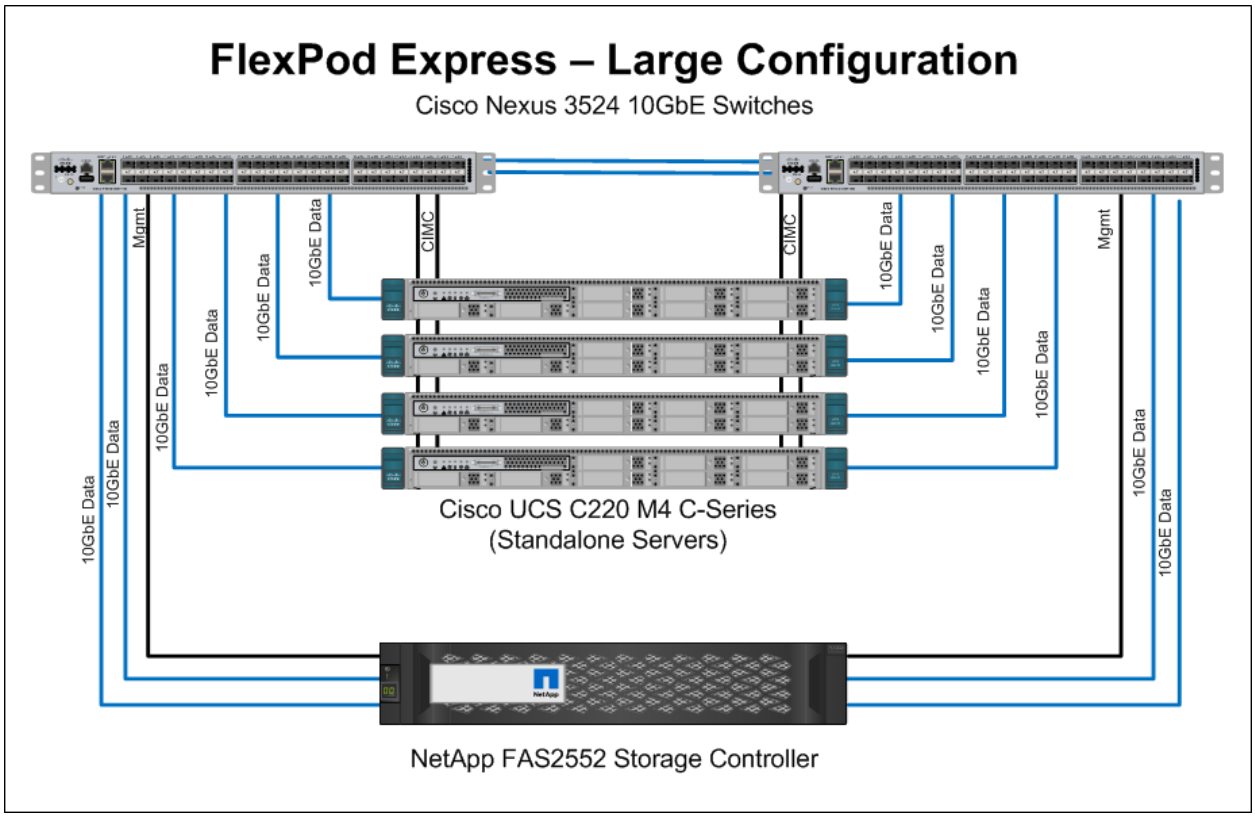
- Combines all application and data needs into a single platform
- Is suitable for small to midsize organizations, remote and departmental deployments
- Provides easy infrastructure scaling
- Reduces cost and complexity

2.1 Solution Technology

The large FlexPod Express configuration uses Cisco UCS C-Series rack servers, Cisco Nexus switches (10GbE), and NetApp FAS storage systems (the NetApp clustered Data ONTAP® operating system: switchless). This document describes the implementation of VMware vSphere 6.0 on the large FlexPod Express offering. The configurations are based on best practices for each component in the solution architecture to enable a reliable enterprise-class infrastructure.

Figure 2 depicts the topology of the FlexPod Express large configuration.

Figure 2) Physical topology of FlexPod Express large configuration.



2.2 Use Case Summary

This document describes the deployment procedures and best practices to set up a FlexPod Express large configuration with VMware vSphere 6.0 as the workload. The server operating system/hypervisor is VMware vSphere ESXi, and an instance of VMware vCenter Server is installed to manage the ESXi instances. The whole infrastructure is supported by NetApp FAS storage systems that serve data over storage area network (SAN) and network-attached storage (NAS) protocols.

3 Technology Requirements

This section includes details of the hardware and software components required to implement the FlexPod Express large configuration.

3.1 Hardware Requirements

Table 1 lists the hardware components required to implement the FlexPod Express large configuration solution.

Table 1) FlexPod Express large configuration hardware requirements.

Layer	Hardware	Quantity
Compute	Cisco UCS C220 M4 rack servers (standalone)	4
Network	Cisco Nexus 3524 switches	2
Storage	NetApp FAS2552 (high-availability pair)	1
Disks	900GB, 10.000-rpm SAS with Advanced Drive Partitioning	24

3.2 Software Requirements

Table 2 lists the software components required to implement the FlexPod Express large configuration.

Table 2) Software components.

Layer	Component	Version or Release	Details
Compute	Cisco UCS C220 M4 rack servers	2.0(3)	Cisco Integrated Management Controller (IMC) software
Network	Cisco Nexus 3524 switches	6.0(2)A6(1)	Cisco NX-OS software
Storage	NetApp FAS2552 high-availability storage	8.3	NetApp Data ONTAP software
Hypervisor	VMware vSphere	6.0	VMware Virtualization Hypervisor Suite
Other software	NetApp Virtual Storage Console (VSC)	6.0	NetApp plug-in for VMware vCenter

4 FlexPod Express Cabling Information

4.1 FlexPod Express Large Configuration

Figure 3 provides a cabling diagram for the FlexPod Express large configuration. Table 3 provides cabling information.

Figure 3) FlexPod Express large configuration cabling diagram.

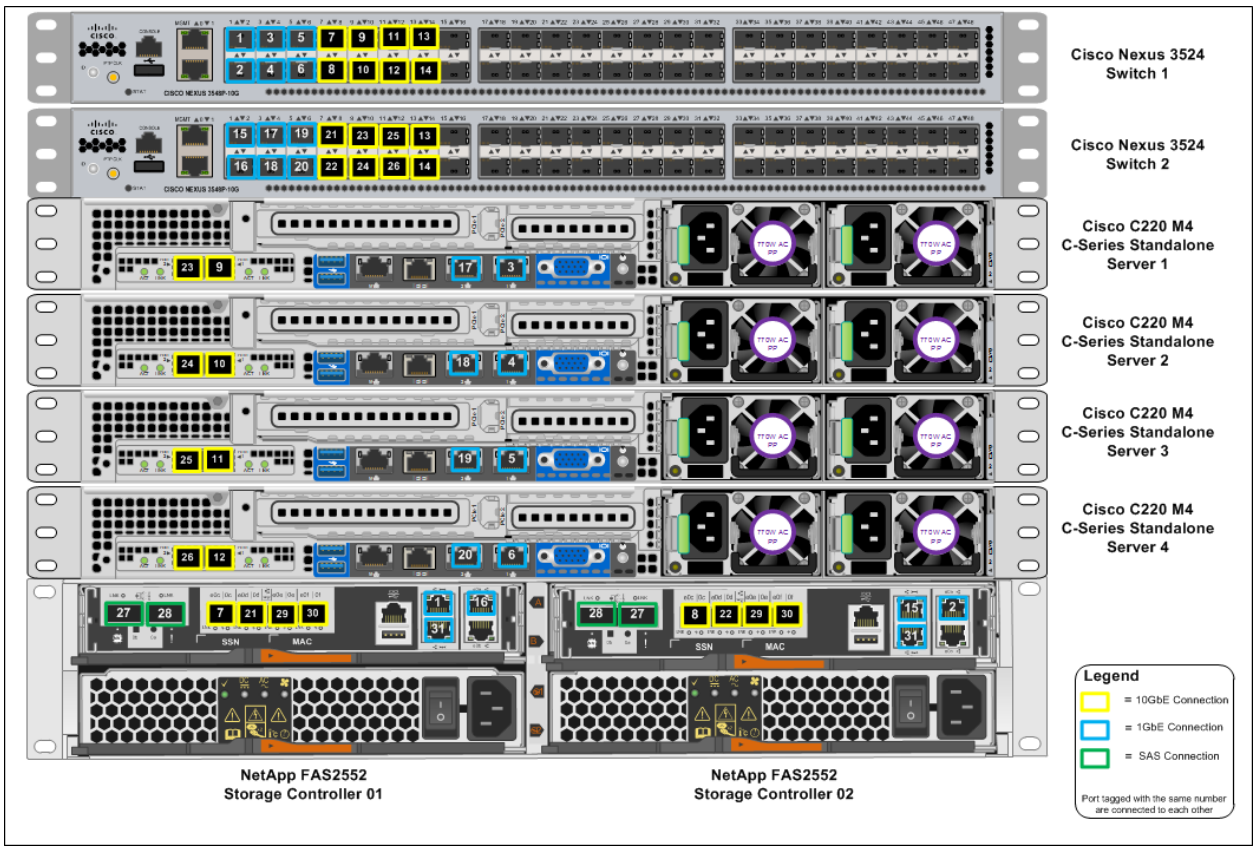


Table 3) Cabling information for the FlexPod Express large configuration.

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
Cisco Nexus 3524 Switch A	Eth1/1	NetApp FAS2552 Storage Controller 01	e0M	1
	Eth1/2	NetApp FAS2552 Storage Controller 02	e0a	2
	Eth1/3	Cisco UCS C220 C-Series Standalone Server 1	LOM1	3
	Eth1/4	Cisco UCS C220 C-Series Standalone Server 2	LOM1	4
	Eth1/5	Cisco UCS C220 C-Series Standalone Server 3	LOM1	5

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
	Eth1/6	Cisco UCS C220 C-Series Standalone Server 4	LOM1	6
	Eth1/7	NetApp FAS2552 Storage Controller 01	e0c	7
	Eth1/8	NetApp FAS2552 Storage Controller 02	e0c	8
	Eth1/9	Cisco UCS C220 C-Series Standalone Server 1	MLOM Port 1	9
	Eth1/10	Cisco UCS C220 C-Series Standalone Server 2	MLOM Port 1	10
	Eth1/11	Cisco UCS C220 C-Series Standalone Server 3	MLOM Port 1	11
	Eth1/12	Cisco UCS C220 C-Series Standalone Server 4	MLOM Port 1	12
	Eth1/13	Cisco Nexus 3524 Switch B	Eth 1/13	13
	Eth1/14	Cisco Nexus 3524 Switch B	Eth 1/14	14

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
Cisco Nexus 3524 Switch B	Eth1/1	NetApp FAS2552 Storage Controller 02	e0M	15
	Eth1/2	NetApp FAS2552 Storage Controller 01	e0a	16
	Eth1/3	Cisco UCS C220 C-Series Standalone Server 1	LOM2	17
	Eth1/4	Cisco UCS C220 C-Series Standalone Server 2	LOM2	18
	Eth1/5	Cisco UCS C220 C-Series Standalone Server 3	LOM2	19
	Eth1/6	Cisco UCS C220 C-Series Standalone Server 4	LOM2	20
	Eth1/7	NetApp FAS2552 Storage Controller 01	e0d	21
	Eth1/8	NetApp FAS2552 Storage Controller 02	e0d	22
	Eth1/9	Cisco UCS C220 C-Series Standalone Server 1	MLOM Port 2	23
	Eth1/10	Cisco UCS C220 C-Series Standalone Server 2	MLOM Port 2	24

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
	Eth1/11	Cisco UCS C220 C-Series Standalone Server 3	MLOM Port 2	25
	Eth1/12	Cisco UCS C220 C-Series Standalone Server 4	MLOM Port 2	26
	Eth1/13	Cisco Nexus 3524 Switch A	Eth1/13	13
	Eth1/14	Cisco Nexus 3524 Switch A	Eth1/14	14

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
NetApp FAS2552 Storage Controller 01	e0e	NetApp FAS2552 Storage Controller 02	e0e	29
	e0f	NetApp FAS2552 Storage Controller 02	e0f	30
	ACP	NetApp FAS2552 Storage Controller 02	ACP	31
	SAS 0b	NetApp FAS2552 Storage Controller 01	SAS 0a	27
	SAS 0a	NetApp FAS2552 Storage Controller 01	SAS 0b	28

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
NetApp FAS2552 Storage Controller 02	e0e	NetApp FAS2552 Storage Controller 01	e0e	29
	e0f	NetApp FAS2552 Storage Controller 01	e0f	30
	ACP	NetApp FAS2552 Storage Controller 01	ACP	31
	SAS 0b	NetApp FAS2552 Storage Controller 01	SAS 0a	27
	SAS 0a	NetApp FAS2552 Storage Controller 01	SAS 0b	28

5 Deployment Procedures

This document provides details for configuring a fully redundant, highly available FlexPod Express system. To reflect this redundancy, the components being configured in each step are referred to as either Component 01 or Component 02. For example, Controller 01 and Controller 02 identify the two

NetApp storage controllers that are provisioned in this document. Switch A and Switch B identify a pair of Cisco Nexus switches that are configured.

Additionally, this document details steps for provisioning multiple Cisco UCS hosts, which are identified sequentially as Server-1, Server-2, and so on.

To indicate that you should include information pertinent to your environment in a given step, `<<text>>` appears as part of the command structure. See the following example for the `vlan create` command:

```
Controller01>vlan create vif0 <<ib_mgmt_vlan_id>>
```

This document intends to enable you to fully configure the FlexPod Express environment. In this process, various steps require you to insert customer-specific naming conventions, IP addresses, and virtual local area network (VLAN) schemes. Table 4 describes the necessary VLANs for deployment, as outlined in this guide. This table can be completed based on the specific site variables and used in implementing the document configuration steps.

Note: If you use separate in-band and out-of-band management VLANs, you must create a Layer 3 route between these VLANs. For this validation, a common management VLAN was used.

Table 4) Required VLANs.

VLAN Name	VLAN Purpose	ID Used in Validating This Document
Management VLAN	VLAN for management interfaces	3051
Native VLAN	VLAN to which untagged frames are assigned	2
Network File System (NFS) VLAN	VLAN for NFS traffic	3054
VMware vMotion VLAN	VLAN designated for the movement of virtual machines from one physical host to another	3052
Virtual machine traffic VLAN	VLAN for virtual machine application traffic	3053
iSCSI-A-VLAN	VLAN for iSCSI traffic on Fabric A	3055
iSCSI-B-VLAN	VLAN for iSCSI traffic on Fabric B	3056

Table 5 lists the VMware virtual machines (VMs) created.

Table 5) VMware virtual machines created.

Virtual Machine Description	Host Name
VMware vCenter Server	
NetApp Virtual Storage Console	

5.1 Cisco Nexus 3524 Deployment Procedure

The following section details the Cisco Nexus 3524 switch configuration for use in a FlexPod Express environment.

Initial Setup of Cisco Nexus 3524 Switch

Upon initial boot and connection to the console port of the switch, the Cisco NX-OS setup automatically starts. This initial configuration addresses basic settings, such as the switch name, the mgmt0 interface configuration, and Secure Shell (SSH) setup, and it defines the policy for control-plane policing.

The first major decision involves the configuration of the management network for the switches. For FlexPod Express, there are two main options for configuring the mgmt0 interfaces. The first involves

configuring and cabling the mgmt0 interfaces into an existing out-of-band network. In this instance, when a management network exists, all that you need are the valid IP addresses, the netmask configuration for this network, and a connection from the mgmt0 interfaces to this network.

The other option, for installations without a dedicated management network, involves cabling together the mgmt0 interfaces of each Cisco Nexus 3524 switch in a back-to-back configuration. Any valid IP address and netmask can be configured on each of the mgmt0 interfaces as long as they are in the same network. Because they are configured back to back with no switch or other device in between, no default gateway configuration is needed and the interfaces should be able to communicate with each other. This link cannot be used for external management access such as SSH access, but it can be used for the virtual PortChannel (vPC) peer keepalive traffic. To enable SSH management access to the switch, configure the in-band interface VLAN IP address on a switched virtual interface (SVI), as discussed later in this document.

1. Power on the switch and follow the on-screen prompts as illustrated here for the initial setup of both the switches, substituting the appropriate values for the switch-specific information.

Cisco Nexus Switch A and Switch B

```
Abort Power On Auto Provisioning and continue with normal setup ?(yes/no)[n]: yes

        ---- System Admin Account Setup ----

Do you want to enforce secure password standard (yes/no): yes
  Enter the password for "admin":<<admin_password>>
  Confirm the password for "admin":<<admin_password>>

        ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus 3500 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus devices must be registered to receive entitled
support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes
  Create another login account (yes/no) [n]: Enter
  Configure read-only SNMP community string (yes/no) [n]:Enter
  Configure read-write SNMP community string (yes/no) [n]:Enter
  Enter the switch name : <<switch_A/B_hostname>>
  Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:Enter
    Mgmt0 IPv4 address : <<switch_A/B_mgmt0_ip_addr>>
    Mgmt0 IPv4 netmask : <<switch_A/B_mgmt0_netmask>>
  Configure the default gateway? (yes/no) [y]:Enter
```

Note: Do not configure the default gateway if the mgmt ports of the Cisco Nexus 3524 switches are connected back to back.

```
  IPv4 address of the default gateway : <<switch_A/B_mgmt0_gateway_ip_addr>>
  Enable the telnet service? (yes/no) [n]:Enter
  Enable the ssh service? (yes/no) [y]:Enter
    Type of ssh key you would like to generate (dsa/rsa) : rsa
    Number of  key bits <768-2048> : 1024
  Configure the ntp server? (yes/no) [n]:Enter
  Configure default interface layer (L3/L2) [L2]:Enter
  Configure default switchport interface state (shut/noshut) [noshut]:Enter
  Configure CoPP System Policy Profile ( default / l2 / l3 ) [default]:Enter

The following configuration will be applied:
  switchname <<switch_A/B_hostname>>
```

```
interface mgmt0
ip address <<switch_A/B_mgmt0_ip_addr>> <<switch_A/B_mgmt0_netmask>>
no shutdown
exit
vrf context management
ip route 0.0.0.0/0 <<switch_A/B_mgmt0_gateway_ip_addr>>
exit
  no telnet server enable
  ssh key rsa 1024 force
  ssh server enable
  system default switchport
  no system default switchport shutdown
  policy-map type control-plane copp-system-policy ( default )


Would you like to edit the configuration? (yes/no) [n]:Enter
Use this configuration and save it? (yes/no) [y]:Enter
```

Upgrading Cisco NX-OS (Optional)

Perform any required software upgrades on the switch at this point in the configuration process. Download and install the latest available Cisco NX-OS software for the Cisco Nexus 3524 switch from the Cisco software download site. There are multiple ways to transfer both the kickstart and system images for Cisco NX-OS to the switch. The most straightforward procedure uses the onboard USB port on the switch. Download the Cisco NX-OS kickstart and system files to a USB drive and plug the USB drive into the external USB port on the Cisco Nexus 3524 switch.

Note: Cisco NX-OS software release 6.0(2)A6(1) is used in this solution.

1. Copy the files to the local bootflash memory and update the switch by following the procedure shown here.

Cisco Nexus Switch A and Switch B

```
copy usb1:<<kickstart_image_file>> bootflash:
copy usb1:<<system_image_file>> bootflash:
install all kickstart bootflash:<<kickstart_image_file>> system bootflash:<<system_image_file>>
```

Note: The switches will install the updated Cisco NX-OS files and reboot.

Enabling Advanced Features

Certain advanced features need to be enabled in Cisco NX-OS to provide additional configuration options.

Note: The interface-vlan feature is required only if you use the back-to-back mgmt0 option described throughout this document. This feature enables an IP address to be assigned to the interface VLAN (SVI), which enables in-band management communication to the switch, such as through SSH.

Enter configuration mode using the command `(config t)` and type the following commands to enable the appropriate features on each switch.

Cisco Nexus Switch A and Switch B

```
feature interface-vlan
feature lacp
feature vpc
```

Performing Global PortChannel Configuration

The default PortChannel load-balancing hash uses the source and destination IP addresses to determine the load-balancing algorithm across the interfaces in the PortChannel. You can achieve better distribution

across the members of the PortChannel by providing more inputs to the hash algorithm beyond the source and destination IP addresses. For the same reason, NetApp highly recommends adding the source and destination TCP ports to the hash algorithm.

From configuration mode (`config t`), type the following commands to configure the global PortChannel load-balancing configuration on each of the switches.

Cisco Nexus Switch A and Switch B

```
port-channel load-balance ethernet source-dest-port
```

Performing Global Spanning-Tree Configuration

The Cisco Nexus platform uses a new protection feature called bridge assurance. Bridge assurance helps protect against a unidirectional link or other software failure and a device that continues to forward data traffic when it is no longer running the spanning-tree algorithm. Ports can be placed in one of several states, including network and edge, depending on the platform.

The recommended setting for bridge assurance is to consider all ports to be network ports by default.

This setting forces the network administrator to review the configuration of each port and helps reveal the most common configuration errors, such as unidentified edge ports or a neighbor that does not have the bridge assurance feature enabled. Also, it is safer to have the spanning tree block many ports rather than not enough, allowing the default port state to enhance the overall stability of the network.

Pay close attention to the spanning-tree state when adding servers, storage, and uplink switches, especially if they do not support bridge assurance. In such cases, you might need to change the port type to make the ports active.

The Bridge Protocol Data Unit (BPDU) guard is enabled on edge ports by default as another layer of protection. To prevent loops in the network, this feature shuts down the port if BPDUs from another switch are seen on this interface.

From configuration mode (`config t`), type the following commands to configure the default spanning-tree options, including the default port type and BPDU guard on each of the switches.

Cisco Nexus Switch A and Switch B

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
```

Configuring Jumbo Frames

Jumbo frames should be configured throughout the network to enable any applications and operating systems to transmit these larger frames without fragmentation. Both the endpoints and all the interfaces between the endpoints (Layer 2 and Layer 3) must support and be configured for jumbo frames to achieve the benefits and to prevent performance problems by fragmenting frames.

From configuration mode (`config t`), type the following commands to enable jumbo frames on each of the switches.

Cisco Nexus Switch A and Switch B

```
policy-map type network-qos jumbo
  class type network-qos class-default
    mtu 9216
system qos
  service-policy type network-qos jumbo
exit
```

Defining VLANs

Before configuring individual ports with different VLANs, the Layer 2 VLANs must be defined on the switch. It is also a good practice to name the VLANs for easy troubleshooting in the future.

From configuration mode (`config t`), type the following commands to define and give descriptions to the Layer 2 VLANs.

Cisco Nexus Switch A and Switch B

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<ib_mgmt_vlan_id>>
  name IB-MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

Configuring Access and Management Port Descriptions

As with assigning names to the Layer 2 VLANs, setting descriptions for all the interfaces can help both with provisioning and with troubleshooting.

From configuration mode (`config t`) in each of the switches, type the following commands to set up the port descriptions.

FlexPod Express Large Configuration

Enter the following port descriptions for the FlexPod Express large configuration.

Cisco Nexus Switch A

```
int eth1/1
  description Controller-01:e0M
int eth1/2
  description Controller-02:e0a
int eth1/3
  description Server1:LOM1
int eth1/4
  description Server2:LOM1
int eth1/5
  description Server3:LOM1
int eth1/6
  description Server4:LOM1
int eth1/7
  description Controller-01:e0c
int eth1/8
  description Controller-02:e0c
int eth1/9
  description Server-1:VIC Port 1
int eth1/10
  description Server-2:VIC Port 1
int eth1/11
  description Server-3:VIC Port 1
int eth1/12
  description Server-4:VIC Port 1
int eth1/13
  description vPC peer-link NX3524-B:1/13
```

Cisco Nexus Switch B

```
int eth1/1
  description Controller-02:e0M
int eth1/2
  description Controller-01:e0a
int eth1/3
  description Server1:LOM2
int eth1/4
  description Server2:LOM2
int eth1/5
  description Server3:LOM2
int eth1/6
  description Server4:LOM2
int eth1/7
  description Controller-01:e0d
int eth1/8
  description Controller-02:e0d
int eth1/9
  description Server-1:VIC Port 2
int eth1/10
  description Server-2:VIC Port 2
int eth1/11
  description Server-3:VIC Port 2
int eth1/12
  description Server-4:VIC Port 2
int eth1/13
  description vPC peer-link NX3524-A:1/13
```

int eth1/14
  description vPC peer-link NX3524-B:1/14
	int eth1/14
	  description vPC peer-link NX3524-A:1/14

Configuring Server and Storage Management Interfaces

The management interfaces for both the server and storage typically use only a single VLAN. Therefore, configure the management interface ports as access ports. Define the management VLAN for each switch and change the spanning-tree port type to edge.

From configuration mode (`config t`), type the following commands to configure the port settings for the management interfaces of both the servers and the storage.

Cisco Nexus Switch A

```
int eth1/1-6
  switchport access vlan <<ib_mgmt_vlan_id>>
  spanning-tree port type edge
exit
```

Cisco Nexus Switch B

```
int eth1/1-6
  switchport access vlan <<ib_mgmt_vlan_id>>
  spanning-tree port type edge
int eth1/3-6
  vpc orphan-port suspend
exit
```

Performing Virtual PortChannel Global Configuration

A virtual PortChannel (vPC) enables links that are physically connected to two different Cisco Nexus switches to appear as a single PortChannel to a third device. The third device can be a switch, server, or any other networking device. A vPC can provide Layer 2 multipathing, which enables you to create redundancy by increasing bandwidth, enabling multiple parallel paths between nodes, and load-balancing traffic where alternative paths exist.

A vPC provides the following benefits:

- Enables a single device to use a PortChannel across two upstream devices
- Eliminates Spanning-Tree Protocol blocked ports
- Provides a loop-free topology
- Uses all available uplink bandwidth
- Provides fast convergence if either the link or a device fails
- Provides link-level resiliency
- Helps provide high availability

The vPC feature requires some initial setup between the two Cisco Nexus switches to function properly. If you use the back-to-back mgmt0 configuration, use the addresses defined on the interfaces and verify that they can communicate by using the ping `<<switch_A/B_mgmt0_ip_addr>>vrf` management command.

From configuration mode (`config t`), type the following commands to configure the vPC global configuration for switch A.

Cisco Nexus Switch A

```
vpc domain 1
  peer-switch
  role priority 10
```

```
  peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source <<switch_A_mgmt0_ip_addr>> vrf
management
  peer-gateway
  auto-recovery
  ip arp synchronize

int eth1/13-14
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<ib_mgmt_vlan_id>>, <<iSCSI_A_vlan_id>>, <<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
  no shut
exit
copy run start
```

From configuration mode (`config t`), type the following commands to configure the vPC global configuration for Switch B.

Cisco Nexus Switch B

```
vpc domain 1
  peer-switch
  role priority 20
  peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source <<switch_B_mgmt0_ip_addr>> vrf
management
  peer-gateway
  auto-recovery
  ip arp synchronize

int eth1/13-14
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<ib_mgmt_vlan_id>>, <<iSCSI_A_vlan_id>>, <<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
no shut
exit
copy run start
```

Configuring Storage PortChannels

The NetApp storage controllers allow an active-active connection to the network using Link Aggregation Control Protocol (LACP). The use of LACP is preferred because it adds both negotiation and logging between the switches. Because the network is set up for vPC, this approach enables you to have active-active connections from the storage to separate physical switches. Each controller will have two links to each of the switches, but all four links are part of the same vPC and interface group (IFGRP).

From configuration mode (`config t`), type the following commands on each of the switches to configure the individual interfaces and the resulting PortChannel configuration for the ports connected to the NetApp FAS controller.

Cisco Nexus Switches A and B and NetApp Storage Controller-01 Configuration

```
int eth1/7
  channel-group 11 mode active
```

```
int Po11
  description vPC to Controller-01
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<ib_mgmt_vlan_id>>,<<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  vpc 11
  no shut
```

Cisco Nexus Switches A and B and NetApp Storage Controller-02 Configuration

```
int eth1/8
  channel-group 12 mode active
int Po12
  description vPC to Controller-02
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<ib_mgmt_vlan_id>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  vpc 12
  no shut
exit
copy run start
```

Configuring Server Connections

The Cisco UCS servers have a two-port virtual interface card, VIC1227, that is used for data traffic and booting of the ESXi operating system using iSCSI. These interfaces are configured to fail over to one another, providing additional redundancy beyond a single link. Spreading these links across multiple switches enables the server to survive even a complete switch failure.

From configuration mode (`config t`), type the following commands to configure the port settings for the interfaces connected to each server.

Cisco Nexus Switch A: Cisco UCS Server-1, Server-2, Server-3, and Server-4 Configuration

```
int eth1/9-12
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_A_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,
<<ib_mgmt_vlan_id>>
  spanning-tree port type edge trunk
  no shut
exit
copy run start
```

Cisco Nexus Switch B: Cisco UCS Server-1, Server-2, Server-3, and Server-4 Configuration

```
int eth1/9-12
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_B_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,
<<ib_mgmt_vlan_id>>
  spanning-tree port type edge trunk
  vpc orphan-port suspend
  no shut
exit
```

```
copy run start
```

Performing in-Band Management SVI Configuration

In-band management using SSH in the FlexPod Express environment is handled by an SVI. To configure in-band management on each switch, configure an IP address on the interface VLAN and set up a default gateway.

From configuration mode (`config t`), type the following commands to configure the Layer 3 SVI for management purposes.

Cisco Nexus Switch A

```
int Vlan <<oob_mgmt_vlan_id>>
ip address <<outofband_mgmt_ip_address_A>>/<<outofband_mgmt_netmask>>
no shut
ip route 0.0.0.0/0 <<outofband_mgmt_gateway>>
```

Cisco Nexus Switch B

```
int Vlan <<oob_mgmt_vlan_id>>
ip address <<outofband_mgmt_ip_address_B>>/<<outofband_mgmt_netmask>>
no shut
ip route 0.0.0.0/0 <<outofband_mgmt_gateway>>
```

5.2 NetApp FAS Storage Deployment Procedure (Part 1)

This section describes the NetApp FAS storage deployment procedure.

NetApp Storage Controller FAS25xx Series

NetApp Hardware Universe

The NetApp Hardware Universe provides supported hardware and software components for a specific NetApp Data ONTAP version. It provides configuration information for all NetApp storage appliances currently supported by Data ONTAP software. It also provides a table of component compatibilities.

1. Make sure that the hardware and software components are supported with the version of Data ONTAP you plan to install by checking the NetApp Hardware Universe at the NetApp Support site.
2. Access the Hardware Universe application to view the system configuration guides. Click the Controllers tab to view the compatibility between NetApp Data ONTAP software versions and NetApp storage appliances with the desired specifications.
3. Alternatively, to compare components by storage appliance, click Compare Storage Systems.

Table 6) NetApp FAS25XX series prerequisites.

Controller FAS255X Series Prerequisites
To plan the physical location of the storage systems, refer to the NetApp Hardware Universe. Refer to the sections on: • Electrical requirements • Supported power cords • Onboard ports and cables Refer to the site requirements guide replacement tutorial for finding NetApp FAS platform information using the Hardware Universe.

Storage Controllers

Follow the physical installation procedures for the controllers in the FAS25xx documentation available at the NetApp Support site.

NetApp Clustered Data ONTAP 8.3

Configuration Worksheet

Before running the setup script, complete the configuration worksheet from the product manual. The configuration worksheet is available in the Clustered Data ONTAP 8.3 Software Setup Guide at the NetApp Support site.

Note: This system will be set up in a two-node switchless cluster configuration.

Table 7) Clustered Data ONTAP software installation prerequisites.

Cluster Detail	Cluster Detail Value
Cluster node 01 IP address	<<var_node01_mgmt_ip>>
Cluster node 01 netmask	<<var_node01_mgmt_mask>>
Cluster node 01 gateway	<<var_node01_mgmt_gateway>>
Cluster node 02 IP address	<<var_node02_mgmt_ip>>
Cluster node 02 netmask	<<var_node02_mgmt_mask>>
Cluster node 02 gateway	<<var_node02_mgmt_gateway>>
Data ONTAP 8.3 URL	<<var_url_boot_software>>

Node 01

To configure node 01, complete the following steps:

1. Connect to the storage system console port. You should see a Loader-A prompt. If the storage system is in a reboot loop, press Ctrl-C to exit the autoboot loop when you see this message:

```
Starting AUTOBOOT press Ctrl-C to abort
```

2. Set boot monitor defaults.

```
Set-defaults
```

3. Allow the system to boot up.

```
autoboot
```

4. Press Ctrl-C when prompted.

Note: If Data ONTAP 8.3 is not the version of software being booted, continue with the following steps to install new software. If Data ONTAP 8.3 is the version being booted, select option 8 and `yes` to reboot the node and go to step 14.

5. To install new software, first select option 7.

```
7
```

6. Answer `yes` to perform an upgrade.

```
y
```

7. Select e0M for the network port you want to use for the download.

```
e0M
```

8. Select yes to reboot now.

```
y
```

9. After reboot, enter the IP address, netmask, and default gateway for e0M in their respective places.

```
<<var_node01_mgmt_ip>> <<var_node01_mgmt_mask>> <<var_node01_mgmt_gateway>>
```

10. Enter the URL where the software can be found.

Note: This web server must be pingable.

```
<<var_url_boot_software>>
```

11. Press Enter for the user name, indicating no user name.

```
Enter
```

12. Enter yes to set the newly installed software as the default to be used for subsequent reboots.

```
y
```

13. Enter yes to reboot the node.

```
y
```

Note: When installing new software, the system might perform firmware upgrades to the BIOS and adapter cards, causing reboots and possible stops at the Loader-A prompt. If these actions occur, the system might deviate from this procedure.

14. When you see `Press Ctrl-C` for the boot menu:

```
Ctrl - C
```

15. Select option 5 to enter into maintenance mode.

```
5
```

16. Remove the disk ownership. Enter Y to remove the disk ownership and offline the existing volumes or aggregates.

```
disk remove_ownership

All disks owned by system ID 536902178 will have their ownership information removed.
Do you wish to continue? y

Volumes must be taken offline. Are all impacted volumes offline(y/n)?? y
Removing the ownership of aggregate disks may lead to partition of aggregates between high-
availability pair.

Do you want to continue(y/n)? y
```

17. Halt the node. The node will enter Loader prompt.

```
halt
```

18. Start Data ONTAP.

```
autoboot
```

19. Press `Ctrl-C` for the boot menu:

```
Ctrl - C
```

20. Select option 4 for clean configuration and initialize all disks.

```
4
```

21. Answer yes to `Zero disks, reset config and install a new file system.`

```
y
```

22. Enter yes to erase all the data on the disks.

