Technical Report

FlexPod Express with Microsoft Windows Server 2012 R2 Hyper-V: Large Configuration

Implementation Guide

Glenn Sizemore, Arvind Ramakrishnan, Karthick Radhakrishnan, NetApp
Jeffrey Fultz, Cisco Systems

October 2014 | TR-4350

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Overview

The large NetApp® FlexPod® Express configuration is a low-cost, standardized infrastructure solution developed to meet the needs of small and midsize businesses. The configuration has been built and tested to deliver a cost-effective, high-value, best-practice architecture. The configuration provides a standardized base platform capable of running a number of business-critical applications while providing scalability options to enable the infrastructure to grow with the demands of the business. The large FlexPod Express configuration is built on an end-to-end 10GbE network infrastructure.

2 Audience

This document describes the architecture and deployment procedures for the large FlexPod Express configuration with the NetApp clustered Data ONTAP® operating system. The intended audience for this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, partner engineers, and customers who want to deploy FlexPod Express.

3 Architecture

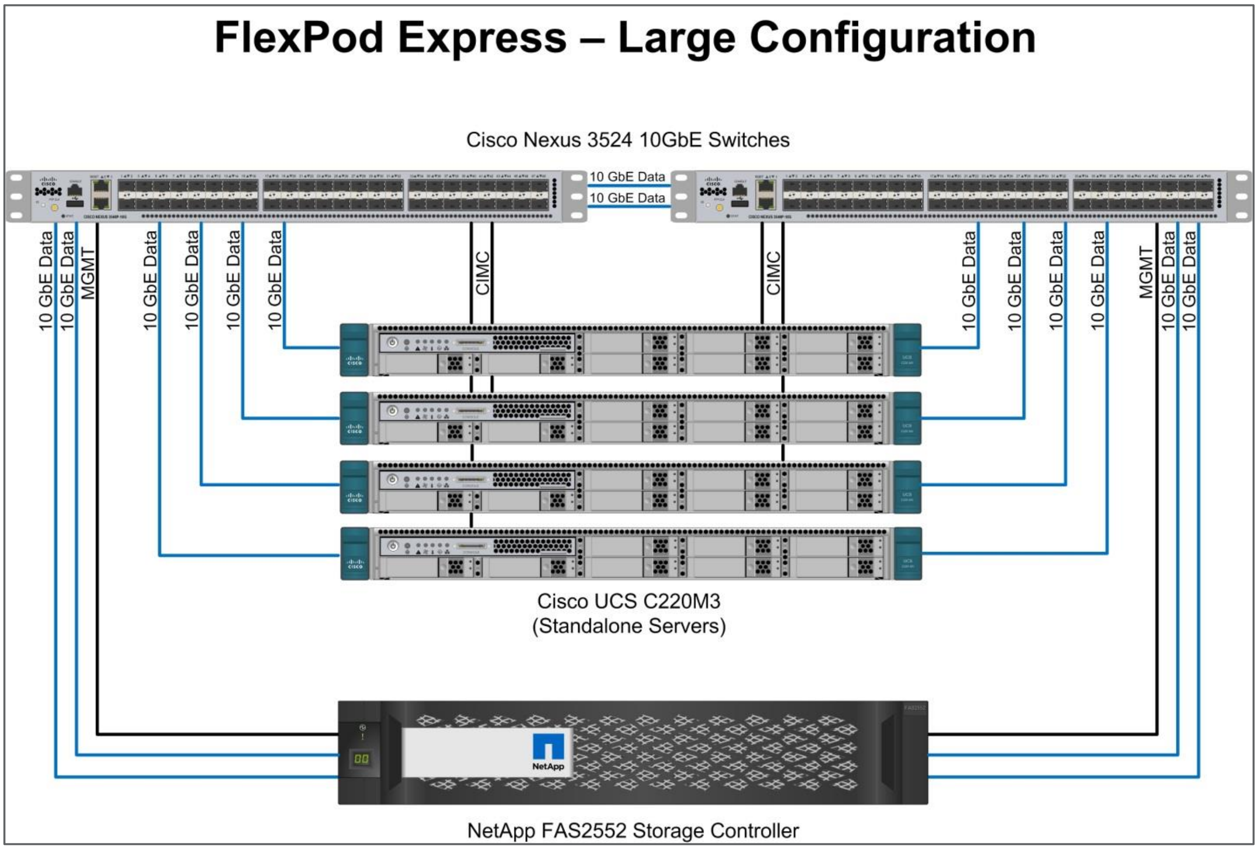
The large FlexPod Express configuration uses Cisco UCS® C-Series rack servers, Cisco Nexus® switches, and NetApp FAS storage (NetApp clustered Data ONTAP: switchless). Although FlexPod Express supports an open ecosystem of virtualization and management software solutions, the architecture described in this document specifically includes Microsoft® Windows Server® 2012 R2 Hyper-V® virtualization and Microsoft System Center Virtual Machine Manager software. NetApp strongly recommends virtualization software and infrastructure management software as part of every FlexPod Express deployment. The configuration uses the best practices for each component to enable a reliable, enterprise-class infrastructure.

3.1 Large Configuration

The large configuration consists of the following components (Figure 1):

- Cisco Nexus 3524 switches
- Cisco UCS C220 M3 rack servers
- NetApp FAS2552 storage controllers
- Microsoft Windows Server 2012 R2
- Microsoft System Center Virtual Machine Manager 2012 R2

Figure 1) Physical topology of FlexPod Express large configuration.



4 Hardware Details

4.1 Large Configuration

Table 1 details the hardware and software configuration of a large FlexPod Express configuration.

Table 1) Small configuration details.

Layer	Component	Quantity
Computing	Cisco UCS C220 M3 Rack Servers (standalone)	4
Network	Cisco Nexus 3524 Switches	2
Storage	NetApp FAS2552 (high-availability pair)	1
Disks	900GB 10,000-rpm SAS	24

5 Software Details

It is important to note the software versions used in this document. Table 2 details the software revisions used throughout this document.

Table 2) Software details.

Layer	Component	Version	Details
Computing	Cisco UCS C220 M3 Rack Servers	2.0(1a)	Cisco Integrated Management Controller (IMC) software
Network	Cisco Nexus 3524 Gigabit Ethernet switches	6.0(2)A1(1d)	Cisco NX-OS Software
Storage	NetApp FAS2552 HA	8.2.2	NetApp Data ONTAP software
Software	Microsoft Windows Server 2012 R2 Hyper-V	2012 R2	Virtualization Hypervisor
	System Center Virtual Machine Manager	2012 R2	Virtualization Management
	NetApp Data ONTAP SMI-S Agent	5.1.2	SMI-S Agent
	NetApp Windows® Host Utilities Kit	6.0.2	NetApp plug-in for Windows
	NetApp SnapDrive® for Windows	7.0.3	LUN provisioning and Snapshot® management
	NetApp SnapManager® for Hyper-V	2.0.3	NetApp plug-in for Hyper-V

6 Configuration Guidelines

This document provides details for configuring a fully redundant, highly available FlexPod Express system. To reflect this redundancy, the component being configured in each step is 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 with this document, and Switch A and Switch B identify the pair of Cisco Nexus switches that are configured.

Additionally, this document details steps for provisioning multiple Cisco UCS hosts, and these are identified sequentially: 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 is intended 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 VLAN schemes. Table 3 describes the VLANs necessary 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 3) Required VLANs.

VLAN Name	VLAN Purpose	ID Used in Validating This Document
Native	VLAN to which untagged frames are assigned	2
Management	VLAN for management interfaces	3051
LiveMigration	VLAN designated for the movement of VMs from one physical host to another	3052

VLAN Name	VLAN Purpose	ID Used in Validating This Document
VM traffic	VLAN for virtual machine application traffic	3053
SMB	VLAN for SMB traffic	3054
Cluster	VLAN for cluster communication	3055

Table 4 lists the Virtual Machines that will be created during this deployment.

Table 4) Virtual machines created.

Virtual Machine Description	Host Name
System Center 2012 R2 Virtual Machine Manager	
NetApp SMI-S Agent	

Use Table 5 to gather all the necessary information required during the deployment.

Table 5) Deployment variables.

Variable	Description	Customer Implementation Value
`<<admin_password>>`	Global default administrative password	
`<<switch_A_hostname>>`	Cisco Nexus A host name	
`<<switch_A_mgmt0_ip_addr>>`	Cisco Nexus A management IP address	
`<<switch_A_mgmt0_netmask>>`	Cisco Nexus A netmask	
`<<switch_B_hostname>>`	Cisco Nexus B host name	
`<<switch_B_mgmt0_ip_addr>>`	Cisco Nexus B management IP address	
`<<switch_B_mgmt0_netmask>>`	Cisco Nexus B netmask	
`<<smb_vlan_id>>`	SMB VLAN ID	
`<<cluster_vlan_id>>`	Cluster communication VLAN ID	
`<<vmotion_vlan_id>>`	LiveMigration VLAN ID	
`<<vmtraffic_vlan_id>>`	Virtual machine traffic VLAN ID	
`<<ib_mgmt_vlan_id>>`	Management VLAN ID	
`<<native_vlan_id>>`	Native VLAN ID	

Variable	Description	Customer Implementation Value
<<inband_mgmt_ip_address>>	In-band management IP addresses for switch A and B virtual interface (SVI)	
<<inband_mgmt_netmask>>	In-band management netmask for SVI	
<<inband_mgmt_gateway>>	In-band management gateway for SVI	
<<controller01_mgmt_ip>>	Management IP address for Controller 01	
<<controller01_mgmt_netmask>>	Controller 01 management netmask	
<<controller01_mgmt_gateway>>	Controller 01 management gateway	
<<controller02_mgmt_ip>>	Management IP address for Controller 02	
<<controller02_mgmt_netmask>>	Controller 02 management netmask	
<<controller02_mgmt_gateway>>	Controller 02 management gateway	
<<url_boot_software>>	Data ONTAP 8.2 URL; format: http://	
<<dns_domain_name>>	Domain Name System (DNS) domain name	
<<nameserver_ip>>	DNS server IP addresses	
<<controller_location>>	Physical location for each controller device	
<<controller01>>	Controller 01 host name	
<<#_of_disks>>	Number of disks to assign to each storage controller	
<<controller02>>	Controller 02 host name	
<<num_disks>>	Number of disks to assign to storage data aggregate	
<<controller01_sp_ip>>	Controller 01 service processor IP address	
<<controller01_sp_netmask>>	Controller 01 service processor netmask	
<<controller01_sp_gateway>>	Controller 01 service processor gateway	

Variable	Description	Customer Implementation Value
<<controller02_sp_ip>>	Controller 02 -service processor IP address	
<<controller02_sp_netmask>>	Controller 02 service processor netmask	
<<controller02_sp_gateway>>	Controller 02 service processor gateway	
<<timezone>>	FlexPod Express time zone	
<<global_ntp_server_ip>>	Network Time Protocol (NTP) server IP address	
<<snmp_contact>>	Storage administrator email address	
<<snmp_location>>	Storage location string	
<<snmp_trap_server_fqdn>>	Fully qualified domain name (FQDN) of fault management system or NetApp DFM	
<<snmp_community>>	Simple Network Management Protocol Version 1 and 2 (SNMP v1 and v2) community name	
<<mailhost>>	Mail server host name	
<<storage_admin_email>>	Storage administrator email address	
<<country_code>>	Two-letter country code	
<<state>>	State or province name	
<<city>>	City name	
<<org>>	Organization or company name	
<<unit>>	Organizational unit name	
<<cimc_server1_ip>>	Cisco IMC IP address for Cisco UCS C220 M3 Server-1	
<<cimc_server2_ip>>	Cisco IMC IP address for Cisco UCS C220 M3 Server-2	
<<cimc_server3_ip>>	Cisco IMC IP address for Cisco UCS C220 M3 Server-3	
<<cimc_server4_ip>>	Cisco IMC IP address for Cisco UCS C220 M3 Server-4	

Variable	Description	Customer Implementation Value
<<cimc_netmask>>	Cisco IMC netmask for Cisco UCS C220 M3 servers	
<<cimc_gateway>>	Cisco IMC gateway for Cisco UCS C220 M3 servers	
<<clustername>>	Storage cluster host name	
<<cluster_base_license_key>>	Cluster base license key	
<<clustermgmt_ip>>	Cluster management IP address for the storage cluster	
<<clustermgmt_netmask>>	Cluster management netmask for the storage cluster	
<<clustermgmt_gateway>>	Cluster management gateway for the storage cluster	
<<controller01_rootaggrname>>	Root aggregate name of Controller 01	
<<security_cert_vserver_common_name>>	Infrastructure virtual server (Vserver) FQDN	
<<security_cert_cluster_common_name>>	Storage cluster FQDN	
<<security_cert_controller01_common_name>>	Controller 01 FQDN	
<<security_cert_controller02_common_name>>	Controller 02 FQDN	
<<security_certificate_vservser_authority>>	Infrastructure Vserver security certificate authority	
<<security_certificate_vserver_serial_no>>	Infrastructure Vserver security certificate serial number	
<<security_certificate_cluster_authority>>	Storage cluster security certificate authority	
<<security_certificate_cluster_serial_no>>	Storage cluster security certificate serial number	
<<security_certificate_controller01_authority>>	Controller 01 security certificate authority	
<<security_certificate_controller01_serial_no>>	Controller 01 security certificate serial	
<<security_certificate_controller02_authority>>	Controller 02 security certificate authority	
<<security_certificate_controller02_serial_no>>	Controller 02 security certificate serial	

Variable	Description	Customer Implementation Value
<<controller01_smb_lif_ip>>	Controller 01 SMB logical interface (LIF) IP address	
<<controller02_smb_lif_ip>>	Controller 02 SMB LIF IP address	
<<controller01_smb_lif_netmask>>	Controller 01 SMB LIF netmask	
<<controller02_smb_lif_netmask>>	Controller 02 SMB LIF netmask	
<<vserver_mgmt_ip>>	Management IP address for Vserver	
<<vserver_mgmt_netmask>>	Subnet mask for Vserver	
<<vsadmin_password>>	Password for Vserver administrator account	

7 FlexPod Express Cabling Information

Figure 2 provides a cabling diagram for the FlexPod Express large configuration, and Table 6 provides the cabling information.

Figure 2) FlexPod Express large configuration cabling diagram.

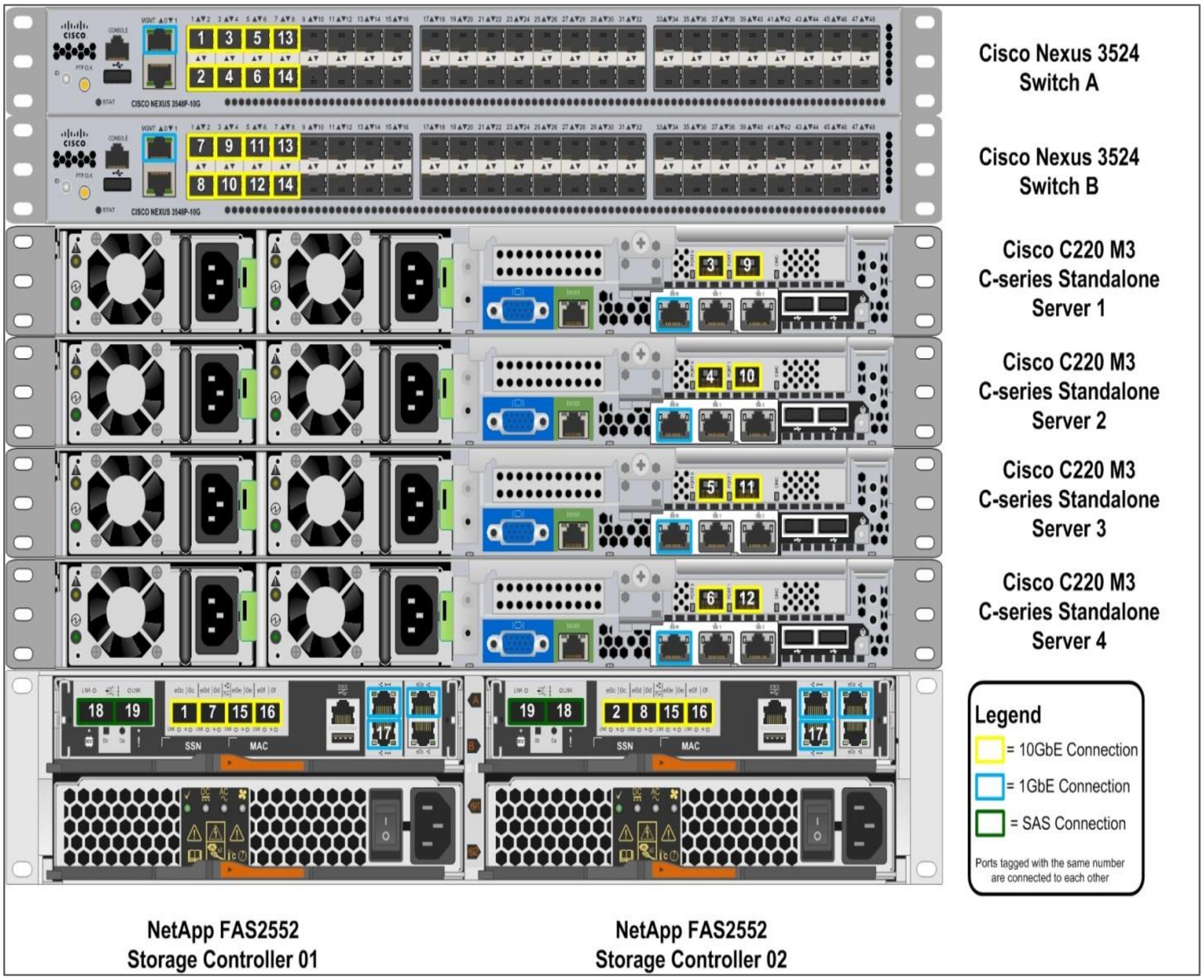

Cisco Nexus 3524 Switch A
1 3 5 13
2 4 6 14
Cisco Nexus 3524 Switch B
7 9 11 13
8 10 12 14
Cisco C220 M3 C-series Standalone Server 1
3 9
Cisco C220 M3 C-series Standalone Server 2
4 10
Cisco C220 M3 C-series Standalone Server 3
5 11
Cisco C220 M3 C-series Standalone Server 4
6 12
18 19
1 7 15 16
17
19 18
2 8 15 16
17
Legend
= 10GbE Connection
= 1GbE Connection
= SAS Connection
Ports tagged with the same number are connected to each other
NetApp FAS2552 Storage Controller 01
NetApp FAS2552 Storage Controller 02

Table 6) Cabling information.

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
Cisco Nexus 3524 Switch A	Eth1/1	NetApp FAS2552 Storage Controller 01	e0c	1
	Eth1/2	NetApp FAS2552 Storage Controller 02	e0c	2
	Eth1/3	Cisco UCS C220M3 Standalone Server-1	Port1/1	3
	Eth1/4	Cisco UCS C220M3 Standalone Server-2	Port1/1	4
	Eth1/5	Cisco UCS C220 M3 Standalone Server-3	Port 1/1	5

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
	Eth1/6	Cisco UCS C220 M3 Standalone Server-4	Port 1/1	6
	Eth1/7	Cisco Nexus 3524 Switch B	Eth1/7	13
	Eth1/8	Cisco Nexus 3524 Switch B	Eth1/7	14

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
Cisco Nexus 3524 Switch B	Eth1/1	NetApp FAS2552 Storage Controller 01	e0d	7
	Eth1/2	NetApp FAS2552 Storage Controller 02	e0d	8
	Eth1/3	Cisco UCS C220 M3 Standalone Server-1	Port1/2	9
	Eth1/4	Cisco UCS C220 M3 Standalone Server-2	Port1/2	10
	Eth1/5	Cisco UCS C220 M3 Standalone Server-3	Port1/2	11
	Eth1/6	Cisco UCS C220 M3 Standalone Server-4	Port1/2	12
	Eth1/7	Cisco Nexus 3048 Switch A	Eth1/7	13
	Eth1/8	Cisco Nexus 3048 Switch A	Eth1/8	14

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
NetApp FAS2552 Storage Controller 01	e0e	NetApp FAS2552 Storage Controller 02	e0e	15
	e0f	NetApp FAS2552 Storage Controller 02	e0f	16
	ACP	NetApp FAS2520 Storage Controller 02	ACP	17
	SAS 0b	NetApp FAS2520 Storage Controller 02	SAS 0a	18
	SAS 0a	NetApp FAS2520 Storage Controller 02	SAS 0b	19

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
NetApp FAS2552 Storage Controller 02	e0e	NetApp FAS2552 Storage Controller 01	e0e	15
	e0f	NetApp FAS2552 Storage Controller 01	e0f	16
	ACP	NetApp FAS2520 Storage Controller 01	ACP	17
	SAS 0b	NetApp FAS2520 Storage Controller 01	SAS 0a	18
	SAS 0a	NetApp FAS2520 Storage Controller 01	SAS 0b	19

8 Cisco Nexus Switch Deployment Procedure

A pair of Cisco Nexus switches that support 10G traffic are required to build the network backbone of this FlexPod Express infrastructure.