```
y
```

Note: The initialization and creation of the root volume can take 90 minutes or more to complete, depending on the number of disks attached. After initialization is complete, the storage system reboots. You can continue to node 02 configuration while the disks for node 01 zero.

Node 02

To configure node 02, complete the following steps:

1. Connect to the storage system console port. You should see a Loader-A prompt. If the storage system is in a reboot loop, press Ctrl-C to exit the autoboot loop when you see this message:

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2. Set the boot monitor defaults.

```
set-defaults
```

3. Allow the system to boot up.

```
autoboot
```

4. Press Ctrl-C when prompted.

```
Ctrl-C
```

Note: If Data ONTAP 8.3 is not the version of software being booted, continue with the following steps to install new software. If Data ONTAP 8.3 is the version being booted, select option 8 and `yes` to reboot the node and go to step 14.

5. To install new software first, select option 7.

```
7
```

6. Answer yes to perform a nondisruptive upgrade.

```
y
```

7. Select e0M for the network port you want to use for the download.

```
e0M
```

8. Select yes to reboot now.

```
y
```

9. Enter the IP address, netmask, and default gateway for e0M in their respective places.

```
<<var_node02_mgmt_ip>> <<var_node02_mgmt_mask>> <<var_node02_mgmt_gateway>>
```

10. Enter the URL where the software can be found.

Note: This web server must be pingable.

```
<<var_url_boot_software>>
```

11. Press Enter for the user name, indicating no user name.

```
Enter
```

12. Select yes to set the newly installed software as the default to be used for subsequent reboots.

```
y
```

13. Select yes to reboot the node.

```
y
```

Note: When installing new software, the system might perform firmware upgrades to the BIOS and adapter cards, causing reboots and possible stops at the Loader-A prompt. If these actions occur, the system might deviate from this procedure.

14. Press Ctrl-C for the boot menu:

```
Ctrl - C
```

15. Select option 5 to enter maintenance mode.

```
5
```

16. Remove the disk ownership. Enter Y to do so and offline the existing volumes or aggregates.

```
disk remove_ownership

All disks owned by system ID 536902178 will have their ownership information removed. Do you wish
to continue? y

Volumes must be taken offline. Are all impacted volumes offline(y/n)?? y

Removing the ownership of aggregate disks may lead to partition of aggregates between high-
availability pair.

Do you want to continue(y/n)? y
```

17. Halt the node. The node will enter Loader prompt.

```
halt
```

18. Start Data ONTAP.

```
autoboot
```

19. Press `Ctrl-C` for the boot menu:

```
Ctrl – C
```

20. Select option 4 for clean configuration and initialize all disks.

```
4
```

21. Answer yes to `Zero disks, reset config and install a new file system.`

```
y
```

22. Enter yes to erase all the data on the disks.

```
y
```

Note: The initialization and creation of the root volume can take 90 minutes or more to complete, depending on the number of disks attached. When initialization is complete, the storage system reboots.

Node Setup in Clustered Data ONTAP

From a console port program attached to the Controller 01 (node 01) console port, execute the node setup script. This script comes up when Data ONTAP 8.3 first boots on a node.

1. Follow these prompts:

```
Welcome to node setup.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the setup wizard.
     Any changes you made before quitting will be saved.
```

```
To accept a default or omit a question, do not enter a value.


This system will send event messages and weekly reports to NetApp Technical
Support.
To disable this feature, enter "autosupport modify -support disable" within 24
hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/

Type yes to confirm and continue {yes}: yes

Enter the node management interface port [e0M]: Enter
Enter the node management interface IP address: <<var_node01_mgmt_ip>>
Enter the node management interface netmask: <<var_node01_mgmt_mask>>
Enter the node management interface default gateway: <<var_node01_mgmt_gateway>>
A node management interface on port e0M with IP address <<var_node01_mgmt_ip>> has been created.


This node has its management address assigned and is ready for cluster setup.

To complete cluster setup after all nodes are ready, download and run the System Setup utility
from the NetApp Support Site and use it to discover the configured nodes.

For System Setup, this node's management address is: <<var_node01_mgmt_ip>>.

Alternatively, you can use the "cluster setup" command to configure the cluster.
```

2. Press the Enter key and log in to the node with the admin user ID and no password to get a node command prompt.

```
::> storage failover modify -mode ha
Mode set to HA.  Reboot node to activate HA.

::> system node reboot

Warning: Are you sure you want to reboot node "localhost"? {y|n}: y
```

3. After reboot, go through the node setup procedure with preassigned values.

```
Welcome to node setup.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the setup wizard.
     Any changes you made before quitting will be saved.

To accept a default or omit a question, do not enter a value.



Enter the node management interface port [e0M]: Enter
Enter the node management interface IP address [<<var_node01_mgmt_ip>>]: Enter
Enter the node management interface netmask [<<var_node01_mgmt_mask>>]: Enter
Enter the node management interface default gateway [<<var_node01_mgmt_gateway>>]: Enter


This node has its management address assigned and is ready for cluster setup.

To complete cluster setup after all nodes are ready, download and run the System Setup utility
from the NetApp Support Site and use it to discover the configured nodes.

For System Setup, this node's management address is: <<var_node01_mgmt_ip>>.

Alternatively, you can use the "cluster setup" command to configure the cluster.
```

4. Log in to the node with the admin user and no password.

5. Repeat steps 1 through 4 for node 2 of the storage cluster.

Cluster Create in NetApp Clustered Data ONTAP

Table 8) Cluster create in clustered Data ONTAP prerequisites.

Cluster Detail	Cluster Detail Value
Cluster name	<<var_clustername>>
Clustered Data ONTAP base license	<<var_cluster_base_license_key>>
Cluster management IP address	<<var_clustermgmt_ip>>
Cluster management netmask	<<var_clustermgmt_mask>>
Cluster management port	<<var_clustermgmt_port>>
Cluster management gateway	<<var_clustermgmt_gateway>>
Cluster node01 IP address	<<var_node01_mgmt_ip>>
Cluster node01 netmask	<<var_node01_mgmt_mask>>
Cluster node01 gateway	<<var_node01_mgmt_gateway>>

The first node in the cluster performs the `cluster create` operation. All other nodes perform a `cluster join` operation. The first node in the cluster is considered node 01.

Using the console session to node 01, type `cluster setup` to bring up the Cluster Setup wizard.

```
cluster setup
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
"help" or "?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and
"exit" or "quit" - if you want to quit the cluster setup wizard.
Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
Do you want to create a new cluster or join an existing cluster? {create, join}:
```

Note: If a log in prompt appears instead of the Cluster Setup wizard, start the wizard by logging in using the factory default settings. Then enter the `cluster setup` command.

To create a new cluster, complete the following steps:

1. Run the following command to create a new cluster:

```
create
```

2. Type `no` for the single node cluster option.

```
Do you intend for this node to be used as a single node cluster? {yes, no} [no]: no
```

3. Type `no` for the cluster network using network switches.

```
Will the cluster network be configured to use network switches? [yes]:no
```

4. The system defaults are displayed. Enter `yes` to use the system defaults. Use the following prompts to configure the cluster ports.

```
Existing cluster interface configuration found:

Port    MTU     IP              Netmask
e0d     9000    169.254.128.103        255.255.0.0
```

```
e0f     9000    169.254.52.249 255.255.0.0

Do you want to use this configuration? {yes, no} [yes]:
```

5. The steps to create a cluster are displayed.

```
Enter the cluster administrators (username "admin") password: <<var_password>>
Retype the password: <<var_password>>
Enter the cluster name: <<var_clustername>>
Enter the cluster base license key: <<var_cluster_base_license_key>>
Creating cluster <<var_clustername>>
Enter an additional license key []:<<var_nfs_license>>
```

Note: The cluster is created. This can take a minute or two.

Note: For this validated architecture, NetApp recommends installing license keys for NetApp SnapRestore®, NetApp FlexClone®, and NetApp SnapManager® Suite technology. Additionally, install all required storage protocol licenses (NFS, iSCSI). After you finish entering the license keys, press Enter.

```
Enter the cluster management interface port [e0a]: e0a
Enter the cluster management interface IP address: <<var_clustermgmt_ip>>
Enter the cluster management interface netmask: <<var_clustermgmt_mask>>
Enter the cluster management interface default gateway: <<var_clustermgmt_gateway>>
```

6. Enter the DNS domain name.

```
Enter the DNS domain names:<<var_dns_domain_name>>
Enter the name server IP addresses:<<var_nameserver_ip>>
```

Note: If you have more than one name server IP address, separate the IP addresses with a comma.

7. Set up the node.

```
Where is the controller located []:<<var_node_location>>
Enter the node management interface port [e0M]: e0M
Enter the node management interface IP address [<<var_node01_mgmt_ip>>]: Enter
Enter the node management interface netmask [<<var_node01_mgmt_mask>>]: Enter
Enter the node management interface default gateway [<<var_node01_mgmt_gateway>>]: Enter
```

Note: The node management interface can be on the same subnet as the cluster management interface, or it can be on a different subnet.

Cluster Join in NetApp Clustered Data ONTAP

Table 9) Prerequisites for cluster join in clustered Data ONTAP.

Cluster Detail	Cluster Detail Value
Cluster name	<<var_clustername>>
Cluster management IP address	<<var_clustermgmt_ip>>
Cluster node02 IP address	<<var_node02_mgmt_ip>>
Cluster node02 netmask	<<var_node02_mgmt_mask>>
Cluster node02 gateway	<<var_node02_mgmt_gateway>>

The first node in the cluster performs the `cluster create` operation. All other nodes perform a `cluster join` operation. The first node in the cluster is considered node 01, and the node joining the cluster in this example is node 02.

To join the cluster, complete the following steps from the console session of node 02:

1. If prompted, enter `admin` in the login prompt.

```
admin
```

2. Type `cluster setup` to bring up the Cluster Setup wizard.

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
"help" or "?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and
"exit" or "quit" - if you want to quit the cluster setup wizard.
Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
Do you want to create a new cluster or join an existing cluster?
{create, join}:
```

Note: If a login prompt is displayed instead of the Cluster Setup wizard, start the wizard by logging in using the factory default settings. Then enter the `cluster setup` command.

3. Run the following command to join a cluster:

```
join
```

4. Data ONTAP detects the existing cluster and agrees to join the same cluster. Follow these prompts to join the cluster.

```
Existing cluster interface configuration found:

Port    MTU     IP              Netmask
e0d     9000    169.254.144.37  255.255.0.0
e0f     9000    169.254.134.33  255.255.0.0

Do you want to use this configuration? {yes, no} [yes]:
```

5. The steps to join a cluster appear.

```
Enter the name of the cluster you would like to join [<<var_clustername>>]:Enter
```

Note: The node should find the cluster name. The cluster joining can take a few minutes.

6. Set up the node.

```
Enter the node management interface port [e0M]: e0M
Enter the node management interface IP address [<<var_node02_mgmt_ip>>]: Enter
Enter the node management interface netmask [<<var_node02_netmask>>]: Enter
Enter the node management interface default gateway [<<var_node02_gw>>]: Enter
```

Note: The node management interface can be on the same subnet as the cluster management interface, or it can be on a different subnet.

Logging in to the Cluster

Open an SSH connection using the cluster IP or host name and log in as the admin user with the password provided during setup.

Zeroing All Spare Disks

To zero all spare disks in the cluster, complete the following step:

1. Run the following command:

```
disk zerospares
```

Setting on-Board UTA2 Ports Personality

1. Verify the “Current Mode” and “Current Type” of the ports by using the `ucadmin show` command.

```
icee1-stcl::> ucadmin show
                     Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------  -----------
icee1-stcl-01
              0c       cna      target     -        -          online
icee1-stcl-01
              0d       cna      target     -        -          online
icee1-stcl-01
              0e       cna      target     -        -          online
icee1-stcl-01
              0f       cna      target     -        -          online
icee1-stcl-02
              0c       cna      target     -        -          online
icee1-stcl-02
              0d       cna      target     -        -          online
icee1-stcl-02
              0e       cna      target     -        -          online
icee1-stcl-02
              0f       cna      target     -        -          online
8 entries were displayed.
```

2. Verify that the current mode of the ports that are in use is `cna` and that the current type is set to `target`. If this is not the case, change the port personality by using the following command:

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode cna -type target
```

Note: The ports must be offline to run the previous command.

Setting Auto-Revert on Cluster Management

1. To set the `auto-revert` parameter on the cluster management interface, enter:

```
network interface modify –vserver <<clustername>> -lif cluster_mgmt –auto-revert true
```

Set Up Management Broadcast Domain

To set up the Default broadcast domain for management network interfaces, complete the following step:

1. Run the following commands:

```
broadcast-domain remove-ports –broadcast-domain Default –ports <<controller01>>:e0b,
<<controller02>>:e0b
```

Enabling Cisco Discovery Protocol (CDP) in NetApp Clustered Data ONTAP

To enable CDP on the NetApp storage controllers, complete the following step:

Note: To be effective, CDP must also be enabled on directly connected networking equipment such as switches and routers.

1. Enable CDP on Data ONTAP.

```
node run -node * options cdpd.enable on
```

Setting Auto-Revert on Cluster Management

To set the `auto-revert` parameter on the cluster management interface, complete the following step:

1. Run the following command:

```
network interface modify –vserver <<var_clustername>> -lif cluster_mgmt –auto-revert true
```

Setting Up Service Processor Network Interface

To assign a static IPv4 address to the service processor on each node, complete the following step:

1. Run the following commands:

```
system service-processor network modify –node <<var_node01>> -address-family IPv4 –enable true –
dhcp none –ip-address <<var_node01_sp_ip>> -netmask <<var_node01_sp_mask>> -gateway
<<var_node01_sp_gateway>>

system service-processor network modify –node <<var_node02>> -address-family IPv4 –enable true –
dhcp none –ip-address <<var_node02_sp_ip>> -netmask <<var_node02_sp_mask>> -gateway
<<var_node02_sp_gateway>>
```

Note: The service processor IP addresses should be in the same subnet as the node management IP addresses.

Enabling Storage Failover in NetApp Clustered Data ONTAP

To confirm that storage failover is enabled, run the following commands in a failover pair:

1. Verify the status of storage failover.

```
storage failover show
```

Note: Both <<var_node01>> and <<var_node02>> must be capable of performing a takeover. Go to step 3 if the nodes are capable of performing a takeover.

2. Enable failover on one of the two nodes.

```
storage failover modify -node <<var_node01>> -enabled true
```

Note: Enabling failover on one node enables it for both nodes.

3. Verify the HA status of the two-node cluster.

Note: This step is not applicable for clusters with more than two nodes.

```
cluster ha show
```

4. Go to step 6 if high availability is configured.
5. Enable HA mode only for the two-node cluster.

Note: Do not run this command for clusters with more than two nodes because it will cause problems with failover.

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. Verify that hardware assist is correctly configured and, if needed, modify the partner IP address.

```
storage failover hwassist show
storage failover modify –hwassist-partner-ip <<var_node02_mgmt_ip>> -node <<var_node01>>
storage failover modify –hwassist-partner-ip <<var_node01_mgmt_ip>> -node <<var_node02>>
```

Creating Jumbo Frame MTU Broadcast Domain in NetApp Clustered Data ONTAP

To create a data broadcast domain with an MTU of 9000, complete the following step:

1. Create broadcast domain on Data ONTAP by running the following commands:

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

Removing Data Ports from Default Broadcast Domain

The 10GE data ports are used for iSCSI/NFS traffic and these ports should be removed from the Default domain. Also, port e0b is never used and should be removed from the Default domain as well. Complete the following steps:

```
broadcast-domain remove-ports -broadcast-domain Default -ports <<var_node01>>:e0c,
<<var_node01>>:e0d, <<var_node02>>:e0c, <<var_node02>>:e0d
```

Disabling Flow Control on UTA2 Ports

A NetApp best practice is to disable flow control on all the UTA2 ports that are connected to external devices.

To disable flow control, run the following command:

```
net port modify -node <<controller01>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<controller01>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<controller01>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<controller01>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<controller02>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<controller02>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<controller02>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<controller02>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second interruption in carrier.
Do you want to continue? {y|n}: y
```

Configuring IFGRP LACP in NetApp Clustered Data ONTAP

This type of interface group requires two or more Ethernet interfaces and a switch that supports LACP. Therefore, make sure that the switch is properly configured.

1. From the cluster prompt, complete the following steps.

```
ifgrp create -node <<var_node01>> -ifgrp a0a -distr-func port -mode multimode_lacp
network port ifgrp add-port -node <<var_node01>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_node01>> -ifgrp a0a -port e0d

ifgrp create -node << var_node02>> -ifgrp a0a -distr-func port -mode multimode_lacp
network port ifgrp add-port -node <<var_node02>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_node02>> -ifgrp a0a -port e0d
```

Configuring Jumbo Frames in NetApp Clustered Data ONTAP

1. To configure a clustered Data ONTAP network port to use jumbo frames (which usually have a maximum transmission unit [MTU] of 9,000 bytes), run the following command from the cluster shell:

```
nbice-fpe1::> network port modify -node <<var_node01>> -port a0a -mtu 9000

Warning: Changing the network port settings will cause a several second interruption in carrier.
Do you want to continue? {y|n}: y

nbice-fpe1::> network port modify -node <<var_node02>> -port a0a -mtu 9000

Warning: Changing the network port settings will cause a several second interruption in carrier.
Do you want to continue? {y|n}: y
```

Creating VLANs in NetApp Clustered Data ONTAP

1. Create NFS VLAN ports and add them to the Data Broadcast Domain.

```
network port vlan create –node <<var_node01>> -vlan-name a0a-<<var_nfs_vlan_id>>
network port vlan create –node <<var_node02>> -vlan-name a0a-<<var_nfs_vlan_id>>

broadcast-domain add-ports -broadcast-domain Infra_NFS -ports <<var_node01>>:a0a-
<<var_nfs_vlan_id>>, <<var_node02>>:a0a-<<var_nfs_vlan_id>>
```

2. Create iSCSI VLAN ports and add them to the Data Broadcast Domain.

```
network port vlan create –node <<var_node01>> -vlan-name a0a-<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_node01>> -vlan-name a0a-<<var_iscsi_vlan_B_id>>
network port vlan create –node <<var_node02>> -vlan-name a0a-<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_node02>> -vlan-name a0a-<<var_iscsi_vlan_B_id>>

broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports <<var_node01>>:a0a-
<<var_iscsi_vlan_A_id>>,<<var_node02>>:a0a-<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports <<var_node01>>:a0a-
<<var_iscsi_vlan_B_id>>,<<var_node02>>:a0a-<<var_iscsi_vlan_B_id>>
```

3. Create IB-MGMT-VLAN ports.

```
network port vlan create –node <<var_node01>> -vlan-name a0a-<<ib_mgmt_vlan_id>>
network port vlan create –node <<var_node02>> -vlan-name a0a-<<ib_mgmt_vlan_id>>
```

Creating Aggregates in NetApp Clustered Data ONTAP

An aggregate containing the root volume is created during the Data ONTAP setup process. To create additional aggregates, determine the aggregate name, the node on which to create it, and the number of disks it will contain.

To create new aggregates, complete the following steps:

1. Run the following commands:

```
aggr create -aggregate aggr1_node01 -node <<var_node01>> -diskcount <<var_num_disks>>
aggr create -aggregate aggr1_node02 -node <<var_node02>> -diskcount <<var_num_disks>>
```

Note: Retain at least one disk (select the largest disk) in the configuration as a spare. A best practice is to have at least one spare for each disk type and size.

Note: Start with five disks; you can add disks to an aggregate when additional storage is required.

Note: The aggregate cannot be created until disk zeroing completes. Run the `aggr show` command to display the aggregate creation status. Do not proceed until `aggr1_node1` is online.

2. Disable NetApp Snapshot® copies for the data aggregate recently created.

```
node run <<var_node01>> aggr options aggr1_node01 nosnap on
node run <<var_node02>> aggr options aggr1_node02 nosnap on
```

3. Delete any existing Snapshot copies for the two data aggregates.

```
node run <<var_node01>> snap delete –A –a –f aggr1_node01
node run <<var_node02>> snap delete –A –a –f aggr1_node02
```

4. Rename the root aggregate on node 01 to match the naming convention for this aggregate on node 02.

```
aggr show
aggr rename –aggregate aggr0 –newname <<var_node01_rootaggrname>>
```

Configuring NTP in NetApp Clustered Data ONTAP

To configure time synchronization on the cluster, complete the following steps:

1. To set the time zone for the cluster, run the following command:

```
timezone <<var_timezone>>
```

Note: For example, in the eastern United States, the time zone is America/New_York.

2. To set the date for the cluster, run the following command:

```
date <ccyymmddhhmm.ss>
```

Note: The format for the date is <[Century][Year][Month][Day][Hour][Minute].[Second]>; for example, 201505181453.17.

3. Configure the Network Time Protocol (NTP) server(s) for the cluster.

```
cluster time-service ntp server create -server <<var_global_ntp_server_ip>>
```

Configuring SNMP in NetApp Clustered Data ONTAP

To configure SNMP, complete the following steps:

1. Configure SNMP basic information, such as the location and contact. When polled, this information is visible as the `sysLocation` and `sysContact` variables in SNMP.

```
snmp contact <<var_snmp_contact>>
snmp location "<<var_snmp_location>>"
snmp init 1
options snmp.enable on
```

2. Configure SNMP traps to send to remote hosts, such as a DFM server or another fault management system.

```
snmp traphost add <<var_oncommand_server_fqdn>>
```

Configuring SNMPv1 in NetApp Clustered Data ONTAP

To configure SNMPv1, complete the following step:

1. Set the shared secret plain-text password, which is called a community.

```
snmp community add ro <<var_snmp_community>>
```

Note: Use the `snmp community delete all` command with caution. If community strings are used for other monitoring products, this command will remove them.

Configuring SNMPv3 in NetApp Clustered Data ONTAP

SNMPv3 requires that a user be defined and configured for authentication. To configure SNMPv3, complete the following steps:

1. Run the `security snmpusers` command to view the engine ID.
2. Create a user called `snmpv3user`.

```
security login create -username snmpv3user -authmethod usm -application snmp
```

3. Enter the authoritative entity's engine ID and select `md5` as the authentication protocol.
4. Enter an eight-character minimum-length password for the authentication protocol when prompted.
5. Select `des` as the privacy protocol.
6. Enter an eight-character minimum-length password for the privacy protocol when prompted.

Configuring AutoSupport HTTPS in NetApp Clustered Data ONTAP

The NetApp AutoSupport™ tool sends support summary information to NetApp through HTTPS. To configure AutoSupport, complete the following step:

1. Run the following command:

```
system node autosupport modify -node * -state enable –mail-hosts <<var_mailhost>> -transport
https -support enable -noteto <<var_storage_admin_email>>
```

Creating Storage Virtual Machine (Vserver)

To create an infrastructure Vserver, complete the following steps:

1. Run the `vserver create` command.

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate aggr1_node01 –rootvolume-
security-style unix
```

2. Add the data aggregate to the Infra_Vserver aggregate list for the NetApp Virtual Storage Console.

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_node01, aggr1_node02
```

3. Select the Vserver data protocols to configure, leaving NFS and iSCSI.

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. Enable and run the NFS protocol in the Infra-SVM Vserver.

```
nfs create -vserver Infra-SVM -udp disabled
```

5. Turn on the SVM vstorage parameter for the NetApp NFS VAAI plug-in.

```
vserver nfs modify –vserver Infra-SVM –vstorage enabled
vserver nfs show
```

Creating Load Sharing Mirror of Vserver Root Volume in NetApp Clustered Data ONTAP

1. Create a volume to be the load sharing mirror of the infrastructure Vserver root volume on each node.

```
volume create –vserver Infra_Vserver –volume rootvol_m01 –aggregate aggr1_node01 –size 1GB –type
DP
volume create –vserver Infra_Vserver –volume rootvol_m02 –aggregate aggr1_node02 –size 1GB –type
DP
```

2. Create a job schedule to update the root volume mirror relationships every 15 minutes.

```
job schedule interval create -name 15min -minutes 15
```

3. Create the mirroring relationships.

```
snapmirror create –source-path //Infra_Vserver/rootvol –destination-path
//Infra_Vserver/rootvol_m01 –type LS -schedule 15min

snapmirror create –source-path //Infra_Vserver/rootvol –destination-path
//Infra_Vserver/rootvol_m02 –type LS -schedule 15min
```

4. Initialize the mirroring relationship.

```
snapmirror initialize-ls-set –source-path //Infra_Vserver/rootvol
```

Creating iSCSI Service in NetApp Clustered Data ONTAP

To create the iSCSI service, complete the following step:

1. Create the iSCSI service on each Vserver. This command also starts the iSCSI service and sets the iSCSI IQN for the Vserver.

```
iscsi create -vserver Infra-SVM
iscsi show
```

Configuring HTTPS Access in NetApp Clustered Data ONTAP

To configure secure access to the storage controller, complete the following steps:

1. Increase the privilege level to access the certificate commands.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. Generally, a self-signed certificate is already in place. Verify the certificate by running the following command:

```
security certificate show
```

3. For each Vserver shown, the certificate common name should match the DNS FQDN of the Vserver. The four default certificates should be deleted and replaced by either self-signed certificates or certificates from a Certificate Authority. To delete the default certificates, run the following commands.

Note: Deleting expired certificates before creating new certificates is a best practice. Run the `security certificate delete` command to delete expired certificates. In the following command, use TAB completion to select and delete each default certificate.

```
security certificate delete [TAB] …
Example: security certificate delete -vserver Infra-SVM -common-name Infra-SVM -ca Infra-SVM -
type server -serial 552429A6
```

4. To generate and install self-signed certificates, run the following commands as one-time commands. Generate a server certificate for Infra-SVM and the cluster Vserver. Again, use TAB completion to aid in completing these commands.

```
security certificate create [TAB] …
Example: security certificate create -common-name infra-svm.ciscorobo.com -type  server -size
2048 -country US -state "California" -locality "San Jose" -organization "Cisco" -unit "UCS" -
email-addr "abc@cisco.com" -expire-days 365 -protocol SSL -hash-function SHA256 -vserver Infra-
SVM
```

5. To obtain the values for the parameters that would be required in the following step, run the `security certificate show` command.
6. Enable each certificate that was just created using the `–server-enabled true` and `–client-enabled false` parameters. Again, use TAB completion.

```
security ssl modify [TAB] …
Example: security ssl modify -vserver clus -server-enabled true -client-enabled false -ca
clus.ciscorobo.com -serial 55243646 -common-name clus.ciscorobo.com
```

7. Configure and enable SSL and HTTPS access and disable HTTP access.

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web service requests to be
         interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http –vserver <<var_clustername>>
```

Note: It is normal for some of these commands to return an error message stating that the entry does not exist.

8. Revert to the admin privilege level and create the setup to allow Vserver logs to be available by the web.

```
set –privilege admin
vserver services web modify –name spi|ontapi|compat –vserver * -enabled true
```

Configuring NFSv3 in NetApp Clustered Data ONTAP

To configure NFS on the Vserver, run all of these commands.

1. Create a new rule for each ESXi host in the default export policy.

   For each ESXi host being created, assign a rule. Each host will have its own rule index. Your first ESXi host will have rule index 1, your second ESXi host will have rule index 2, and so on.

```
vserver export-policy rule create –vserver Infra-SVM -policyname default –ruleindex 1 –protocol
nfs -clientmatch <<var_esxi_host1_nfs_ip>> -rorule sys –rwrule sys -superuser sys –allow-suid
false
vserver export-policy rule create –vserver Infra-SVM -policyname default –ruleindex 2 –protocol
nfs -clientmatch <<var_esxi_host2_nfs_ip>> -rorule sys –rwrule sys -superuser sys –allow-suid
false
vserver export-policy rule show
```

2. Assign the NetApp FlexPod® export policy to the infrastructure Vserver root volume.

```
volume modify –vserver Infra-SVM –volume rootvol –policy default
```

Creating FlexVol in NetApp Clustered Data ONTAP

To create a NetApp FlexVol® volume, complete the following step:

1. The following information is required to create a FlexVol volume: the volume's name, size, and the aggregate on which it will exist. Create two VMware datastore volumes and a server boot volume.

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate aggr1_node01 -size 500GB -
state online -policy default -junction-path /infra_datastore_1 -space-guarantee none -percent-
snapshot-space 0

volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_node01 -size 100GB -state
online -policy default -junction-path /infra_swap -space-guarantee none -percent-snapshot-space 0
-snapshot-policy none

volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_node01 -size 100GB -state
online -policy default -space-guarantee none -percent-snapshot-space 0
```

Creating LUNs in NetApp Clustered Data ONTAP

To create LUNs, complete the following step:

1. Create two boot LUNs.

```
lun create -vserver Infra-SVM –volume esxi_boot -lun VM-Host-Infra-01 -size 15GB -ostype vmware -
space-reserve disabled
lun create -vserver Infra-SVM –volume esxi_boot -lun VM-Host-Infra-02 -size 15GB -ostype vmware -
space-reserve disabled
lun create -vserver Infra-SVM –volume esxi_boot -lun VM-Host-Infra-03 -size 15GB -ostype vmware -
space-reserve disabled
lun create -vserver Infra-SVM –volume esxi_boot -lun VM-Host-Infra-04 -size 15GB -ostype vmware –
space-reserve disabled
```

Enabling Deduplication in NetApp Clustered Data ONTAP

To enable deduplication on appropriate volumes, complete the following step:

1. Run the following commands:

```
volume efficiency on –vserver Infra-SVM –volume infra_datastore_1
volume efficiency on –vserver Infra-SVM –volume esxi_boot
```

Creating iSCSI LIFs in NetApp Clustered Data ONTAP

To create iSCSI LIFs, complete the following step:

1. Create four iSCSI LIFs, two on each node.

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data -data-protocol iscsi -
home-node <<var_node01>> -home-port a0a-<<var_iscsi_vlan_A_id>> -address
<<var_node01_iscsi_lif01a_ip>> -netmask <<var_node01_iscsi_lif01a_mask>> –status-admin up –
failover-policy disabled –firewall-policy data –auto-revert false

network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data -data-protocol iscsi -
home-node <<var_node01>> -home-port a0a-<<var_iscsi_vlan_B_id>> -address
<<var_node01_iscsi_lif01b_ip>> -netmask <<var_node01_iscsi_lif01b_mask>> –status-admin up –
failover-policy disabled –firewall-policy data –auto-revert false

network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data -data-protocol iscsi -
home-node <<var_node02>> -home-port a0a-<<var_iscsi_vlan_A_id>> -address
<<var_node02_iscsi_lif01a_ip>> -netmask <<var_node02_iscsi_lif01a_mask>> –status-admin up –
failover-policy disabled –firewall-policy data –auto-revert false

network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data -data-protocol iscsi -
home-node <<var_node02>> -home-port a0a-<<var_iscsi_vlan_B_id>> -address
<<var_node02_iscsi_lif01b_ip>> -netmask <<var_node02_iscsi_lif01b_mask>> –status-admin up –
failover-policy disabled –firewall-policy data –auto-revert false

network interface show
```

Creating NFS LIFs in NetApp Clustered Data ONTAP

To create NFS LIFs, complete the following step:

1. Create an NFS logical interface (LIF).

```
network interface create -vserver Infra-SVM -lif nfs_infra_swap -role data -data-protocol nfs -
home-node <<var_node01>> -home-port a0a-<<var_nfs_vlan_id>> –address
<<var_node01_nfs_lif_infra_swap_ip>> -netmask <<var_node01_nfs_lif_infra_swap_mask>> -status-
admin up –failover-policy broadcast-domain-wide –firewall-policy data –auto-revert true

network interface create -vserver Infra-SVM -lif nfs_infra_datastore_1 -role data -data-protocol
nfs -home-node <<var_node01>> -home-port a0a-<<var_nfs_vlan_id>> -address
<<var_node01_nfs_lif_infra_datastore_1_ip>> -netmask
<<var_node01_nfs_lif_infra_datastore_1_mask>> -status-admin up –failover-policy broadcast-domain-
wide –firewall-policy data –auto-revert true

network interface show
```

Note: NetApp recommends creating a new LIF for each datastore.

Adding the Infrastructure Vserver Administrator

To add the infrastructure Vserver administrator and Vserver administration logical interface in the out-of-band management network, complete the following step:

1. Run the following commands:

```
network interface create –vserver Infra-SVM –lif vsmgmt –role data –data-protocol none –home-node
<<var_node02>> -home-port  e0a –address <<var_vserver_mgmt_ip>> -netmask
<<var_vserver_mgmt_mask>> -status-admin up –failover-policy broadcast-domain-wide –firewall-
policy mgmt –auto-revert true
```

Note: The Vserver management IP here should be in the same subnet as the storage cluster management IP.

2. Create a default route to allow the Vserver management interface to reach the outside world.

```
network route create –vserver Infra-SVM -destination 0.0.0.0/0 –gateway
<<var_vserver_mgmt_gateway>>

network route show
```

3. Set a password for the Vserver vsadmin user and unlock the user.

```
security login password –username vsadmin –vserver Infra-SVM
Enter a new password:  <<var_password>>
Enter it again:  <<var_password>>

security login unlock –username vsadmin –vserver Infra-SVM
```

5.3 Cisco UCS C-Series Rack Server Deployment Procedure

The following section provides a detailed procedure for configuring a Cisco UCS C-Series standalone rack server for use in the large FlexPod Express configuration.

Performing Initial Cisco UCS C-Series Standalone Server Setup for Cisco IMC

These steps provide details for the initial setup of the Cisco IMC interface for Cisco UCS C-Series standalone servers.