This document details the implementation of a FlexPod Express solution with the Cisco Nexus 3524 switches. However, these switches can be replaced with the latest Cisco Nexus 9000 Series switches, which are fully supported in FlexPod Express.

Cisco Nexus 9000 Series

The Cisco Nexus 9000 Series delivers proven high performance and density, low latency, and exceptional power efficiency in a broad range of compact form factors. Operating in Cisco NX-OS software mode (standalone mode) or in Application Centric Infrastructure (ACI) mode, these switches are ideal for traditional or fully automated data center deployments.

The Cisco Nexus 9000 standalone mode FlexPod Express design consists of a single pair of Cisco Nexus 9000 top-of-rack switches. When leveraging the ACI mode, the Cisco Nexus 9500 and 9300 switches are deployed in a spine-leaf architecture.

ACI is a holistic architecture with centralized automation and policy-driven application profiles. ACI delivers software flexibility with the scalability of hardware performance. Key characteristics of ACI include:

- Simplified automation by an application-driven policy model
- Centralized visibility with real-time application health monitoring
- Open software flexibility for DevOps teams and ecosystem partner integration
- Scalable performance and multi-tenancy in hardware

The future of networking with ACI is about providing a network that is deployed, monitored, and managed in a fashion that supports DevOps and rapid application change.

Users will also be able to start with the Cisco Nexus 9000 switches in standalone mode and easily migrate to the ACI mode.

8.1 Performing Initial Cisco Nexus 3524 Switch Setup

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 defines the control-plane policing policy.

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 already exists, all you need are valid IP addresses and 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 the mgmt0 interfaces of each Cisco Nexus 3524 switch together in a back-to-back configuration. Any valid IP address and netmask can be configured on each mgmt0 interface 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 they should be able to communicate with each other. This link cannot be used for external management access such as SSH access, but it will be used for the virtual PortChannel (vPC) peer keep alive traffic. To enable SSH management access to the switch, you need to configure the in-band interface VLAN IP address on an 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 switches, substituting the appropriate values for the switch-specific information.

Switches A and 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
```

8.2 Upgrading the Software (Optional)

You should 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 3048 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)A1(1d) is used in this solution.

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

Switches A and 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>>
```

2. The switch will install the updated Cisco NX-OS files and reboot.

8.3 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 are using the back-to-back connection with mgmt0. This feature allows 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 (`config t)` command and type the following commands to enable the appropriate features on each switch.

Switches A and B

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

8.4 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. Better distribution across the members of the PortChannels can be achieved by providing more inputs to the hash algorithm beyond the source and destination IP addresses. For that reason, adding the source and destination TCP ports to the hash algorithm is highly recommended.

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

Switches A and B

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

8.5 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 will force the network administrator to review the configuration of each port and will help reveal the most common configuration such as unidentified edge ports or a neighbor that does not have bridge assurance enabled. Also, it is safer to have spanning tree block too many ports 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 those cases, you may need to change the port type to make the ports active.

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 will shut 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 switch.

Switches A and B

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

8.6 Configuring Jumbo Frames

Jumbo frames should be configured throughout the network to allow any applications and operating systems to transmit these larger frames without fragmentation. Note that both endpoints and all 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 switch.

Switches A and B

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

8.7 Defining VLANs

Before configuring individual ports with different VLANs, those layer 2 VLANs must be defined on the switch. It's also good practice to name the VLANs to help with any troubleshooting in the future.

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

Switches A and B

```
vlan <<smb_vlan_id>>
  name SMB-VLAN
vlan <<livemigration_vlan_id>>
  name LiveMigration-VLAN
vlan <<cluster_vlan_id>>
  name Cluster-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
```

8.8 Configuring Access and Management Port Descriptions

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

From configuration mode (`config t)` in each switch, 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.

Switch A **Switch B**

```
int eth1/1
  description Controller-01:e0c
int eth1/2
  description Controller-02:e0c
int eth1/3
  description Server-1:Port-1/1
int eth1/4
  description Server-2:Port-1/1
int eth1/5
  description Server-3:Port-1/1
int eth1/6
  description Server-4:Port-1/1
int eth1/7
  description vPC peer-link NX3524-B:1/7
int eth1/8
  description vPC peer-link NX3524-B:1/8
int eth1/24
  description Uplink to Infrastructure
```

```
int eth1/1
  description Controller-01:e0d
int eth1/2
  description Controller-02:e0d
int eth1/3
  description Server-1:Port-1/2
int eth1/4
  description Server-2:Port-1/2
int eth1/5
  description Server-3:Port-1/2
int eth1/6
  description Server-4:Port-1/2
int eth1/7
  description vPC peer-link NX3524-A:1/7
int eth1/8
  description vPC peer-link NX3524-A:1/8
int eth1/24
  description Uplink to Infrastructure
```

8.9 Performing Virtual PortChannel Global Configuration

The vPC feature requires some initial setup between the two Cisco Nexus switches to function properly. If you are using the back-to-back mgmt0 configuration, be sure to 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.

Switch A

```
vpc domain 50
  role priority 10
  peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source <<switch_A_mgmt0_ip_addr>> vrf
management

int eth1/7-8
  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 <<smb_vlan_id>>,<<livemigration_vlan_id>>, <<cluster_vlan_id>>,
<<vmtraffic_vlan_id>>, <<ib_mgmt_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.

Switch B

```
vpc domain 50
  role priority 20
  peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source <<switch_B_mgmt0_ip_addr>> vrf
management

int eth1/7-8
  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 <<smb_vlan_id>>,<<livemigration_vlan_id>>, <<cluster_vlan_id>>,
<<vmtraffic_vlan_id>>, <<ib_mgmt_vlan_id>>
  spanning-tree port type network
  vpc peer-link
  no shut
exit
copy run start
```

8.10 Configuring Storage PortChannels

The NetApp storage controllers allow an active-active connection to the network by 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 allows you to have active-active connections from the storage to completely separate physical switches. Each controller will have two links to each switch, but all four are part of the same vPC and interface group (ifgrp).

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

Switches A and B

```
int eth1/1
  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 <<smb_vlan_id>>,<<ib_mgmt_vlan_id>>
  spanning-tree port type edge trunk
  vpc 11
  no shut
```

Switches A and B

```
int eth1/2
  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 <<smb_vlan_id>>,<<ib_mgmt_vlan_id>>
  spanning-tree port type edge trunk
  vpc 12
  no shut
exit
copy run start
```

8.11 Configuring Server Connections

The Cisco UCS servers have virtual interface cards that serve data in and out of the servers. Each server is connected to both of the Cisco Nexus 3524 switches in a virtual port-channel configuration. With this redundant connectivity the server is able to survive 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.

FlexPod Express Large Configuration

Switches A and B

```
int eth1/3
  channel-group 13 mode active

int Po13
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<smb_vlan_id>>, <<livemigration_vlan_id>>, <<cluster_vlan_id>>,
<<vmtraffic_vlan_id>>, <<ib_mgmt_vlan_id>>
  spanning-tree port type edge trunk
  vpc 13
  no shut
exit

int eth1/4
  channel-group 14 mode active

int Po14
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<smb_vlan_id>>, <<livemigration_vlan_id>>, <<cluster_vlan_id>>,
<<vmtraffic_vlan_id>>, <<ib_mgmt_vlan_id>>
  spanning-tree port type edge trunk
  vpc 14
  no shut
exit

int eth1/5
  channel-group 15 mode active

int Po15
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<smb_vlan_id>>, <<livemigration_vlan_id>>, <<cluster_vlan_id>>,
<<vmtraffic_vlan_id>>, <<ib_mgmt_vlan_id>>
  spanning-tree port type edge trunk
  vpc 15
  no shut
exit

int eth1/6
  channel-group 16 mode active

int Po16
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<smb_vlan_id>>, <<livemigration_vlan_id>>, <<cluster_vlan_id>>,
<<vmtraffic_vlan_id>>, <<ib_mgmt_vlan_id>>
  spanning-tree port type edge trunk
  vpc 16
  no shut
exit
copy run start
```

8.12 Performing In-Band Management SVI Configuration

In-band management that uses SSH in the FlexPod Express environment is handled by an SVI. To configure this in-band management on each switch, you must 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.

Switches A and B

```
int Vlan <<ib_mgmt_vlan_id>>
  ip address <<inband_mgmt_ip_address>>/<<inband_mgmt_netmask>>
  no shut

ip route 0.0.0.0/0 <<inband_mgmt_gateway>>
```

8.13 Saving the Configuration

Save the configuration on both switches for configuration persistence.

Switches A and B

```
copy run start
```

8.14 Uplinking to Existing Network Infrastructure

Depending on the available network infrastructure, several methods and features can be used to uplink the FlexPod Express environment. If an existing Cisco Nexus environment is present, you should use vPC to uplink the Cisco Nexus 3048 switches included in the FlexPod Express environment to the infrastructure. Be sure to type `copy run start` to save the configuration on each switch after configuration is complete.

9 NetApp FAS Storage Deployment Procedure

This section describes the NetApp FAS storage deployment procedure.

9.1 Prerequisites for NetApp FAS2500 Series Controller Installation

Table 7 lists the prerequisites for installing the NetApp FAS2500 series controller.

Table 7) NetApp FAS2500 series controller prerequisites.

Requirement	Reference	Comments
Physical site where storage system needs to be installed must be ready.	Site Requirements Guide	Refer to the “Site Preparation” section.
Storage system connectivity requirements must be met.	Site Requirements Guide	Refer to the “System Connectivity Requirements” section.
Storage system general power requirements must be met.	Site Requirements Guide	Refer to the “Circuit Breaker, Power Outlet Balancing, System Cabinet Power Cord Plugs, and Console Pinout Requirements” section.
Storage system model-specific requirements must be met.	Site Requirements Guide	Refer to the “NetApp FAS2500 Series Systems” section.

NetApp Hardware Universe

The NetApp Hardware Universe provides supported hardware and software components for the specific Data ONTAP version. It provides configuration information for all NetApp storage appliances currently supported by the 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 that you plan to install by checking the NetApp Hardware Universe at the NetApp Support site.
2. Access the NetApp Hardware Universe application to view the system configuration guides. Click the Controllers tab to view the compatibility between Data ONTAP software versions and NetApp storage appliances with the desired specifications.
3. Alternatively, to compare components by storage appliance, click Compare Storage Systems.

Storage Controllers

Follow the physical installation procedures for the controllers in the NetApp FAS2500 documentation available at the NetApp Support site.

Controller 01

1. Connect to the storage system console port. You should see a `Loader-A` prompt. However, 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. From the `Loader-A` prompt, enter:

```
printenv
```

3. If the `last-OS-booted-ver` parameter is not set to 8.2.2, proceed to step 4 to load Data ONTAP 8.2.2 software. If Data ONTAP 8.2.2 is already loaded, proceed to step 16.
4. Allow the system to boot.

```
boot_ontap
```

5. Press Ctrl-C when the `Press Ctrl-C for Boot Menu` message appears

   Note: If Data ONTAP 8.2.2 is not the version of software being booted, proceed with the following steps to install new software. If Data ONTAP 8.2.2 is the version being booted, select option 8 and yes to reboot the node. Then proceed with step 15.

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

```
7
```

7. Answer yes to perform a nondisruptive upgrade.

```
y
```

8. Select `e0M` as the network port you want to use for the download.

```
e0M
```

9. Select yes to reboot now.

```
y
```

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

```
<<controller01_mgmt_ip>> <<controller01_mgmt_netmask>> <<controller01_mgmt_gateway>>
```

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

```
<<url_boot_software>>
```

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

```
Enter
```

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

```
y
```

14. 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` prompt. If these actions occur, the system might deviate from this procedure.

15. Press Ctrl-C to exit autoboot when you see this message:

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

16. From the `Loader-A` prompt, enter:

```
printenv
```

Note: If `bootarg.init.boot_clustered true` is not listed, the system is not set to boot in clustered Data ONTAP.

17. If the system is not set to boot in clustered Data ONTAP, at the `Loader-A` prompt, enter the following command to make the system boot in clustered Data ONTAP:

```
setenv bootarg.init.boot_clustered true
setenv bootarg.bsdportname e0M
```

18. At the `Loader-A` A prompt, enter:

```
autoboot
```

19. When you see `Press Ctrl-C for Boot Menu`, press:

```
Ctrl - C
```

20. Select option 5 to enter Maintenance mode.

```
5
```

21. When prompted with `Continue with boot?`, enter `y`.
22. Use the `disk show –n` command to view how many disks are unowned.
23. Use the `disk assign –n <<#_of_disks>>` command to assign disks to Controller-01.

Note: For the small and medium FlexPod Express configurations, `<<#_of_disks>>` should equal 9 for Controller 01.

24. To verify the HA status of your environment, run the following command:

```
ha-config show
```

Note: If either component is not in HA mode, use the `ha-config modify` command to put the components in HA mode.

25. Reboot the controller by using the halt command.
26. At the `Loader-A` prompt, enter:

```
autoboot
```

27. When you see `Press Ctrl-C for Boot Menu`, press:

```
Ctrl - C
```

28. Select option 4 for `clean configuration and initialize all disks`.

```
4
```

29. Answer yes to `zero disks, reset config and install a new file system`.

```
y
```

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

```
y
```

Note: The initialization and creation of the root volume can take 75 minutes or more to complete, depending on the number of disks attached. After initialization is complete, the storage system reboots. You can continue to Controller 02 configuration while the disks for Controller 01 are zeroing.

Controller 02

1. Connect to the storage system console port. You should see a `Loader-A` prompt. However, 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. From the `Loader-A` prompt, enter:

```
printenv
```

3. If the `last-OS-booted-ver` parameter is not set to 8.2.2, proceed to step 4 to load Data ONTAP 8.2.2 software. If Data ONTAP 8.2.2 is already loaded, proceed to step 16.
4. Allow the system to boot up.

```
boot_ontap
```

5. Press Ctrl-C when `Press Ctrl-C for Boot Menu` is displayed.

```
Ctrl-C
```

Note: If Data ONTAP 8.2.2 is not the version of software being booted, proceed with the following steps to install new software. If Data ONTAP 8.2.2 is the version being booted, then select option 8 and yes to reboot the node. Then proceed with step 15.

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

```
7
```

7. Answer yes to perform a nondisruptive upgrade.

```
y
```

8. Select `e0M` as the network port you want to use for the download.

```
e0M
```

9. Select yes to reboot now.

```
y
```

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

```
<<controller02_mgmt_ip>> <<controller02_mgmt_netmask>> <<controller02_mgmt_gateway>>
```

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

Note: This web server must be pingable.

```
<<url_boot_software>>
```

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

```
Enter
```

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

```
y
```

14. 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.

15. Press Ctrl-C to exit autoboot when you see this message:

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

16. From the `Loader-A` prompt, enter:

```
printenv
```

Note: If `bootarg.init.boot_clustered true` is not listed, the system is not set to boot in clustered Data ONTAP.

17. If the system is not set to boot in clustered Data ONTAP, at the `Loader-A` prompt, enter the following command to make the system boot in clustered Data ONTAP:

```
setenv bootarg.init.boot_clustered true
setenv bootarg.bsdportname e0M
```

18. At the `Loader-A` prompt, enter:

```
autoboot
```

19. When you see `Press Ctrl-C for Boot Menu`, press:

```
Ctrl - C
```

20. Select option 5 to enter Maintenance mode.

```
5
```

21. When prompted with `Continue with boot?,` enter `y`.
22. Use the `disk show -n` command to view how many disks are unowned.
23. Use the `disk assign -n <<#_of_disks>>` command to assign disks to Controller 02.

    Note: For the small and medium FlexPod Express configurations, `<<#_of_disks>>` should equal 3 for Controller 02.

24. To verify the HA status of your environment, run the following command:

```
ha-config show
```

    Note: If either component is not in HA mode, use the `ha-config modify` command to put the components in HA mode.

25. Reboot the controller by using the `halt` command.
26. At the `Loader-A` prompt, enter:

```
autoboot
```

27. When you see `Press Ctrl-C for Boot Menu, press:`

```
Ctrl - C
```

28. Select option 4 for `clean configuration and initialize all disks`.

```
4
```

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

```
y
```

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

```
y
```

Note: The initialization and creation of the root volume can take 75 minutes or more to complete, depending on the number of disks attached. When initialization is complete, the storage system reboots.

9.2 Creating Clusters in Clustered Data ONTAP

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 Controller 01.

Controller 01

1. During the first node boot, the Cluster Setup wizard starts running on the console.

```
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 appears instead of the Cluster Setup wizard, start the wizard by logging in with the factory default settings and then enter the `cluster setup` command.

2. Enter the following command to create a new cluster:

```
create
```

3. Follow these steps to activate high availability and set `Loader-A` storage failover.

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

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

Non-HA mode, Reboot node to activate HA

Do you want to reboot now to set storage failover (SFO) to HA mode? {yes, no}
[yes]: Enter
```

4. After the reboot, continue with the cluster create operation.
5. The existing cluster interface configuration is displayed.

```
Existing cluster interface configuration found:
```

```
Port    MTU     IP              Netmask
e0d     9000    169.254.250.41  255.255.0.0
e0f     9000    169.254.175.136 255.255.0.0

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

> **Note:** Before you accept the preceding configuration, make sure that the correct ports are listed for the cluster interfaces. If the correct interfaces are not listed, enter `no` and accept the system defaults.

6. Accept the configuration by pressing the Enter key.
7. The steps to create a cluster are displayed.

```
Enter the cluster name: <<clustername>>
Enter the cluster base license key: <<cluster_base_license_key>>
Creating cluster <<clustername>>
```

> **Note:** The cluster is created; this can take a minute or two.

```
Enter an additional license key []:
```

> **Note:** For this validated architecture, you should install license keys for the NetApp SnapRestore®, NFS, FlexClone®, and SnapManager suite.

8. After you finish entering the license keys, press Enter.

```
Enter the cluster administrator’s (username “admin”) password: <<admin_password>>
Retype the password: <<admin_password>>
Enter the cluster management interface port [e0a]: Enter
Enter the cluster management interface IP address: <<clustermgmt_ip>>
Enter the cluster management interface netmask: <<clustermgmt_netmask>>
Enter the cluster management interface default gateway: <<clustermgmt_gateway>>
```

9. Enter the DNS domain name.

```
Enter the DNS domain names:<<dns_domain_name>>
Enter the name server IP addresses:<<nameserver_ip>>
```

> **Note:** If you have more than one name server IP address, separate them with commas.

10. Set up the node.

```
Where is the controller located []:<<controller_location>>
Enter the node management interface port [e0M]: Enter
Enter the node management interface IP address: <<controller01_mgmt_ip>>
Enter the node management interface netmask:<<controller01_mgmt_netmask>>
Enter the node management interface default gateway:<<controller01_mgmt_gateway>>
Enable IPv4 DHCP on the service processor interface [no]:Enter
Enter the service processor interface IP address: <<controller01_sp_ip>>
Enter the service processor interface netmask: <<controller01_sp_netmask>>
Enter the service processor interface default gateway: <<controller01_sp_gateway>>
```

11. Press Enter to accept the NetApp AutoSupport™ message.
12. Log in to the cluster.
13. Disable `disk autoassign`.

```
storage disk option modify -autoassign off
```

9.3 Joining Clusters in Clustered Data ONTAP

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 Controller 01, and the node joining the cluster in this example is Controller 02.