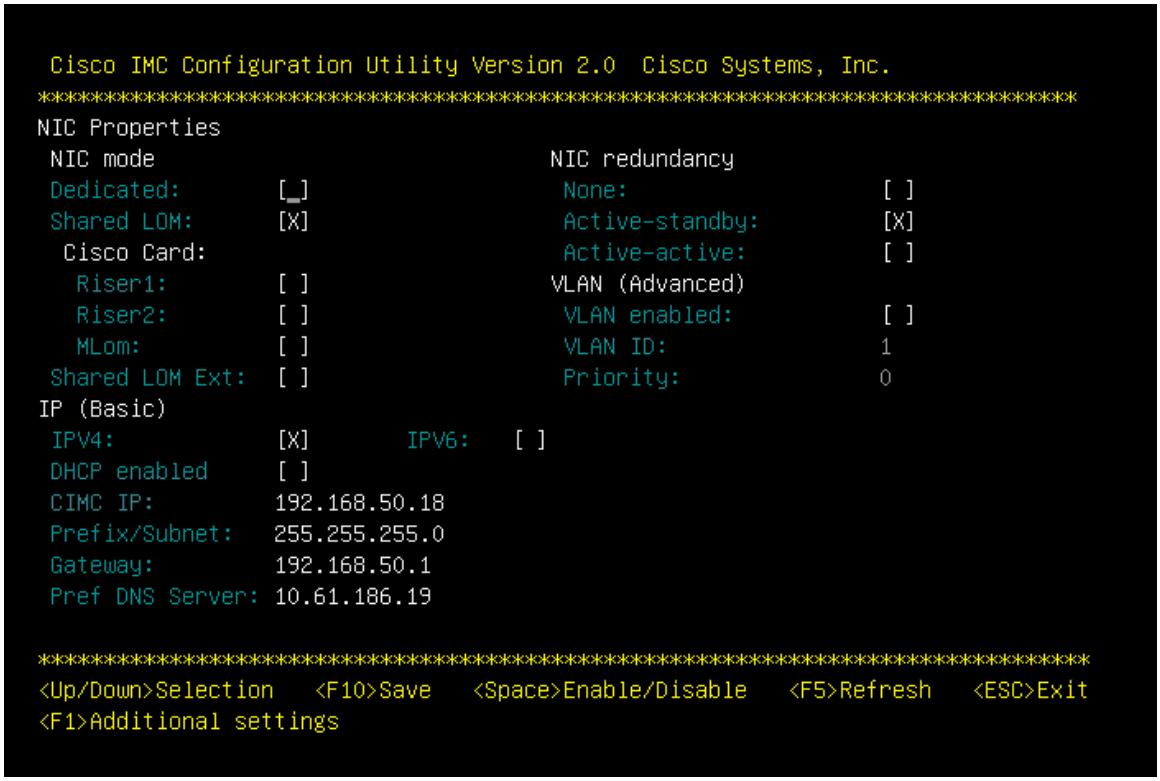
All Servers

1. Attach the Cisco keyboard, video, and mouse (KVM) dongle (provided with the server) to the KVM 1.port on the front of the server. Plug a VGA monitor and USB keyboard into the appropriate KVM dongle ports.
2. Power on the server and press F8 when prompted to enter the Cisco IMC configuration.

3. In the Cisco IMC configuration utility, set the following options:

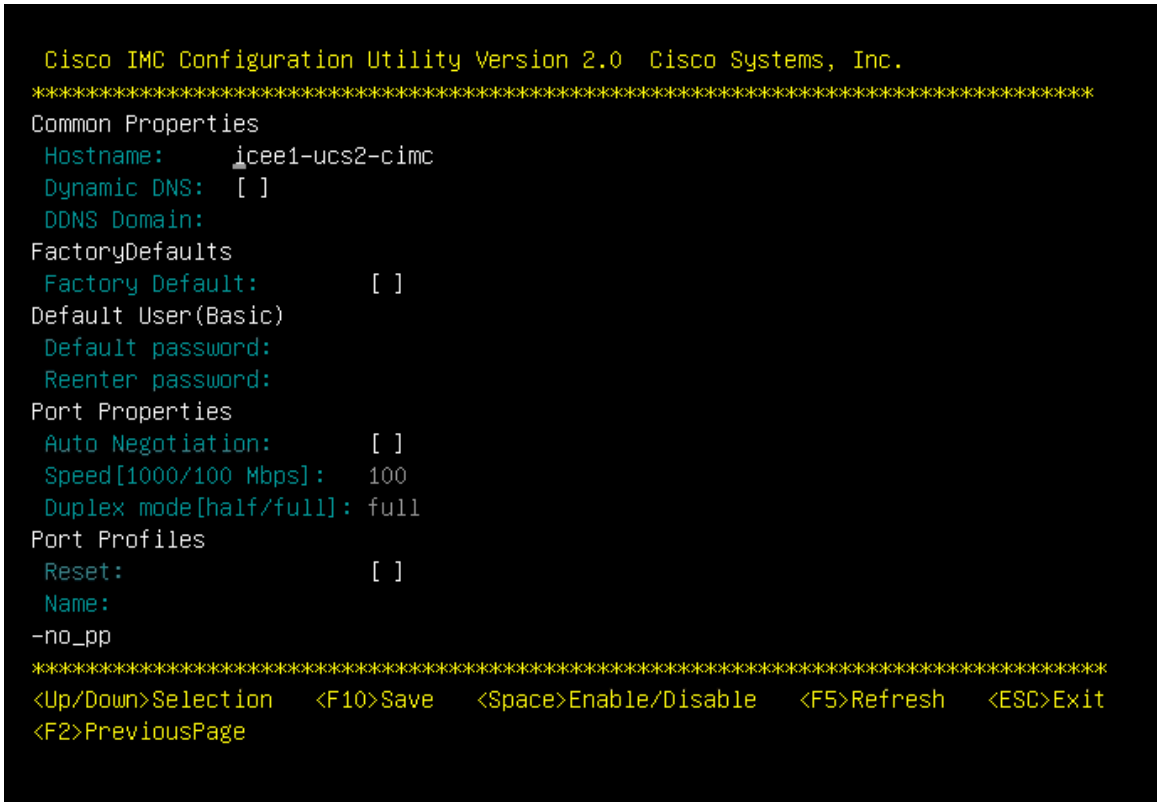
- Network Interface Card (NIC) Mode:
  - Dedicated [X]
- IP (Basic):
  - IPV4: [X]
  - DHCP enabled: [ ]
  - CIMC IP:<<cimc_ip>>
  - Prefix/Subnet:<<cimc_netmask>>
  - Gateway: <<cimc_gateway>>

- VLAN (Advanced): Leave cleared to disable VLAN tagging.
  - NIC Redundancy
  - None: [X]



4. Press F1 to see additional settings.

- Common Properties:
  - Host name: <<esxi_host_name>>
  - Dynamic DNS: [ ]
  - Factory Defaults: Leave cleared.
- Default User (Basic):
  - Default password: <<admin_password>>
  - Reenter password: <<admin_password>>
  - Port Properties: Use default values.
  - Port Profiles: Leave cleared.



5. Press F10 to save the Cisco IMC interface configuration.
6. After the configuration is saved, press Esc to exit.

Note: Upgrade the Cisco C-Series rack-mount server software to the latest version. This document uses version 2.0(3j).

Configuring Cisco UCS C-Series Servers iSCSI Boot

In this document, VIC1227 is used for iSCSI boot.

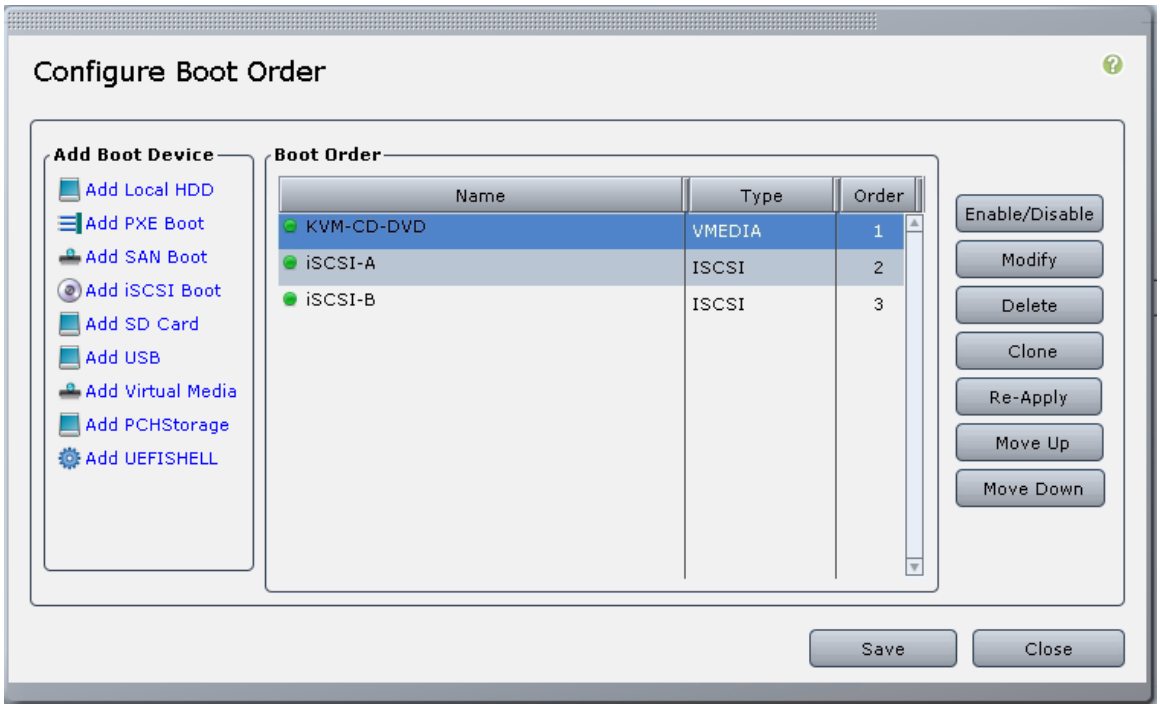
Boot Order Configuration

1. From the Cisco IMC interface browser window (do not close the virtual KVM window), click the Server tab and choose BIOS.
2. Choose Configure Boot Order and click OK.
3. In the Boot Order section, remove all the entries and configure the following:

- Add Virtual Media
  - Name: KVM-CD-DVD
  - Sub Type: KVM MAPPED DVD
  - State: Enabled
- Add iSCSI Boot
  - Name: iSCSI-A
  - State: Enabled
  - Order: 2
  - Slot: MLOM

- Port: 0

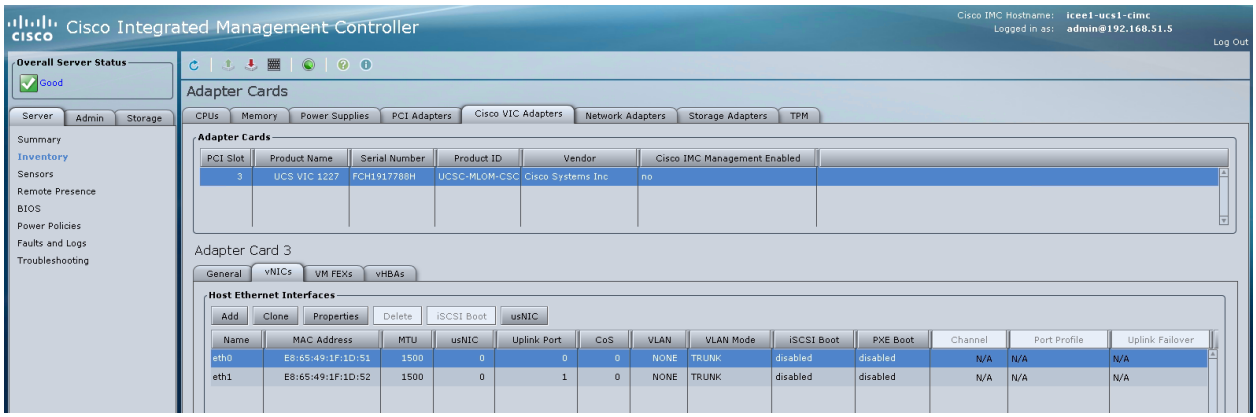
4. Click Add Device.
   - Name: iSCSI-B
   - State: Enabled
   - Order: 3
   - Slot: MLOM
   - Port: 1
5. Click Add Device.
6. Click Save. Click Close.
7. Click Save Changes.



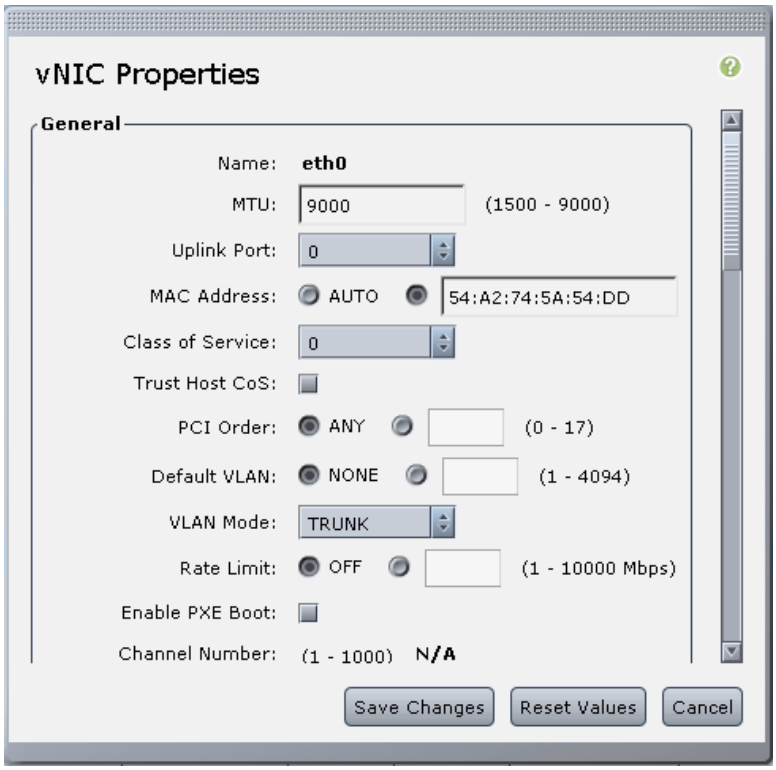
Configuring Cisco VIC1227 for iSCSI Boot

These steps provide details for configuring the Cisco VIC1227 for iSCSI boot.

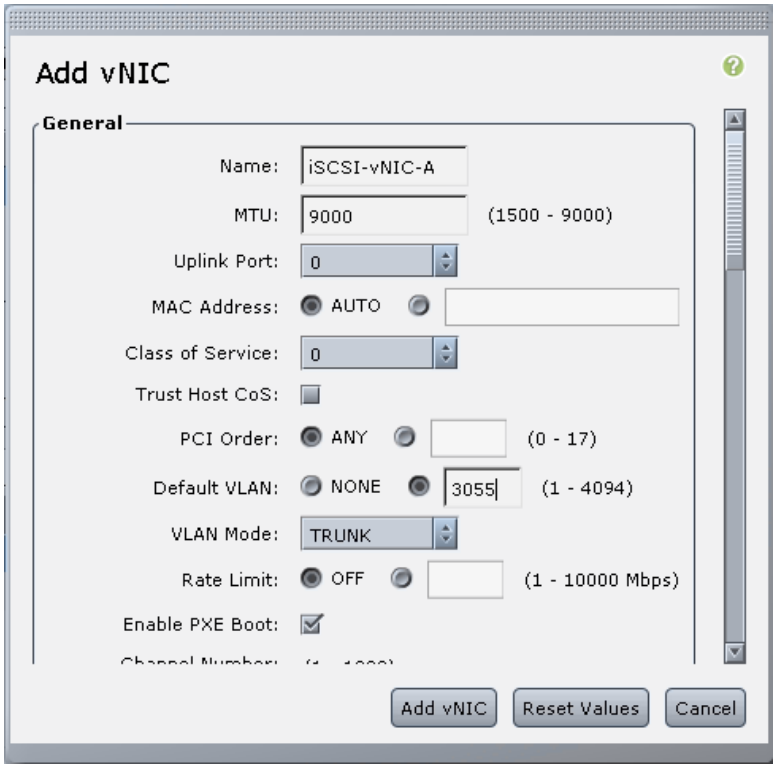
1. From the Cisco IMC interface browser window, click Inventory.
2. On the right pane, click Cisco VIC Adapters.
3. From the Adapter Cards section, select UCS VIC 1227.
4. From the Host Ethernet Interfaces section, select the vNICs tab.



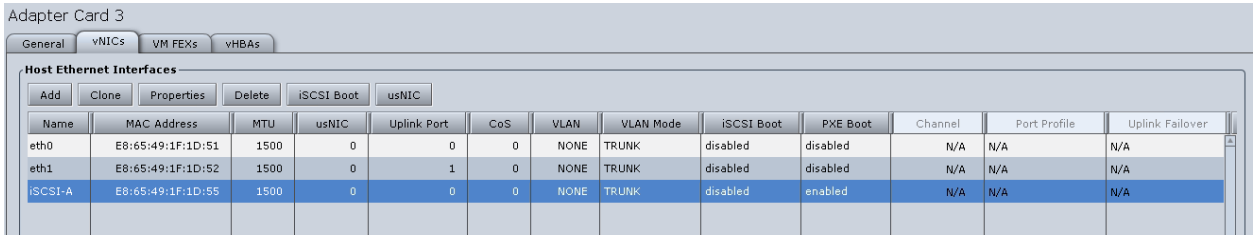
5. Select eth0 and click Properties.
6. Set the MTU to 9000.



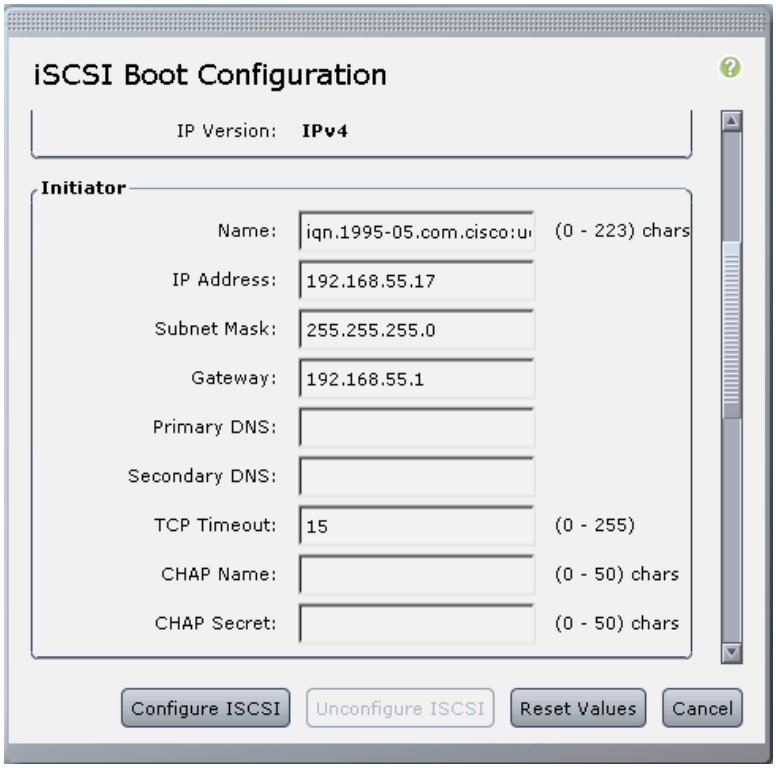
7. Repeat steps 5 and 6 for eth1.
8. Click Add to create a new vNIC.
9. In the Add vNIC window, complete the following settings:
   - Name: iSCSI-vNIC-A
   - MTU: 9000
   - Default VLAN: <<var_iscsi_vlan_a>>
   - VLAN Mode: TRUNK
   - Enable PXE Boot: check



10. Click Add vNIC. Click OK.
11. Select the newly created vNIC "`iSCSI-vNIC-A`" and click the iSCSI Boot button located on the top of the Host Ethernet Interfaces section.

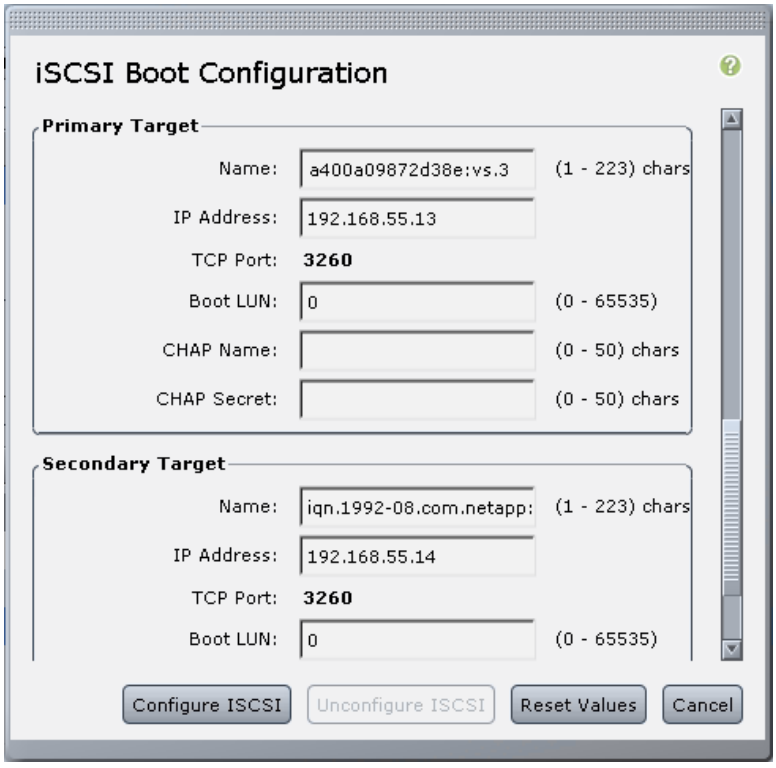


12. From the iSCSI Boot Configuration window, enter the Initiator details, as shown below.

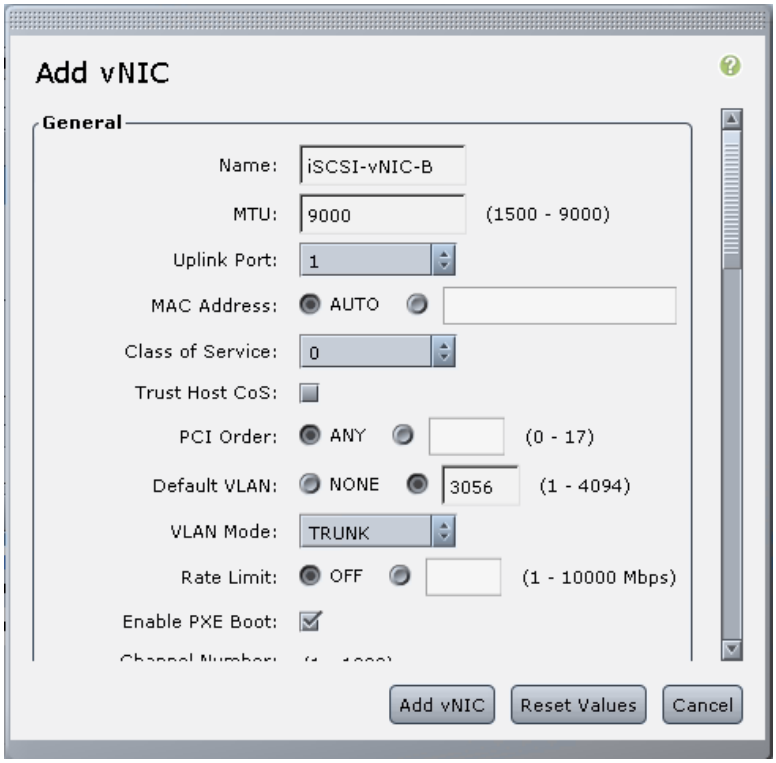


13. Enter the primary target details.
    - Name: IQN number of Infra-SVM.
    - IP Address: IP address of iscsi_lif01a
    - Boot LUN: 0
14. Enter the secondary target details.
    - Name: IQN number of Infra-SVM.
    - IP Address: IP address of iscsi_lif02a
    - Boot LUN: 0

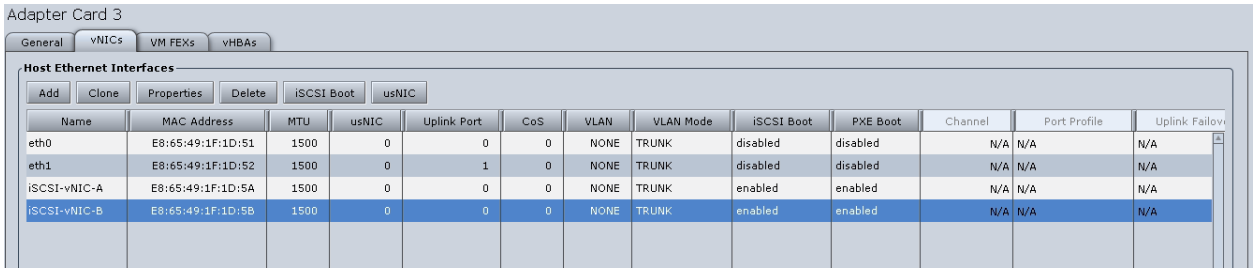
    Note: You can obtain the storage IQN number by using the `vserver iscsi show` command.



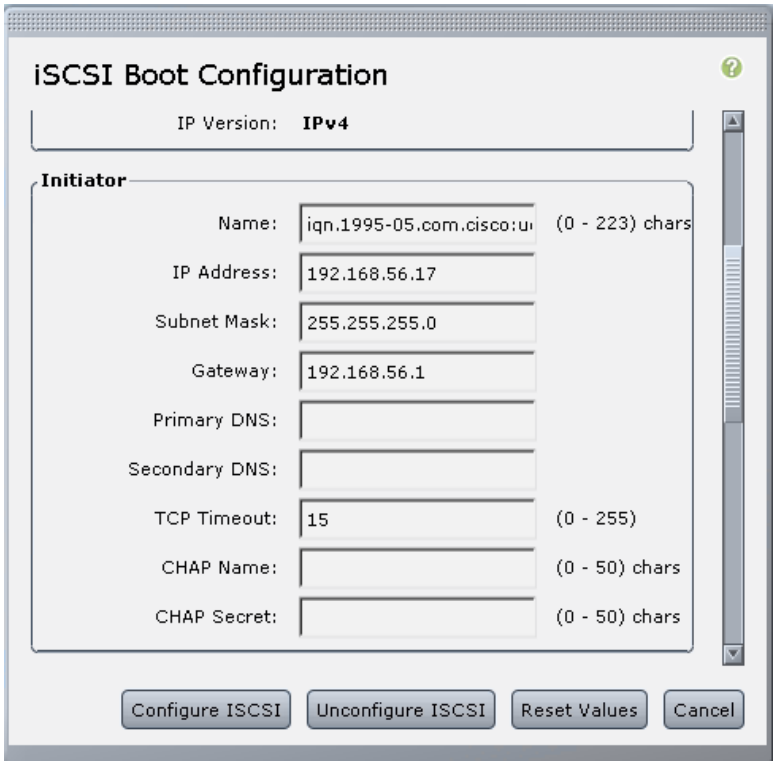
15. Click Configure ISCSI.
16. In the Host Ethernet Interfaces section, click Add to create a new vNIC.
17. In the Add vNIC window, complete the following settings:
    - Name: iSCSI-vNIC-B
    - MTU: 9000
    - Uplink Port: 1
    - Default VLAN: `<<var_iscsi_vlan_b>>`
    - VLAN Mode: TRUNK
    - Enable PXE Boot: check



18. Click OK.
19. Select the newly created vNIC "`iSCSI-vNIC-B`" and click the iSCSI Boot button located on the top of the Host Ethernet Interfaces section.

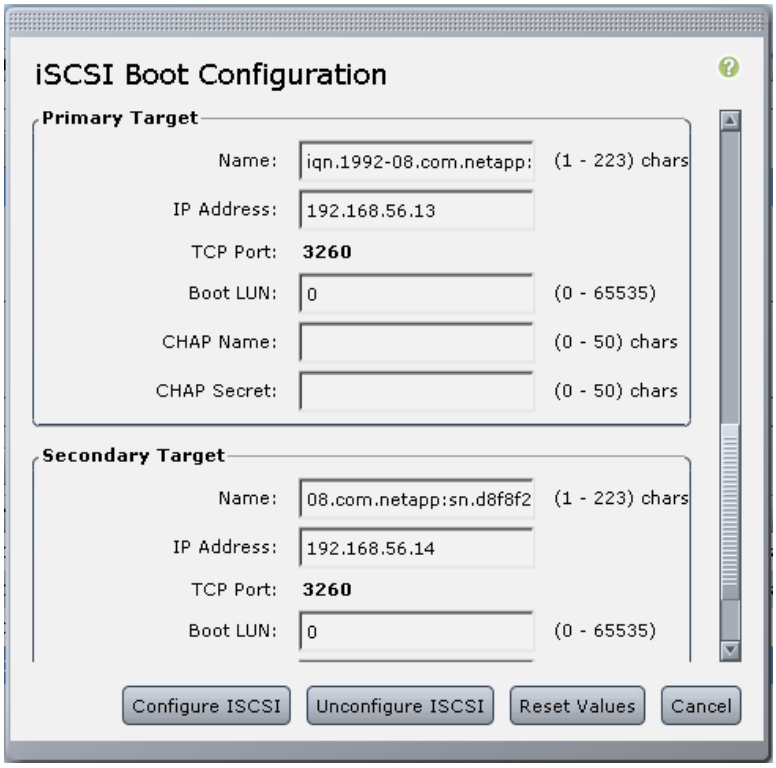


20. From the iSCSI Boot Configuration window, enter the Initiator details, as shown below.



21. Enter the primary target details.
    - Name: IQN number of Infra-SVM.
    - IP Address: IP address of iscsi_lif01b
    - Boot LUN: 0
22. Enter the secondary target details.
    - Name: IQN number of Infra-SVM.
    - IP Address: IP address of iscsi_lif02b
    - Boot LUN: 0

    Note: You can obtain the storage IQN number by using the `vserver iscsi show` command.



23. Click Configure ISCSI.

5.4 NetApp FAS Storage Deployment Procedure (Part 2)

NetApp Clustered Data ONTAP SAN Boot Storage Setup

Creating iSCSI Igroups

To create igroups, complete the following step.

Note: Get the initiator iSCSI IQNs from the server configuration.

1. From the cluster management node SSH connection, run the following commands:

```
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-01 –protocol iscsi –ostype vmware –
initiator <<var_vm_host_infra_01_iSCSI-A_vNIC_IQN>>, <<var_vm_host_infra_01_iSCSI-B_vNIC_IQN>>
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-02 –protocol iscsi –ostype vmware –
initiator <<var_vm_host_infra_02_iSCSI-A_vNIC_IQN>>, <<var_vm_host_infra_02_iSCSI-B_vNIC_IQN>>
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-03 –protocol iscsi –ostype vmware –
initiator <<var_vm_host_infra_03_iSCSI-A_vNIC_IQN>>, <<var_vm_host_infra_03_iSCSI-B_vNIC_IQN>>
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-04 –protocol iscsi –ostype vmware –
initiator <<var_vm_host_infra_04_iSCSI-A_vNIC_IQN>>, <<var_vm_host_infra_04_iSCSI-B_vNIC_IQN>>
igroup create –vserver Infra-SVM –igroup MGMT-Hosts –protocol iscsi –ostype vmware –initiator
<<var_vm_host_infra_01_iSCSI-A_vNIC_IQN>>, <<var_vm_host_infra_01_iSCSI-B_vNIC_IQN>>,
<<var_vm_host_infra_02_iSCSI-A_vNIC_IQN>>, <<var_vm_host_infra_02_iSCSI-B_vNIC_IQN>>,
<<var_vm_host_infra_03_iSCSI-A_vNIC_IQN>>, <<var_vm_host_infra_03_iSCSI-B_vNIC_IQN>>,
<<var_vm_host_infra_04_iSCSI-A_vNIC_IQN>>, <<var_vm_host_infra_04_iSCSI-B_vNIC_IQN>>
```

Note: To view the three igroups created in this step, run the `igroup show` command.

Mapping Boot LUNs to Igroups

To map boot LUNs to igroups, complete the following step:

1. From the cluster management SSH connection, run the following commands:

```
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra-01 –igroup VM-Host-Infra-01 –lun-
id 0
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra-02 –igroup VM-Host-Infra-02 –lun-
id 0
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra-03 –igroup VM-Host-Infra-03 –lun-
id 0
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra-04 –igroup VM-Host-Infra-04 –lun-
id 0
```

5.5 VMware vSphere 6.0 Deployment Procedure

This section provides detailed procedures for installing VMware ESXi 6.0 in a FlexPod Express configuration. The deployment procedures that follow are customized to include the environment variables described in previous sections.

Multiple methods exist for installing VMware ESXi in such an environment. This procedure uses the virtual KVM console and virtual media features of the Cisco IMC interface for Cisco UCS C-Series servers to map remote installation media to each individual server.

Logging in to Cisco IMC Interface for Cisco UCS C-Series Standalone Servers

The following steps detail the method for logging in to the Cisco IMC interface for Cisco UCS C-Series standalone servers. You must log in to the Cisco IMC interface to run the virtual KVM, which enables the administrator to begin installation of the operating system through remote media.

All Hosts

1. Navigate to a web browser and enter the IP address for the Cisco IMC interface for the Cisco UCS C-Series. This step launches the Cisco IMC GUI application.
2. Log in to the Cisco IMC GUI using the admin user name and credentials.
3. In the main menu, select the Server tab.
4. Click Launch KVM Console.
5. From the virtual KVM console, select the Virtual Media tab.
6. Select Map CD/DVD.
7. Browse to the VMware ESXi 6.0 installer ISO image file and click Open. Click Map Device.
8. Select the Power menu and choose Power Cycle System (cold boot). Click Yes.

Installing VMware ESXi

The following steps describe how to install VMware ESXi on each host.

All Hosts

1. When the system boots, the machine detects the presence of the VMware ESXi installation media.
2. Select the VMware ESXi installer from the menu that appears.
3. After the installer is finished loading, press Enter to continue with the installation.
4. After reading the end-user license agreement, accept it and continue with the installation by pressing F11.
5. Select the NetApp LUN that was previously set up as the installation disk for ESXi and press Enter to continue with the installation.
6. Select the appropriate keyboard layout and press Enter to continue.
7. Enter and confirm the root password and press Enter to continue.
8. The installer will warn you that existing partitions will be removed on the volume. Continue with the installation by pressing F11.

9. After the installation is complete, unmap the VMware ESXi installation image on the Virtual Media tab of the KVM console so that the server reboots into VMware ESXi and not the installer.
10. The Virtual Media window might warn you that it is preferable to eject the media from the guest. Because you cannot do this in this example (and the media is read-only), unmap the image anyway by selecting Yes.