Controller 02

1. During the node boot, the Cluster Setup wizard starts running on the console.

```
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 appears instead of the Cluster Setup Wizard, start the wizard by logging in using the factory default settings, and then enter the `cluster setup` command.

2. Enter the following command to join a cluster:

```
join
```

3. Follow these steps to activate high availability and set storage failover:

```
Non-HA mode, Reboot node to activate HA

Do you want to reboot now to set storage failover (SFO) to HA mode? {yes, no}
[yes]: Enter
```

4. After the reboot, continue with the cluster join operation. The existing cluster interface configuration is displayed:

```
Existing cluster interface configuration found:

Port    MTU     IP              Netmask
e0e     9000    169.254.49.199  255.255.0.0
e0f     9000    169.254.132.123 255.255.0.0

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

Note: Before accepting this configuration, make sure that the correct ports are listed for the cluster interfaces.

5. Accept the configuration by pressing the Enter key. The steps to create a cluster are displayed.

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

Note: The node should find the cluster name automatically.

Note: The cluster join operation can take a minute or two.

6. Set up the node.

```
Enter the node management interface port [e0M]: Enter
Enter the node management interface IP address: <<controller02_mgmt_ip>>
Enter the node management interface netmask: Enter
Enter the node management interface default gateway: Enter
Enable IPv4 DHCP on the service processor interface [no]:Enter
Enter the service processor interface IP address: <<controller02_sp_ip>>
Enter the service processor interface netmask: <<controller02_sp_netmask>>
Enter the service processor interface default gateway: <<controller02_sp_gateway>>
```

7. Press Enter to accept the AutoSupport message.
8. Log in to the cluster interface with the admin user ID and <<admin_password>>.

9. Disable the disk `autoassign` option by entering the following command:

```
storage disk option modify -node <<controller02>> -autoassign off
```

9.4 Logging in to the Cluster

Open an SSH connection to cluster IP or host name and log in to the admin user with the password you provided earlier.

9.5 Zeroing All Spare Disks

1. To zero all spare disks in the cluster, enter the following command:

```
disk zerospares
```

9.6 Setting Onboard 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 the Current Type is set to “`target`”. If not, 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.

9.7 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
```

9.8 Configuring Failover Group Management in Clustered Data ONTAP

1. Create a cluster management port failover group.

```
network interface failover-groups create -failover-group fg-clus-mgmt -node <<controller01>> -
port e0a
network interface failover-groups create -failover-group fg-clus-mgmt -node <<controller02>> -
port e0a
```

9.9 Assigning the Management Failover Group to the Cluster Management LIF

1. Assign the management port failover group to the cluster management LIF.

```
network interface modify -vserver <<clustername>> -lif cluster_mgmt –failover-group fg-clus-mgmt
```

9.10 Configuring Failover Group Node Management in Clustered Data ONTAP

1. Create node management port failover groups.

```
network interface failover-groups create -failover-group fg-node-mgmt01 -node <<controller01>> -
port e0a
network interface failover-groups create -failover-group fg-node-mgmt01 -node <<controller01>> -
port e0M
network interface failover-groups create -failover-group fg-node-mgmt02 -node <<controller02>> -
port e0a
network interface failover-groups create -failover-group fg-node-mgmt02 -node <<controller02>> -
port e0M
```

9.11 Assigning Node Management Failover Groups to Node Management LIFs

1. Assign the management port failover group to the cluster management LIF.

```
network interface modify -vserver <<controller01>> -lif mgmt1 -auto-revert true -failover-group
fg-node-mgmt01
network interface modify -vserver <<controller02>> -lif mgmt1 -auto-revert true -failover-group
fg-node-mgmt02
```

9.12 Upgrading the Service Processor on Each Node to the Latest Release

With Data ONTAP 8.2, you must upgrade to the latest service processor firmware to take advantage of the latest updates available for the remote management device.

1. Enter this command to obtain the version of the service processor firmware that is currently running on your storage system:

```
system node service-processor show
```

2. Using a web browser, connect to http://support.netapp.com/NOW/cgi-bin/fw.
3. Select the storage platform.
4. Select Service Process Image for installation from the Data ONTAP prompt.
5. Check the latest firmware version that is available for your storage platform. If your storage system is not running the latest version, proceed to the download page for the latest release of the service processor firmware for your storage platform.
6. Using the instructions on this page, update the service processors on both nodes in your cluster. You will need to download the .zip file to a web server that can be reached from the cluster management interface. In step 2 of the instructions, substitute the following command:

```
system node image get –node * -package http://web_server_name/path/SP_FW.zip -replace-package
true
```

7. Run step 3 on each node if service processor automatic updating is not enabled.
8. View the status of the service processor upgrade using steps 4 and 5.

9.13 Configuring AutoSupport HTTPS in Clustered Data ONTAP

NetApp AutoSupport sends support summary information to NetApp through HTTPS.

1. Run the following command to configure AutoSupport:

```
system node autosupport modify -node * –mail-hosts <<mailhost>> -noteto <<storage_admin_email>>
Warning: Do you want to continue running this command? {y|n}:y
```

9.14 Creating Aggregates

A 64-bit aggregate containing the root volume is created during the Data ONTAP setup process. To create additional 64-bit aggregates, determine the aggregate name, the node on which to create it, and the number of disks that it will contain.

1. Run the following command to create new aggregates:

```
aggr create -aggregate aggr1_controller01 -nodes <<controller01>> -diskcount <<num_disks>>
aggr create -aggregate aggr1_controller02 -nodes <<controller02>> -diskcount <<num_disks>>
```

Note: For the large FlexPod Express configuration, start with five disks initially; you can add disks to an aggregate when additional storage is required.

Note: The aggregate cannot be created until disk zeroing completes. Use the `aggr show` command to display aggregate creation status. Do not proceed until aggr1_controller01 is online.

2. Disable Snapshot copies for the two data aggregates just created.

```
node run <<controller01>> aggr options aggr1_controller01 nosnap on
node run <<controller02>> aggr options aggr1_controller02 nosnap on
```

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

```
node run <<controller01>> snap delete –A –a –f aggr1_controller01
node run <<controller02>> snap delete –A –a –f aggr1_controller02
```

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

```
aggr show
aggr rename –aggregate aggr0 –newname aggr0_controller01
```

9.15 Disabling Flow Control on UTA2 Ports

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

1. 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
```

9.16 Configuring ifgrp LACP in 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 configured properly.

1. To create interface groups (ifgrps), run the following commands on the command line:

```
ifgrp create -node <<controller01>> -ifgrp a0a -distr-func port -mode multimode_lacp
network port ifgrp add-port -node <<controller01>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<controller01>> -ifgrp a0a -port e0d
ifgrp create -node <<controller02>> -ifgrp a0a -distr-func port -mode multimode_lacp
network port ifgrp add-port -node <<controller02>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<controller02>> -ifgrp a0a -port e0d
```

Note: All interfaces must be in the down status before being added to an interface group.

Note: The interface group name must follow the standard naming convention of <number><letter>, where <number> is an integer in the range 0 to 999 without leading zeros, and <letter> is a lowercase letter.

9.17 Configuring VLANs in Clustered Data ONTAP

1. Follow these steps to create a VLAN interface for SMB data traffic:

```
network port vlan create –node <<controller01>> -vlan-name a0a-<<smb_vlan_id>>
network port vlan create –node <<controller02>> -vlan-name a0a-<<smb_vlan_id>>
```

2. Follow these steps to create a VLAN interface for in-band management traffic:

```
network port vlan create –node <<controller01>> -vlan-name a0a-<<ib_mgmt_vlan_id>>
network port vlan create –node <<controller02>> -vlan-name a0a-<<ib_mgmt_vlan_id>>
```

9.18 Configuring Jumbo Frames in Clustered Data ONTAP

1. To configure a NetApp clustered Data ONTAP network port to use jumbo frames (which usually have a maximum transmission unit (MTU) of 9000 bytes), run the following command from the cluster shell:

```
network port modify -node <<controller01>> -port a0a -mtu 9000

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

network port modify –node <<controller01>> -port a0a-<<smb_vlan_id>> -mtu 9000

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

network port modify –node <<controller02>> -port a0a -mtu 9000

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

network port modify –node <<controller02>> -port a0a-<<smb_vlan_id>> -mtu 9000

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

9.19 Configuring Cisco Discovery Protocol in Clustered Data ONTAP

Enable Cisco Discovery Protocol (CDP) on the NetApp storage controllers by using the following procedure.

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
```

9.20 Configuring NTP in Clustered Data ONTAP

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

1. Set the time zone for the cluster.

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

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

2. Set the date for the cluster.

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

   Note: The format for the date is:

   `<[Century][Year][Month][Day][Hour][Minute].[Second]>`; for example, `201309231128.50`

3. Configure NTP for each node in the cluster.

```
system services ntp server create -node <<controller01>> -server <<global_ntp_server_ip>>
system services ntp server create -node <<controller02>> -server <<global_ntp_server_ip>>
```

9.21 Configuring SNMP in Clustered Data ONTAP

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

```
snmp contact <<snmp_contact>>
snmp location “<<snmp_location>>”
snmp init 1
options snmp.enable on
```

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

```
snmp traphost add <<snmp_trap_server_fqdn>>
```

9.22 Configuring SNMPv1 in Clustered Data ONTAP

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

```
snmp community delete all
snmp community add ro <<snmp_community>>
```

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

9.23 Configuring SNMPv3 in Clustered Data ONTAP

SNMPv3 requires that a user be defined and configured for authentication.

1. Create a user called `snmpv3user`.

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

2. Enter the authoritative entity's engine ID and select MD5 as the authentication protocol. Use the command `security snmpusers` to view the engine ID.
3. Enter a password with a minimum length of eight characters for the authentication protocol when prompted.
4. Confirm the authentication protocol password.
5. Select DES as the privacy protocol.
6. Enter a password with a minimum length of eight characters for the privacy protocol when prompted.
7. Confirm the privacy protocol password.

9.24 Configuring HTTPS Access in Clustered Data ONTAP

Secure access to the storage controller must be configured.

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. Check it by using the following command:

```
security certificate show
```

3. Run the following commands as one-time commands to generate and install self-signed certificates.

   You can also use the `security certificate delete` command to delete expired certificates.

```
security certificate create -vserver infra_svm -common-name <<security_cert_vserver_common_name>>
-type server -size 2048 -country <<country_code>> -state <<state>> -locality <<city>> -
organization <<org>> -unit <<unit>> -email-addr <<storage_admin_email>>

security certificate create -vserver <<clustername>> -common-name
<<security_cert_cluster_common_name>> -type server -size 2048 -country <<country_code>> -state
<<state>> -locality <<city>> -organization <<org>> -unit <<unit>> -email-addr
<<storage_admin_email>>

security certificate create -vserver <<controller01>> -common-name
<<security_cert_controller01_common_name>> -type server -size 2048 -country <<country_code>> -
state <<state>> -locality <<city>> -organization <<org>> -unit <<unit>> -email-addr
<<storage_admin_email>>

security certificate create -vserver <<controller02>> -common-name
<<security_cert_controller02_common_name>> -type server -size 2048 -country <<country_code>> -
state <<state>> -locality <<city>> -organization <<org>> -unit <<unit>> -email-addr
<<storage_admin_email>>
```

4. Configure and enable SSL and HTTPS access and disable telnet access.

```
system services web modify -external true -sslv3-enabled true
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http -action allow
system services firewall policy create -policy mgmt -service http -action deny -ip-list 0.0.0.0/0

security ssl modify -vserver infra_svm -common-name <<security_cert_vserver_common_name>> -
server-enabled true -client-enabled false -ca <<security_certificate_vservser_authority>> -serial
<<security_certificate_vserver_serial_no>>

security ssl modify -vserver <<clustername>> -common-name <<security_cert_cluster_common_name>> -
server-enabled true -client-enabled false -ca <<security_certificate_cluster_authority>> -serial
<<security_certificate_cluster_serial_no>>

security ssl modify -vserver <<controller01>> -common-name
<<security_cert_controller01_common_name>> -server-enabled true -client-enabled false -ca
<<security_certificate_controller01_authority>> -serial
<<security_certificate_controller01_serial_no>>
```

```
security ssl modify -vserver <<controller02>>-common-name
<<security_cert_controller02_common_name>> -server-enabled true -client-enabled false -ca
<<security_certificate_controller02_authority>> -serial
<<security_certificate_controller02_serial_no>>

set –privilege admin
```

5. It is normal for some of these commands to return x messages stating that the entry does not exist.

9.25 Setting Up Vserver

To create an infrastructure Vserver, complete the following steps:

1. Run the Vserver setup wizard.

```
vserver setup

Welcome to the Vserver Setup Wizard, which will lead you through
the steps to create a virtual storage server that serves data to clients.

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 your answers to previous questions, and
"exit" if you want to quit the Vserver Setup Wizard. Any changes
you made before typing "exit" will be applied.

You can restart the Vserver Setup Wizard by typing "vserver setup". To accept a default
or omit a question, do not enter a value.

Vserver Setup wizard creates and configures only data Vservers.
If you want to create a Vserver with Infinite Volume use the vserver create command.


Step 1. Create a Vserver.
You can type "back", "exit", or "help" at any question.
```

2. Enter the Vserver name.

```
Enter the Vserver name:infra_svm
```

3. Select the Vserver data protocols to configure.

```
Choose the Vserver data protocols to be configured {nfs, cifs, fcp, iscsi, ndmp}: cifs
```

4. Select the Vserver client services to configure.

```
Choose the Vserver client services to configure {ldap, nis, dns}:dns
```

5. Enter the Vserver’s root volume aggregate.

```
Enter the Vserver's root volume aggregate {aggr1_controller01, aggr1_controller02}
[aggr1_controller01]: aggr1_controller01
```

6. Enter the Vserver language setting. English is the default [C.UTF-8].

```
Enter the Vserver language setting, or "help" to see all languages [C.UTF-8]:Enter
```

7. Enter the Vserver’s security style.

```
Enter the Vserver root volume's security style {mixed, ntfs, unix} [unix]: ntfs
```

8. Do not create the data volume.

```
Do you want to create a data volume?  {yes, no} [yes]: no
```

9. Do not create the logical interface.

```
Do you want to create a logical interface?  {yes, no} [yes]: no
```

10. Answer yes to `Do you want to configure DNS?`

```
Do you want to configure DNS? {yes, no} [yes]: yes
Enter the comma separated DNS domain names: <dns domain name>
Enter the comma separated DNS server IP addresses: <dns server ipaddresses>
```

11. Answer no to `Do you want to configure CIFS?`

```
Do you want to configure CIFS?{yes, no} [yes]: no
```

12. Add the data aggregate to the `infra_svm` aggregate list for NetApp Virtual Storage Console.

```
vserver modify -vserver infra_svm -aggr-list aggr1_controller01, aggr1_controller02
```

9.26 Creating Load Sharing Mirror of Vserver Root Volume in 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_svm –volume rootvol_m01 –aggregate aggr1_controller01 –size 1GB –
type DP
volume create –vserver infra_svm –volume rootvol_m02 –aggregate aggr1_controller02 –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_svm:rootvol -destination-path infra_svm:rootvol_m01 -type LS
-schedule 15min

snapmirror create -source-path infra_svm:rootvol -destination-path infra_svm:rootvol_m02 -type LS
-schedule 15min
```

4. Initialize the mirroring relationship.

```
snapmirror initialize-ls-set -source-path infra_svm:rootvol
```

9.27 Failover Groups NAS in Clustered Data ONTAP

1. Create an in-band management port failover group.

```
network interface failover-groups create -failover-group fg-ib-mgmt-<<var_ib-mgmt_vlan_id>> -node
<<var_node01>> -port a0a-<<var_ib-mgmt_vlan_id>>
network interface failover-groups create -failover-group fg-ib-mgmt-<<var_ib-mgmt_vlan_id>> -node
<<var_node02>> -port a0a-<<var_ib-mgmt_vlan_id>>
```

2. Create an SMB port failover group.

```
network interface failover-groups create -failover-group fg-smb-<<var_smb_vlan_id>> -node
<<var_node01>> -port a0a-<<var_smb_vlan_id>>
network interface failover-groups create -failover-group fg-smb-<<var_smb_vlan_id>> -node
<<var_node02>> -port a0a-<<var_smb_vlan_id>>
```

9.28 Creating an SMB LIF in Clustered Data ONTAP

1. Create an SMB logical interface (LIF).

```
network interface create -vserver infra_svm -lif smb_lif01 -role data -data-protocol cifs -home-
node <<var_node01>> -home-port a0a-<<var_smb_vlan_id>> -address <<var_node01_smb_lif_ip>> -
netmask <<var_node01_smb_lif_mask>> -status-admin up -failover-policy priority -firewall-policy
data -auto-revert true -failover-group fg-smb-<<var_smb_vlan_id>>

network interface create -vserver infra_svm -lif smb_lif02 -role data -data-protocol cifs -home-
node <<var_node02>> -home-port a0a-<<var_smb_vlan_id>> -address <<var_node02_smb_lif_ip>> -
```

```
netmask <<var_node02_smb_lif_mask>> -status-admin up -failover-policy priority -firewall-policy
data -auto-revert true -failover-group fg-smb-<<var_smb_vlan_id>>
```

9.29 Adding Infrastructure SVM Administrator

1. Add the infrastructure SVM administrator and SVM administration logical interface in the out-of-band management network with the following commands:

```
network interface create -vserver infra_svm -lif vsmgmt -role data -data-protocol none -home-node
<<var_node02>> -home-port a0a-<<var_ib-mgmt_vlan_id>>  -address <<var_vserver_mgmt_ip>> -netmask
<<var_vserver_mgmt_mask>> -status-admin up -failover-policy nextavail -firewall-policy mgmt -
auto-revert true -failover-group fg-ib-mgmt-<<var_ib-mgmt_vlan_id>>

network routing-groups route create -vserver infra_svm -routing-group d<<var_in-band-network>> -
destination 0.0.0.0/0 -gateway <<var_in-band_gateway>>

security login password -username vsadmin -vserver infra_svm
Enter a new password:  <<var_vsadmin_password>>
Enter it again:  <<var_vsadmin_password>>

security login unlock -username vsadmin -vserver infra_svm
```

9.30 Configuring SMB in Clustered Data ONTAP

Run all commands to configure SMB on the Vserver.

1. Secure the default rule for the default export policy and create the FlexPod export policy.

```
vserver export-policy rule modify -vserver infra_svm -policyname default -ruleindex 1 -rorule
never -rwrule never -superuser none

vserver export-policy create -vserver infra_svm FlexPod
```

2. Create a new rule for the FlexPod export policy.

Note: For each Hyper-V host being created, as well as the SCVMM, and SQL hosts create a rule. Each host will have its own rule index. The first Hyper-V host will have rule index 1, the second Hyper-V host will have rule index 2, and so on. Alternatively, you can assign the subnet by allocating the entire network through a single rule.

```
vserver export-policy rule create -vserver infra_svm -policyname FlexPod -ruleindex 1 -protocol
cifs -clientmatch <<var_vmhost_host1_smb_ip>> -rorule sys -rwrule sys -superuser sys -allow-suid
false
```

3. Assign the FlexPod export policy to the infrastructure Vserver root volume.

```
volume modify -vserver infra_svm -volume rootvol -policy FlexPod
```

4. Create the CIFS service and add it to Active Directory®.

```
vserver cifs create -vserver infra_svm -cifs-server infrasvm -domain <<var_dnsdomain>>

In order to create an Active Directory machine account for the CIFS server, you must
supply the name and password of a Windows account with sufficient privileges to add
computers to the "CN=Computers" container within the "FlexPod.com" domain.

Enter the user name: adminXX

Enter the password: XXnetapp!
```

9.31 Configuring FlexVol in Clustered Data ONTAP

The following information is required to create a NetApp FlexVol® volume: the volume's name and size, and the aggregate on which it will exist. Create the SCVMM Pool, a server boot volume, a Cluster

Quorum volume, and a volume to hold the System Center Databases. Also, update the Vserver root volume load sharing mirrors.

```
volume create -vserver infra_svm -volume witness -aggregate aggr1_controller01 -size 100GB -state
online -policy FlexPod -space-guarantee none -percent-snapshot-space 0 -junction-path /quorum

volume create -vserver infra_svm -volume sc_sql_db -aggregate aggr1_controller01 -size 1TB -state
online -policy FlexPod -space-guarantee none -percent-snapshot-space 0 -junction-path /sc_sql_db

volume create -vserver infra_svm -volume scvmm_pool0 -aggregate aggr1_controller02 -size 4TB -
state online -policy FlexPod -space-guarantee none -percent-snapshot-space 0 -junction-path
/scvmm_pool0

snapmirror update-ls-set -source-path infra_svm:rootvol
```

9.32 Enabling Deduplication in Clustered Data ONTAP

1. Enable deduplication on appropriate volumes.

```
volume efficiency on -vserver infra_svm -volume scvmm_pool0
volume efficiency on -vserver infra_svm -volume sc_sql_db
```

9.33 Creating SMB Shares

1. Create a qtree in the SCVMM pool to house the infrastructure VMs and SCVMM library.

```
qtree create -volume scvmm_pool0 -qtree infrastructure -security-style ntfs -vserver infra_svm
qtree create -volume scvmm_pool0 -qtree vmmlibrary -security-style ntfs -vserver infra_svm
```

Note: These are collocated to enable ODX to rapidly deploy VMs utilizing FlexClone for files.

2. Create a qtree in the witness volume to house the file share witness.

```
qtree create -volume witness -qtree hyperv -security-style ntfs -vserver infra_svm
```

3. Create a qtree in the System Center SQL volume to house the SCVMM database.

```
qtree create -volume sc_sql_db -qtree scvmm -security-style ntfs -vserver infra_svm
```

4. Create the qtree quota policy for the infrastructure VM share and SCVMM library.

```
quota policy rule create -policy-name default -volume scvmm_pool0 -type tree -disk-limit 500g -
target infrastructure
quota policy rule create -policy-name default -volume scvmm_pool0 -type tree -disk-limit 500g -
target vmmlibrary
```

5. Create the qtree quota policy for the file share witness.

```
quota policy rule create -policy-name default -volume witness -type tree -disk-limit 5g -target
hyperv
```

6. Create the qtree quota policy for the SCVMM database share.

```
quota policy rule create -policy-name default -volume sc_sql_db -type tree -disk-limit 500g -
target scvmm
```

7. Create the SMB share to house the infrastructure virtual machines and SCVMM library.

```
share create -share-name infrastructure -path /scvmm_pool0/infrastructure -share-properties
browsable,continuously-available -vserver infra_svm
share create -share-name vmmlibrary -path /scvmm_pool0/vmmlibrary -share-properties
browsable,continuously-available -vserver infra_svm
```

8. Create the SMB share to house the file share witness.

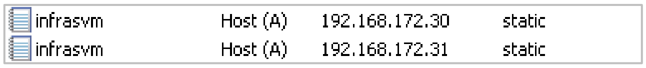
```
share create -share-name hyperv-witness -path /witness/hyperv -share-properties browsable -
vserver infra_svm
```

9. Create the SMB share to house the SCVMM database.

```
share create -share-name scvmmdb -path /sc_sql_db/scvmm -share-properties browsable,continuously-
available -vserver infra_svm
```

9.34 Adding a Domain Name Service Record for the SMB LIFs

1. Open DNS Manager and navigate to the forward lookup zone for the domain. Right-click the forward lookup zone and select New Host (A or AAAA) …
2. Enter the SVM CIFS host name and the SMB data LIF IP address. Click Add Host.
3. Click OK to acknowledge the DNS record creation.
4. Repeat for the second SMB LIF.
5. Click Done to close the New Host window.



infrasvm	Host (A)	192.168.172.30	static
infrasvm	Host (A)	192.168.172.31	static

10 Cisco UCS C-Series Rack Server Deployment Procedure

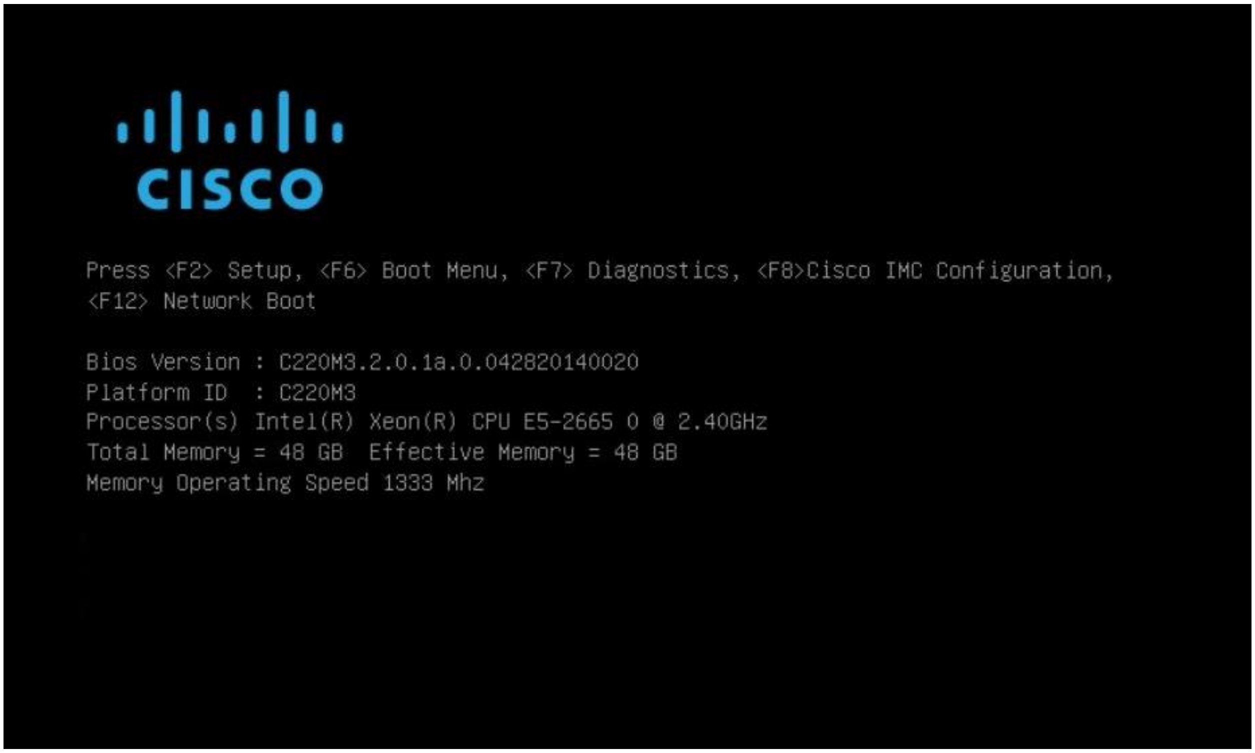
The following section provides a detailed procedure for configuring a Cisco UCS C-Series standalone rack server for use in either the small or medium FlexPod Express configuration.

10.1 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 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.

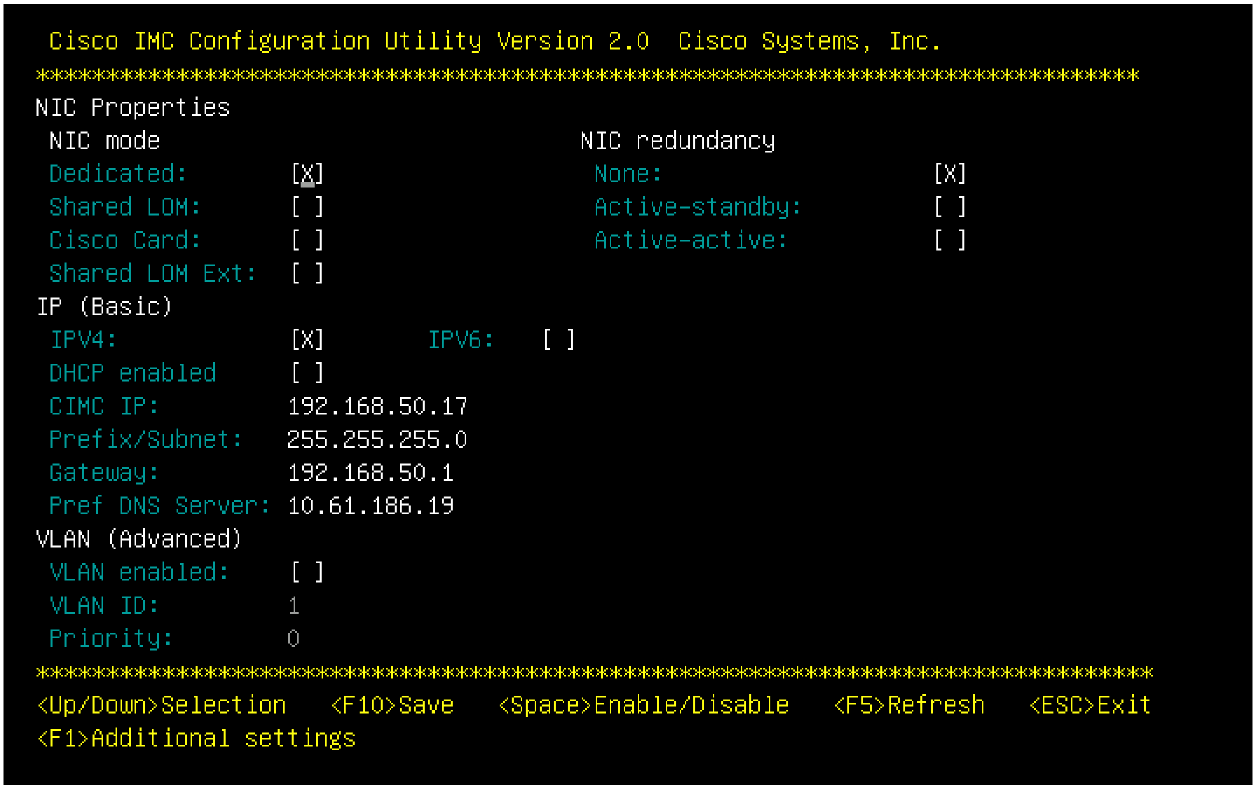


```
Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8>Cisco IMC Configuration,
<F12> Network Boot

Bios Version : C220M3.2.0.1a.0.042820140020
Platform ID  : C220M3
Processor(s) Intel(R) Xeon(R) CPU E5-2665 0 @ 2.40GHz
Total Memory = 48 GB  Effective Memory = 48 GB
Memory Operating Speed 1333 Mhz
```

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

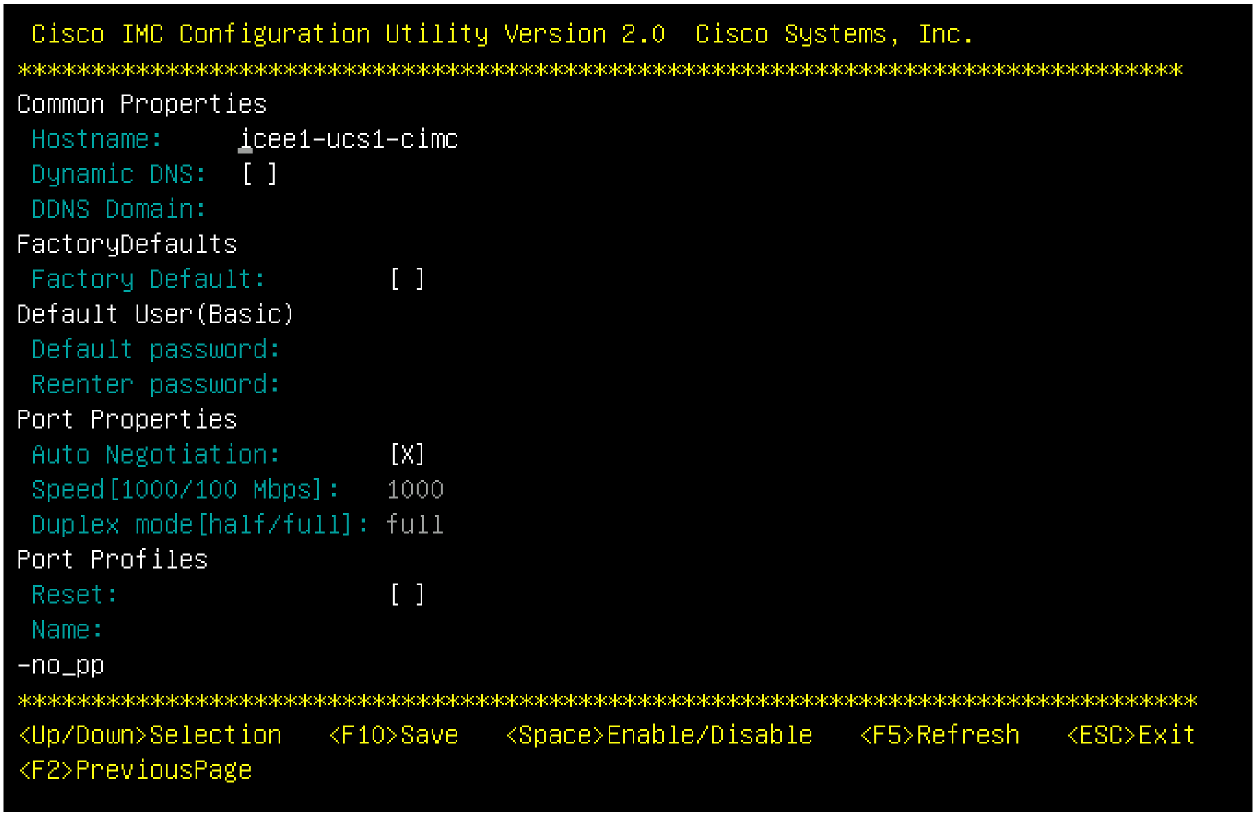
- Network Interface Card (NIC) Mode:
  - Dedicated [X]
- IP (Basic):
  - IPV4: [X]
  - DHCP enabled: [ ]
  - CIMC IP:`<<cimc_ip>>`
  - Prefix/Subnet:`<<cimc_netmask>>`
  - Gateway: `<<cimc_gateway>>`
- VLAN (Advanced): Leave unchecked to disable VLAN tagging.
  - NIC Redundancy:
  - None: [X]