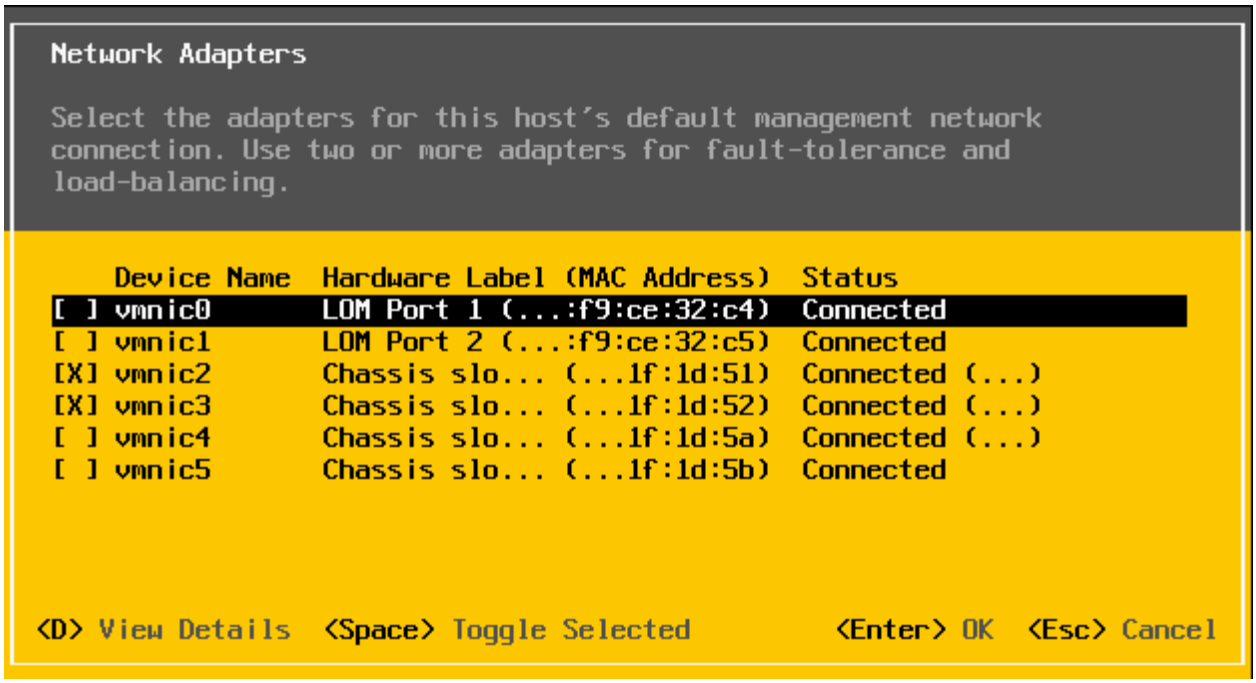
Setting Up VMware ESXi Host Management Networking

The following steps describe how to add the management network for each VMware ESXi host.

All Hosts

1. After the server has finished rebooting, enter the option to customize the system by pressing F2.
2. Log in with root as the login name and the root password previously entered during the installation process.
3. Select the Configure Management Network option.
4. Select Network Adapters and press Enter.
5. Select the desired ports for vSwitch0. Press Enter.

   Note: The VIC ports eth0 and eth1 are selected because LOM ports are configured for CIMC management.



6. Select VLAN (optional) and press Enter.
7. Enter the VLAN ID: `<<ib_mgmt_vlan_id>>`. Press Enter.
8. From the Configure Management Network menu, configure the IP address of the management interface by selecting the IP Configuration option. Then press Enter.
9. Use the space bar to select the static IP address and network configuration.
10. Enter the IP address for managing the VMware ESXi host: `<<esxi_host_mgmt_ip>>`.
11. Enter the subnet mask for the VMware ESXi host: `<<esxi_host_mgmt_netmask>>`.
12. Enter the default gateway for the VMware ESXi host: `<<esxi_host_mgmt_gateway>>`.

13. Press Enter to accept the changes to the IP configuration.
14. Enter the IPv6 configuration menu.
15. Use the space bar to disable IPv6 by unselecting the Enable IPv6 (restart required) option. Press Enter.
16. Enter the menu to configure the DNS settings.
17. Because the IP address is assigned manually, the DNS information must also be entered manually.
18. Enter the primary DNS server's IP address: `<<nameserver_ip>>`.
19. (Optional) Enter the secondary DNS server's IP address.
20. Enter the FQDN for the VMware ESXi host: `<<esxi_host_fqdn>>`.
21. Press Enter to accept the changes to the DNS configuration.
22. Exit the Configure Management Network submenu by pressing Esc.
23. Press Y to confirm the changes and reboot the server.
24. Log out of the VMware Console by pressing Esc.

Downloading VMware vSphere Client and vSphere Remote Command Line

The following steps provide details for downloading the VMware vSphere Client and installing the remote command line.

1. Open a web browser on a management workstation and navigate to the management IP address of one of the VMware ESXi hosts.
2. Download and install both the VMware vSphere Client and the Microsoft Windows version of the VMware vSphere remote command line.

Downloading Updated Cisco VIC eNICDriver

The following steps provide details for downloading Cisco virtual interface card (VIC) eNIC driver.

Note: The eNIC version used in this configuration is 2.1.2.62.

1. Open a web browser on the management workstation and download the VIC driver from this link.
2. Extract the `.vib` file from the downloaded zip file by navigating to:

   ```
   enic-2.1.2.62-esx55-2340678.zip > enic-2.1.2.62-esx55-offline_bundle-2340678.zip > vib20 > net-enic.> Cisco_bootbank_net-enic_2.1.2.62-1OEM.550.0.0.1331820.vib
   ```

3. Document the saved location.

Loading the Updated Cisco VIC eNIC Driver

All Hosts

To load the updated versions of the eNIC driver for the Cisco VIC, follow these steps for all the hosts from vSphere Client:

1. Log into vSphere Client and select the host in the inventory.
2. Click the Summary tab to view the environment summary.
3. From Resources > Storage, right-click datastore1 and choose Browse Datastore.
4. Click the fourth button and select Upload File.
5. Navigate to the saved location for the downloaded eNIC driver version and select `Cisco_bootbank_net-enic_2.1.2.62-1OEM.550.0.0.1331820.vib`.
6. Click Open to open the file.

7. Click Yes to upload the .vib file to datastore1.
8. From the management workstation, open the VMware vSphere Remote CLI that was previously installed.
9. At the command prompt, run the following command to account for each host (eNIC):

```
esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> -d <<var_thumbprint>> software
vib install -d /vmfs/volumes/datastore1/Cisco_bootbank_net-enic_2.1.2.62-1OEM.550.0.0.1331820.vib
```

Note: Remove `-d <<var_thumbprint>>` from the above command to obtain the thumbprint.

10. From the vSphere Client, right-click the host in the inventory and select Reboot.
11. Click Yes to continue.
12. Enter a reason for the reboot and click OK.
13. Repeat steps 1 through 12 for all hosts.

Logging in to VMware ESXi Hosts Using the VMware vSphere Client

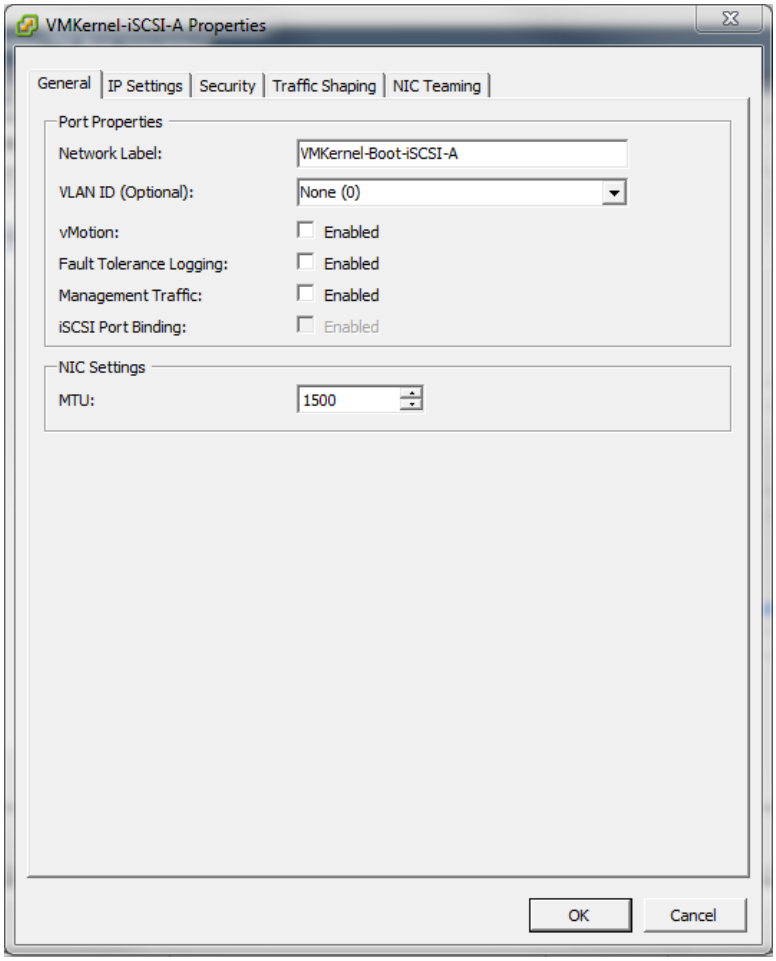
This step provides details for logging in to each VMware ESXi host using the VMware vSphere Client.

All Hosts

1. Open the recently downloaded VMware vSphere Client and enter the IP address of the host to which you want to connect: `<<esxi_host_mgmt_ip>>`.
2. Enter root for the user name.
3. Enter the root password.
4. Click Login to connect.

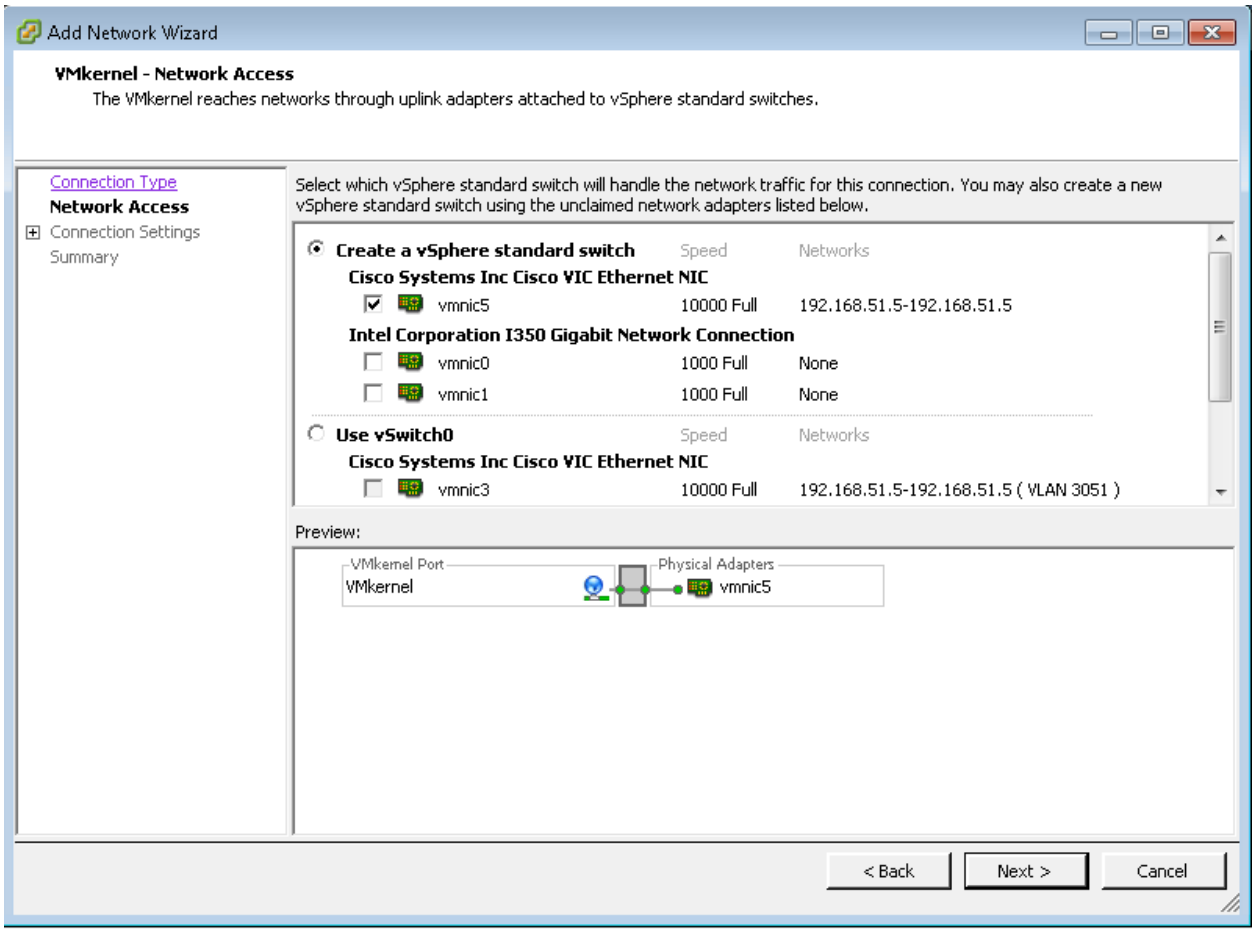
Setting Up iSCSI Networking for iSCSI Booted Servers

1. Launch the VMware vSphere Client.
2. Connect to the host with the `root` user ID and password.
3. In the right pane of the vSphere Client, click the Configuration tab.
4. In the Hardware pane select Networking.
5. To the right of iScsBootvSwitch, select Properties.
6. Select the vSwitch configuration and click Edit.
7. Change the MTU to 9000 and click OK.
8. Select the iScsBootPG configuration and click Edit.
9. Change the Network label to VMKernel-Boot-iSCSI-A.
10. Change the MTU to 9000.
11. Do not set a VLAN.

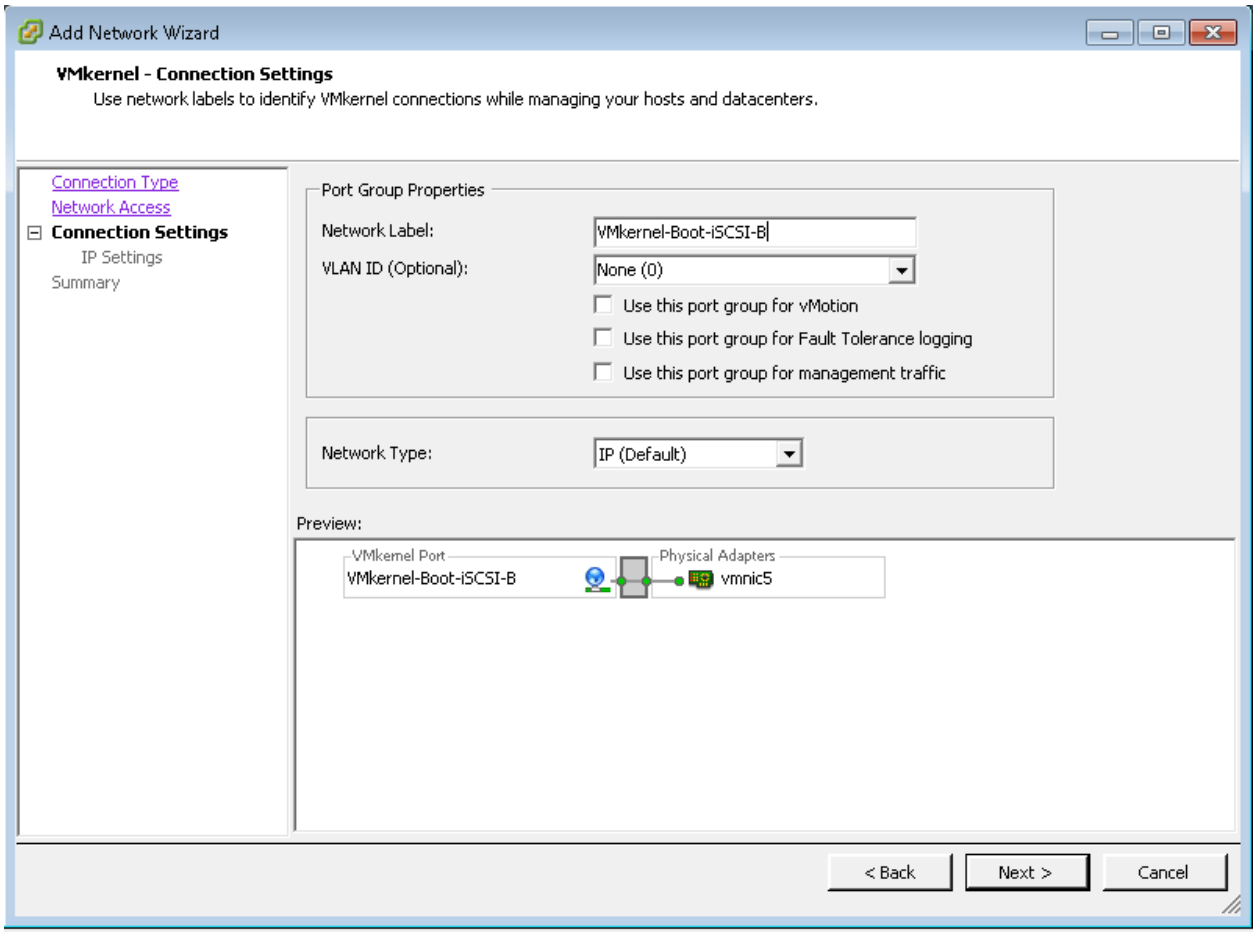


12. Click OK.
13. Click Close to close the iScsiBootvSwitch Properties window.
14. On the right, select Add Networking.
15. Select the VMkernel Connection type and click Next.
16. Select vmnic5.

    Note: vmnic4 is used by iSCSI-A and vmnic5 is used by iSCSI-B.



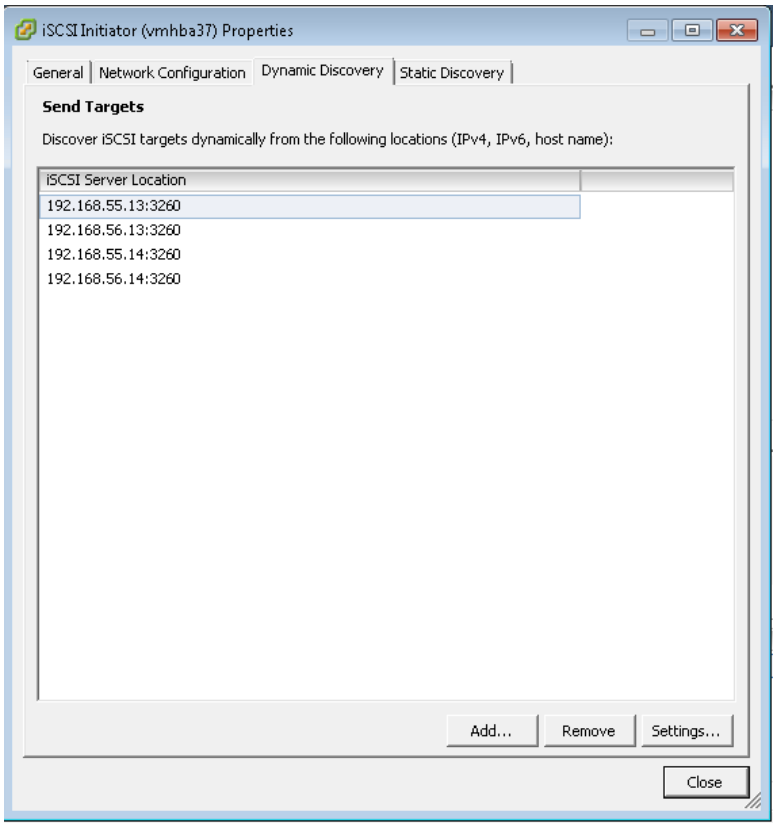
17. Click Next.
18. Set the Network Label to VMkernel-Boot-iSCSI-B. Leave the VLAN ID set to None.



19. Click Next.
20. Enter the IP address and subnet mask.

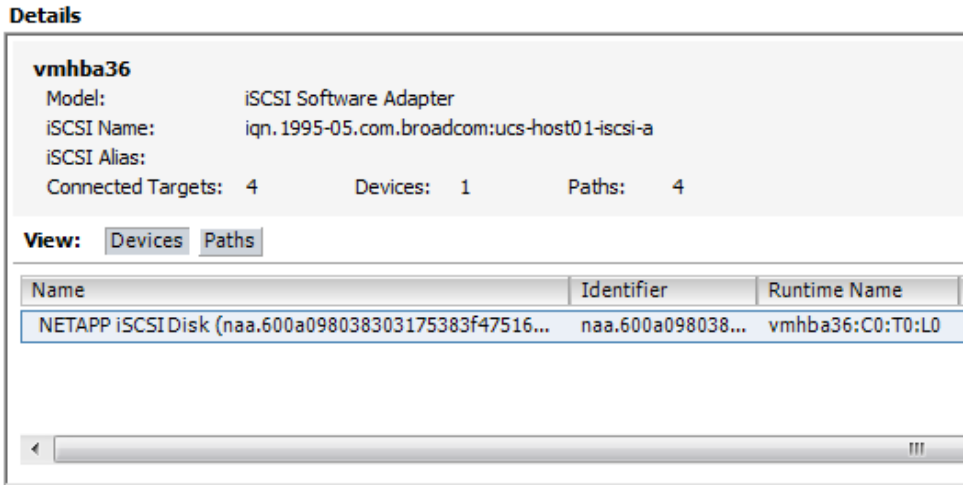
Note: Log in to Cisco CIMC and navigate to Inventory > Cisco VIC Adapters > vNICs. Get the initiator IP address of iSCSI-vNIC-B.

21. Click Next and Finish to create the vSwitch and VMkernel port.
22. Select Properties to the right of vSwitch1.
23. In the vSwitch1 Properties window, select the vSwitch configuration and click Edit.
24. Change the MTU to 9000 and click OK.
25. Select the VMkernel-Boot-iSCSI-B configuration and click Edit.
26. Change the MTU to 9000 and click OK.
27. Click Close to close the vSwitch1 Properties window.
28. Click Storage Adapters in the Hardware pane.
29. Select the iSCSI Software Adapter and click Properties.
30. Select the Dynamic Discovery tab and click Add.
31. Enter the IP address of `iscsi_lif01a`.
32. Enter the IP addresses of `iscsi_lif01b`, `iscsi_lif02a`, and `iscsi_lif02b`.



33. Click Close and then click Yes to rescan the host bus adapter.

    You should now see four connected paths in the Details pane.



Setting Up VMkernel Ports and the Virtual Switch

The following steps provide details for setting up VMkernel ports and virtual switches.

All Hosts

1. In the VMware vSphere Client, select the host on the left pane.
2. Select the Configuration tab.

3. Select the Networking link in the Hardware box.
4. Select the Properties link in the right field on vSwitch0.
5. Select the vSwitch configuration and click Edit.
6. On the General tab, change the MTU to 9000.
7. On the NIC Teaming tab, change all adapters so that they are active adapters by clicking each individual adapter and using the Move Up button to the right.
8. Close the properties for vSwitch0 by clicking OK.
9. Select the Management Network configuration and click Edit.
10. Change the network label to `VMkernel-MGMT` and select the Management Traffic checkbox.
11. Finalize the edits for the management network by clicking OK.
12. Select the VM Network configuration and click Edit.
13. Change the network label to `IB-MGMT Network` and enter `<<var_ib-mgmt_vlan_id>>` in the VLAN ID (optional) field.
14. Finalize the edits for the VM network by clicking OK.
15. Click Add to add a network element.
16. Select Virtual Machine.
17. Enter NFS-Network for the network label and enter the VLAN ID: `<<nfs_vlan_id>>`.
18. Click Next.
19. Click Finish.
20. Click Add to add a network element.
21. Select the VMkernel button and click Next.
22. Change the network label to VMkernel-NFS and enter the VLAN ID (optional): `<<nfs_vlan_id>>`.
23. Continue creating the NFS VMkernel by clicking Next.
24. For the NFS VLAN interface for the host, enter `<<esxi_host_nfs_ip>>` `<<esxi_host_nfs_netmask>>`.
25. Continue creating the NFS VMkernel by clicking Next.
26. Finalize creating the NFS VMkernel interface by clicking Finish.
27. Select the VMkernel-NFS configuration and click Edit.
28. Change the MTU to 9000.
29. Finalize the edits for the VMkernel NFS network by clicking OK.
30. Click Add to add a network element.
31. Select the VMkernel button and click Next.
32. Change the network label to VMkernel-vMotion and enter the VLAN ID (optional): `<<vmotion_vlan_id>>`.
33. Select the checkbox to use this port group for VMware vMotion.
34. Continue creating the VMware vMotion VMkernel by clicking Next.
35. For the VMware vMotion VLAN interface for the host, enter: `<<esxi_host_vmotion_ip>>` `<<esxi_host_vmotion_netmask>>`.
36. Continue with the VMware vMotion VMkernel creation by clicking Next.
37. Finalize creating the VMware vMotion VMkernel by clicking Finish.
38. Select the VMkernel vMotion configuration and click Edit.
39. Change the MTU to 9000.

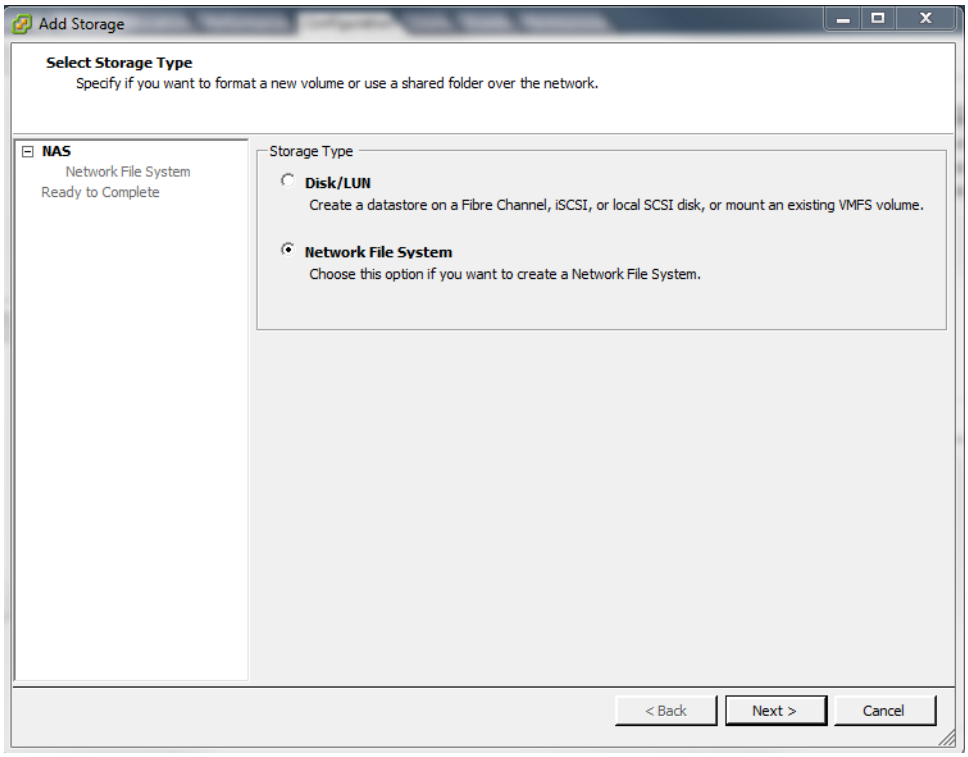
40. Finalize the edits for the VMware vMotion VMkernel network by clicking OK.
41. Click Add to add a network element.
42. Leave the virtual machine connection type selected and click Next.
43. Change the network label to VM-Network and enter the VLAN ID (optional): `<<vmtraffic_vlan_id>>`.
44. Click Next.
45. Click Finish.
46. Close the dialog box to finalize the VMware ESXi host networking setup.

Mounting Required Datastores

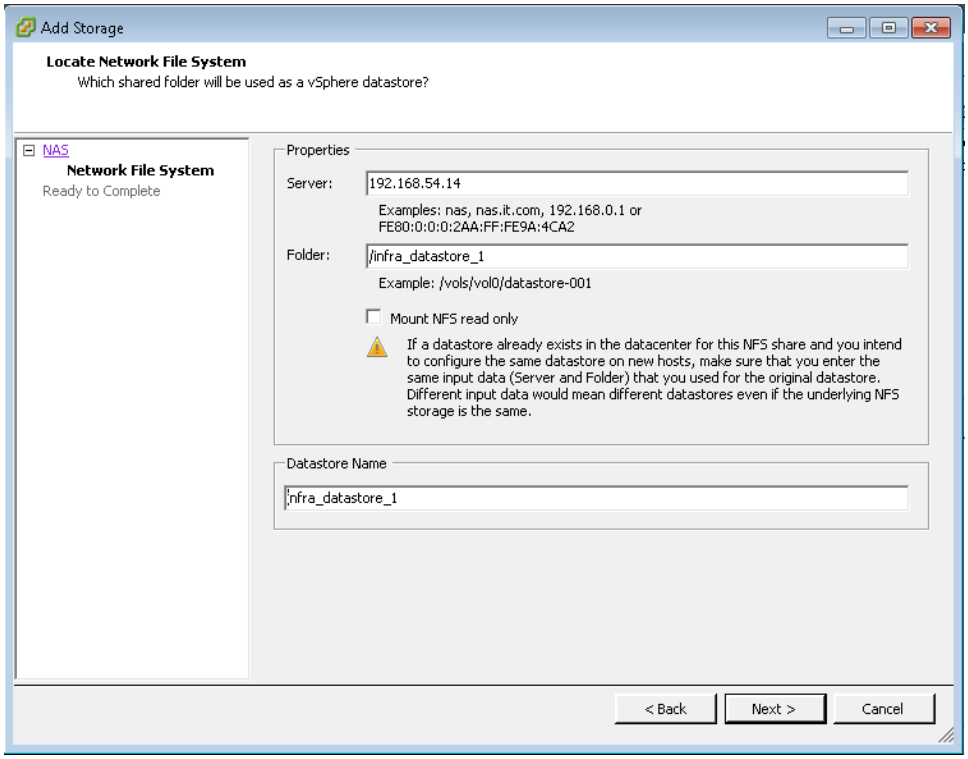
This step provides details for mounting the required datastores.

All Hosts

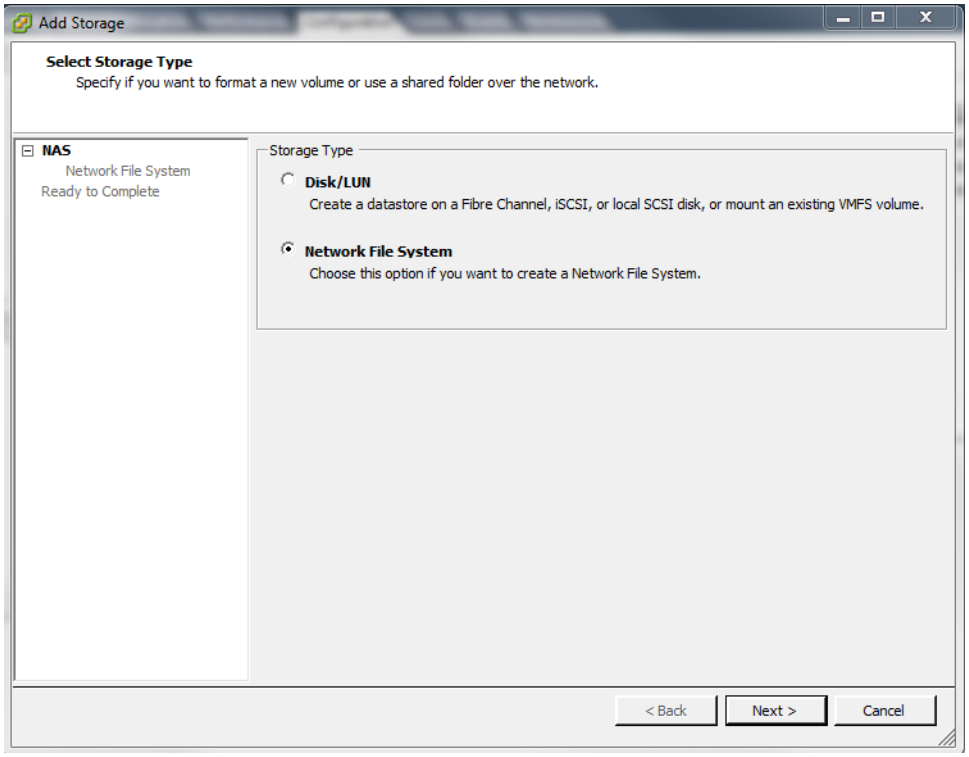
1. In each VMware vSphere Client, select the host on the left pane.
2. Go to the Configuration tab to enable configurations.
3. Click the Storage link in the Hardware box.
4. In the right pane in the Datastore section, click Add Storage.



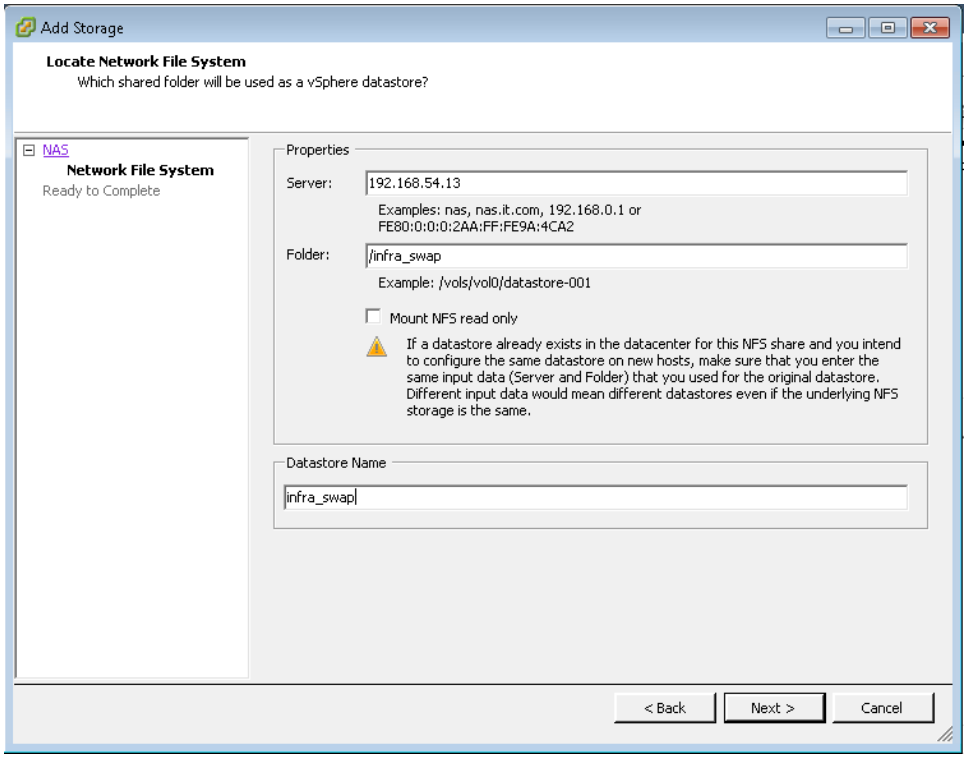
5. The Add Storage wizard appears. Select the Network File System button and click Next.
6. Enter the server IP address: `<<controller01_ nfs_infra_datastore_1_ip>>`.
7. Enter the path for the NFS export: `/infra_datastore_1`.
8. Make sure that the Mount NFS read-only checkbox is left cleared.
9. Enter the datastore name: `infra_datastore_1`.



10. Continue creating the NFS datastore by clicking Next.
11. Finalize creating the NFS datastore by clicking Finish.
12. In the right pane in the Datastore section, click Add Storage.
    The Add Storage wizard appears.
13. Select the Network File System button and click Next.



14. Enter the server IP address: `<<controller01_nfs_lif_ip>>`.
15. Enter the path for the NFS export: `/infra_swap`.
16. Make sure that the Mount NFS read-only checkbox is left cleared.
17. Enter the datastore name: `infra_swap`.