```
 Cisco IMC Configuration Utility Version 2.0  Cisco Systems, Inc.
********************************************************************************
NIC Properties
 NIC mode                                   NIC redundancy
 Dedicated:        [X]                       None:                    [X]
 Shared LOM:       [ ]                       Active-standby:          [ ]
 Cisco Card:       [ ]                       Active-active:           [ ]
 Shared LOM Ext:   [ ]
IP (Basic)
 IPV4:             [X]         IPV6:    [ ]
 DHCP enabled      [ ]
 CIMC IP:          192.168.50.17
 Prefix/Subnet:    255.255.255.0
 Gateway:          192.168.50.1
 Pref DNS Server:  10.61.186.19
VLAN (Advanced)
 VLAN enabled:     [ ]
 VLAN ID:          1
 Priority:         0
*********************************************************************************
<Up/Down>Selection   <F10>Save   <Space>Enable/Disable   <F5>Refresh   <ESC>Exit
<F1>Additional settings
```

Press F1 to see additional settings.

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



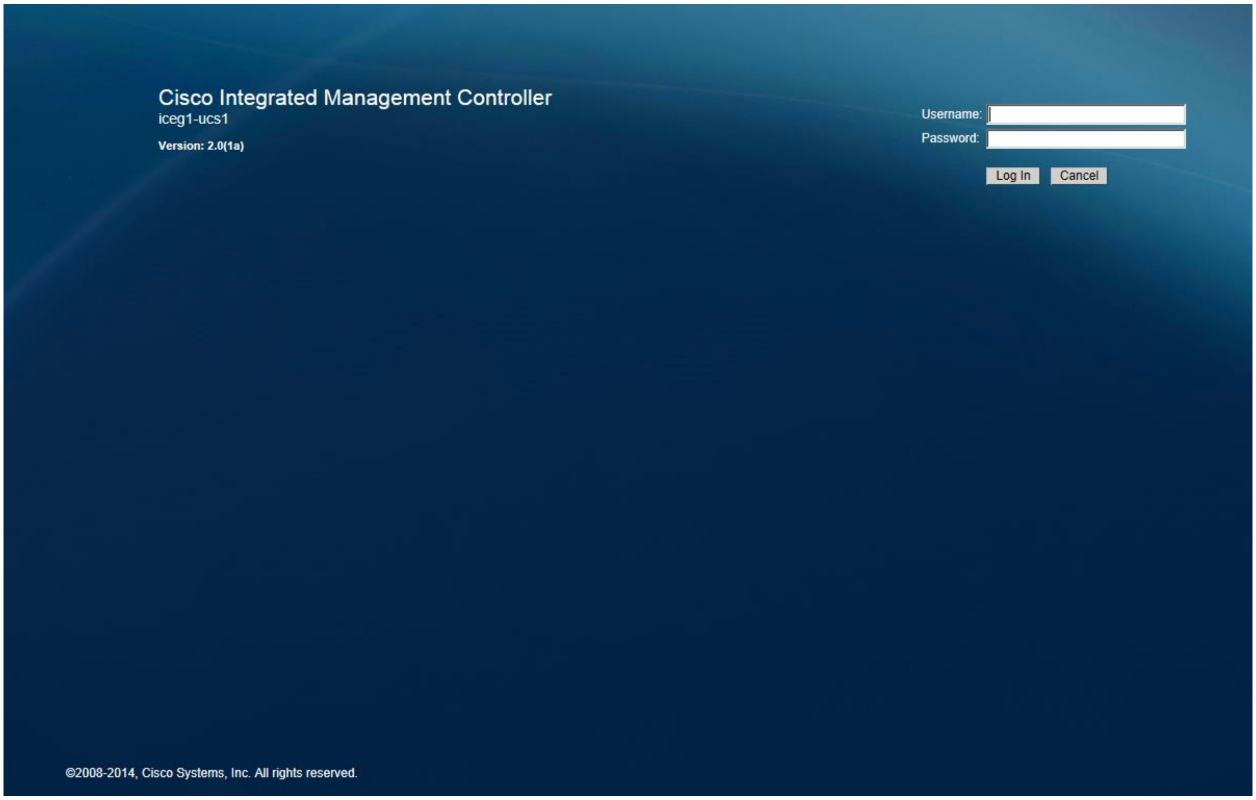
```
 Cisco IMC Configuration Utility Version 2.0  Cisco Systems, Inc.
********************************************************************************
Common Properties
 Hostname:      icee1-ucs1-cimc
 Dynamic DNS:   [ ]
 DDNS Domain:
FactoryDefaults
 Factory Default:         [ ]
Default User(Basic)
 Default password:
 Reenter password:
Port Properties
 Auto Negotiation:        [X]
 Speed[1000/100 Mbps]:    1000
 Duplex mode[half/full]:  full
Port Profiles
 Reset:                   [ ]
 Name:
-no_pp
*********************************************************************************
<Up/Down>Selection   <F10>Save   <Space>Enable/Disable   <F5>Refresh   <ESC>Exit
<F2>PreviousPage
```

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

10.2 Configuring the Cisco Virtual Interface Card MTU

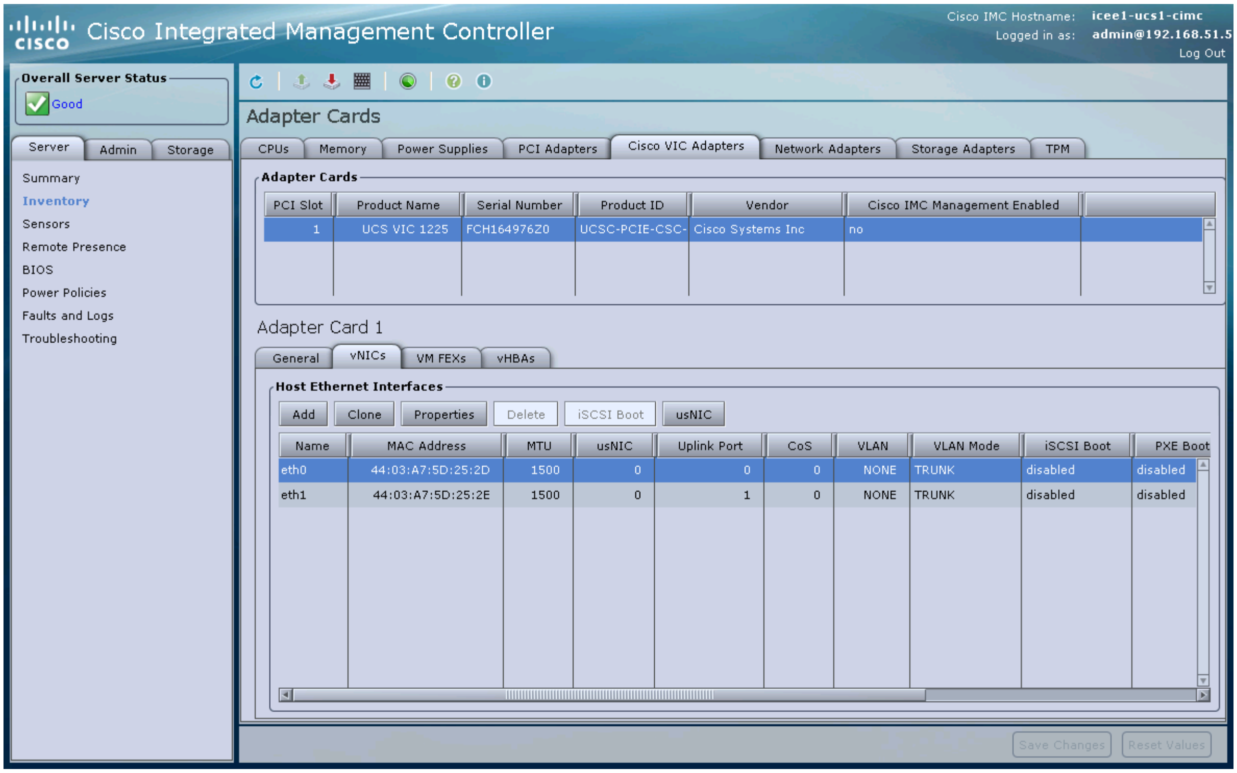
All Servers

1. Open a web browser and browse to the Cisco IMC interface IP address.
2. Log into the Cisco IMC interface, the default user name is admin and use the admin password: `<<admin_password>>` set in the CIMC interface setup.



Cisco Integrated Management Controller
iceg1-ucs1
Version: 2.0(1a)

3. After successfully logging in, click the Inventory tab and select Cisco VIC Adapters. From the Adapter Card 1 section, select the vNICs.



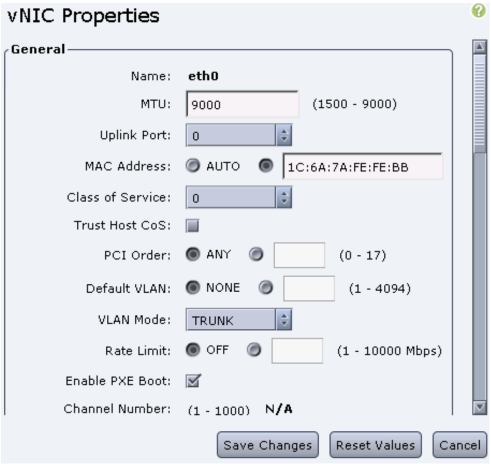
Adapter Cards

PCI Slot	Product Name	Serial Number	Product ID	Vendor	Cisco IMC Management Enabled
1	UCS VIC 1225	FCH164976Z0	UCSC-PCIE-CSC-	Cisco Systems Inc	no

Host Ethernet Interfaces

Name	MAC Address	MTU	usNIC	Uplink Port	CoS	VLAN	VLAN Mode	iSCSI Boot	PXE Boot
eth0	44:03:A7:5D:25:2D	1500	0	0	0	NONE	TRUNK	disabled	disabled
eth1	44:03:A7:5D:25:2E	1500	0	1	0	NONE	TRUNK	disabled	disabled

4. Select eth0 and click Properties.
5. In the vNIC properties dialog box, set the MTU to 9000 and click Save Changes.


vNIC Properties

General

Name: eth0
MTU: 9000 (1500 - 9000)
Uplink Port: 0
MAC Address: ○ AUTO ● 1C:6A:7A:FE:FE:BB
Class of Service: 0
Trust Host CoS: □
PCI Order: ● ANY ○ (0 - 17)
Default VLAN: ● NONE ○ (1 - 4094)
VLAN Mode: TRUNK
Rate Limit: ● OFF ○ (1 - 10000 Mbps)
Enable PXE Boot: ☑
Channel Number: (1 - 1000) N/A

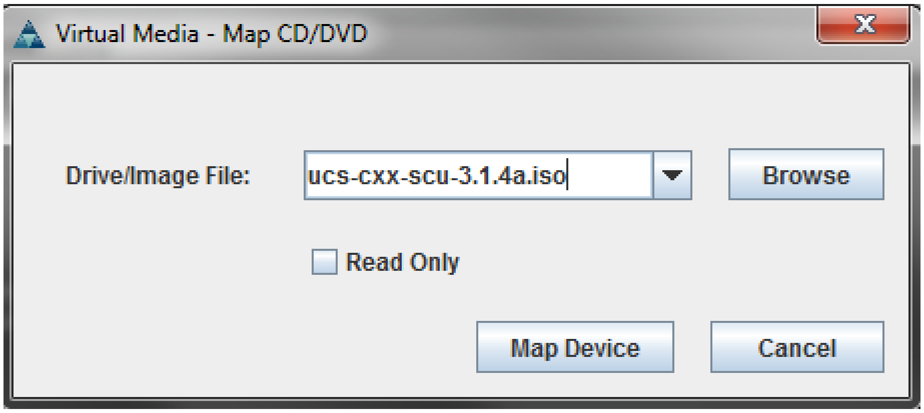
6. Select eth1 and click Properties.
7. In the vNIC properties dialog box, set the MTU to 9000 and click Save Changes.

10.3 Installing Windows Server 2012 R2

All Servers

1. Open a web browser and browse to the Cisco IMC interface IP address.

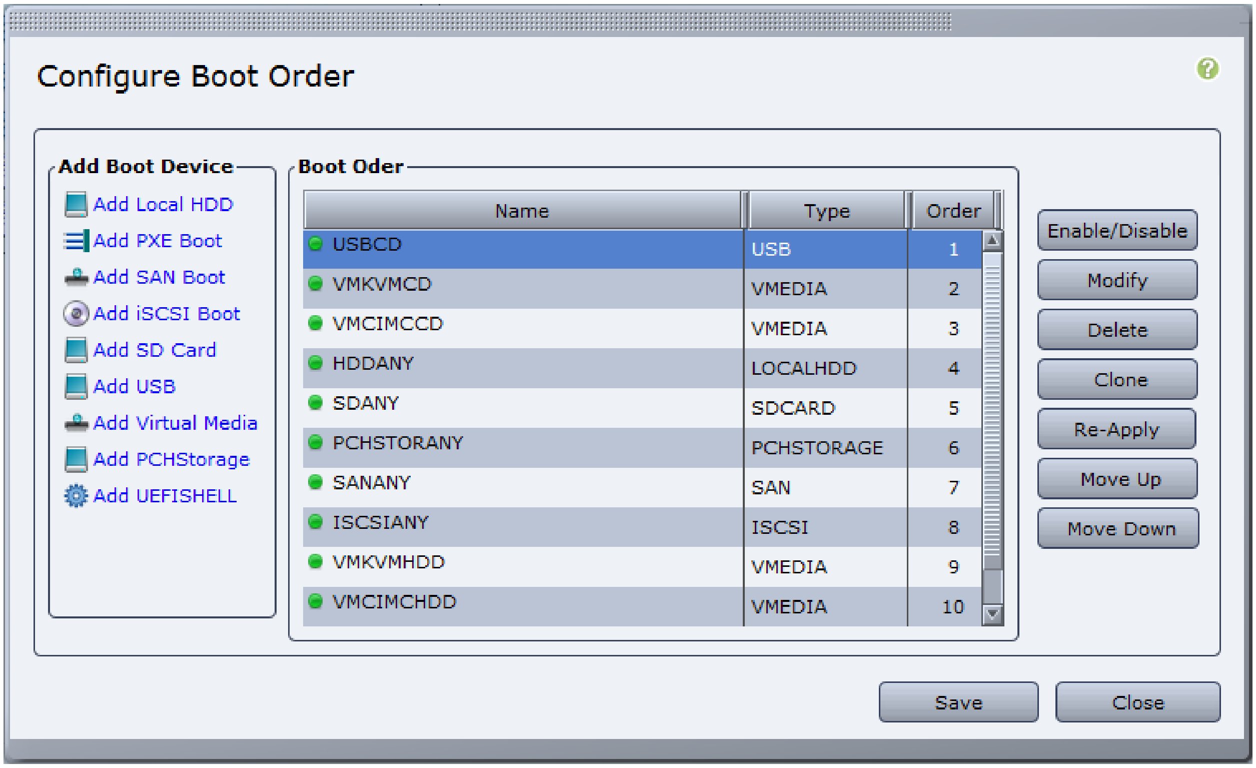
2. Log into the Cisco IMC interface, the default username is `admin` and use the admin password: <<admin_password>> set in the Cisco IMC interface setup.
3. After logging in, click the Server tab and then choose Summary. Choose Launch KVM Console.
4. The virtual KVM window opens. Choose Virtual Media at the top of the window.
5. Click Activate Virtual Devices.
6. Click Map CD/DVD.
7. Browse to the location of the Server Configuration Utility ISO image and select it. Click Map Device.



Drive/Image File: ucs-cxx-scu-3.1.4a.iso

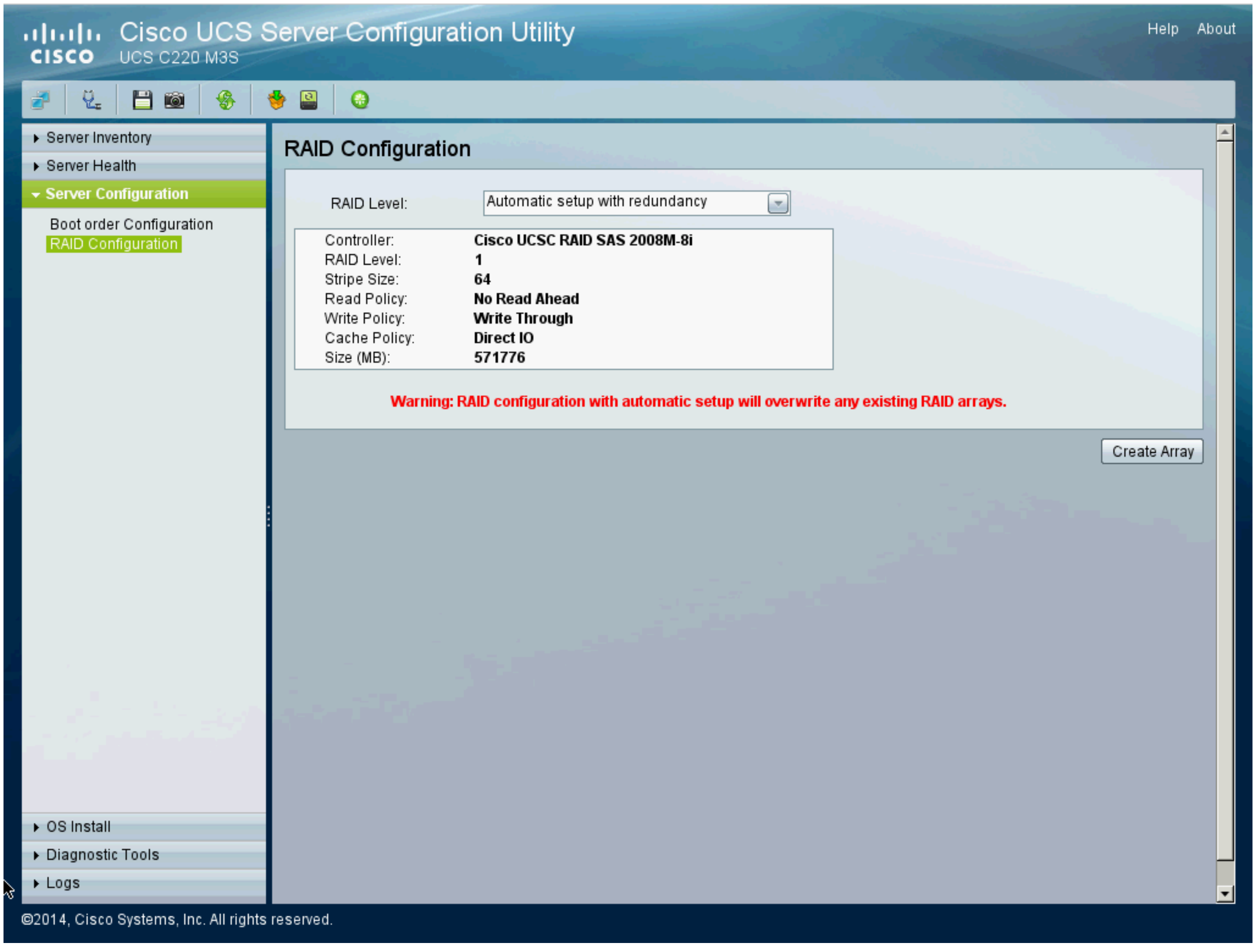
□ Read Only

8. Return to the Cisco IMC interface browser window (do not close the virtual KVM window), click the Server tab, and choose BIOS.
9. Choose Configure Boot Order and click OK.
10. Make sure the boot options are configured as follows:



Name	Type	Order
USBCD	USB	1
VMKVMCD	VMEDIA	2
VMCIMCCD	VMEDIA	3
HDDANY	LOCALHDD	4
SDANY	SDCARD	5
PCHSTORANY	PCHSTORAGE	6
SANANY	SAN	7
ISCSIANY	ISCSI	8
VMKVMHDD	VMEDIA	9
VMCIMCHDD	VMEDIA	10

11. Click the Server tab and choose Summary. Choose Power Cycle Server.
12. Return to the virtual KVM window. Click the KVM tab at the top of the window.
13. The server should now boot into the Server Configuration Utility.
14. Click the Server Configuration tab in the left pane.
15. Choose RAID Configuration.
16. In the upper-right corner, click the Configure ⚙ button.
17. In the RAID Level drop-down box, choose Automatic Setup with Redundancy. Click Create Array.



RAID Configuration

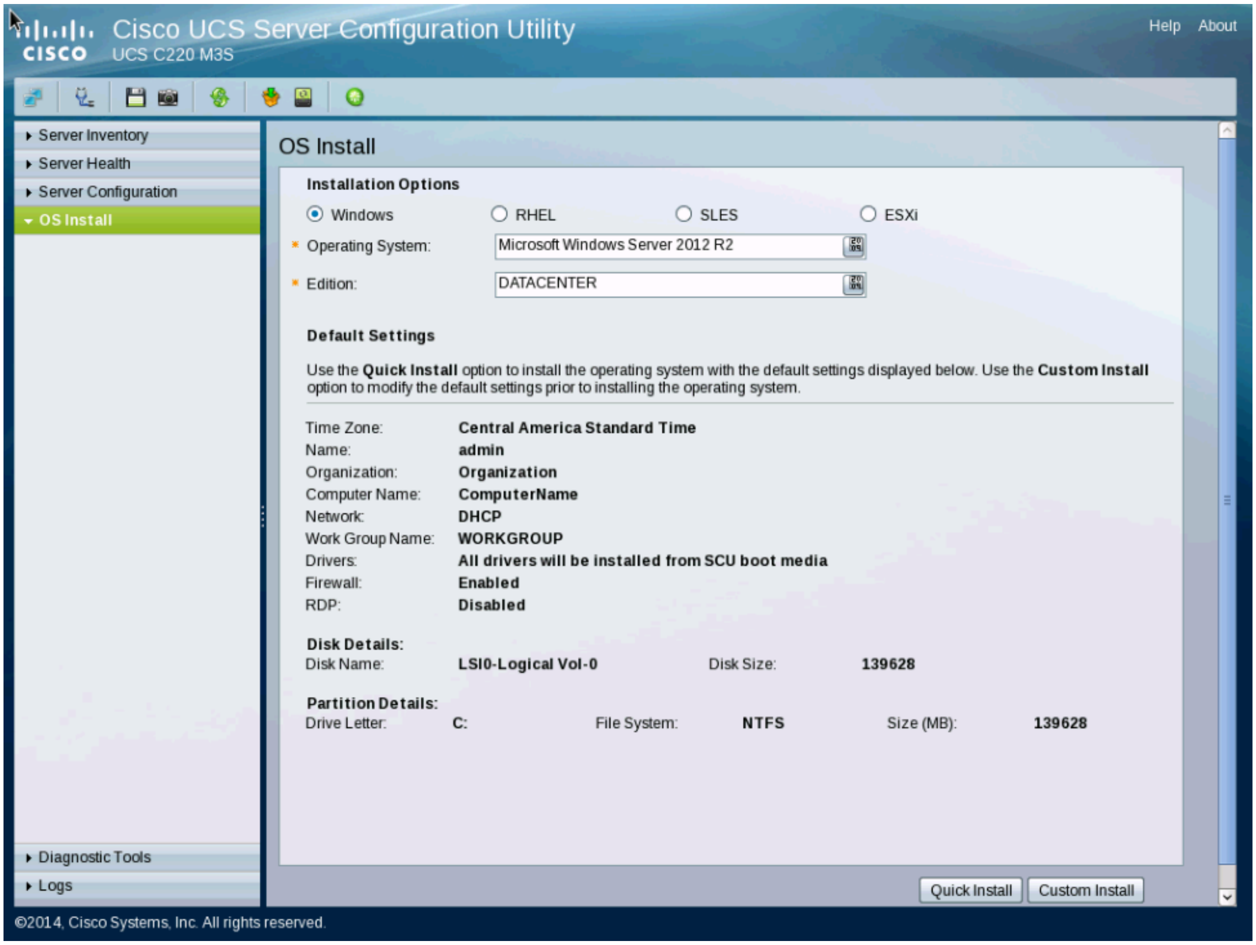
RAID Level: Automatic setup with redundancy

Controller:	Cisco UCSC RAID SAS 2008M-8i
RAID Level:	1
Stripe Size:	64
Read Policy:	No Read Ahead
Write Policy:	Write Through
Cache Policy:	Direct IO
Size (MB):	571776

Warning: RAID configuration with automatic setup will overwrite any existing RAID arrays.

©2014, Cisco Systems, Inc. All rights reserved.

18. When the RAID configuration is complete, close the virtual KVM window.
19. Select the OS Install tab.
20. Select the Windows Installation Option and select Microsoft Windows Server 2012 R2. Then select DATACENTER as the edition.
21. Click the Quick Install button.



OS Install

Installation Options

● Windows ○ RHEL ○ SLES ○ ESXi

* Operating System: Microsoft Windows Server 2012 R2

* Edition: DATACENTER

Default Settings

Use the **Quick Install** option to install the operating system with the default settings displayed below. Use the **Custom Install** option to modify the default settings prior to installing the operating system.

Time Zone:	**Central America Standard Time**
Name:	**admin**
Organization:	**Organization**
Computer Name:	**ComputerName**
Network:	**DHCP**
Work Group Name:	**WORKGROUP**
Drivers:	**All drivers will be installed from SCU boot media**
Firewall:	**Enabled**
RDP:	**Disabled**

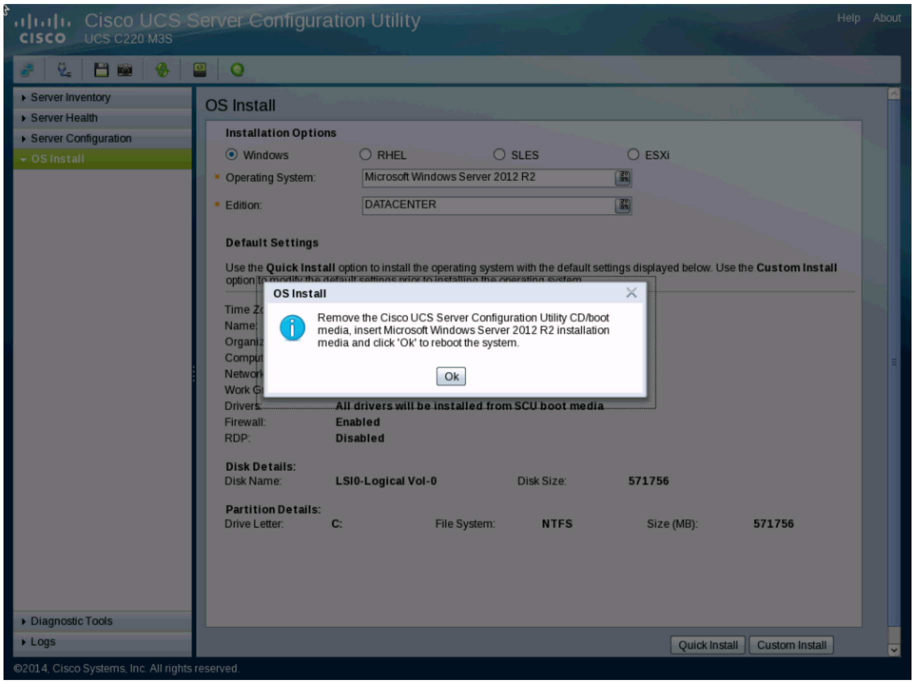
Disk Details:

Disk Name: **LSI0-Logical Vol-0** Disk Size: **139628**

Partition Details:

Drive Letter: **C:** File System: **NTFS** Size (MB): **139628**

22. When prompted, unmap the Server Configuration Utility and map the Windows Server 2012 R2 installation media. Then click OK to continue the automated installation.



OS Install

Installation Options

● Windows ○ RHEL ○ SLES ○ ESXi

* Operating System: Microsoft Windows Server 2012 R2

* Edition: DATACENTER

Default Settings

Use the **Quick Install** option to install the operating system with the default settings displayed below. Use the **Custom Install** option to modify the default settings prior to installing the operating system.

OS Install

Remove the Cisco UCS Server Configuration Utility CD/boot media, insert Microsoft Windows Server 2012 R2 installation media and click 'Ok' to reboot the system.

Ok

Time Z
Name:
Organiz
Comput
Network
Work G
Drivers: **All drivers will be installed from SCU boot media**
Firewall: **Enabled**
RDP: **Disabled**

Disk Details:
Disk Name: **LSI0-Logical Vol-0** Disk Size: **571756**

Partition Details:
Drive Letter: **C:** File System: **NTFS** Size (MB): **571756**

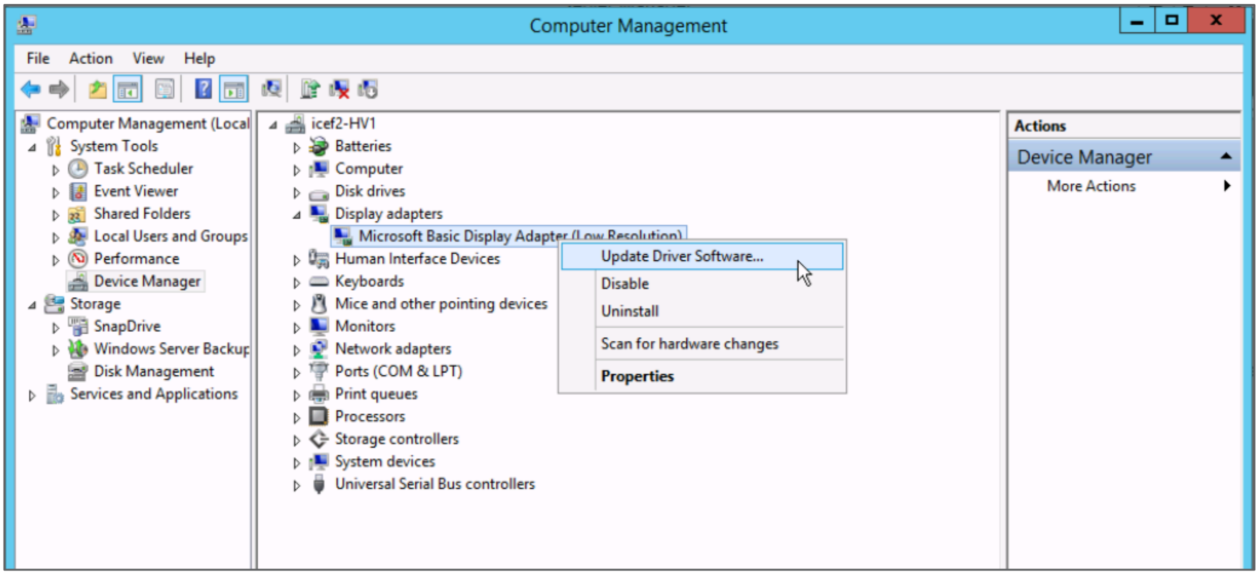
23. The server will automatically reboot and perform an automated installation of Windows Server 2012 R2.
24. The machine will reboot several times while installing Windows. When the installation is completed, windows will enter the out-of-box setup experience.
25. Enter the relevant region information and click Next.
26. Accept the license agreement.
27. Enter an administrator password on the Settings page and click Finish.

10.4 Updating Windows Drivers

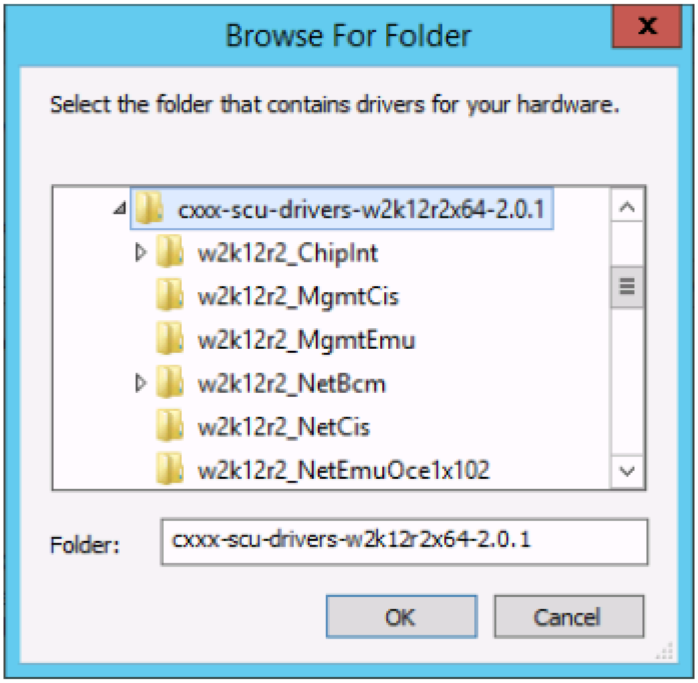
The following steps describe how to update the drivers on physical components that are used by the Windows operating system.

All Hosts

1. Log in to Windows with the administrator password entered previously during installation.
2. Open a web browser and navigate to http://software.cisco.com/download/type.html?mdfid=284296253&catid=null&softwareid=283291009.
3. Select Windows 2012r2 64-bit as the platform and download the latest version of the drivers package.
4. Extract the downloaded drivers package.
5. Launch the Windows Server Manager utility, select Tools on the top right of the window, and select Computer Management.
6. From the Computer Management window, under System Tools, select Device Manager.
7. Expand Display Adapters and right-click Microsoft Basic Display Adapter (Low Resolution).
8. Select Update Driver Software.



9. Click Browse My Computer for Driver Software.
10. Using the Browse button, navigate to the root folder of the extracted drivers package and click OK.


Browse For Folder

Select the folder that contains drivers for your hardware.

Folder: cxxx-scu-drivers-w2k12r2x64-2.0.1

11. Click Next, and the Windows display driver is installed.

    Note: You may lose the display for some time when the driver update is in progress.

12. Click Close when the driver update has completed.
13. Repeat the previous steps to update the drivers on any other devices.

    Note: NetApp recommends that you update the drivers on the network adapters and storage controllers. You may need to restart the system while updating the drivers on some devices.

14. If applicable, update the drivers on the chipset as follows:
    a. Navigate to the root folder of the extracted drivers package.
    b. Within the root folder, browse to the folder `w2k12r2_ChipInt`.
    c. Launch the Setup application file by double-clicking it.
    d. Click Run and then Next.
    e. Click Yes to accept the license agreement.
    f. Click Next after reviewing the readme file.
    g. Click Finish when the setup is complete.

10.5 Installing Windows Features

The following steps describe how to install the required Windows Server 2012 R2 features.

All Servers

1. From the Cisco IMC virtual KVM console, select the Virtual Media tab.
2. Click Map CD/DVD.
3. Browse to the Windows Server 2012 R2 installer ISO image file and click Map Device.
4. Log in to Windows with the administrator password previously entered during installation.
5. Launch a Microsoft Windows PowerShell® prompt by right-clicking the PowerShell icon in the taskbar and selecting Run as Administrator.
6. Enable remote management and remote desktop using the SCONFIG application.