18. Continue creating the NFS datastore by clicking Next.
19. Finalize creating the NFS datastore by clicking Finish.

Moving the Virtual Machine Swap-File Location

These steps provide details for moving the virtual machine swap-file location.

All Hosts

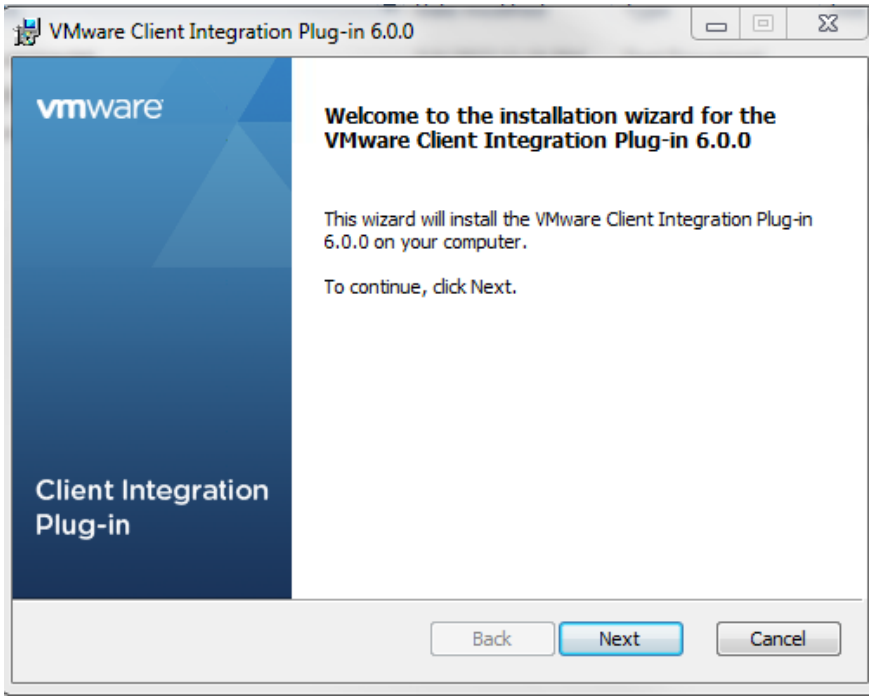
1. Select the host in the left pane in the VMware vSphere Client.
2. Go to the Configuration tab to enable configuration.
3. Click the Virtual Machine Swapfile Location link in the Software box.
4. In the right pane, click Edit.
5. Select the Store the Swap File in a Swap File Datastore Selected Below button.
6. Select the infra_swap datastore.
7. Finalize moving the swap-file location by clicking OK.

5.6 VMware vCenter 6.0 Deployment Procedure

The procedures in the following subsections provide detailed instructions for installing VMware vCenter 6.0 in a FlexPod Express environment. After the procedures are completed, a VMware vCenter Server will be configured.

Installing the VMware Client Integration Plug-in

1. Download the .iso installer for the vCenter Server Appliance and Client Integration Plug-in.
2. Mount the ISO image to the Windows virtual machine or physical server on which you want to install the Client Integration Plug-in to deploy the vCenter Server Appliance.
3. In the software installer directory, navigate to the vcsa directory and double-click VMware-ClientIntegrationPlugin-6.0.0.exe. The Client Integration Plug-in installation wizard appears.

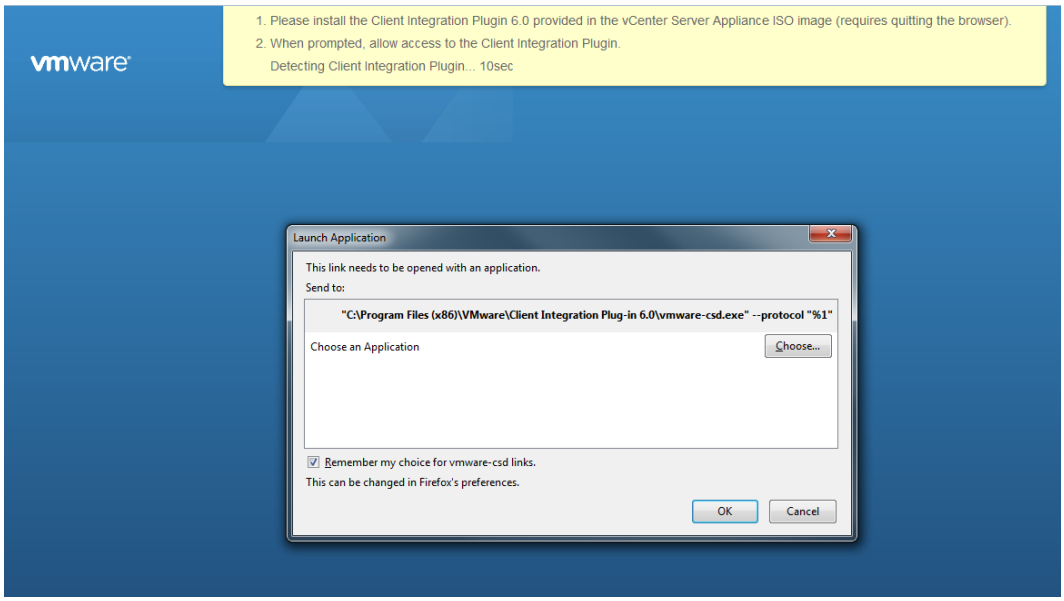


4. On the Welcome page, click Next.
5. Read and accept the terms in the End-User License Agreement and click Next.
6. Click Next.
7. Click Install.

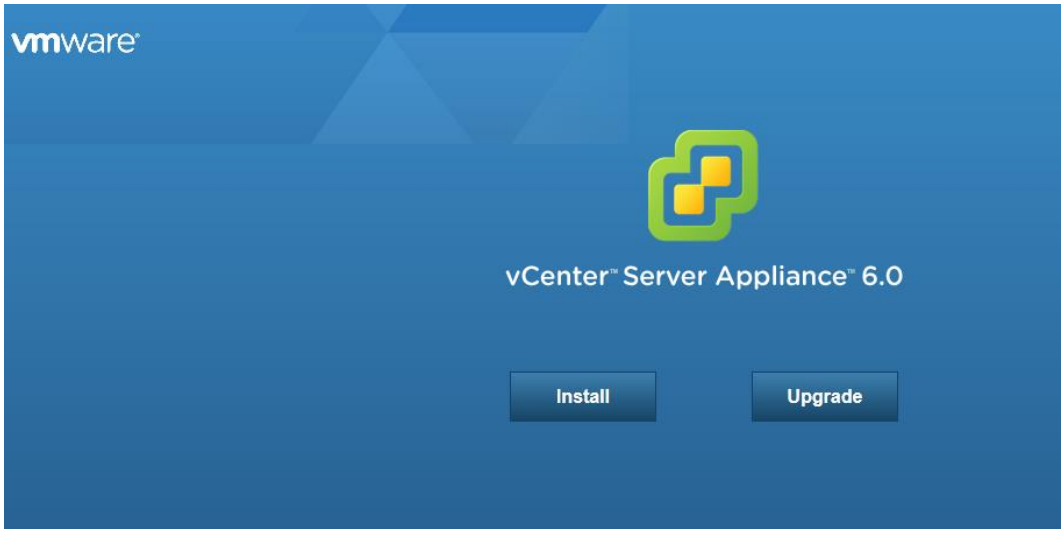
Building the VMware vCenter Virtual Machine

To build the VMware vCenter virtual machine, complete the following steps:

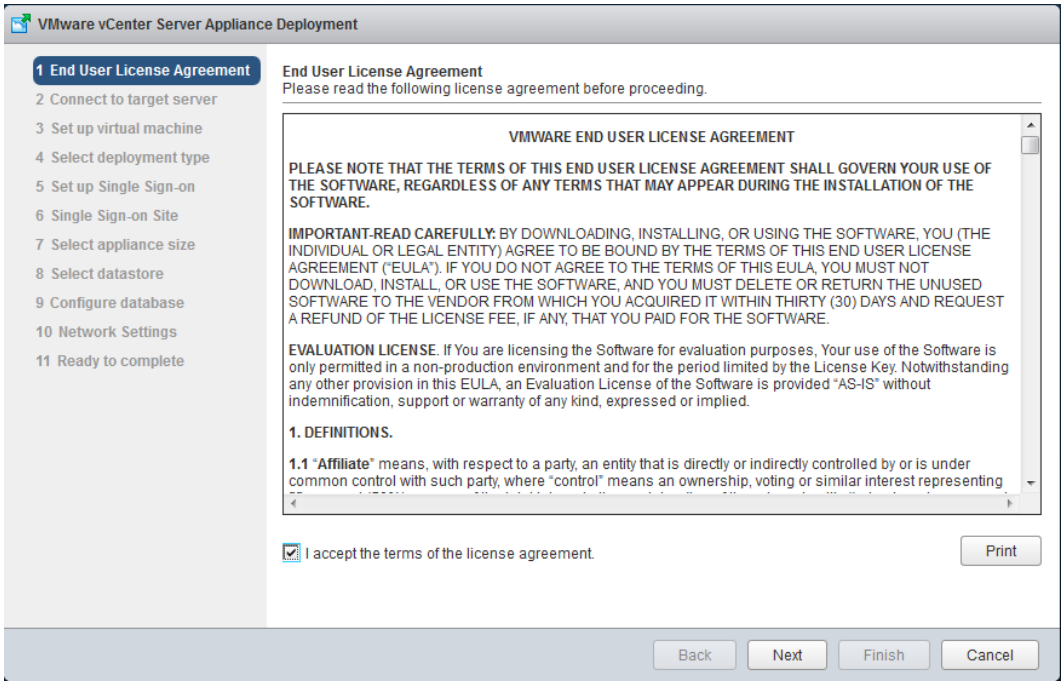
1. In the software installer directory, double-click `vcsa-setup.html`.
2. Allow the plug-in to run on the browser when prompted.



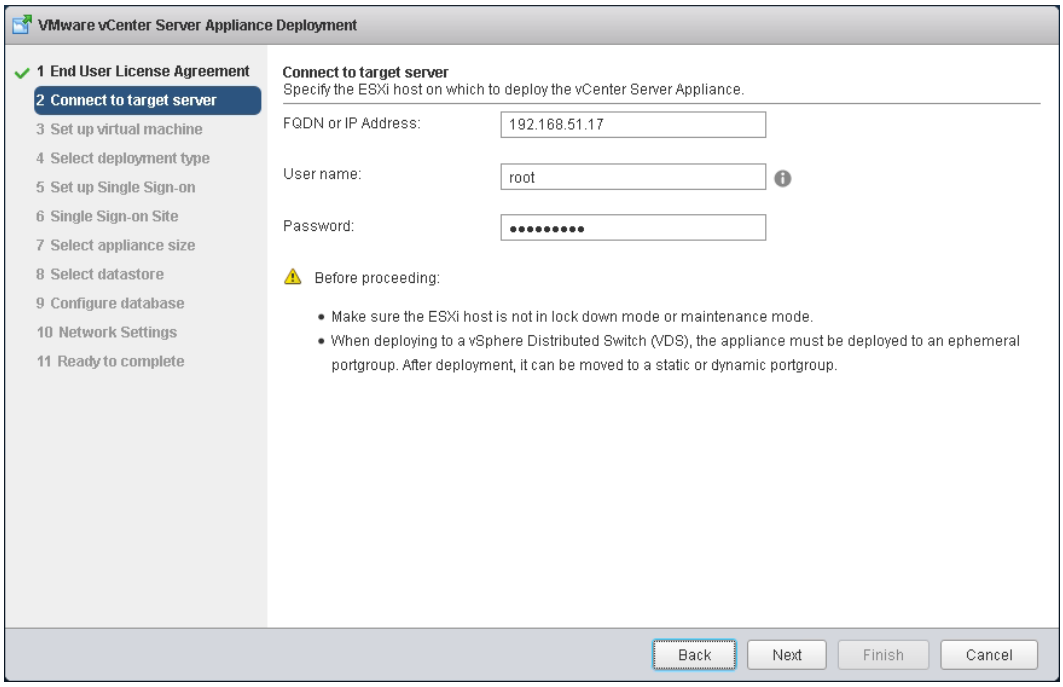
3. On the Home page, click `Install` to start the vCenter Server Appliance deployment wizard.



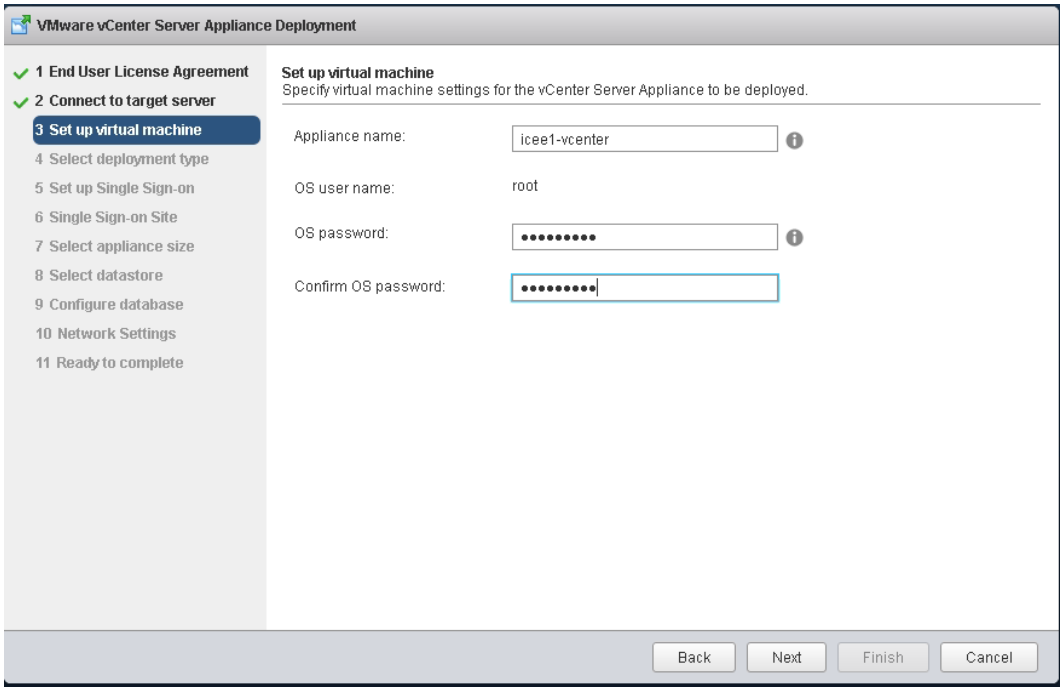
4. Read and accept the license agreement, and click Next.



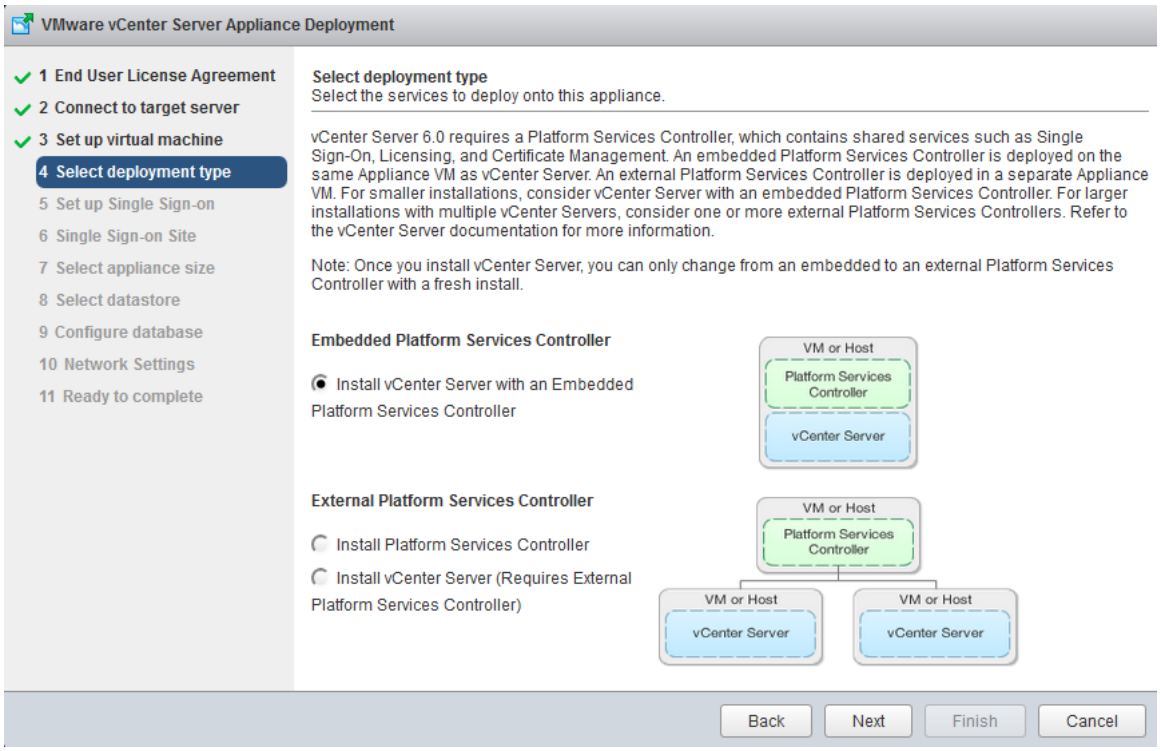
5. In the Connect to target server page, enter the ESXi host name, user name, and password.



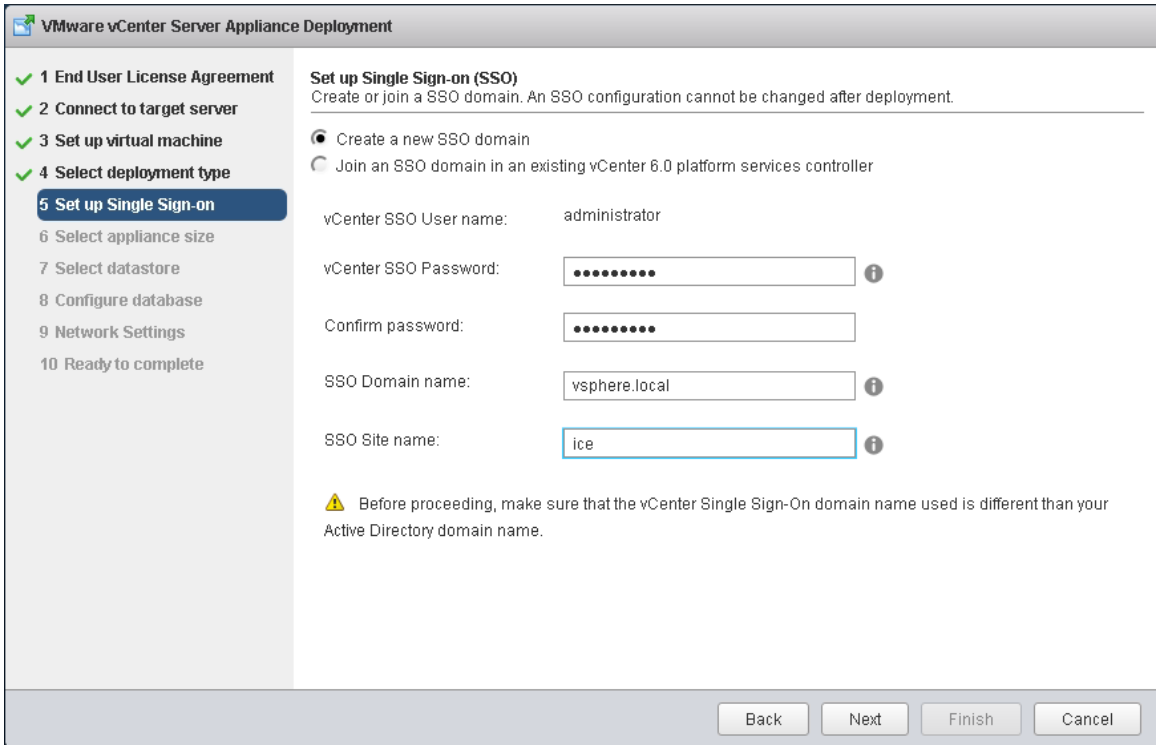
6. Click Yes to accept the certificate.
7. Enter the appliance name and password details in the Set up virtual machine page.



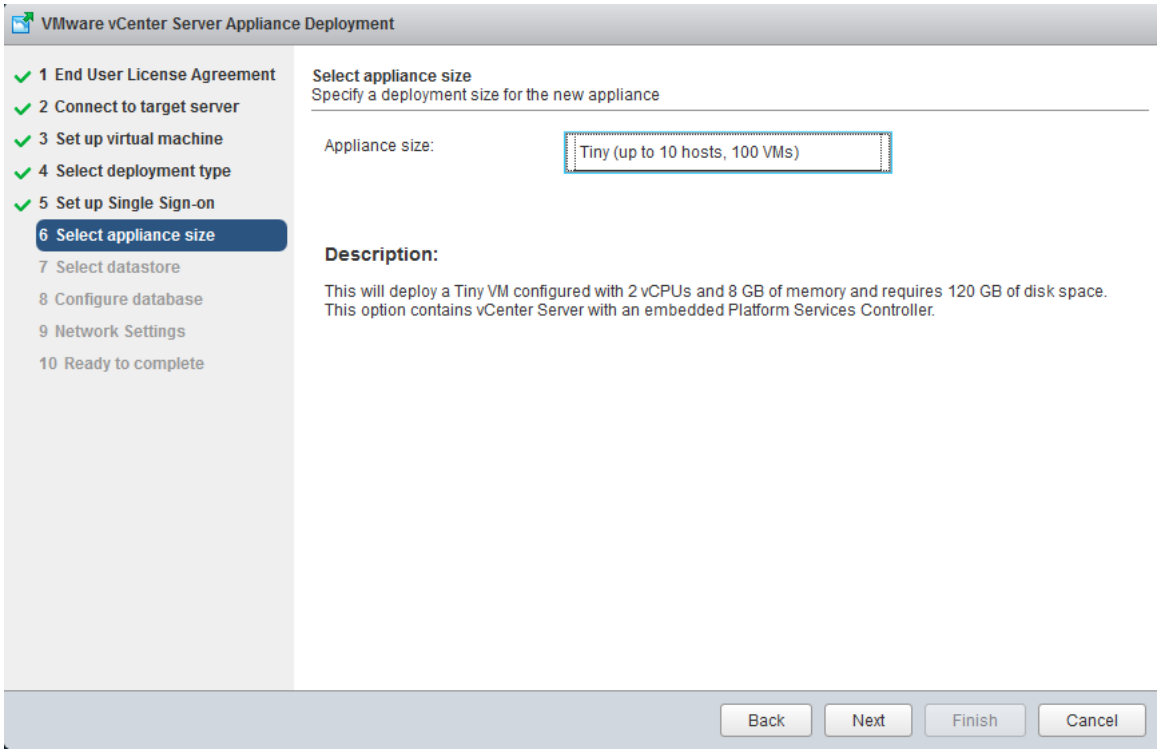
8. In the Select deployment type page, choose `Install vCenter Server with an Embedded Platform Services Controller`.



9. Click Next.
10. In the Set Up Single Sign-On page, select `Create a new SSO domain`.
11. Enter the SSO password, domain name, and site name.

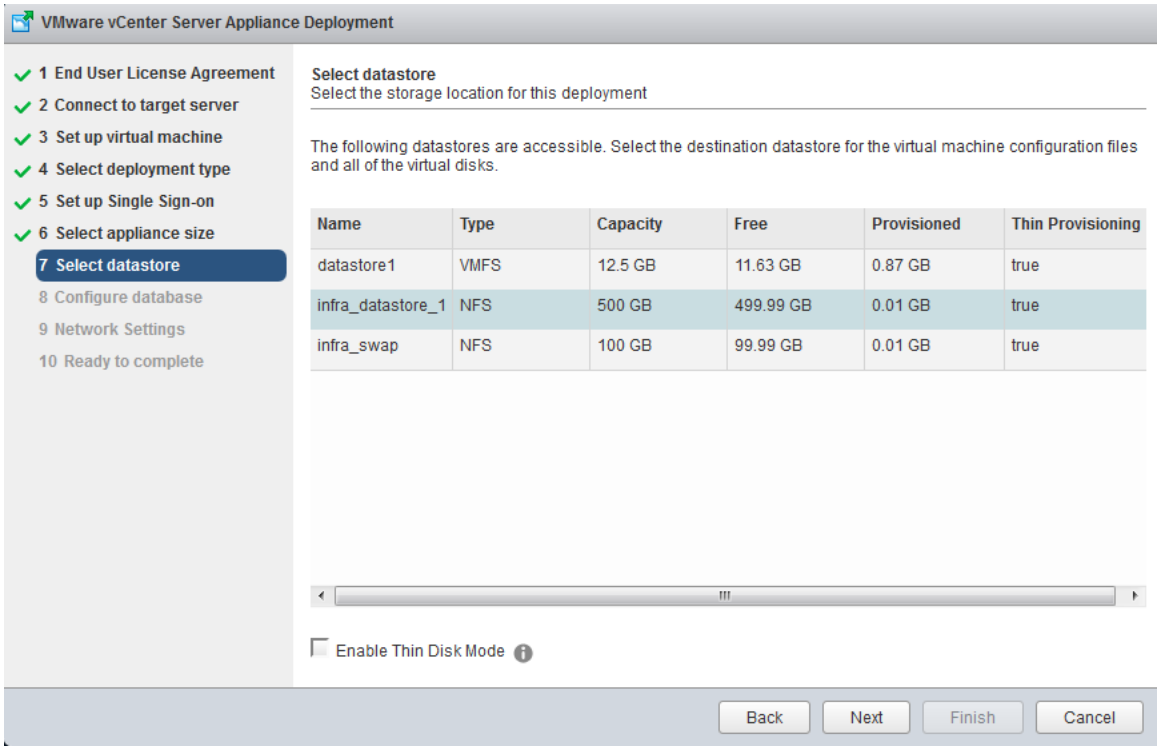


12. Click Next.
13. Select the appliance size. For example, `Tiny (up to 10 hosts, 100 VMs).`

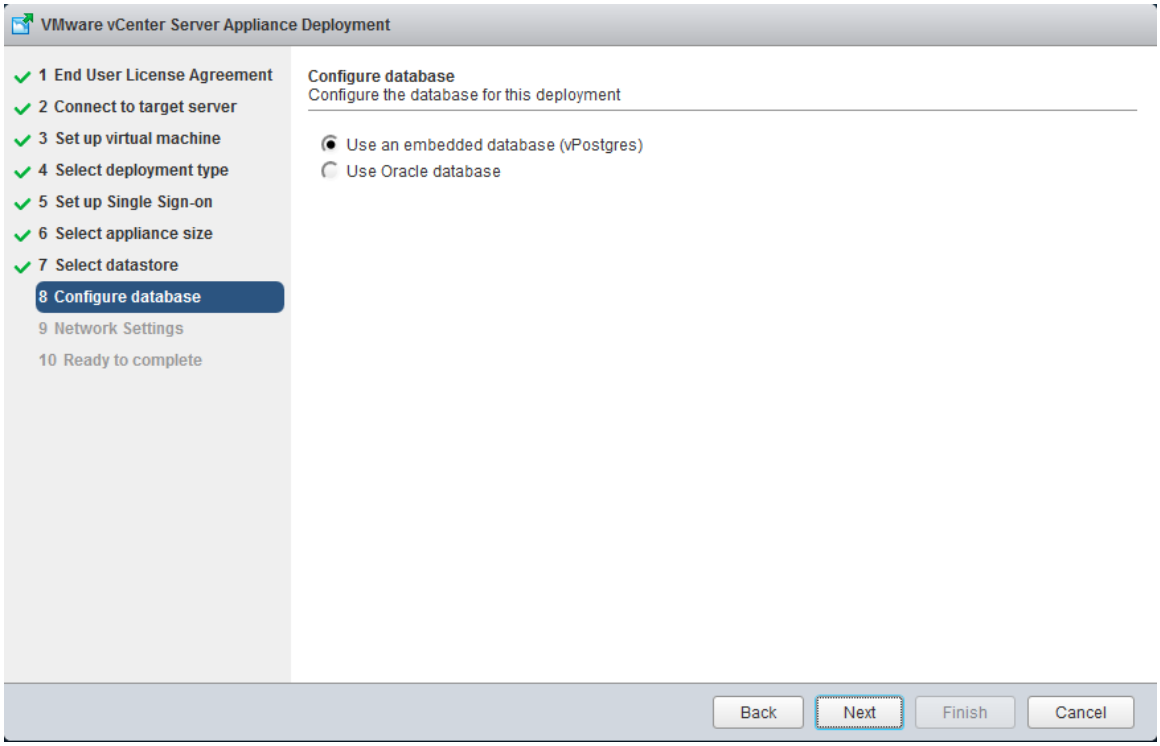


14. Click Next.

15. In the Select Datastore page, choose `infra_datastore_1`.

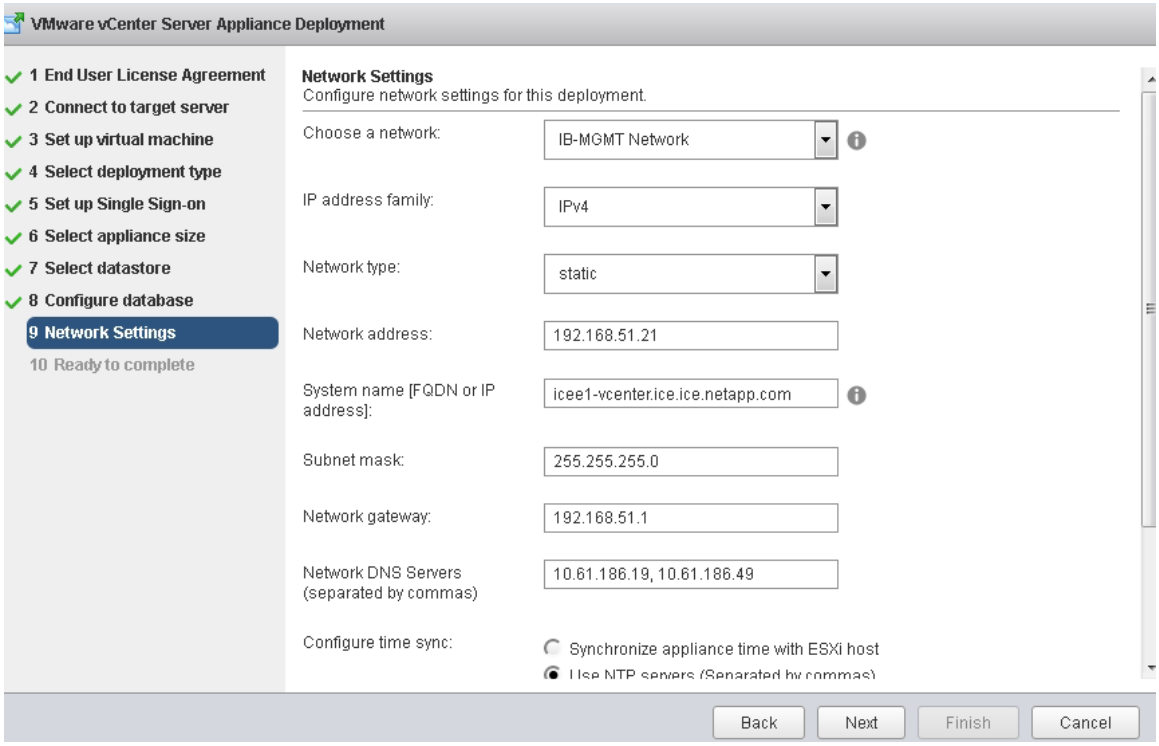


16. Click Next.
17. Select Use an embedded database in the Configure Database page. Click Next.

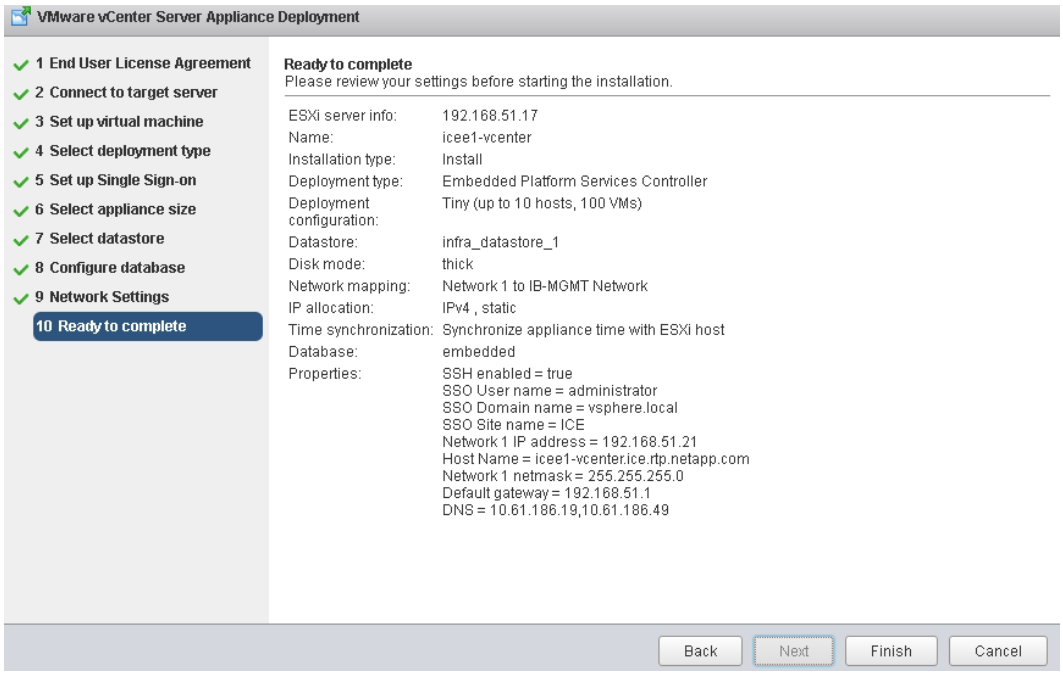


18. In the Network Settings page, configure these settings:

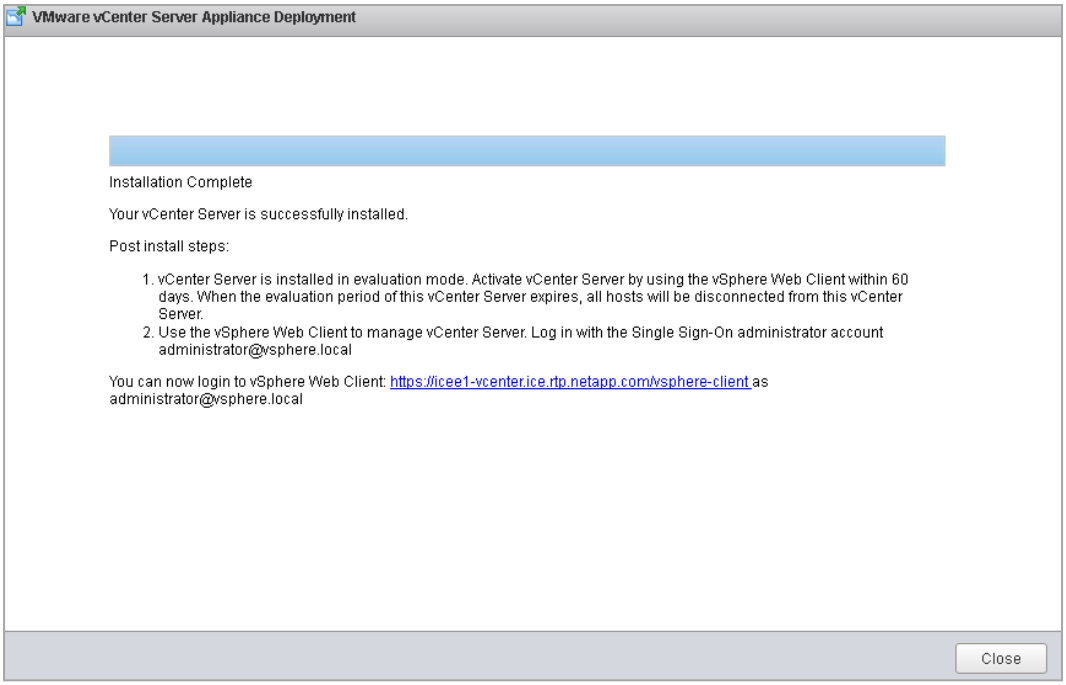
- Choose a network: IB-MGMT-Network
- IP address family: IPV4
- Network type: static
- Network address: <<var_vcenter_ip>>
- System name: <<var_vcenter_fqdn>>
- Subnet mask: <<var_vcenter_subnet_mask>>
- Network gateway: <<var_vcenter_gateway>>
- Network DNS Servers: <<var_dns_server>>
- Configure time sync: Use NTP servers
- Enable SSH (optional)



19. Review the configuration and click Finish.

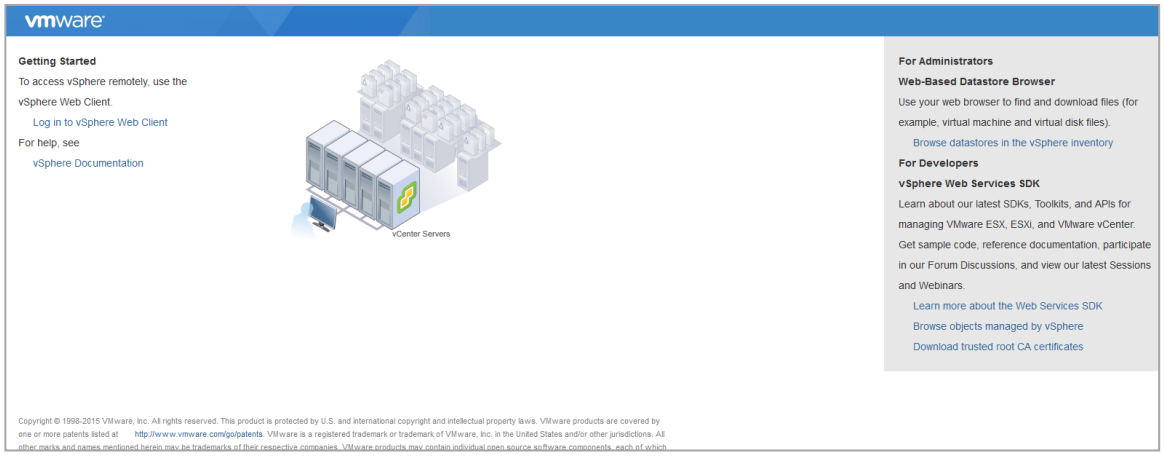


20. The vCenter appliance installation will take a few minutes to complete.

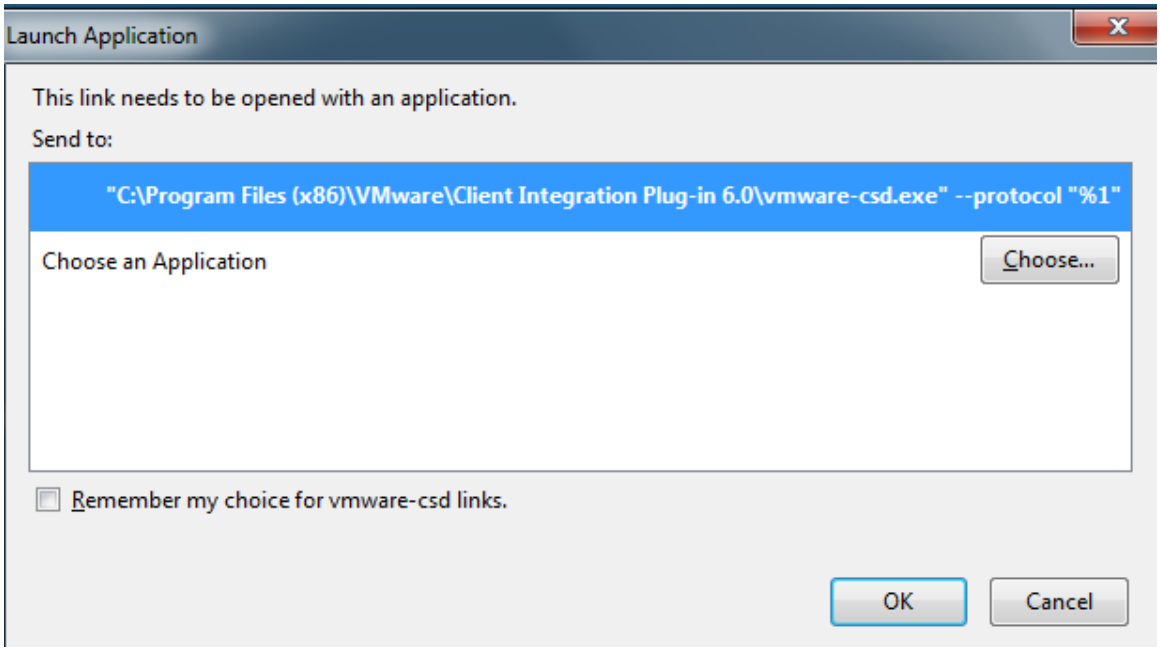


Setting Up VMware vCenter Server

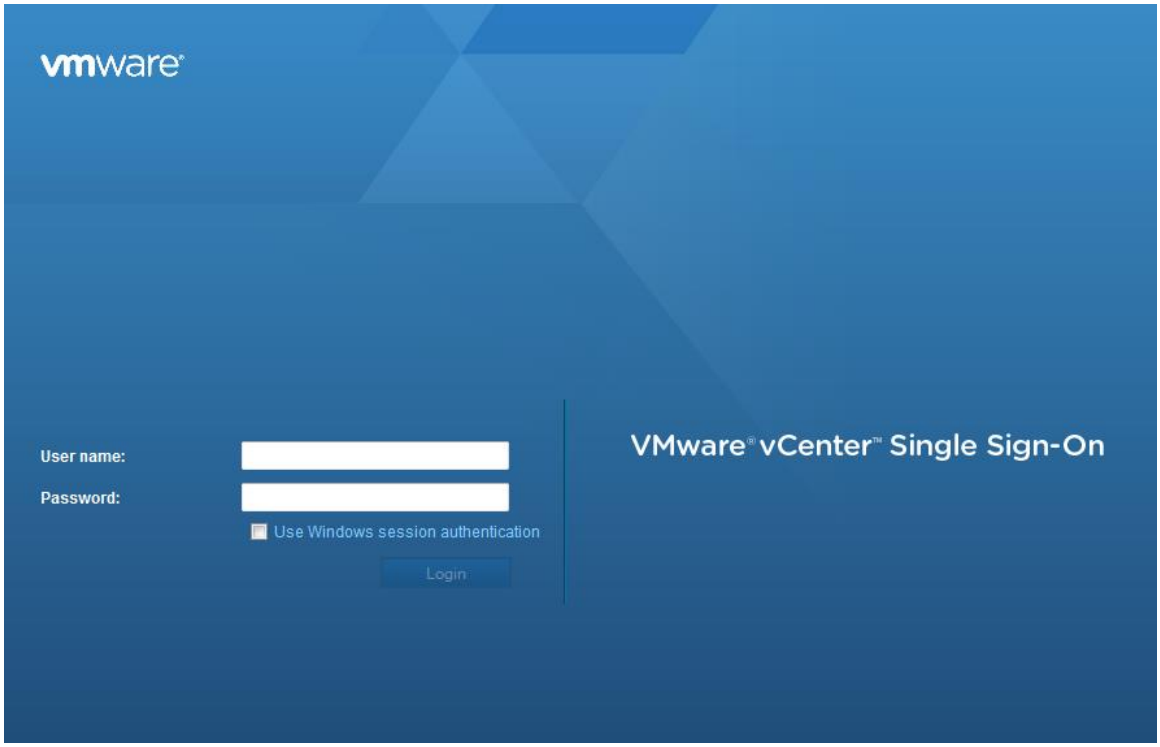
1. Using a web browser, navigate to `https://<<var_vcenter_ip>>`.



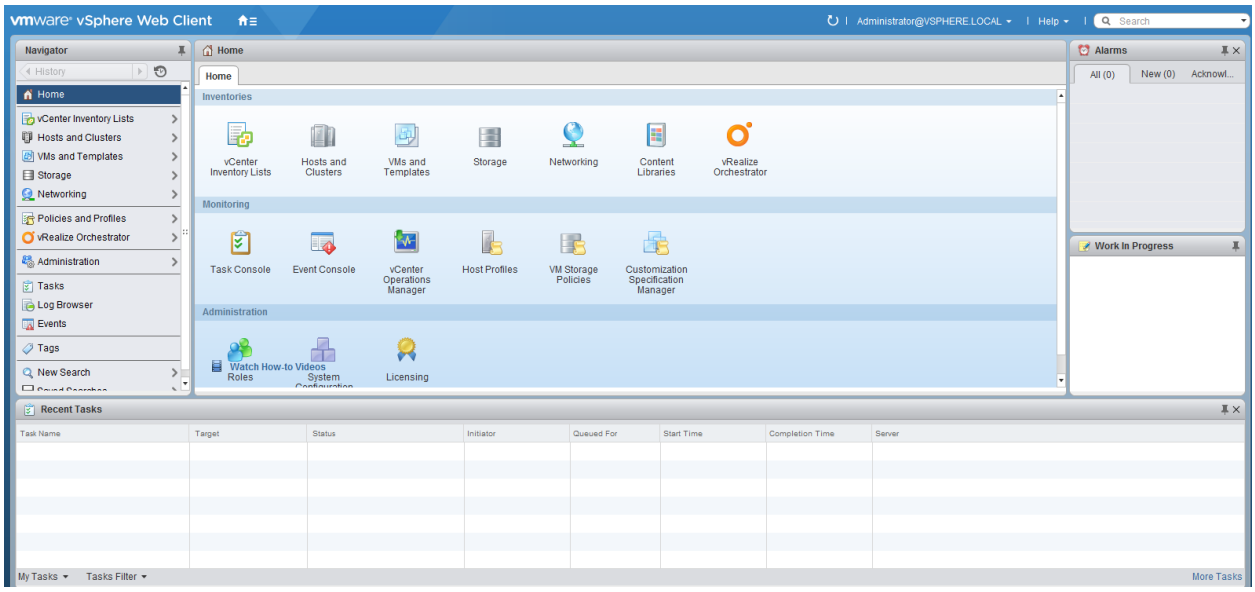
2. Click Log in to vSphere Web Client.
3. Click OK in the Launch Application window.

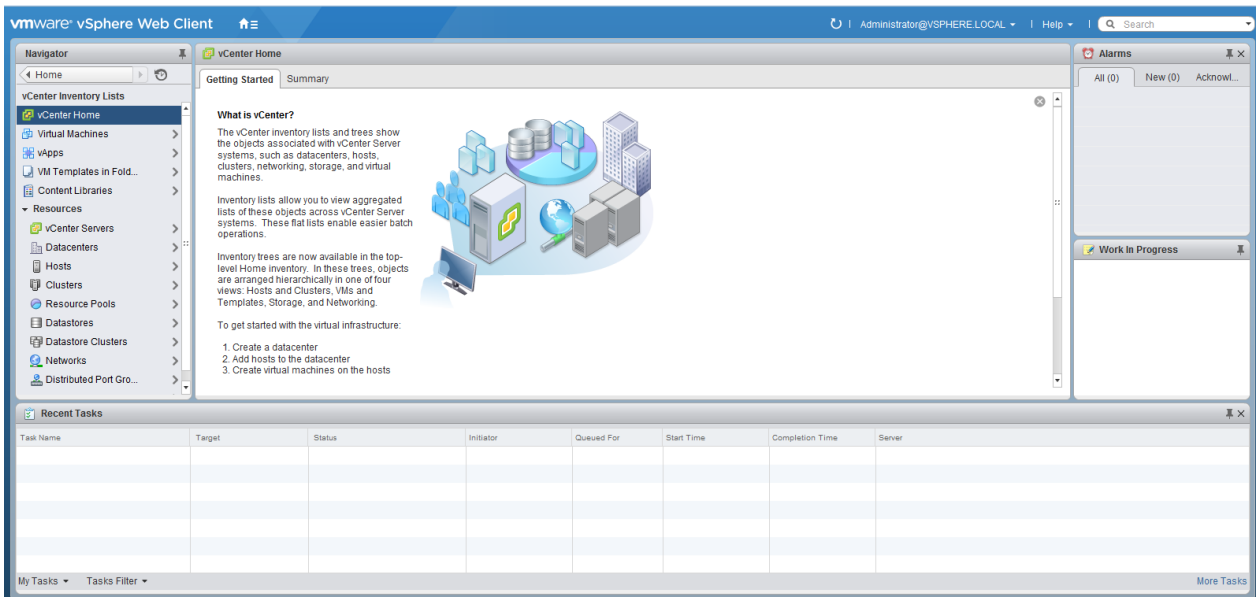


4. Log in using the single sign-on user name and password created during the vCenter installation.

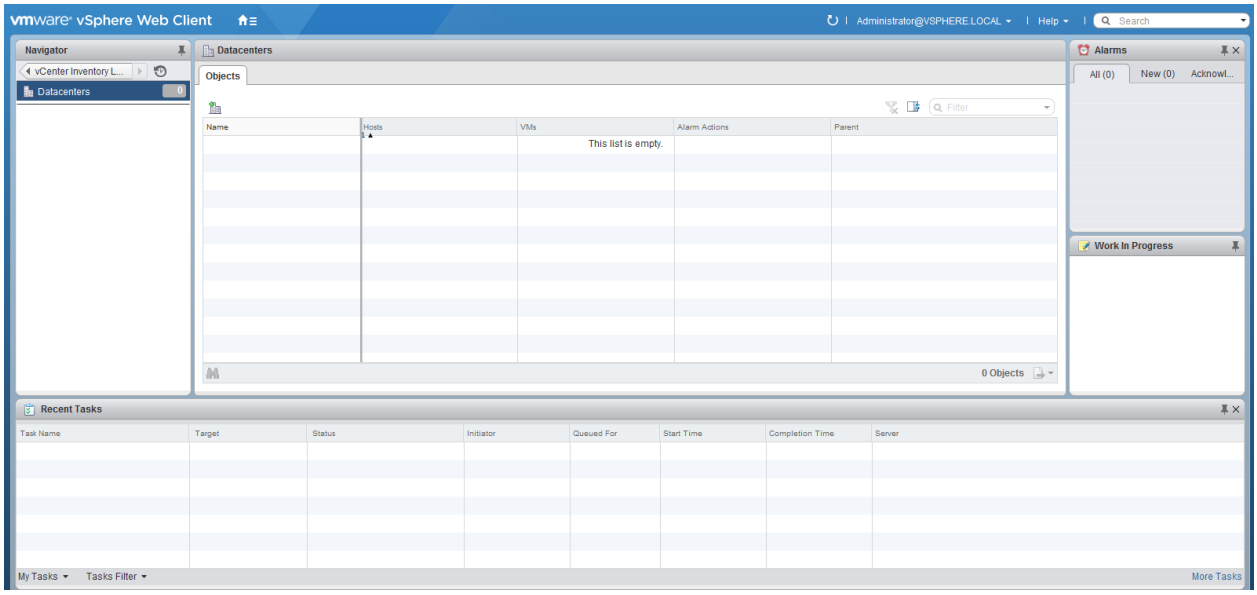


5. Navigate to vCenter Inventory Lists on the left pane.

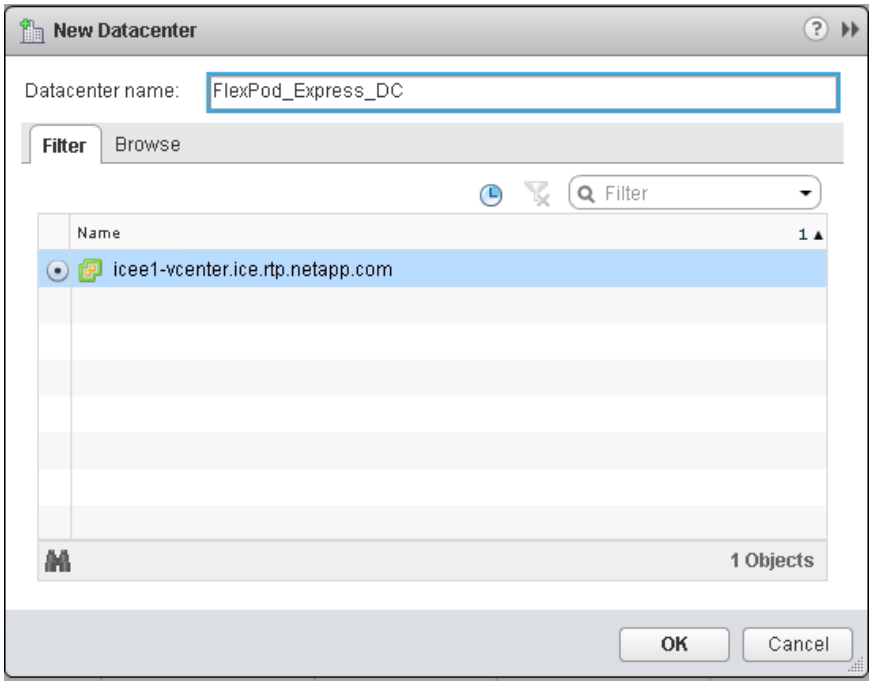




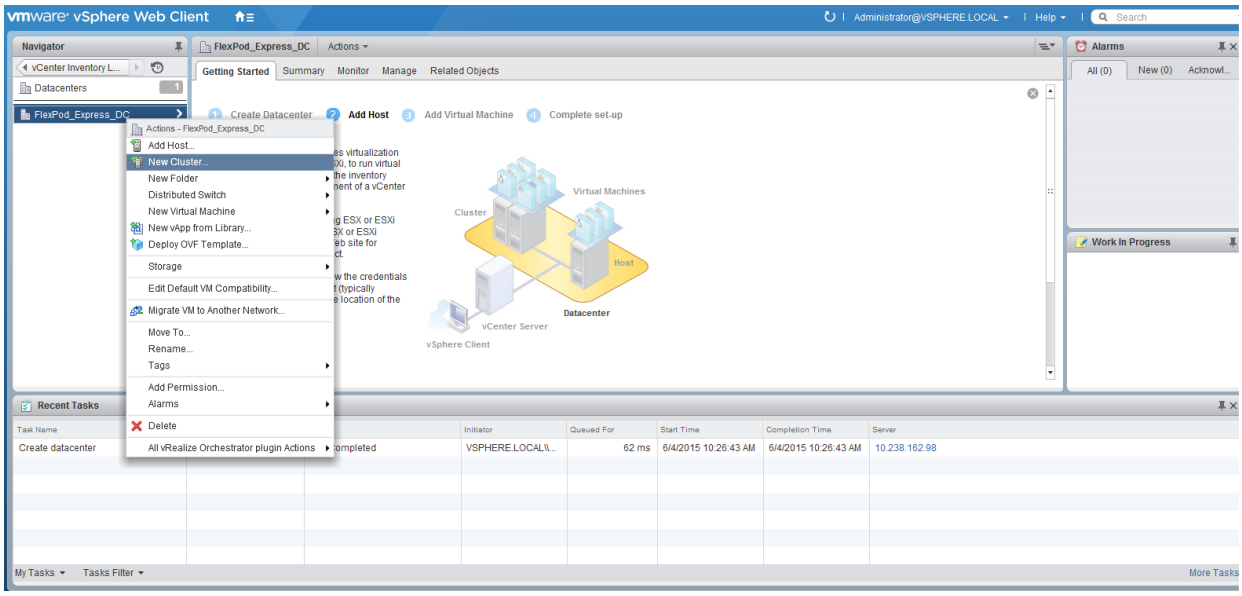
6. Under Resources, click Datacenters in the left plane.



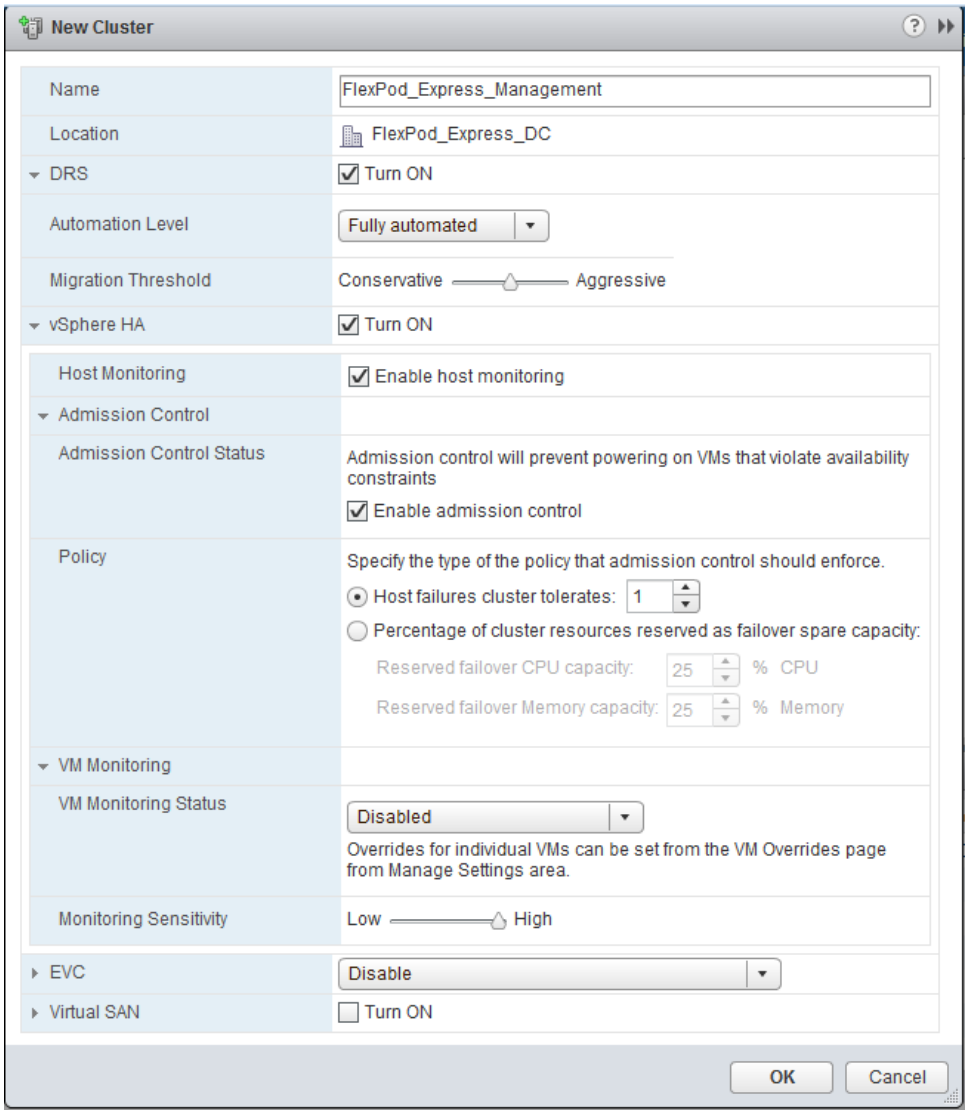
7. To create a data center, click the icon in the center pane with a green plus symbol above it.
8. Type `FlexPod_Express_DC` in the Datacenter name field.
9. Select the vCenter Name/IP option and click OK.



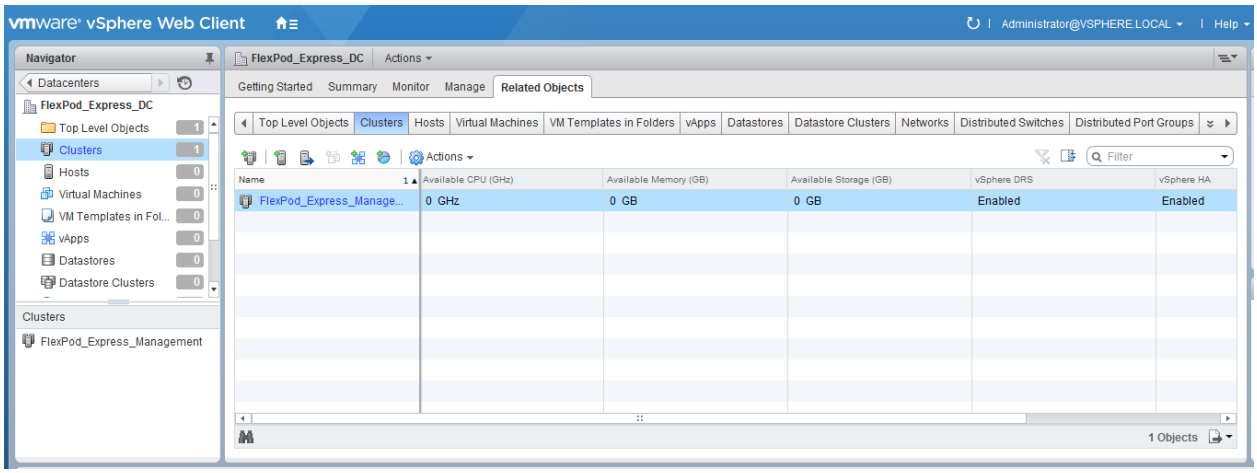
10. Right-click FlexPod_Express_DC in the list in the center pane. Click New Cluster.



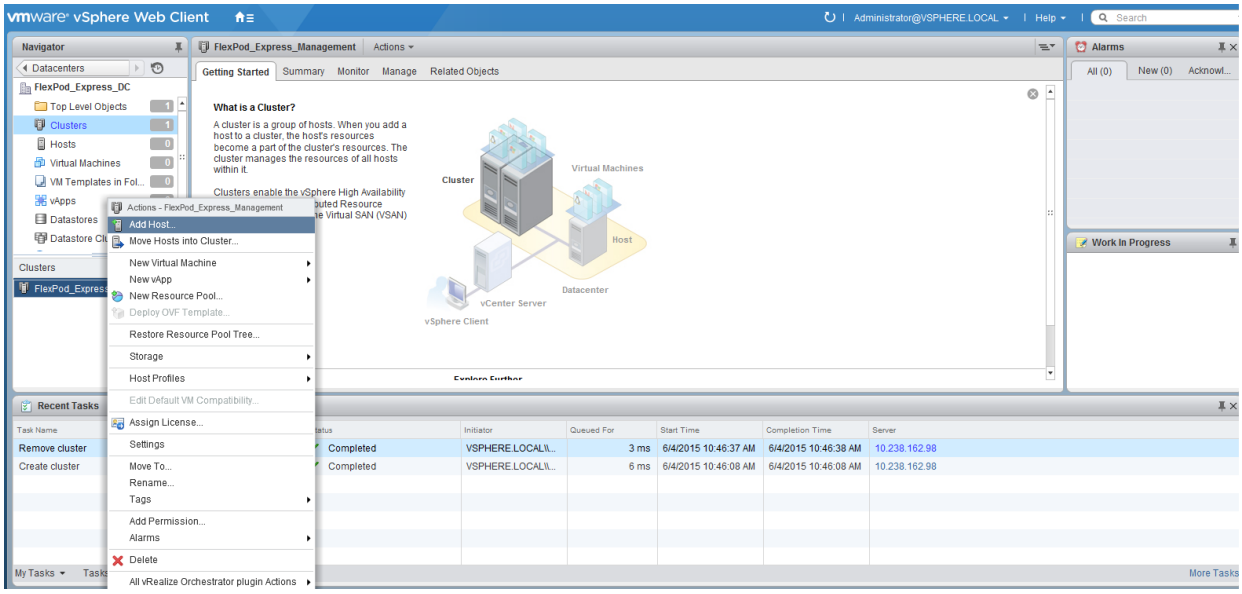
11. Name the cluster FlexPod_Express_Management.
12. Check the box beside DRS. Retain the default values.
13. Check the box beside vSphere HA. Retain the default values.



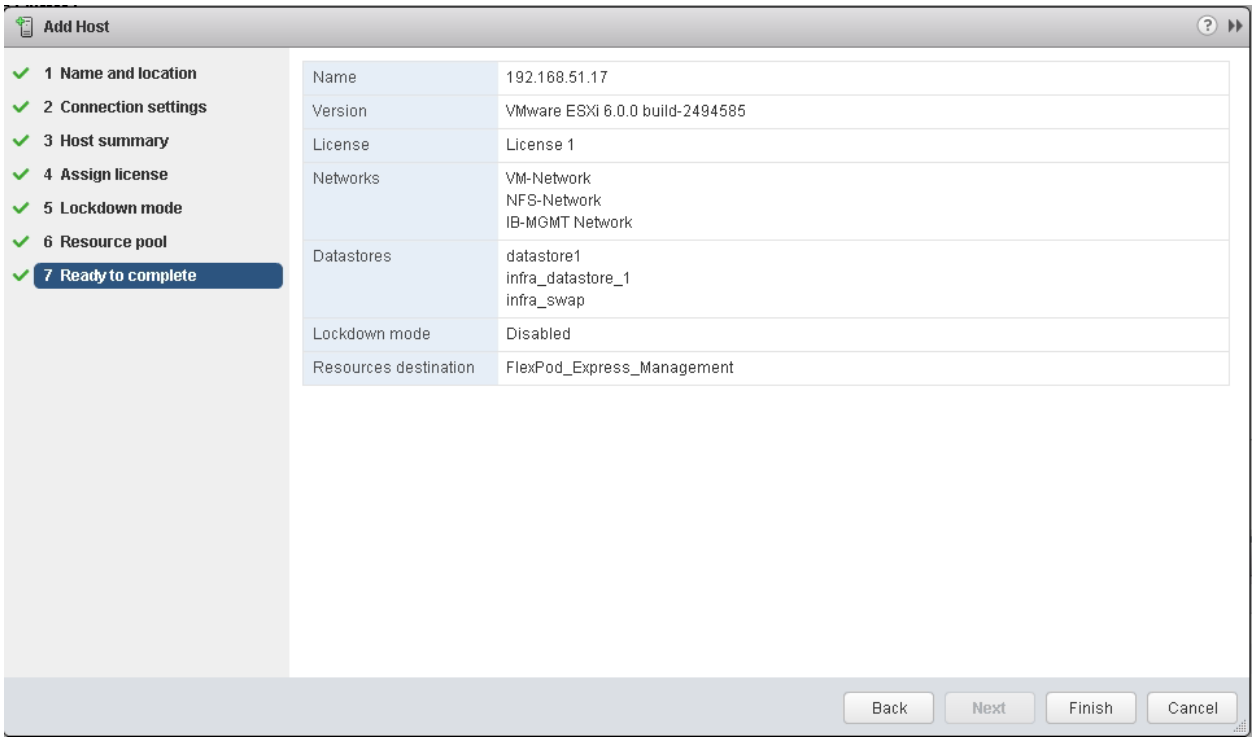
14. Click OK to create the new cluster.
15. On the left pane, double-click `FlexPod_Express_DC`.
16. Click Clusters.



17. Under the Clusters pane, right-click FlexPod_Express_Management and click Add Host.



18. In the Host field, enter either the IP address or the host name of one of the VMware ESXi hosts. Click Next.
19. Type root as the user name and the root password. Click Next to continue.
20. Click Yes to accept the certificate.
21. Review the host details and click Next to continue.
22. Assign a license and click Next to continue.
23. Click Next to continue.
24. Click Next to continue.
25. Review the configuration parameters. Then click Finish to add the host.



26. Repeat steps 18 through 25 to add the remaining VMware ESXi hosts to the cluster.

Setting Up VMware ESXi Dump Collector for iSCSI-Booted Hosts

ESXi hosts booted with iSCSI using the VMware iSCSI software initiator need to be configured for core dumps to the ESXi Dump Collector that is part of vCenter. The Dump Collector is enabled by default on the vCenter appliance.