```
SCONFIG
```

7. Select Configure Remote Management.
8. Select Enable Remote Management.
9. Select Return to the main menu.
10. Select Remote Desktop.
11. Enter `E` to Enable.
12. Enter `2` to allow any version of remote desktop. After this step, you will be returned to the main menu.
13. Select Exit to Command Line.
14. Add the .NET 3.5, Hyper-V, Multipath I/O (MPIO), and clustering features by entering the following command:

```
Add-WindowsFeature Hyper-V, NET-Framework-Core, Failover-Clustering, Multipath-IO `
    -IncludeManagementTools -Source E:\sources\sxs -Restart
```

Note: Assuming the ISO image is mounted to drive E:\.

15. Unmap the Windows Server 2012 R2 Installation media from the Virtual Media tab.

10.6 Configuring Windows

The following steps describe how to configure the network for each Hyper-V host.

All Servers

1. Log in with the Administrator password previously entered during installation.
2. Launch a PowerShell prompt by right-clicking the PowerShell icon in the taskbar, and selecting Run as Administrator.

3. Find the 10GbE interfaces by running the following command:

```
PS C:\Users\Administrator> Get-NetAdapter

Name       InterfaceDescription            ifIndex Status       MacAddress        LinkSpeed
----       --------------------            ------- ------       ----------        ---------
Ethernet 4 Cisco VIC Ethernet Interface #2      15 Up           44-03-A7-5D-25-2E   10 Gbps
Ethernet 3 Cisco VIC Ethernet Interface         14 Up           44-03-A7-5D-25-2D   10 Gbps
Ethernet 2 Cisco 1GigE I350 LOM #2              13 Disconnected 00-06-F6-E6-40-BF     0 bps
Ethernet   Cisco 1GigE I350 LOM                 12 Disconnected 00-06-F6-E6-40-BE     0 bps
```

4. Configure jumbo frames on the physical interfaces.

```
Set-NetAdapterAdvancedProperty -Name Ethernet* -DisplayName "Jumbo Packet" -DisplayValue "9014
Bytes" –EA SilentlyContinue
Set-NetAdapterAdvancedProperty -Name Ethernet* -DisplayName "Jumbo Packet" -DisplayValue "9014" –
EA SilentlyContinue
```

5. Create a NIC team. From a PowerShell prompt enter:

```
New-NetLbfoTeam -Name TM1 -TeamMembers <10GBE_nic1>, <10GBE_nic2> -TeamingMode lacp -
LoadBalancing HyperVPort
```

Note: From the example output used in step 3, the command would be:

```
New-NetLbfoTeam -Name TM1 -TeamMembers 'Ethernet 3','Ethernet 4' -TeamingMode lacp -LoadBalancing
HyperVPort
```

6. Remove the IP stack from the TM NIC interface.

```
Get-NetAdapter TM1 | set-NetAdapterBinding -ComponentID ms_tcpip* -Enabled $false
```

7. Create Hyper-V virtual switch for the management, and VM traffic.

```
New-VMSwitch -Name VMComm -NetAdapterName TM1 -AllowManagementOS $false
```

8. Create VM NICs.

```
Add-VMNetworkAdapter -ManagementOS -Name Mgmt -SwitchName VMComm
Add-VMNetworkAdapter -ManagementOS -Name Cluster -SwitchName VMComm
Add-VMNetworkAdapter -ManagementOS -Name LM -SwitchName VMComm
Add-VMNetworkAdapter -ManagementOS -Name SMB -SwitchName VMComm
Set-VMNetworkAdapterVlan -ManagementOS -VMNetworkAdapterName Mgmt -Access -AccessVlanId
<<ib_mgmt_vlan_id>>
Set-VMNetworkAdapterVlan -ManagementOS -VMNetworkAdapterName SMB -Access -AccessVlanId
<<smb_vlan_id>>
Set-VMNetworkAdapterVlan -ManagementOS -VMNetworkAdapterName LM -Access -AccessVlanId
<<livemigraion_vlan_id>>
Set-VMNetworkAdapterVlan -ManagementOS -VMNetworkAdapterName CSV -Access -AccessVlanId
<<cluster_vlan_id>>
```

9. Configure jumbo frames on the select interfaces.

```
Set-NetAdapterAdvancedProperty -Name *SMB*,*LM*,*Cluster* -DisplayName "Jumbo Packet" -
DisplayValue "9014 Bytes" –EA SilentlyContinue
Set-NetAdapterAdvancedProperty -Name *SMB*,*LM*,*Cluster* -DisplayName "Jumbo Packet" -
DisplayValue "9014" –EA SilentlyContinue
```

10. Set IP address information for each host NIC.

```
New-NetIPAddress -InterfaceAlias 'vEthernet (Mgmt)' -IPAddress <Mgmt_Ipaddress> -DefaultGateway
<<Mgmt_gateway>> -PrefixLength <Mgmt_network_prefix>
New-NetIPAddress -InterfaceAlias 'vEthernet (CSV)' -IPAddress <CSV_ipaddress> -Prefix
<CSV_prefix>
New-NetIPAddress -InterfaceAlias 'vEthernet (LM)' -IPAddress <LM_ipaddress> -Prefix <LM_prefix>
New-NetIPAddress -InterfaceAlias 'vEthernet (SMB)' -IPAddress <SMB_ipaddress> -Prefix <SMB
prefix>
```

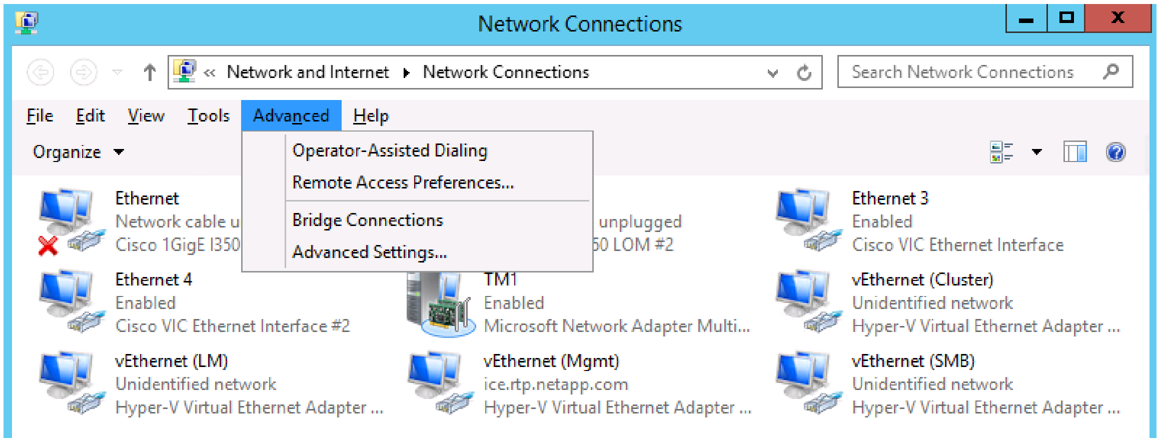
11. Disable DNS registration for all NICs.

```
Set-DnsClient -InterfaceAlias * -Register $false
```

12. Turn registration back on and configure DNS for the mgmt NIC.

```
Set-DnsClient -InterfaceAlias 'vEthernet (Mgmt)' -Register $true -ConnectionSpecificSuffix
<dns_connection_suffix>
Set-DnsClientServerAddress -InterfaceAlias 'vEthernet (Mgmt)' -ServerAddresses <dns_server_ips>
```

13. From the CLI, enter `control netconnections` to open the Network Connections control panel.
14. Press the Alt key to access the Advanced menu.
15. Click the Advanced tab and select Advanced Settings.


Network Connections
« Network and Internet ▸ Network Connections
Search Network Connections
File Edit View Tools Advanced Help
Organize ▾
Operator-Assisted Dialing
Remote Access Preferences...
Bridge Connections
Advanced Settings...

Ethernet
Network cable u... unplugged
Cisco 1GigE I350 ...50 LOM #2

Ethernet 3
Enabled
Cisco VIC Ethernet Interface

Ethernet 4
Enabled
Cisco VIC Ethernet Interface #2

TM1
Enabled
Microsoft Network Adapter Multi...

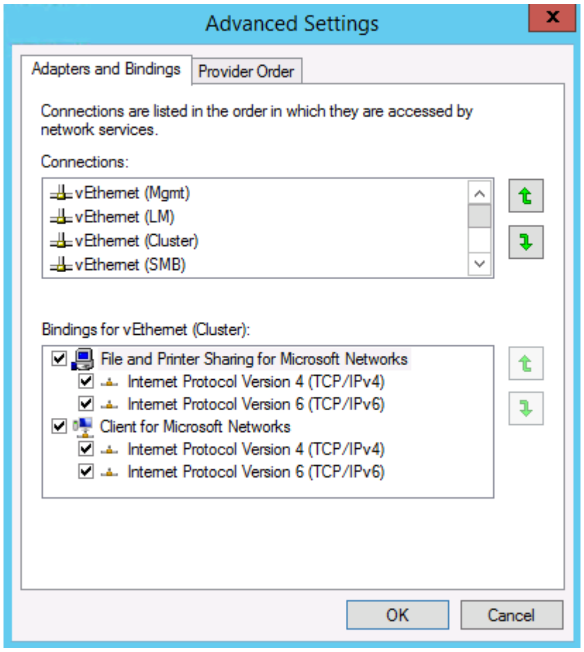
vEthernet (Cluster)
Unidentified network
Hyper-V Virtual Ethernet Adapter ...

vEthernet (LM)
Unidentified network
Hyper-V Virtual Ethernet Adapter ...

vEthernet (Mgmt)
ice.rtp.netapp.com
Hyper-V Virtual Ethernet Adapter ...

vEthernet (SMB)
Unidentified network
Hyper-V Virtual Ethernet Adapter ...

16. Use the green arrows to modify the connection binding order as follows:
    a. vEthernet (MGMT)
    b. vEthernet (LM)
    c. vEthernet (Cluster)
    d. vEthernet (SMB)



Connections are listed in the order in which they are accessed by network services.

Connections:

- vEthernet (Mgmt)
- vEthernet (LM)
- vEthernet (Cluster)
- vEthernet (SMB)

Bindings for vEthernet (Cluster):

☑ File and Printer Sharing for Microsoft Networks
  ☑ Internet Protocol Version 4 (TCP/IPv4)
  ☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Client for Microsoft Networks
  ☑ Internet Protocol Version 4 (TCP/IPv4)
  ☑ Internet Protocol Version 6 (TCP/IPv6)

17. Rename the server and join the domain.