1. On the Management workstation, open the VMware vSphere CLI command prompt.
2. Set each iSCSI-booted ESXi host to coredump to the ESXi Dump Collector by running the following commands:

```
esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> system coredump network set --
interface-name vmk0 --server-ipv4 <<var_vcenter_server_ip> --server-port 6500
esxcli -s <<var_vm_host_infra_02_ip>> -u root -p <<var_password>> system coredump network set --
interface-name vmk0 --server-ipv4 <<var_vcenter_server_ip> --server-port 6500
esxcli -s <<var_vm_host_infra_03_ip>> -u root -p <<var_password>> system coredump network set --
interface-name vmk0 --server-ipv4 <<var_vcenter_server_ip> --server-port 6500
esxcli -s <<var_vm_host_infra_04_ip>> -u root -p <<var_password>> system coredump network set --
interface-name vmk0 --server-ipv4 <<var_vcenter_server_ip> --server-port 6500
```

```
esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> system coredump network set --
enable true
esxcli -s <<var_vm_host_infra_02_ip>> -u root -p <<var_password>> system coredump network set --
enable true
esxcli -s <<var_vm_host_infra_03_ip>> -u root -p <<var_password>> system coredump network set --
enable true
esxcli -s <<var_vm_host_infra_04_ip>> -u root -p <<var_password>> system coredump network set --
enable true
```

```
esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> system coredump network check
esxcli -s <<var_vm_host_infra_02_ip>> -u root -p <<var_password>> system coredump network check
```

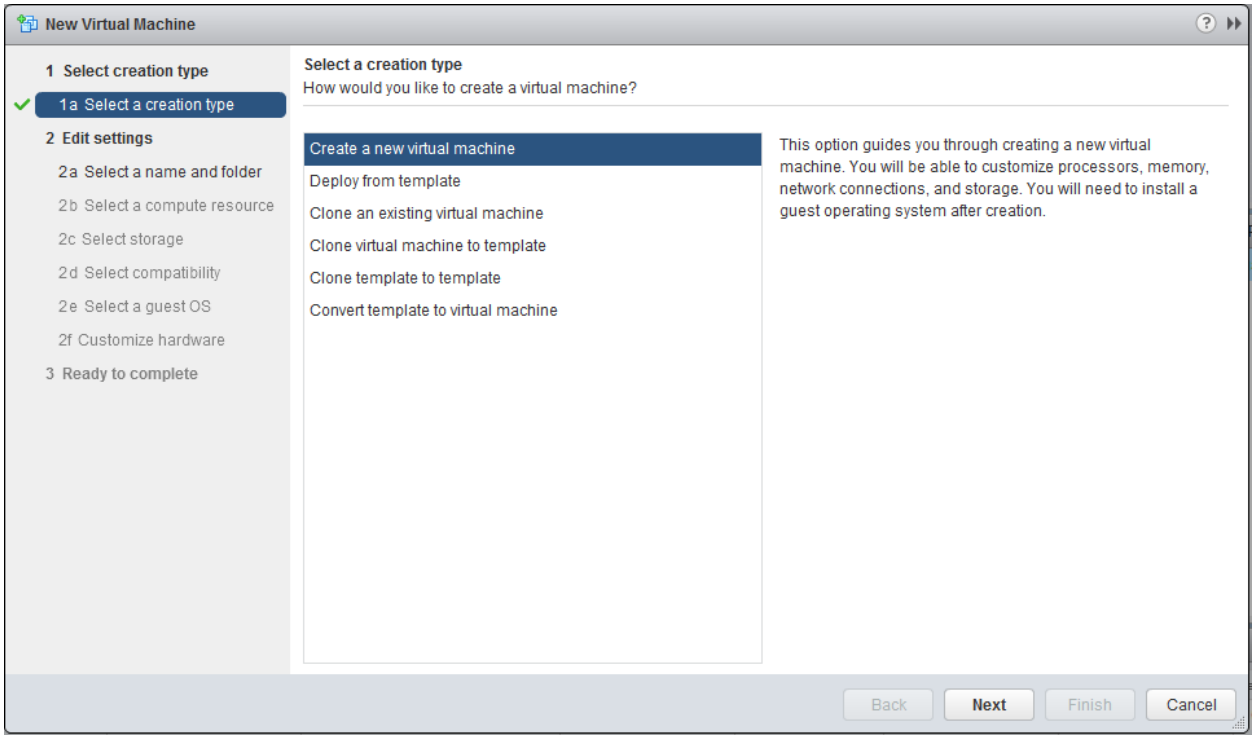
```
esxcli -s <<var_vm_host_infra_03_ip>> -u root -p <<var_password>> system coredump network check
esxcli -s <<var_vm_host_infra_04_ip>> -u root -p <<var_password>> system coredump network check
```

Setting Up a Microsoft Windows Template

To create a Microsoft Windows template, complete the following steps:

Note: Download Microsoft Windows 2012 R2 (64-bit) and upload it in a datastore.

1. Log in to the VMware vCenter Server by using the VMware vSphere Client.
2. In the VMware vSphere Client, navigate to vCenter Inventory Lists > Clusters > FlexPod_Express_Management.
3. Right-click the cluster and select New Virtual Machine.
4. Select Create a new virtual machine and click Next.

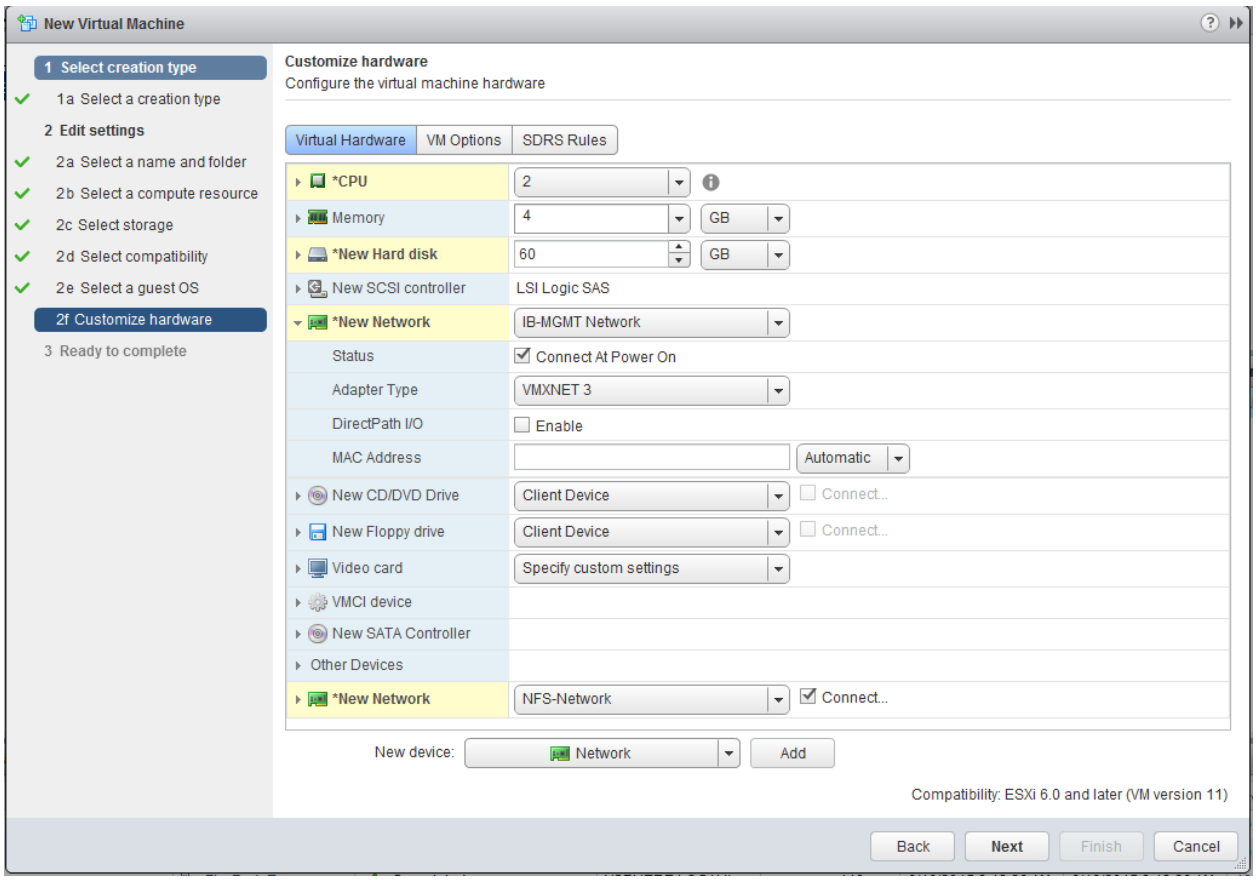


5. Enter a name for the virtual machine and select the FlexPod_Express_DC data center. Click Next.
6. Make sure that FlexPod_Express_Management cluster is selected and click Next.
7. Select `infra_datastore_1`. Click Next.
8. In the Select compatibility window, select ESXi6.0 and later. Click Next.
9. Verify that the Microsoft Windows option and the Microsoft Windows Server 2012 (64-bit) version are selected. Click Next.
10. Select the Virtual Hardware tab and customize the hardware as follows.
    a. Set the following:
    - CPU: 2
    - Memory: 4GB
    - New Hard Disk: 60GB
    - New Network: IB-MGMT Network

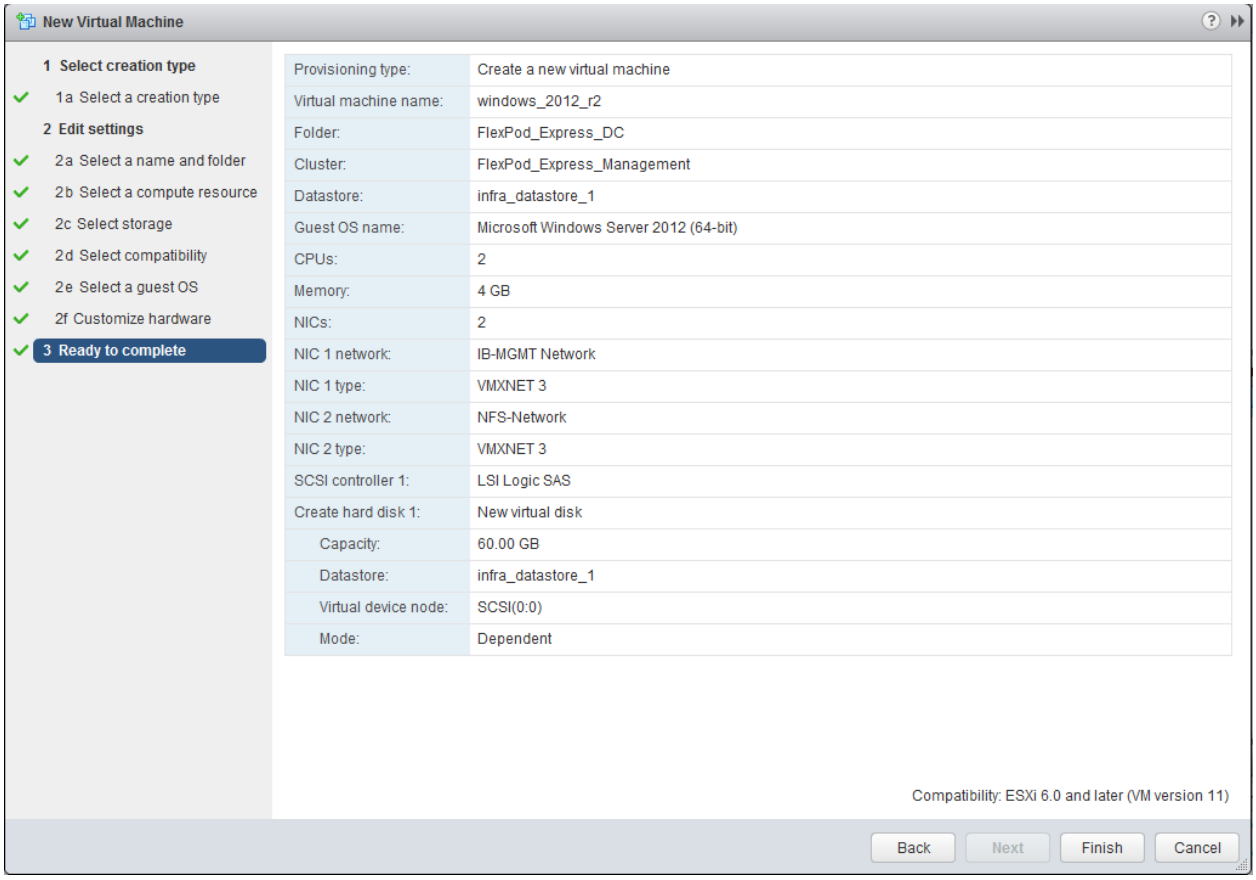
- Select Connect At Power On.
- Adapter Type: VMXNET 3

b. From the New device menu, select Network and click Add.

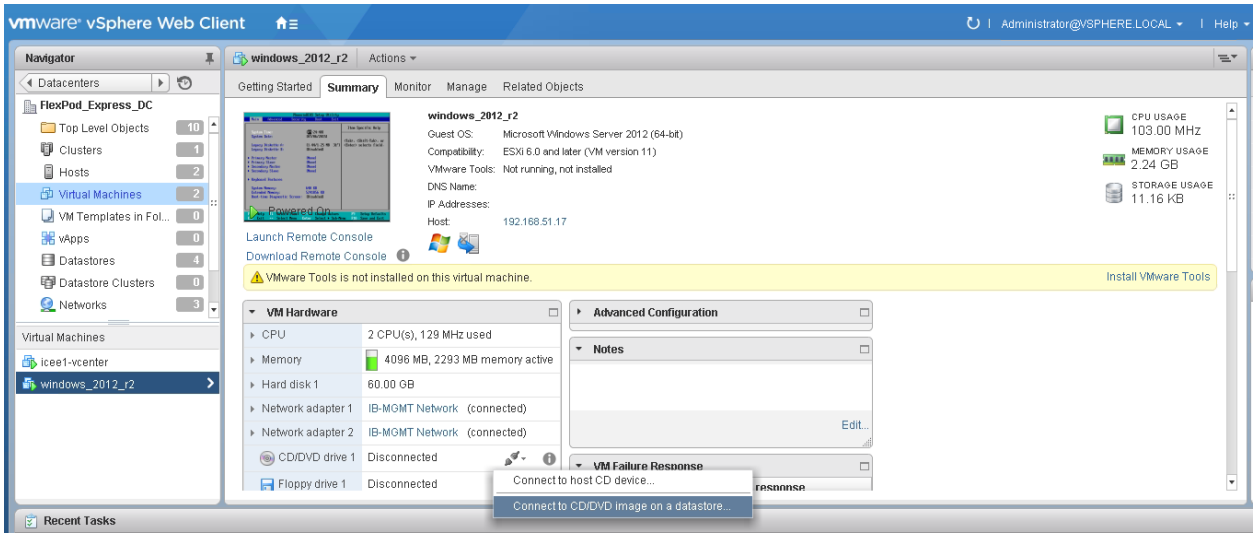
- New Network: IB-MGMT Network
- Select Connect At Power On.
- Adapter Type: VMXNET 3



11. Click the VM Options tab. Under Boot Options, select Force BIOS setup.
12. Click Next.
13. Review the virtual machine settings and click Finish.

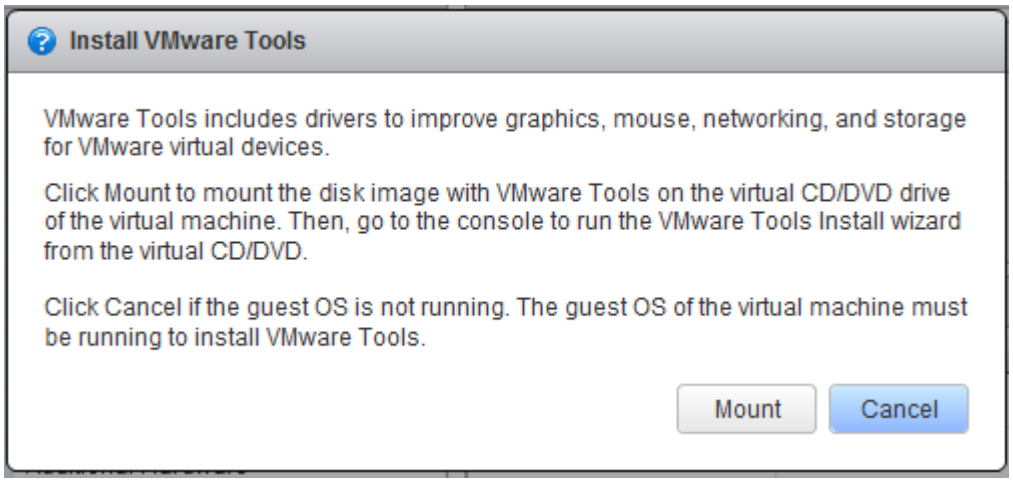


14. Navigate to vCenter Inventory Lists > Clusters > FlexPod_Express_Management.
15. In the Virtual Machines pane, select the newly created VM. In the center pane, click the Summary tab.
16. Right-click the VM and click Power on.
17. Right-click the virtual machine and select Open Console.
18. In the Summary tab, expand the VM Hardware section.
19. Click the plug icon next to “CD/DVD drive 1” and select Connect to CD/DVD image on a datastore.



20. Navigate to the Microsoft Windows 2012 ISO image.
21. From the VM console, click `Send Ctrl+Alt+Delete`.

    The Microsoft Windows installer starts.
22. Select the appropriate language, time and currency format, and keyboard. Click Next.
23. Click Install Now. Enter the product license key and click Next.
24. Select `Windows Server 2012 R2 Standard (Server with a GUI)` and click Next.
25. Read and accept the license terms and click Next.
26. Select Custom (advanced). Make sure that Disk 0 Unallocated Space is selected. Click Next to allow the Microsoft Windows installation to complete.
27. After the Microsoft Windows installation is complete and the virtual machine has rebooted, enter and confirm the administrator password. Click Finish.
28. Log in to the VM desktop.
29. From the vSphere Web Client, click `Install VMware Tools` in the VM Summary tab.
30. Click Mount.



31. If prompted to eject the Microsoft Windows installation media before running the setup for the VMware tools, click OK. Then click OK again.
32. From the connected CD drive, run setup64.exe.
33. In the VMware Tools installer window, click Next.
34. Make sure that Typical is selected and click Next.
35. Click Install.
36. If prompted to trust software from VMware, select the checkbox to always trust and click Install.
37. Click Finish.
38. Click Yes to restart the virtual machine.
39. After the reboot is complete, select `Send Ctrl+Alt+Del` and then enter the password to log in to the virtual machine.
40. Set the time zone for the virtual machine and the IP address, gateway, and host name.

    Note: A reboot is required.
41. Log back in to the virtual machine and download and install all required Microsoft Windows updates.

    Note: This process requires several reboots.

42. Right-click the virtual machine in VMware vCenter and click Clone to Template.
43. Enter the name `windows_2012_r2_template` for the clone.
44. Select the data center `FlexPod_Express_DC`. Click Next.
45. Select the cluster `FlexPod_Express_Management` as the target cluster to host the template. Click Next.
46. Select `infra_datastore_1`. Click Next.
47. Click Finish.

5.7 NetApp Virtual Storage Console 6.0 Deployment Procedure

This section provides detailed instructions to deploy NetApp Virtual Storage Console (VSC) 6.0.

NetApp VSC 6.0 Preinstallation Considerations

The following licenses are required to run NetApp VSC on storage systems that run clustered Data ONTAP 8.3:

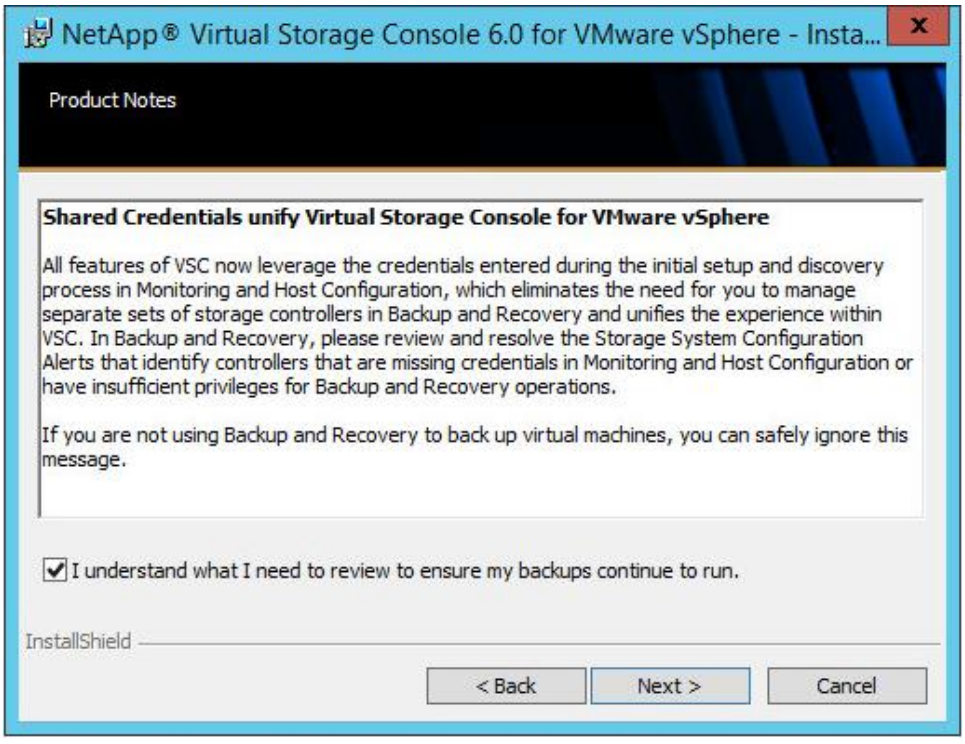
- Protocol licenses (NFS)
- NetApp SnapRestore (for backup and recovery)
- NetApp SnapManager Suite

Installing NetApp VSC 6.0

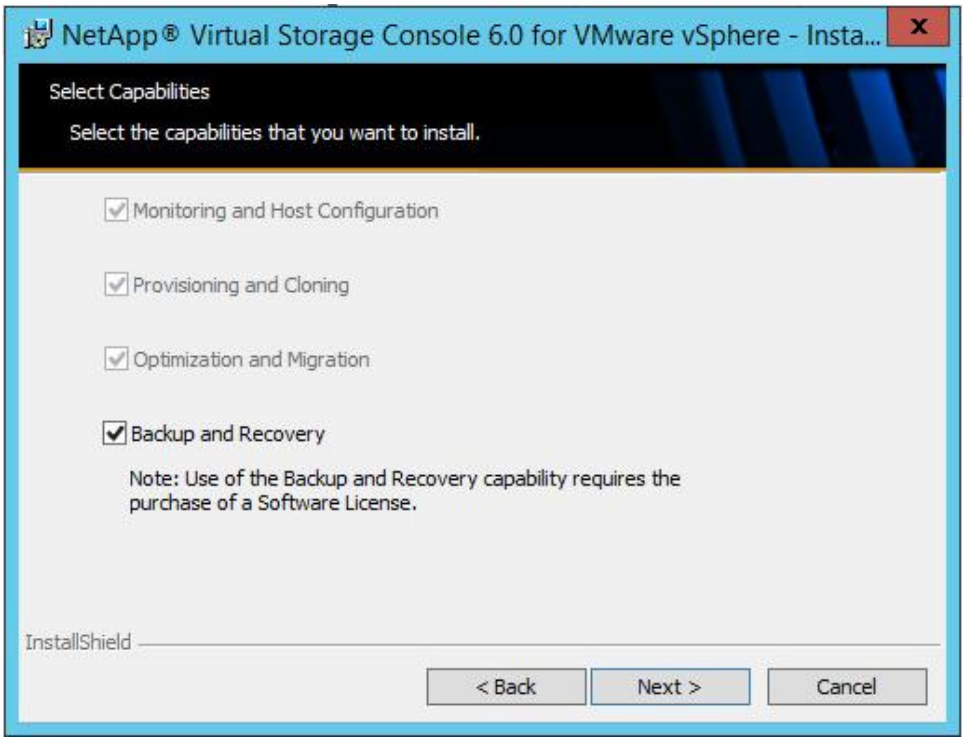
To install the VSC 6.0 software, complete the following steps:

1. Log in to the vCenter Server using the vSphere Client.
2. On the right-side pane, click VMs and Templates.
3. Select `windows_2012_r2_template` on the right pane, right-click it, and select `New VM from this Template`.
4. Provide a name for the VSC VM and select `FlexPod_Express_DC` as the location for the VM. Click Next.
5. Select the `FlexPod_Express_Management` cluster and click Next.
6. Select `infra_datastore_1` and click Next.
7. Click Next.
8. Review the VM settings and click Finish.
9. Select the newly created VM and select `Power on the virtual machine` on the right pane.
10. Right-click the VM and select `Open Console`.
11. Log in to the VM as administrator, assign an IP address, and join the machine to the Active Directory domain. Install the current version of Adobe Flash Player on the VM. Install all Windows updates on the VM.
12. Download the x64 version of the Virtual Storage Console 6.0 from the NetApp Support site.
13. Right-click the file downloaded and select `Run As Administrator`.
14. On the Installation wizard Welcome page, select the language and click OK.
15. Click Next.

16. Select the checkbox to accept the message and click Next.

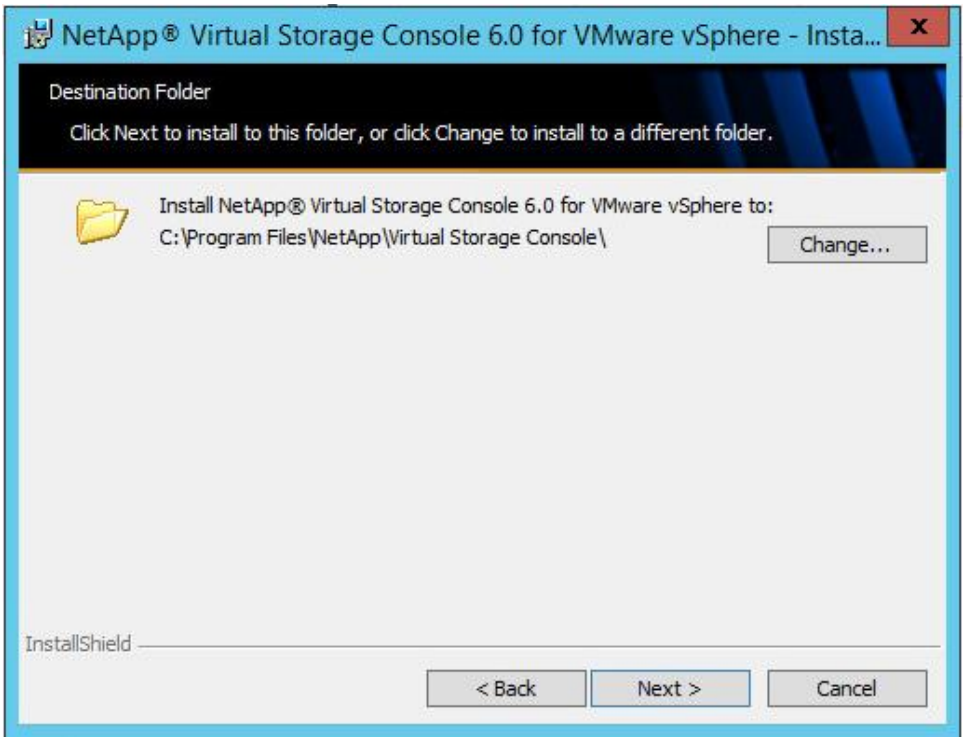


17. Select the backup and recovery capability and click Next.



Note: The backup and recovery capability requires an additional license.

18. Click Next to accept the default installation location.



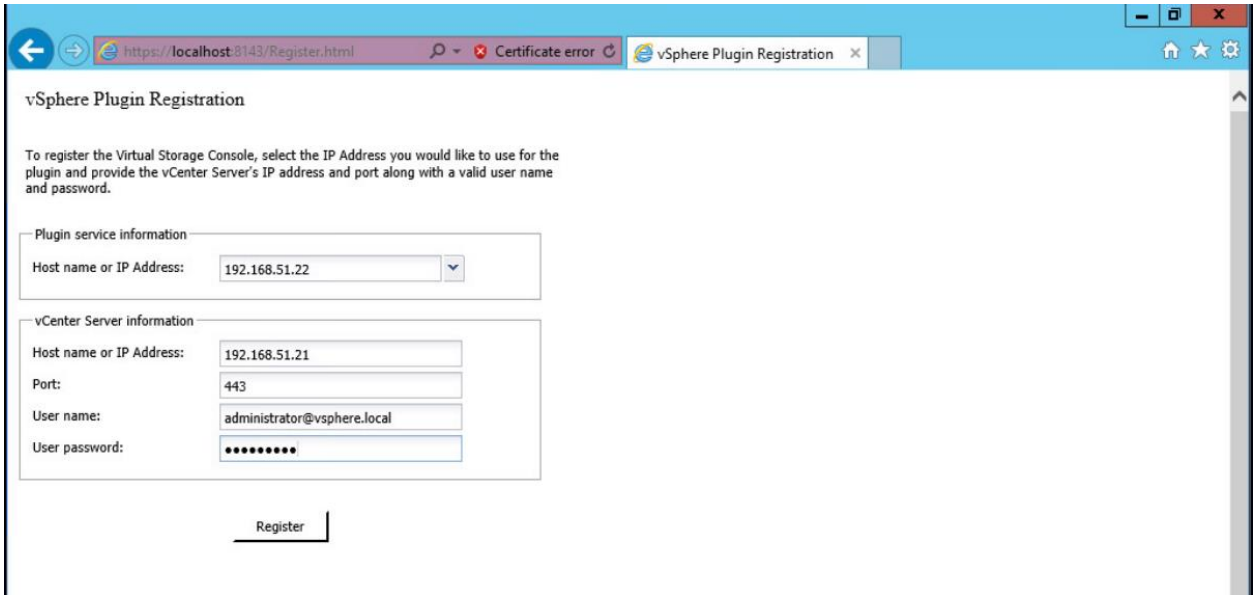
19. Click Install.

20. Click Finish.

Registering VSC with VMware vCenter Server

To register the VSC with the vCenter Server, complete the following steps:

1. A browser window with the registration URL opens automatically when the installation phase is complete. If it does not, open a browser on the VSC VM and navigate to `https://localhost:8143/Register.html`.
2. Click Continue to this website (not recommended).
3. In the Plug-in Service Information section, select the local IP address that the vCenter Server uses to access the VSC server from the drop-down list.
4. In the vCenter Server Information section, enter the host name or IP address, user name (SSO user name), and user password for the vCenter Server. Click Register to complete the registration.



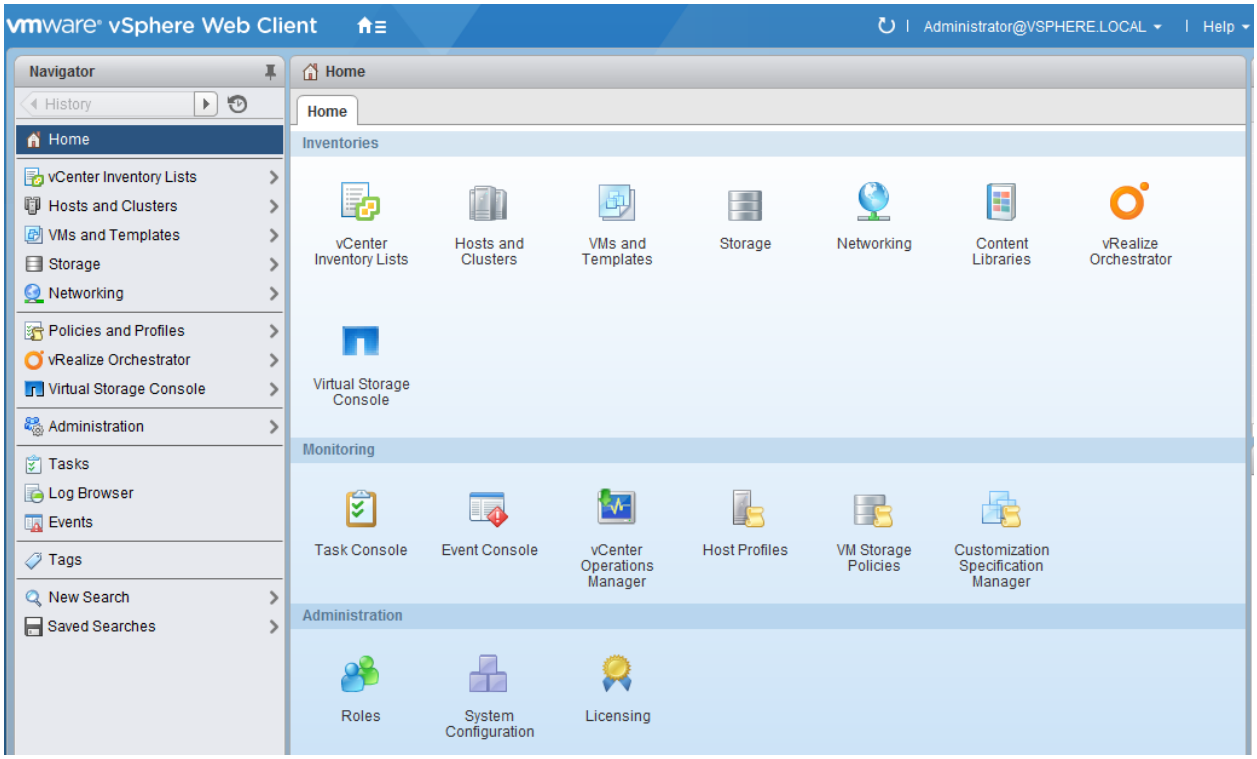
5. Upon successful registration, the storage controllers are discovered automatically.

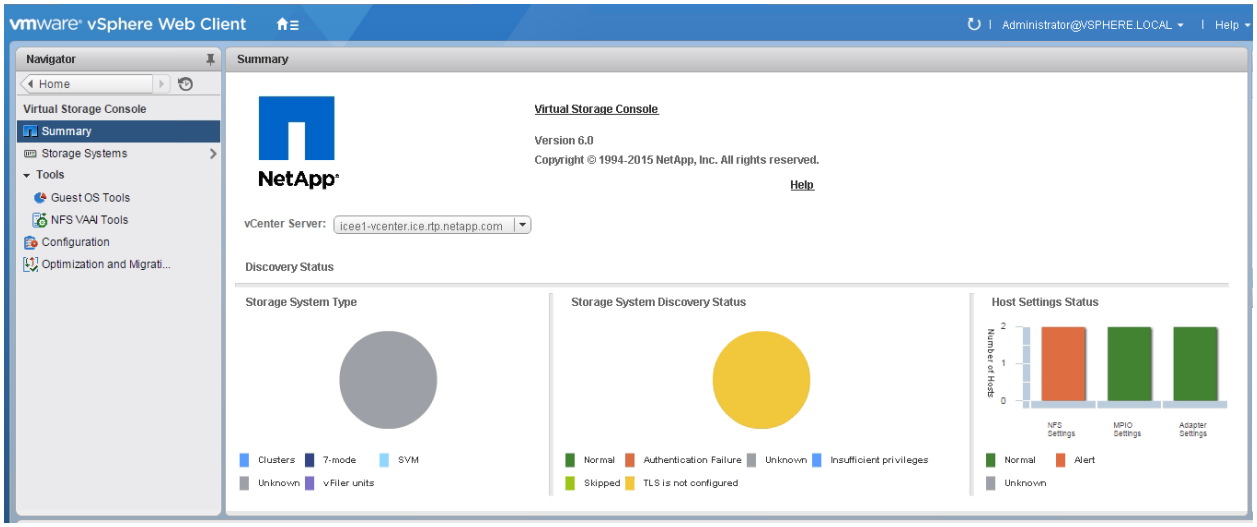
   Note: The storage discovery process takes some time.

Updating Credentials for Storage Resources

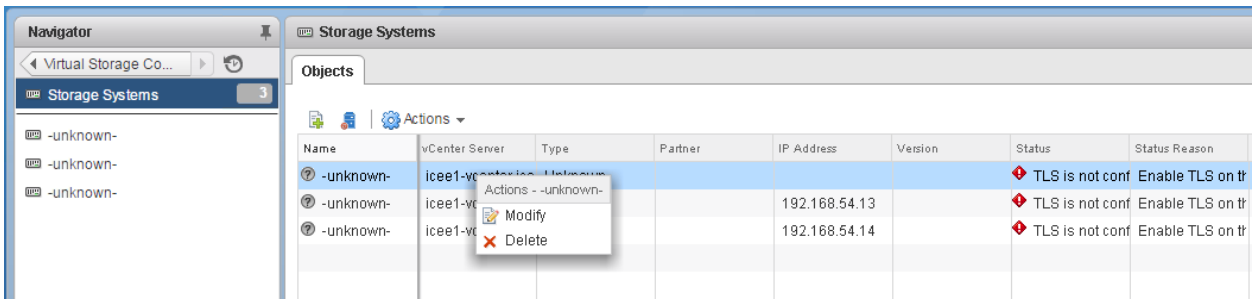
To discover storage resources for the Monitoring and Host Configuration and the Provisioning and Cloning capabilities, complete the following steps:

1. Using the vSphere Web Client, log in to the vCenter Server. If the vSphere Web Client was previously opened, close it and then reopen it.
2. In the Home screen, click the Home tab and click Virtual Storage Console.

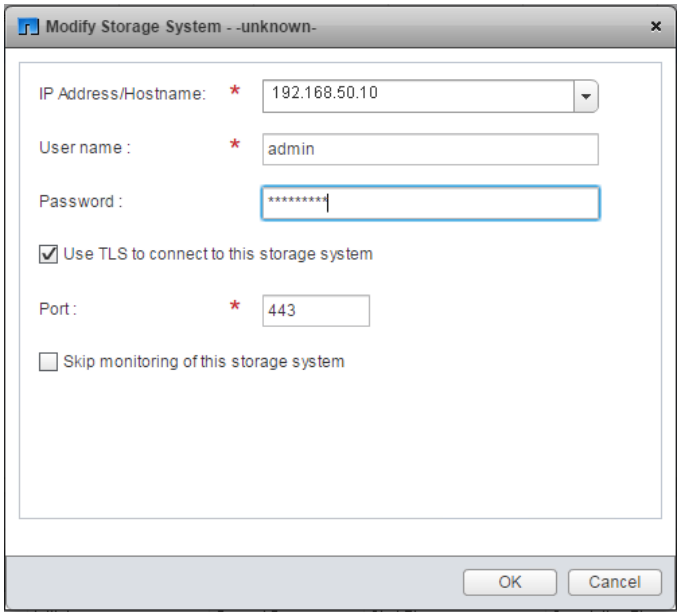




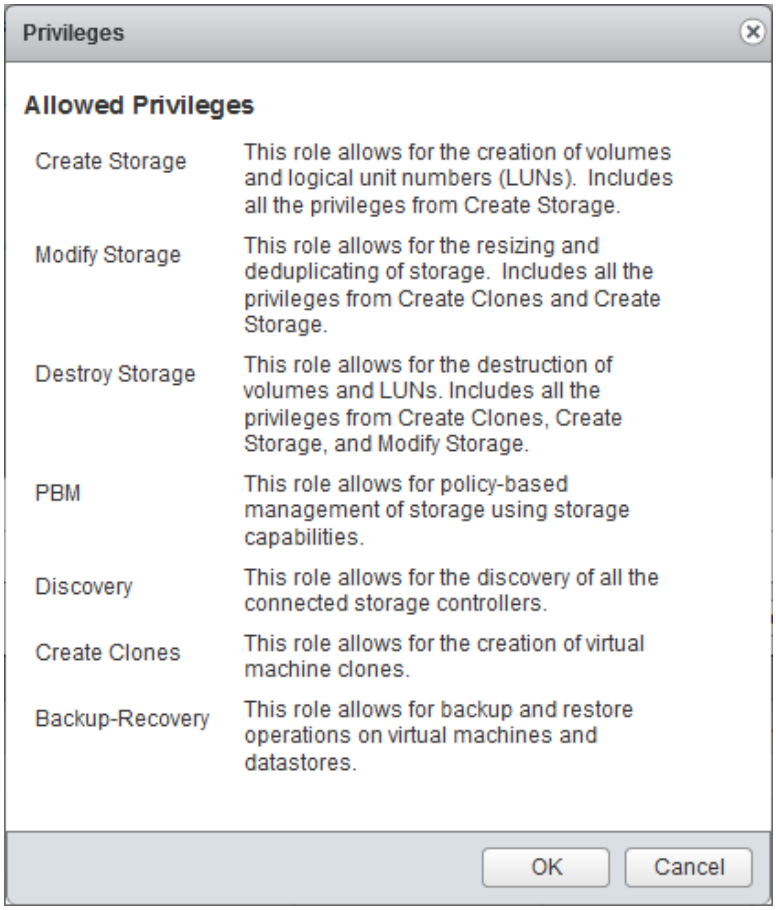
3. In the navigation pane, select Storage Systems if it is not selected by default.



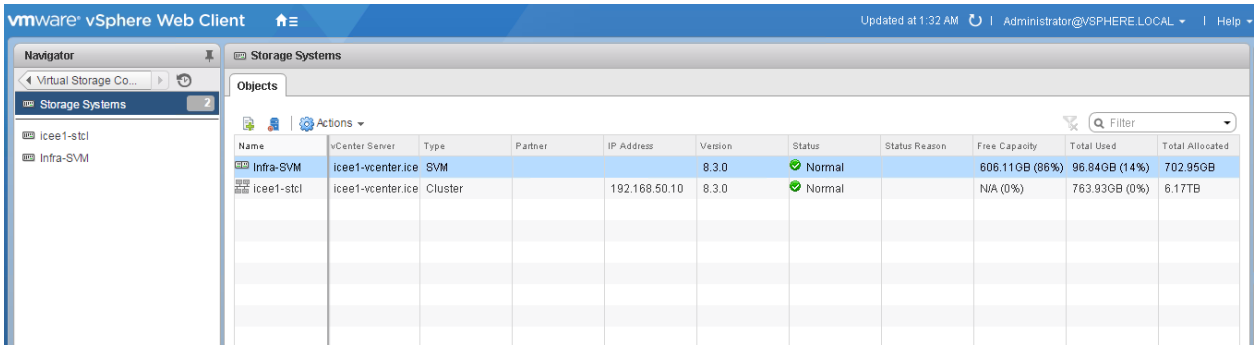
4. Right-click the unknown controller and select Modify.



5. Enter the storage cluster management IP address in the Management IP Address field. Enter admin for the user name and the admin password for the password. Make sure that Use SSL is selected. Click OK.



6. Click OK to accept the controller privileges.
7. Refresh the vSphere Web Client to view the updated information.

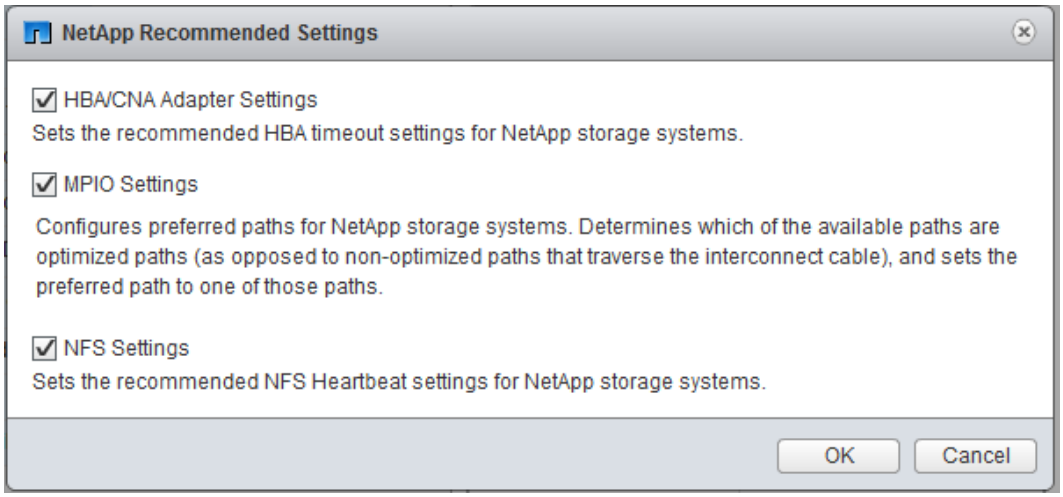


Optimal Storage Settings for VMware ESXi Hosts

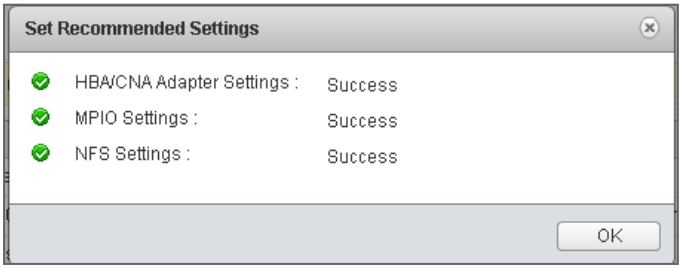
VSC enables the automated configuration of storage-related settings for all ESXi hosts that are connected to NetApp storage controllers. To use these settings, complete the following steps:

1. From the Home screen, click Hosts and Clusters. For each ESXi host, right-click and select NetApp VSC > Set Recommended Values for these hosts.
2. Check the settings that are to be applied to the selected vSphere hosts. Click OK to apply the settings.

Note: This functionality sets values for HBAs and CNAs, sets appropriate paths and path-selection plug-ins, and verifies appropriate settings for software-based I/O (NFS and iSCSI).



3. Click OK.



VSC 5.0 Backup and Recovery

Prerequisites to Use Backup and Recovery Capability

Check that the storage systems that contain the datastores and virtual machines for which you are creating backups have valid storage credentials. Check before you use the Backup and Recovery capability to schedule backups and restore your datastores, virtual machines, or virtual disk files.

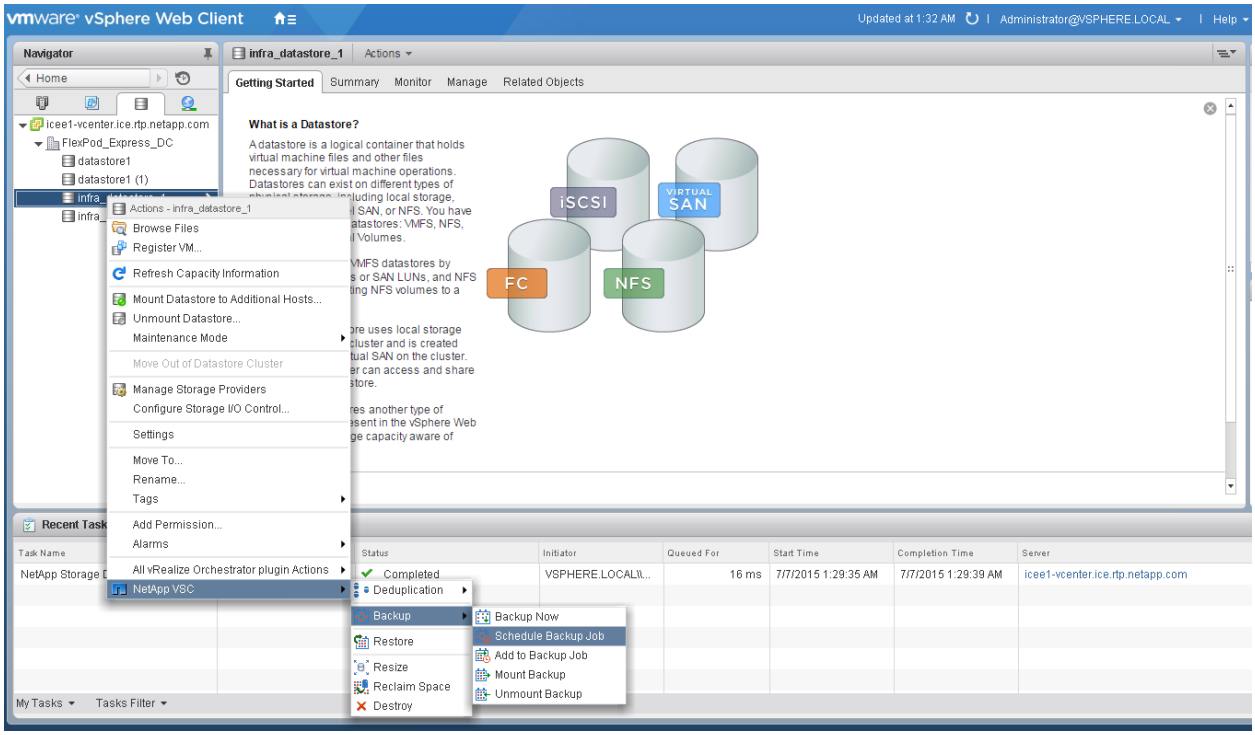
If you plan to use the SnapMirror update option, add all the destination storage systems with valid storage credentials.

Configuring Backup and Recovery

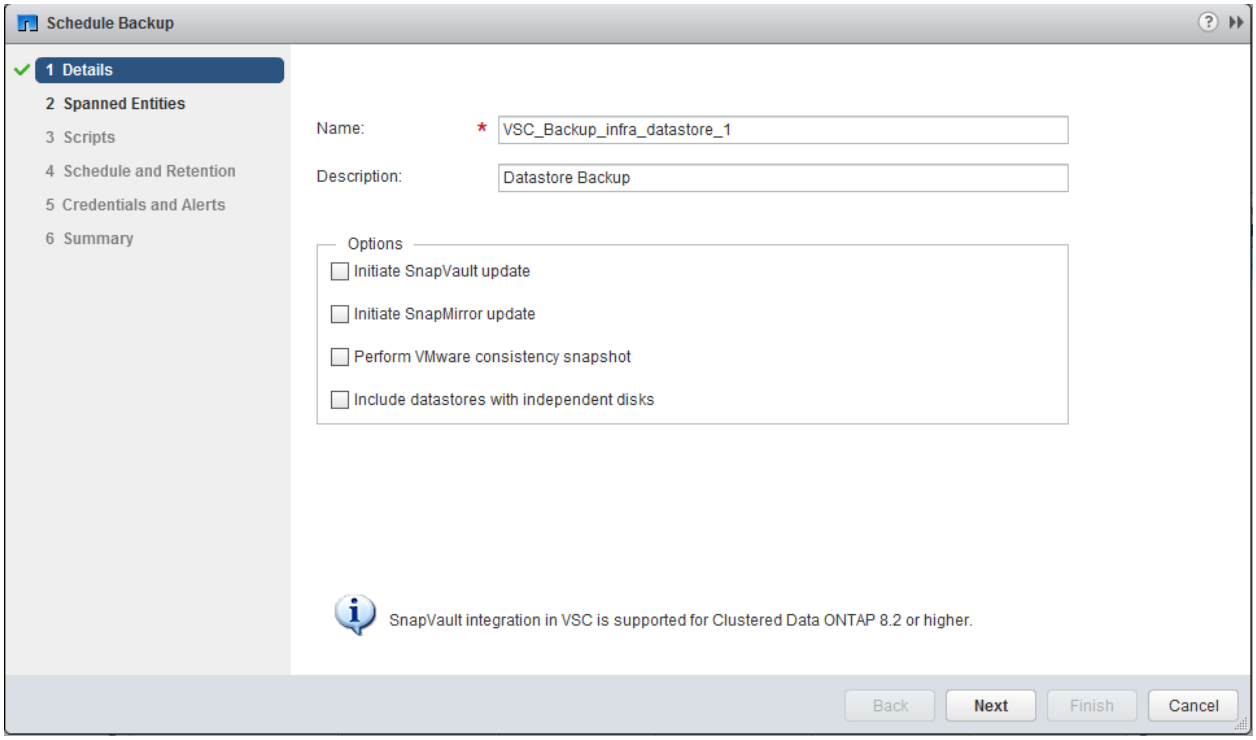
The following steps detail the procedure to configure a backup job for a datastore.

1. From the Home screen, click Storage in the Home tab.
2. Right-click the datastore that you need to back up. Select NetApp VSC > Backup > Schedule Backup Job.

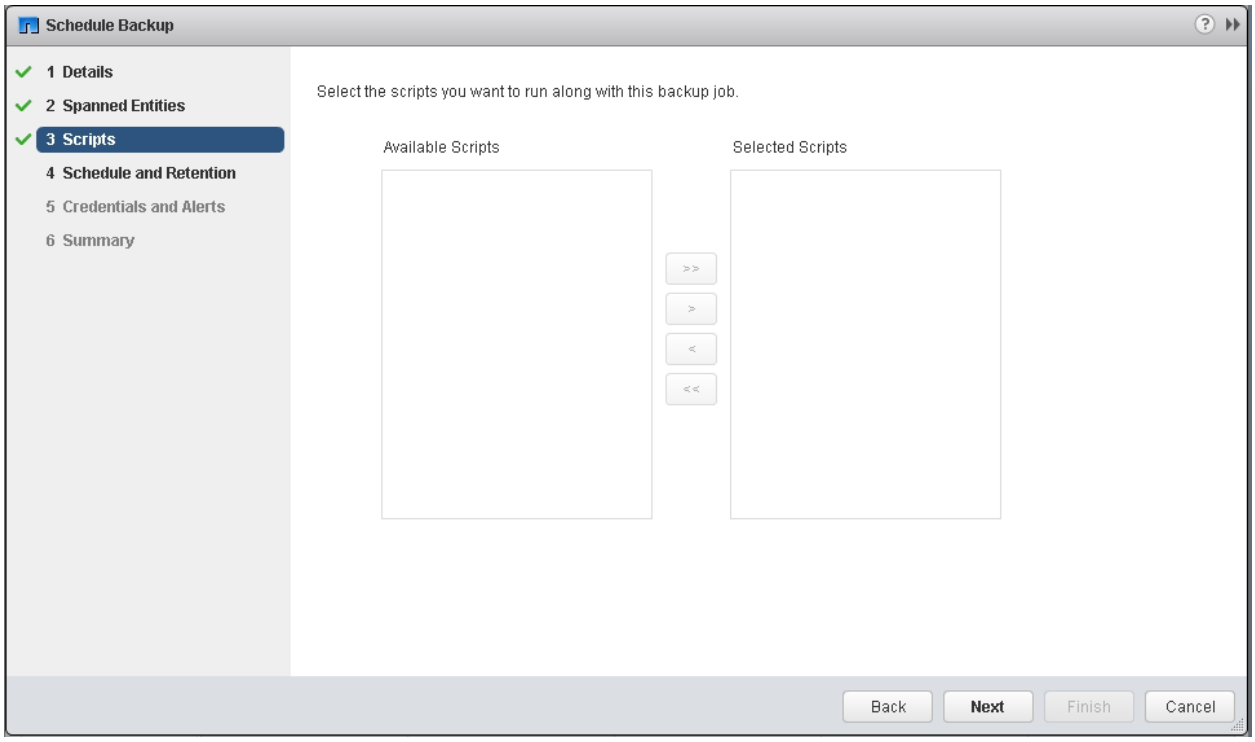
Note: If you prefer one-time backup, then choose Backup Now instead of Schedule Backup.



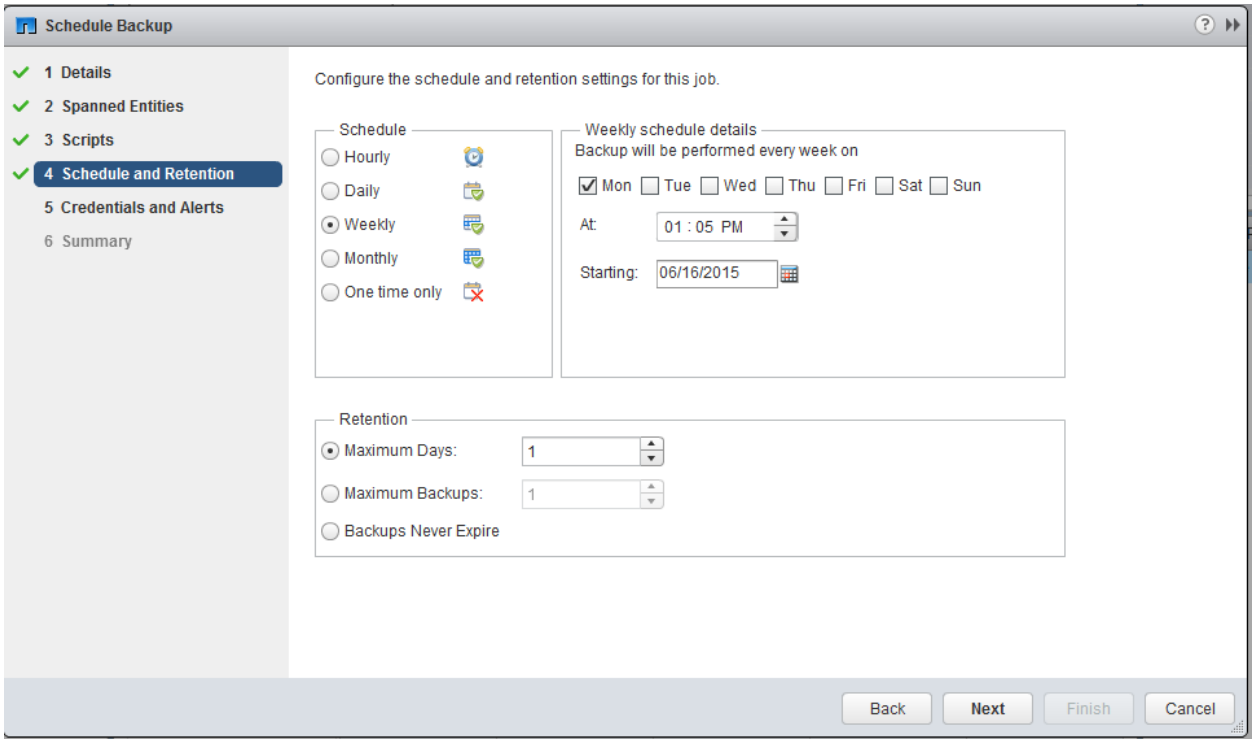
3. Type a backup job name and description.



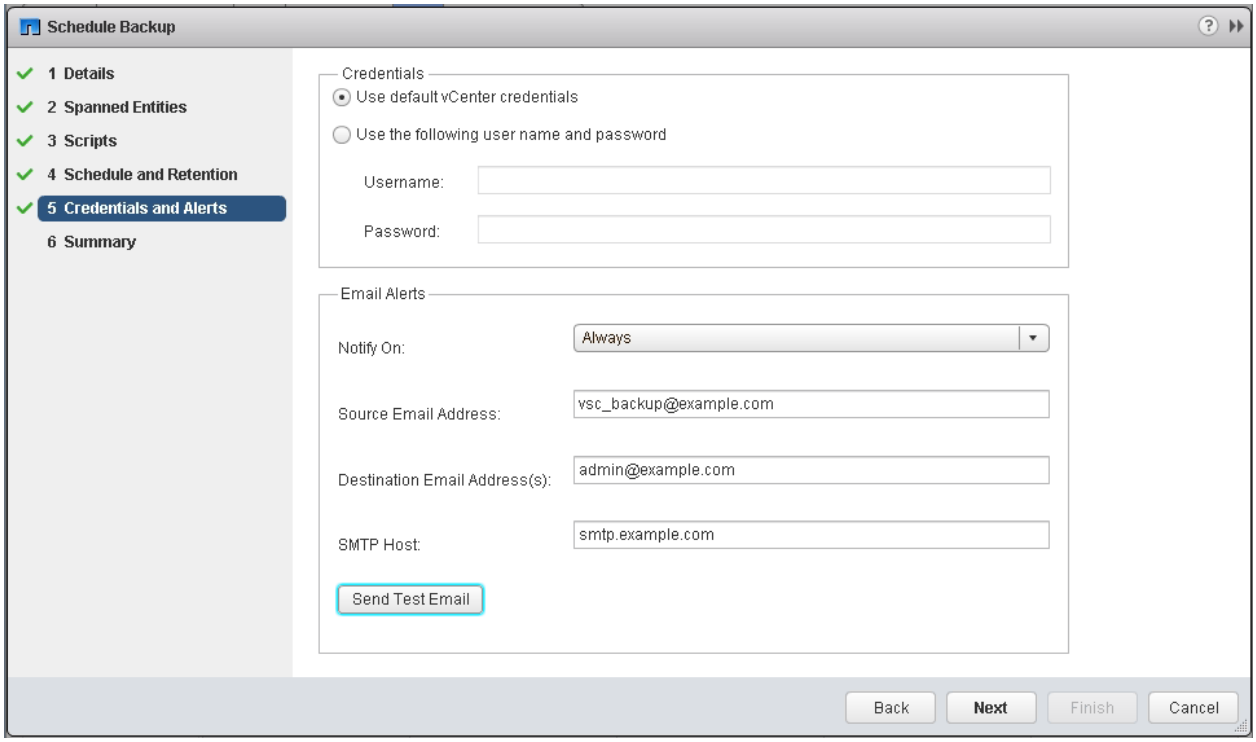
4. Click Next.
5. Click Next.
6. Select one or more backup scripts if available and click Next.



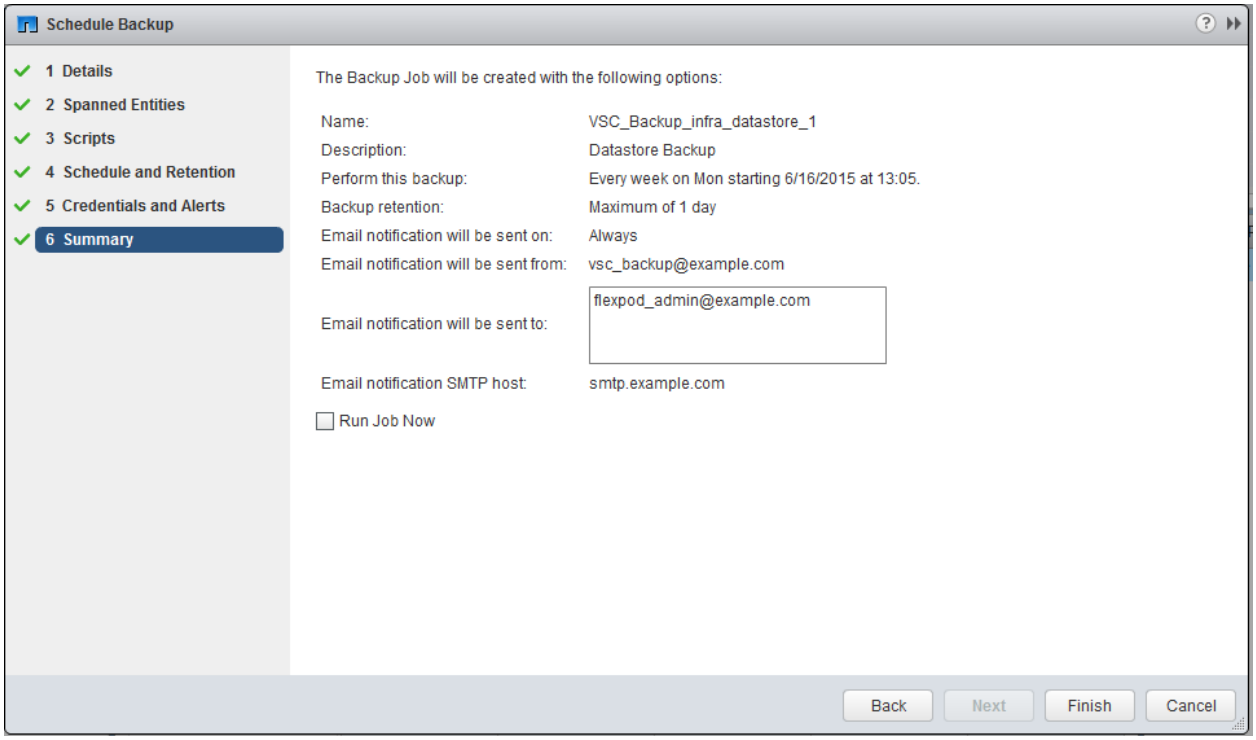
7. Select the hourly, daily, weekly, or monthly schedule that you want for this backup job and click Next.



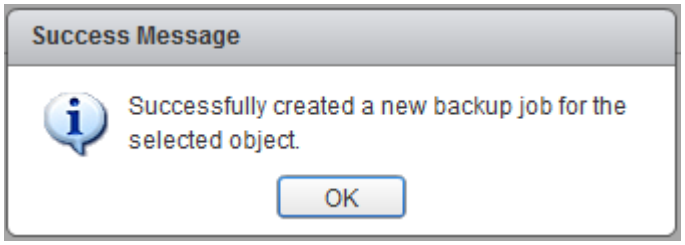
8. Use the default vCenter credentials or type the user name and password for the vCenter Server and click Next.
9. Specify backup retention details as per requirements. Enter an e-mail address for receiving e-mail alerts. You can add multiple e-mail addresses by using semicolons to separate e-mail addresses. Click Next.



10. Review the Summary page and click Finish. If you want to run the job immediately, select the Run Job Now option and then click Finish.



11. Click OK.



12. On the storage cluster interface, you can disable automatic Snapshot copies of the volume by typing this command:

```
volume modify –volume infra_datastore_1 –snapshot-policy none
```

13. To delete any existing automatic Snapshot copies that were created on the volume, type the following command:

```
volume snapshot show –volume infra_datastore_1
volume snapshot delete –volume infra_datastore_1 -snapshot *
Press Y to confirm deletion.
```

6 Bill of Materials

This section details the hardware and software components used in validating the large FlexPod Express configuration.

Table 6) Large configuration components.

Part Number	Product Description	Quantity Required
Cisco Components		
Network Switches		
N3K-C3524P-10G	Cisco Nexus 3524 24 10G Ports	2
N2200-PAC-400W	N2K/N3K AC Power Supply Std airflow (port side exhaust)	4
CAB-C13-C14-AC	Power cord C13 to C14 (recessed receptacle) 10A	4
N3548-24P-LIC	Cisco Nexus 3524 Factory Installed 24 port license	2
N3K-C3064-ACC-KIT	Cisco Nexus 3064PQ Accessory Kit	2
N3548-BAS1K9	Cisco Nexus 3500 Base License	2
NXA-FAN-30CFM-F	Cisco Nexus 2K/3K Single Fan forward airflow (port side exhaust)	8
N3KUK9-602A1.1D	NX-OS Release 6.0(2)A1(1d)	2
CON-SNT-3524P10G	Cisco SMARTNET 8X5XNBD Nexus 3524 24 10G Ports	2
Cisco UCS Compute		
UCSC-C220-M4L	UCS C220 M4 LFF w/o CPU mem HD PCIe PSU rail kit	4
UCS-CPU-E52640D	2.60 GHz E5-2640 v3/90W 8C/20MB Cache/DDR4 1866MHz	8
UCS-MR-1X162RU-A	16GB DDR4-2133-MHz RDIMM/PC4-17000/dual rank/x4/1.2v	32
UCSC-MLOM-CSC-02	Cisco UCS VIC1227 VIC MLOM - Dual Port 10Gb SFP+	4
CAB-C13-C14-AC	Power cord C13 to C14 (recessed receptacle) 10A	8
UCSC-PSU1-770W	770W AC Hot-Plug Power Supply for 1U C-Series Rack Server	8
UCSC-BBLKD-L	3.5-inch HDD Blanking Panel	16
UCSC-HS-C220M4	Heat sink for UCS C220 M4 rack servers	8
UCSC-RAILB-M4	Ball Bearing Rail Kit for C220 M4 and C240 M4 rack servers	4
C1UCS-OPT-OUT	Cisco ONE Data Center Compute Opt Out Option	4
CON-SNT-C220M4L	SMARTNET 8X5XNBD UCS C220 M4 LFF w/o CPU mem HD	4
NetApp Components		
FAS2552A-001-R6	FAS2552 High Availability System	2
X80101A-R6-C	Bezel,FAS2552,R6,-C	1
FAS2552-213-R6-C	FAS2552,24x900GB,10K,-C	1
X1558A-R6-C	Power Cable,In-Cabinet,48-IN,C13-C14,-C	2
SVC-FLEXPOD-SYSTEMS	Systems Used in FlexPod Solution, Attach PN	1
X6560-R6-C	Cable,Ethernet,0.5m RJ45 CAT6,-C	1

NetApp Components		
X1983-3-R6	Cable,Twinax CU,SFP+,3M,X1962/X1963/X1968	4
X6557-EN-R6-C	Cbl,SAS Cntlr-Shelf/Shelf-Shelf/HA,0.5m,EN,-C	2
X6566B-2-R6	Cable,Direct Attach CU SFP+ 10G,2M	2
DOC-2552-C	Documents,2552,-C	1
X5526A-R6-C	Rackmount Kit,4-Post,Universal,-C,R6	1
OS-ONTAP-CAP2-1P-C	OS Enable,Per-0.1TB,ONTAP,Perf-Stor,1P,-C	216
SWITCHLESS	2-Node Switchless Cluster	1
SW-2-2552A-SMGR-C	SW-2,SnapManager Suite,2552A,-C	2
SW-2-2552A-SRESTORE-C	SW-2,SnapRestore,2552A,-C	2
SW-2-2552A-FLEXCLN-C	SW-2,FlexClone,2552A,-C	2
SW-2-2552A-ISCSI-C	SW-2,iSCSI,2552A,-C	2
SW-ONTAP8.2.2-CLM	SW,Data ONTAP8.2.2,Cluster-Mode	2
SW-2-2552A-CIFS-C	SW-2,CIFS,2552A,-C	2
SW-2-2552A-NFS-C	SW-2,NFS,2552A,-C	2
SVC-A2-IN-NBR-E	HW Support,Standard2 Replace,Inst,NBD,e	1
SW-SSP-A2-IN-NBR-E	SW Subs,Standard2 Replace,Inst,NBD,e	1
SVC-INST-A2-IN1-NBR-E	Initial Install,Standard2 Replace,Inst,NBD,e	1
CS-OS-SUPPORT-ONTAP	OS Support Entitlement, ONTAP	1
SES-SYSTEM	SupportEdge Standard, Premium, or equivalent service from an authorized support services partner[1]	1

Note: The 1Gb management connection to the Cisco Nexus 3524 requires GLC-Ts.

7 Conclusion

FlexPod Express is the optimal shared infrastructure foundation on which to deploy a variety of IT workloads. Cisco and NetApp created a platform that is both flexible and scalable for multiple use cases and applications. One common use case is to deploy VMware vSphere as the virtualization solution, as described in this document. The flexibility and scalability of FlexPod also enable customers to start out

[1] SupportEdge Premium is required for cooperative support.

with a right-sized infrastructure that can ultimately grow with and adapt to their evolving business requirements.

References

This report refers to the following documents and resources:

- NetApp FAS2500 Storage
  http://www.netapp.com/in/products/storage-systems/fas2500/
- Cisco UCS C-Series Rack Servers
  http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-c-series-rack-servers/index.html
- Cisco UCS Virtual Interface Card 1227
  http://www.cisco.com/c/en/us/products/interfaces-modules/ucs-virtual-interface-card-1227/index.html
- VMware vSphere
  http://www.vmware.com/in/products/vsphere
- Interoperability Matrix Tools
  - VMware and Cisco UCS
    http://www.vmware.com/resources/compatibility/search.php
  - NetApp, Cisco UCS, and VMware
    http://support.netapp.com/matrix

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.

NVA-0017-DEPLOY-0915