```
Rename-Computer <ServerName> -restart
Add-Computer -DomainName <dns_connection_suffix> -Restart
```

Note: A dialog box prompts for a password. After the password is entered, the server reboots.

18. Upon reboot, launch a PowerShell prompt by right-clicking the PowerShell icon in the taskbar, and selecting Run as Administrator.

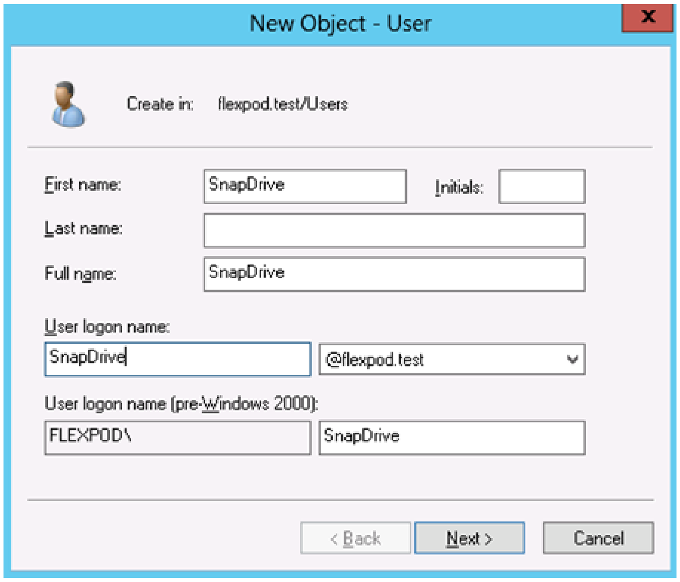
Installing NetApp SnapDrive

The following section describes how to install NetApp SnapDrive for Windows. For detailed installation procedures, refer to the SnapDrive Installation Guide.

All Hosts

1. In Active Directory, create a SnapDrive service account.

Note: This account requires no special delegation, and the same account can be used for multiple hosts.



Create in: flexpod.test/Users

First name: SnapDrive

Initials:

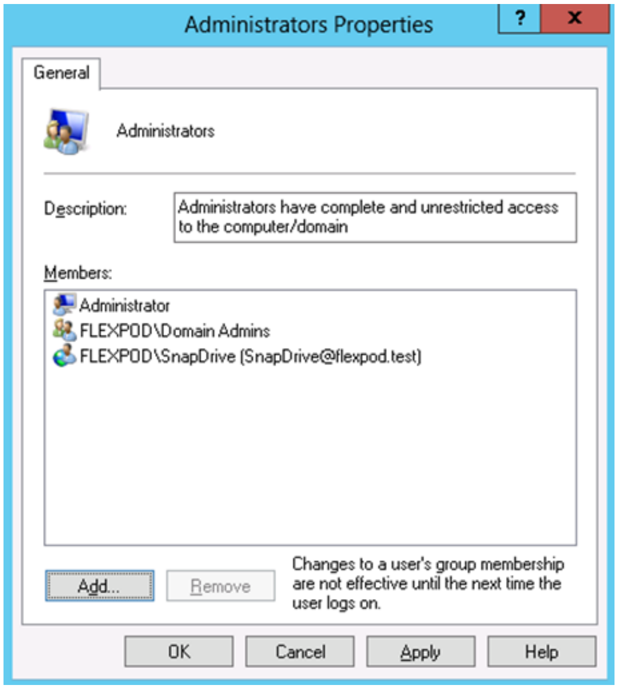
Last name:

Full name: SnapDrive

User logon name: SnapDrive @flexpod.test

User logon name (pre-Windows 2000): FLEXPOD\ SnapDrive

2. Add the SnapDrive service account to the local administrator's group in Windows.



Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

Members:

Administrator
FLEXPOD\Domain Admins
FLEXPOD\SnapDrive (SnapDrive@flexpod.test)

Changes to a user's group membership are not effective until the next time the user logs on.

3. Download the SnapDrive installer from the NetApp Support site.
4. Launch the installer and click Next.
5. Select the Storage Based Licensing method and click Next.
6. Enter your user name and organization information, and click Next.
7. Validate the installation path and click Next.
8. Select the Enable SnapDrive to Communicate Through the Windows Firewall checkbox and click Next.
9. Enter the information for the SnapDrive service account and click Next.
10. On the SnapDrive Web Service Configuration page, click Next.
11. Clear the Enable Preferred Storage System IP Address checkbox and click Next.
12. Clear the Enable Transport Protocol Settings checkbox and click Next.
13. Leave Enable Unified Manager Configuration unchecked and click Next.
14. Click Install.
15. After the installation has finished, launch a new PowerShell prompt by right-clicking the PowerShell icon in the taskbar and selecting Run as Administrator.

    Note: A new prompt is required to register the `sdcli` as executable.

16. Configure the SnapDrive preferred IP settings for each storage controller.

```
sdcli preferredIP set -f <<var_vserver_name>> -IP << var_vserver_mgmt_ip>>
```

17. Configure the SnapDrive transport protocol authentication configuration for each storage controller.

```
Set-SdStorageConnectionSetting -StorageSystem <<var_vserver_mgmt>> -protocol https -credential
vsadmin
```

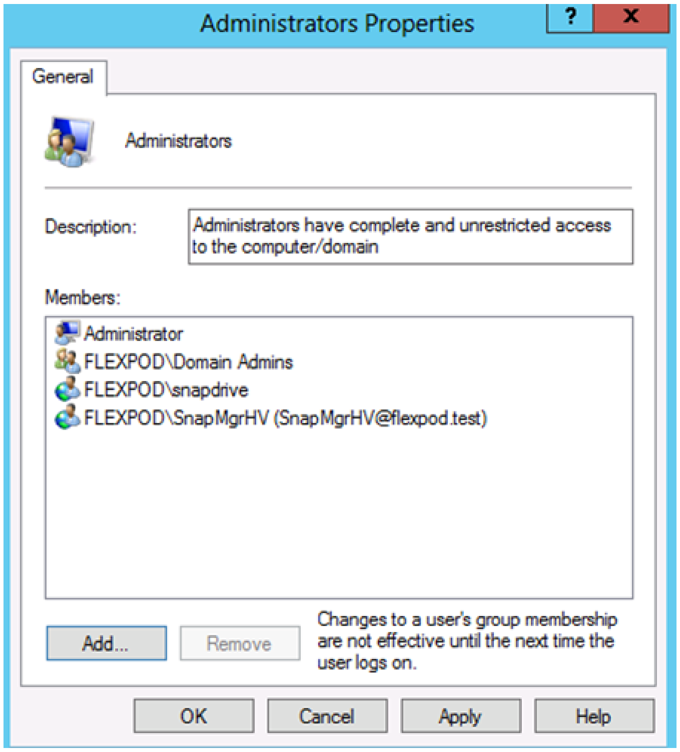
Installing NetApp SnapManager for Hyper-V

The following section describes how to install NetApp SnapManager for Hyper-V (SMHV). For detailed installation procedures, refer to the SnapManager 2.0 for Hyper-V SnapManager Installation and Administration Guide.

1. In Active Directory, create an SMHV service account.

   Note: This account requires no special delegation, and the same account can be used for multiple hosts.

2. Add the SMHV service account to the local administrator's group in Windows.



Administrators Properties

General

Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

Members:

Administrator
FLEXPOD\Domain Admins
FLEXPOD\snapdrive
FLEXPOD\SnapMgrHV (SnapMgrHV@flexpod.test)

Changes to a user's group membership are not effective until the next time the user logs on.

3. Download the SMHV installer from the NetApp Support site.
4. Launch the installer and click Next.
5. Select the Storage Based Licensing method and click Next.
6. Validate the installation path and click Next.
7. Enter the information for the SMHV service account and click Next.
8. On the SMHV Web Service Configuration page, click Next.
9. Click Install.

10.7 Creating Windows Failover Cluster

To create the Windows failover cluster, log into any one of the Hyper-V hosts and complete the following steps:

1. Create the Windows failover cluster.

```
New-Cluster -Name <cluster_name> -Node <hostnames> -NoStorage -StaticAddress <cluster_ip_address>
```

Note: Additional servers can be added to the cluster at a later stage.

2. Name the cluster networks according to their usage. Use the following commands to name the networks.

```
Get-ClusterNetworkInterface | ? Name -like *Cluster* | Group Network| %{ (Get-ClusterNetwork
$_.Name).Name = 'Cluster'}
Get-ClusterNetworkInterface | ? Name -like *LM* | Group Network| %{ (Get-ClusterNetwork
$_.Name).Name = 'LM'}
Get-ClusterNetworkInterface | ? Name -like *SMB* | Group Network| %{ (Get-ClusterNetwork
$_.Name).Name = 'SMB'}
Get-ClusterNetworkInterface | ? Name -like *Mgmt* | Group Network| %{ (Get-ClusterNetwork
$_.Name).Name = 'Mgmt'}
```

3. Set cluster network role types to allow only client connections on the management network and to prevent cluster communication on the iSCSI network.

```
(Get-ClusterNetwork Cluster).role = 1
(Get-ClusterNetwork LM).role = 1
(Get-ClusterNetwork SMB).role = 0
(Get-ClusterNetwork Mgmt).role = 3
```

Note: A setting of 0 prevents all cluster traffic, 1 allows cluster communication, and 3 allows both client and cluster communication.

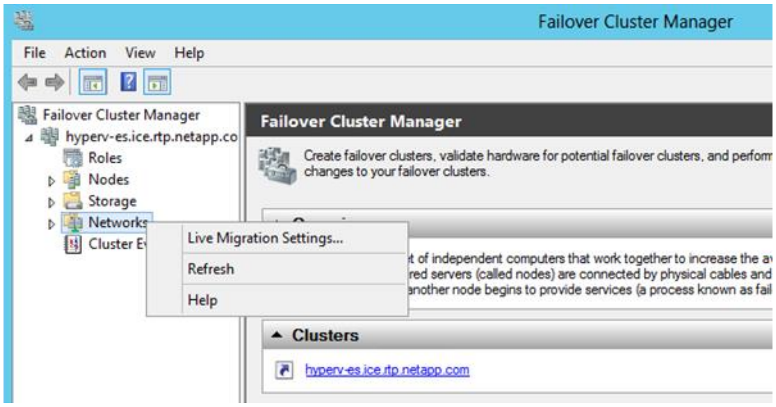
Configuring Live Migration

The preferred live migration network can be set through either the GUI or the CLI. The CLI requires modifying the registry; as such, NetApp recommends using the GUI.

Configuring Using the GUI

To configure the live migration network through the GUI, complete the following steps:

1. From Server Manager, select Tools and then select Failover Cluster Manager.
2. Expand the cluster tree on the left, right-click Networks, and select Live Migration Settings.



Create failover clusters, validate hardware for potential failover clusters, and perform changes to your failover clusters.

t of independent computers that work together to increase the a
red servers (called nodes) are connected by physical cables and
another node begins to provide services (a process known as fail

3. Make sure that the only option selected is the live migration network and click OK.

Configuring Using the CLI

To configure the live migration network through the CLI, complete the following step:

1. Configure the live migration network.

```
$LiveMigrate = Get-Clusternetwork LM
$Cluster = Get-Clusternetwork Cluster
```

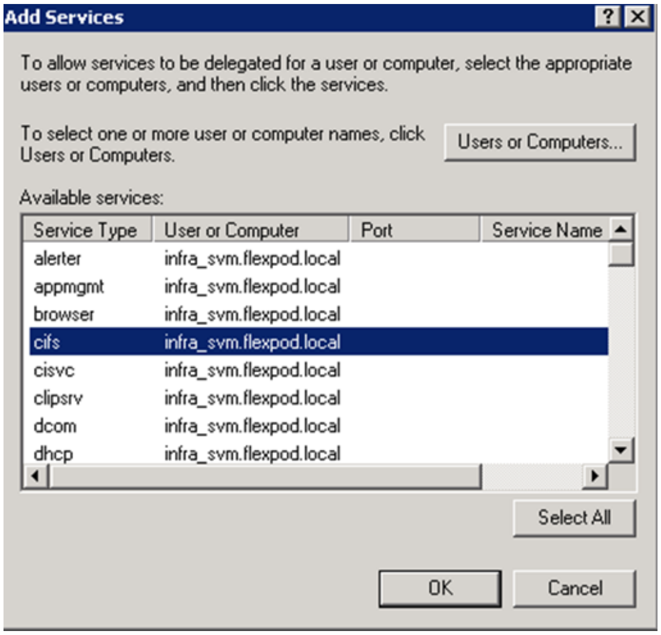
```
$MGMT = Get-Clusternetwork MGMT
$SMB = Get-Clusternetwork SMB

$includeIDs = $LiveMigrate.id
$excludeIDs = $MGMT.id + ";" + $SMB.id + ";" + $Cluster.id
Set-ItemProperty -Path "HKLM:\Cluster\ResourceTypes\Virtual Machine\Parameters" -Name
MigrationExcludeNetworks -Value $excludeIDs
Set-ItemProperty -Path "HKLM:\Cluster\ResourceTypes\Virtual Machine\Parameters" -Name
MigrationNetworkOrder -Value $includeIDs
```

Configuring Constrained Delegation for Hyper-V Hosts

Although the hosts have the required permissions to access the SMB share, you may encounter access-denied errors when trying to remotely manage the hosts. To avoid these error messages, configure constrained delegation for the Hyper-V hosts by completing the following steps:

1. In Active Directory Users and Computers, browse to the Computer objects for each Hyper-V host.
2. Right-click the object and select Properties.
3. Select the Delegation tab.
    a. Select Trust This Computer for Delegation to the Specific Services Only.
    b. Select Use Kerberos Only.
    c. Click Add.
4. Click the Users or Computers button on the top of the Add Services dialog box.
5. Enter the name of the infrastructure storage virtual machine (SVM) and click OK.
6. Select CIFS and click OK.



Add Services

To allow services to be delegated for a user or computer, select the appropriate users or computers, and then click the services.

To select one or more user or computer names, click Users or Computers.

Available services:

Service Type	User or Computer	Port	Service Name
alerter	infra_svm.flexpod.local		
appmgmt	infra_svm.flexpod.local		
browser	infra_svm.flexpod.local		
cifs	infra_svm.flexpod.local		
cisvc	infra_svm.flexpod.local		
clipsrv	infra_svm.flexpod.local		
dcom	infra_svm.flexpod.local		
dhcp	infra_svm.flexpod.local		

7. Click OK.
8. Repeat steps 1 through 7 for each Hyper-V host.

Changing Management Cluster to Use a File Share Witness

To change the management cluster to use the quorum disk, complete the following steps on one server only.

1. Open an SSH connection to the cluster IP or host name and log in as the admin user using the password you provided earlier.
2. Remove the Everyone permission from the witness share.

```
cifs share access-control delete -share hyperv-witness -user-or-group Everyone -vserver infra_svm
```

3. Add permissions for the following accounts with NTFS full control permissions over the share:
   - Hyper-V Node 1
   - Hyper-V Node 2
   - Hyper-V Node 3
   - Hyper-V Node 4
   - Hyper-V Cluster Name Object (CNO)

```
share access-control create -share hyperv-witness -user-or-group FLEXPOD\HyperV1$ -permission
full_Control -vserver infra_svm
share access-control create -share hyperv-witness -user-or-group FLEXPOD\HyperV2$ -permission
full_Control -vserver infra_svm
share access-control create -share hyperv-witness -user-or-group FLEXPOD\HyperV3$ -permission
full_Control -vserver infra_svm
share access-control create -share hyperv-witness -user-or-group FLEXPOD\HyperV4$ -permission
full_Control -vserver infra_svm
share access-control create -share hyperv-witness -user-or-group FLEXPOD\HyperV$ -permission
full_Control -vserver infra_svm
```

4. Launch a PowerShell prompt by right-clicking the PowerShell icon in the taskbar and selecting Run as Administrator.
5. Set the cluster to use the SMB share created previously.

```
Set-ClusterQuorum -FileShareWitness \\infrasvm\hyperv-witness
```

Validating Management Cluster

To validate the management cluster, complete the following steps on one server only:

1. Select the cluster in the navigation pane and click Validate Cluster.
2. Select Run All Tests and click Next.
3. Select the shared disks on the cluster and click Next.
4. Confirm the selected options and click Next.
5. Review and correct any failures that are listed in the validation report.

   Note: The Validation wizard reports the following warnings, which can be safely disregarded because they apply only to configurations that utilize Microsoft Storage Spaces.

   ```
   Successfully issued call to Persistent Reservation REGISTER using
   Invalid RESERVATION KEY 0xc, SERVICE ACTION RESERVATION KEY 0xd, for
   Test Disk 0 from node VMHost-Mgmt1.flexpod.local.
   Test Disk 0 does not support SCSI-3 Persistent Reservations commands
   needed by clustered storage pools that use the Storage Spaces
   subsystem. Some storage devices require specific firmware versions
   or settings to function properly with failover clusters. Contact
   your storage administrator or storage vendor for help with
   configuring the storage to function properly with failover clusters
   that use Storage Spaces.
   ```

11 System Center 2012 R2 Virtual Machine Manager

The procedures in the following subsections provide detailed instructions for installing System Center 2012 R2 Virtual Machine Manager (VMM) in a FlexPod environment.

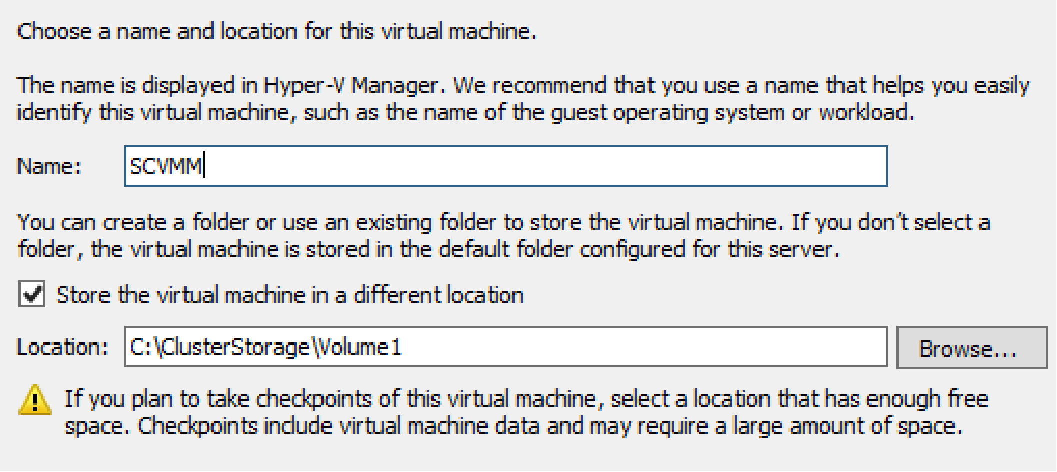
Table 8) VM requirements.

Role	Virtual CPU	RAM (GB)	Virtual Hard Disk (GB)
Virtual Machine Manager	4	8	60
SMI-S Agent	1	4	60

11.1 Building the SMI-S and SCVMM VMs

One Server Only

1. In the Failover Cluster Manager, right-click Roles, select Virtual Machines, and then select New Virtual Machine.
2. Select the host for the new VM and click OK.
3. On the New Virtual Machine welcome screen, click Next.
4. Enter the name for the VM (for example, SCVMM), select the Store the Virtual Machine in a Different Location checkbox, and enter the path for the CSV. Click Next.



Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: SCVMM

You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☑ Store the virtual machine in a different location

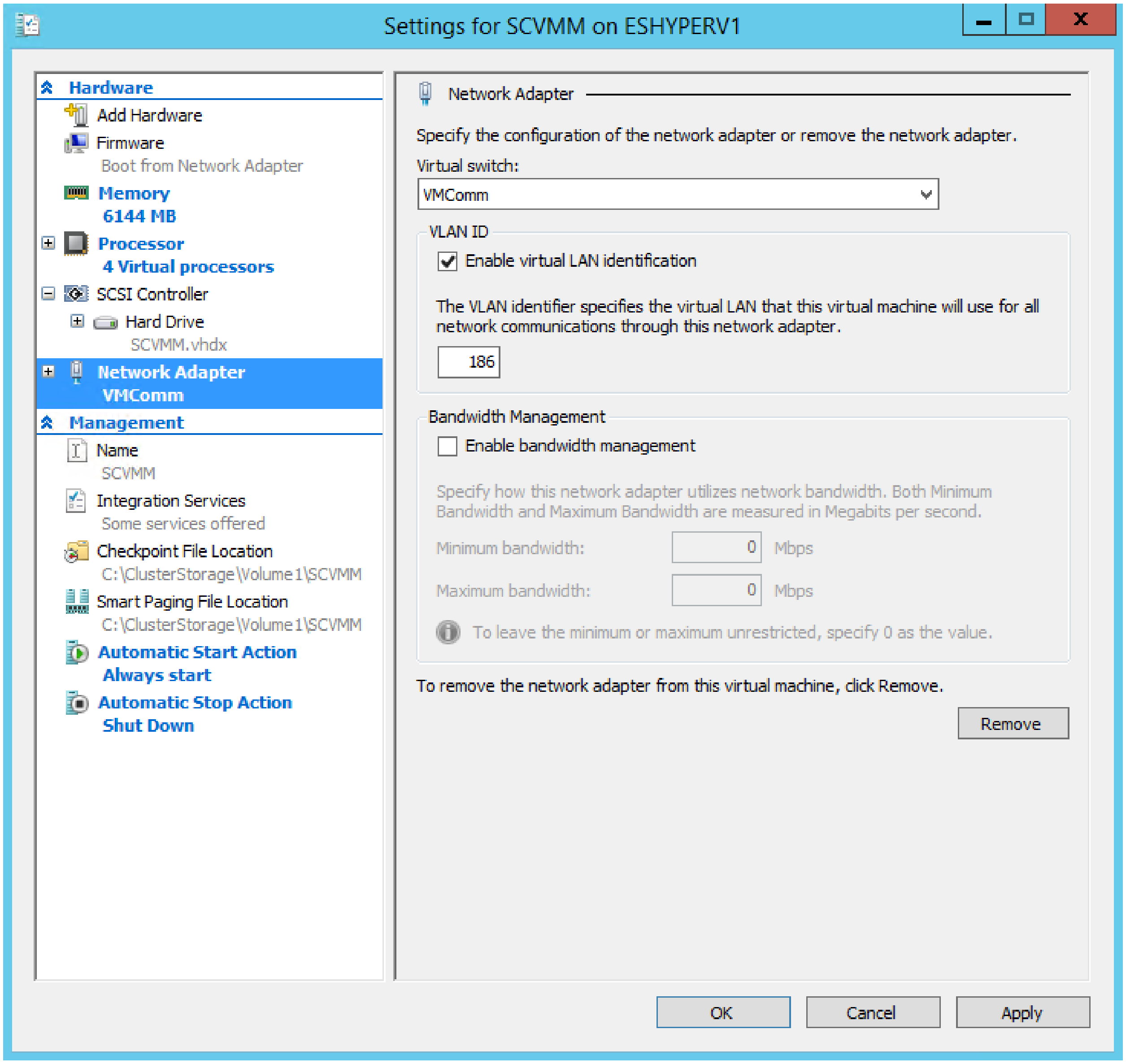
Location: C:\ClusterStorage\Volume1

If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

5. Select Generation 2 and click Next.
6. Enter the startup memory for the VM and select the Use Dynamic Memory for This Virtual Machine checkbox. Click Next.
7. Select VMComm Network and click Next.
8. Set the size for the new VHDX and click Next.
9. Select Install an Operating System from a Bootable Image File and provide the path to the Windows Server 2012 R2 ISO. Click Finish.
10. Click Finish in the High Availability Wizard Summary.
11. Repeat steps 1 through 10 for each remaining VM.

11.2 Configuring SMI-S and SCVMM VMs

1. In the Failover Cluster Manager, select Roles, right-click the VM to be modified, and select Settings.
2. Select Memory and set the Dynamic Memory Maximum RAM to the Startup RAM.
3. Select CPU and set the CPU to the desired amount outlined in Table 8.
4. Select Network Adapter, select the Enable Virtual LAN Identification checkbox, and enter the value for `<<ib_mgmt_vlan_id>>`.
5. Select Automatic Start Action and choose the Always Start This Virtual Machine Automatically option.
6. Select Automatic Stop Action and choose the Shut Down the Guest Operating System option.
7. Click OK to save the modifications.
8. Repeat steps 1 through 7 for each remaining VM.



Settings for SCVMM on ESHYPERV1

Network Adapter

Specify the configuration of the network adapter or remove the network adapter.

Virtual switch: VMComm

VLAN ID

☑ Enable virtual LAN identification

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

186

Bandwidth Management

☐ Enable bandwidth management

Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.

Minimum bandwidth: 0 Mbps

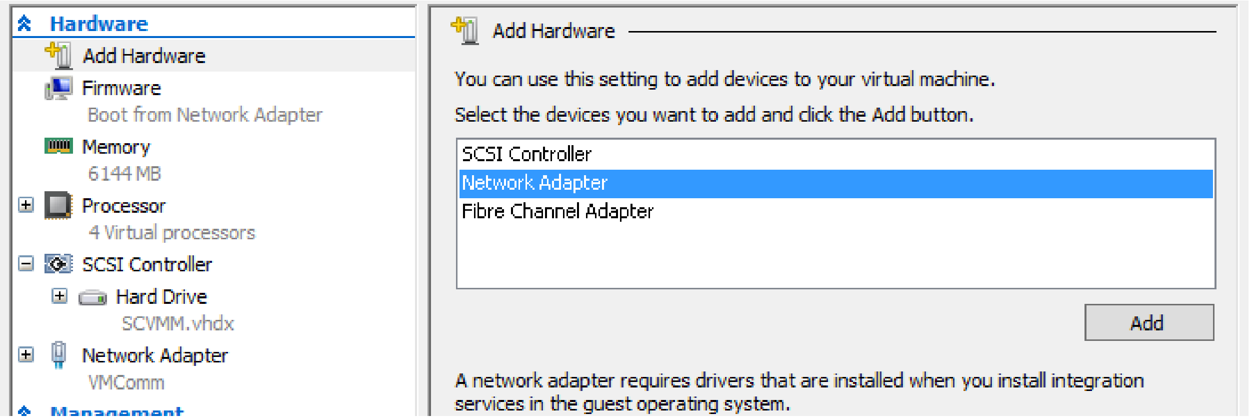
Maximum bandwidth: 0 Mbps

To leave the minimum or maximum unrestricted, specify 0 as the value.

To remove the network adapter from this virtual machine, click Remove.

11.3 Adding SMB Network Adapter to the SCVMM VM

1. In Failover Cluster Manager, select Roles. Right-click the SCVMM VM and select Settings.
2. From the Add Hardware section, select Network Adapter and click Add.



You can use this setting to add devices to your virtual machine.

Select the devices you want to add and click the Add button.

A network adapter requires drivers that are installed when you install integration services in the guest operating system.

3. Select the VMComm virtual switch, select the checkbox to enable virtual LAN identification, and enter the <<smb_vlan_id>>.
4. Click OK to save the modifications.

11.4 Installing Windows Server 2012 R2 on the VMs

1. In the Failover Cluster Manager, select Roles, right-click the desired VM, and select Connect.
2. Click the green Start button to power on the VM and boot into the Windows installer.
3. After the installer has finished loading, enter the relevant region information and click Next.
4. Click Install Now.
5. Enter the product key and click Next.
6. Select Windows Server 2012 R2 Datacenter (Server with a GUI) and click Next.
7. After reviewing the EULA, accept the license terms and click Next.
8. Select Custom: Install Windows Only (Advanced).
9. Select Drive 0, and click Next to continue with the installation.
10. When Windows has finished installing, enter an administrator password on the settings page and click Finish.
11. Log in to the server console and launch a PowerShell prompt. Install .NET 3.5 by running the following command:

```
Add-WindowsFeature -Name NET-Framework-Core -Source D:\sources\sxs
```

12. Install important and recommended Windows updates and reboot.
13. Configure network adapter settings if you are using static IPs.

    Note: The SCVMM VM has three network adapters. Look for the MAC address of the adapters in the VM Settings menu and assign the IP addresses appropriately.

14. Rename the VM and add it to Active Directory.
15. Repeat steps 1 through 14 for each remaining VM.

11.5 Installing the NetApp SMI-S Agent

To install the NetApp SMI-S Agent, complete the following procedures.

Prerequisites

The following environment prerequisites must be met before you proceed.

Accounts

1. Verify that the following local account has been created:

User Name	Purpose	Permissions
SMIS-User	SMI-S access account	**Note:** This account does not need any special delegation. This is **not** a domain account. It must be a local account in Windows.

2. Verify that the following account is a member of the local administrator's group:
   - SMIS-User

Installing the SMI-S Agent

You must complete the following steps to install the NetApp SMI-S agent:

1. Download the Data ONTAP SMI-S Agent installer from http://mysupport.netapp.com/NOW/download/software/smis/Windows/5.1.1/smisagent-5-1-1.msi.
2. Unblock the downloaded file:

```
Unblock-file ~\Downloads\smisagent-5-1-1.msi
```

3. Install the agent by running the following command:

```
~\Downloads\smisagent-5-1-1.msi /qb
```

11.6 Installing the SMI-S Provider

The following steps need to be completed to install the NetApp SMI-S agent.

1. Right-click smisagent-5-1-2 and select Install from the context menu to begin the setup.
2. On the Welcome to the Data ONTAP SMI-S Agent Setup Wizard page, click Next.
3. On the Ready to Install Data ONTAP SMI-S Agent page, click Install.
4. On the Completed the Data ONTAP SMI-S Agent Setup wizard, click Finish to complete the installation.

11.7 Configuring the SMI-S Provider

The following steps needs to be completed to configure the NetApp SMI-S provider. To complete the following steps you must be logged into the SMI-S Agent server as a local administrator.

You must complete the following steps to configure the NetApp SMI-S provider:

1. In the Open App screen, right-click the Data ONTAP SMI-S Agent and select Run as Administrator at the bottom of the screen.
2. Change the directory into the SMI-S program files.

```
cd %ProgramFiles(x86)%\ONTAP\smis\pegasus\bin
```

3. Add the SVM credentials to the SMI-S Agent.

```
Smis addsecure <VserverIpAddress> <VserverAdmin> <VserverAdminPassword>
```

4. Enable user authentication with the `cimconfig` command.

```
Cimconfig -p -s enableAuthentication=true
```

5. Restart the agent/cimserver.

```
Smis cimserver restart
```

6. Add the SMI-S Run As account to the SMI-S configuration.

```
cimuser -a -u SMIS-User -w <password>
```

11.8 Installing System Center Virtual Machine Manager

To install SCVMM in a minimal configuration, complete the following steps.

Prerequisites

You must meet the following environment prerequisites before you proceed.

Accounts

Verify that the following accounts have been created:

User name	Purpose	Permissions
<DOMAIN>\SCVMM-SVC	Virtual Machine Manager Service Account	This account needs full administrator permissions on the VMM server virtual machine. It runs the VMM service.
<DOMAIN>\SQL-SVC	SQL Server Service Account	This account will need full administrator permissions on the VMM server and runs the service account for all instances. This account must also be added to the SQL-Admins group and as a sysadmin in all instances.
<DOMAIN>\SnapDrive	SnapDrive for Windows	This account needs to be an administrator on the SCVMM VM.

Groups

1. Verify that the following security groups have been created:

Security group name	Group scope	Members
<DOMAIN>\SCVMM-Admins	Global	SCVMM-SVC
<DOMAIN>\SQL-Admins	Global	All SQL Server administrators for the fabric management solution. The user account being used to install SQL Server should be in this group.

2. Verify the following accounts and/or groups are members of the Local Administrators group on the Virtual Machine Manager virtual machine:
   – SnapDrive
   – Virtual Machine Manager Admins group
   – Virtual Machine Manager Service Account

- SQL Service Account
- SQL Admins Group

Installing the Windows Assessment and Deployment Kit

The Virtual Machine Manager installation requires that the Windows Assessment and Deployment Kit (ADK) be installed on the VMM management server. The Windows ADK can be downloaded from http://www.microsoft.com/en-us/download/details.aspx?id=39982.

During installation, only the deployment tools and the Windows Preinstallation Environment features are selected. This installation also assumes that the VMM servers have Internet access. If that is not the case, you can perform an offline installation.

The following steps outline how to install the Windows ADK on the VMM management server:

1. From the Windows ADK installation media source, right-click adksetup.exe and select Run as administrator from the context menu to begin setup. If prompted by user account control, select Yes to allow the installation to make changes to the computer.
2. A splash screen appears. In the Specify Location dialog box, accept the default folder location of %ProgramFiles%\Windows Kits\8.1 and click Next to continue.
3. In the Join the Customer Experience Improvement Program (CEIP) dialog box, select the option to either participate or not participate in the CEIP by providing selected system information to Microsoft. Click Next to continue.
4. In the License Agreement dialog box, click Accept to continue.
5. In the Select the Features You Want to Install dialog box, select the following option checkboxes:
   - Deployment Tools
   - Windows Preinstallation Environment (Windows PE)
6. Make sure all other option checkboxes are deselected. Click Install to begin the installation.
7. When installation is complete, deselect the Launch the Getting Started Guide checkbox and click Close to exit the installation wizard.

Installing the WSUS RSAT Tools

The Virtual Machine Manager installation requires the Windows Server Update Services (WSUS) Remote Server Administration Tools (RSAT) to be installed on the VMM management server. To install WSUS RSAT:

1. Launch a PowerShell prompt by right-clicking the PowerShell icon in the taskbar and selecting Run as Administrator.
2. Add Failover Cluster, Multipath-IO, and the WSUS console by entering the following command:

```
Add-WindowsFeature –Name UpdateServices-RSAT –IncludeManagementTools –Restart
```

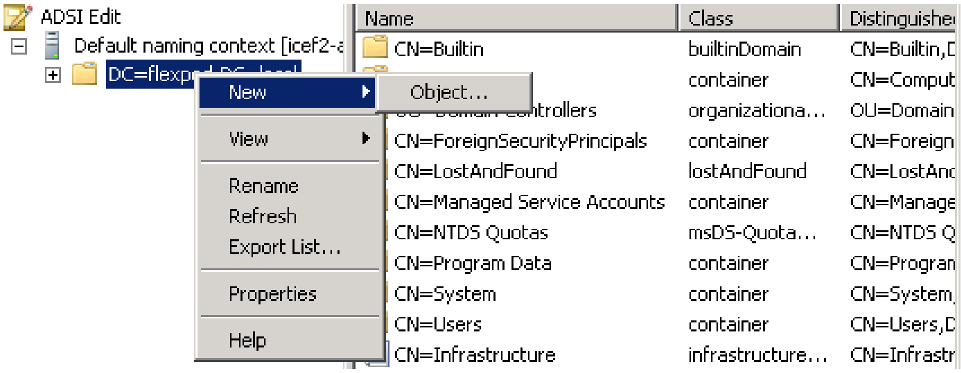
Creating the VMM Distributed Key Management Container Active Directory Domain Services

The VMM installation requires that an Active Directory container be created to house the distributed key information for VMM.

Note: If VMM will be deployed by using an account with rights to create containers in Active Directory Domain Services, you can skip this step.

Perform the following steps to create an Active Directory Domain Services container to house the distributed key information. These instructions assume that a Windows Server 2008 R2 domain controller is in use; similar steps would be followed for other versions of Active Directory, including Windows Server 2008, Windows Server 2012, and Windows Server 2012 R2:

1. Log in to a domain controller with a user that has domain administrator privileges and run `adsiedit.msc`.
2. Right-click the ADSI Edit node and select Connect to… from the context menu.
3. In the Connections Settings dialog box in the Connection Point section, select the Select a Well-Known Naming Context option. Select Default Naming Context from the drop-down menu and click OK.
4. Expand Domain Default Naming Context [<computer fully qualified domain name>], expand <distinguished name of domain>, right-click the root node, and select New > Object from the Context menu.



Name	Class	Distinguishe
CN=Builtin	builtinDomain	CN=Builtin,D
	container	CN=Comput
trollers	organizationa…	OU=Domain
CN=ForeignSecurityPrincipals	container	CN=Foreign
CN=LostAndFound	lostAndFound	CN=LostAnc
CN=Managed Service Accounts	container	CN=Manage
CN=NTDS Quotas	msDS-Quota…	CN=NTDS Q
CN=Program Data	container	CN=Progran
CN=System	container	CN=System,
CN=Users	container	CN=Users,D
CN=Infrastructure	infrastructure…	CN=Infrastr

5. In the Create Object dialog box, select Container and then click Next.
6. In the Value text box, type VMMDKM and then click Next.
7. Click Finish to create the container object.
8. Within ADSI Edit, right-click the new VMMDKM object and then click Properties.
9. In the VMMDKM Properties dialog box, click the Security tab. Click Add to add the VMM Service Account and VMM Admins Group. Grant the security principals full control permissions.
10. Click OK three times and close ADSI Edit.

Installing NetApp SnapDrive

The following section describes how to install NetApp SnapDrive for Windows. For detailed information regarding the installation, refer to the SnapDrive Installation Guide.

1. Download the SnapDrive installer from http://support.netapp.com/NOW/download/software/snapdrive_win/7.0.3/SnapDrive7.0.3_x64.exe.
2. Launch the installer and click Next.
3. Select the Storage based Licensing method and click Next.
4. Enter the user name and organization information and click Next.
5. Validate the installation path and click Next.
6. Select the Enable SnapDrive to communicate through the Windows Firewall checkbox and click Next.
7. Enter the account information for the SnapDrive service account and click Next.
8. Click Next through the SnapDrive Web Service Configuration.
9. Clear the Enable Preferred storage system IP Address checkbox and click Next.

10. Clear the Enable Transport Protocol Settings checkbox and click Next
11. Leave Enable Unified Manger Configuration cleared and click Next.
12. Leave Enable Hyper-V Server pass-through disk cleared and click Next.
13. Click Install.
14. After the installation is complete, reboot the server to finish the installation.
15. Launch a new PowerShell prompt by right-clicking the PowerShell icon in the taskbar and selecting Run as Administrator.

    Note: A new prompt is required to register the sdcli executable.

16. Configure the SnapDrive IP settings for each controller.

```
sdcli preferredIP set -f <<var_vserver_mgmt>> -IP << var_vserver_mgmt_ip>>
```

17. Configure the SnapDrive transport protocol authentication for each controller.

```
set-SdStorageConnectionSetting –StorageSystem <<var_vserver_mgmt>> -protocol https -credential
vsadmin
```

Preparing SMB Shares

Prepare the SQL Server[®] and SCVMM Library shares by assigning the required permissions.

1. Open an SSH connection to the cluster IP or host name and log in to the admin user with the password you provided earlier.
2. Remove the Everyone permission from the SQL share.

```
cifs share access-control delete -share scvmmdb -user-or-group Everyone -vserver infra_svm
```

3. Add permissions to the following accounts with NTFS full control permissions over the share:
   - SQL Admins Group

```
share access-control create -share scvmmdb -user-or-group FLEXPOD\SQL-Admins -permission
full_Control -vserver infra_svm
```

4. Remove the Everyone permission from the SCVMM Library share.

```
cifs share access-control delete -share vmmlibrary -user-or-group Everyone -vserver infra_svm
```

5. Add permissions to the following accounts with NTFS full control permissions over the share:
   - SCVMM SVC Account
   - SCVMM Machine Account

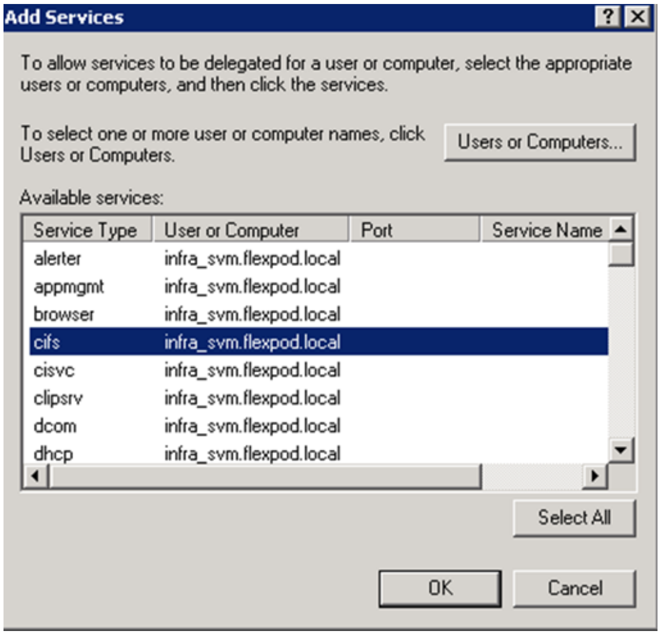
```
share access-control create -share vmmlibrary -user-or-group FLEXPOD\SCVMM$ -permission
full_Control -vserver infra_svm
share access-control create -share vmmlibrary -user-or-group FLEXPOD\SCVMM-SVC -permission
full_Control -vserver infra_svm
```

Configuring Constrained Delegation

Although the hosts have the required permissions to access the SMB share, you may encounter access-denied errors when trying to remotely manage the database. To avoid these error messages, configure constrained delegation for the SCVMM host by completing the following steps:

1. In Active Directory Users and Computers, browse to the Computer objects for the SCVMM VM.
2. Right-click the object and select Properties.
3. Select the Delegation tab.
   a. Select Trust This Computer for Delegation to the Specific Services Only.

   b. Select Use Kerberos Only.
   c. Click Add.
4. Click the Users or Computers button on the top of the Add Services dialog box.
5. Enter the name of the infrastructure storage virtual machine (SVM) and click OK.
6. Select CIFS and click OK.



To allow services to be delegated for a user or computer, select the appropriate users or computers, and then click the services.

To select one or more user or computer names, click Users or Computers.

Available services:

Service Type	User or Computer	Port	Service Name
alerter	infra_svm.flexpod.local		
appmgmt	infra_svm.flexpod.local		
browser	infra_svm.flexpod.local		
cifs	infra_svm.flexpod.local		
cisvc	infra_svm.flexpod.local		
clipsrv	infra_svm.flexpod.local		
dcom	infra_svm.flexpod.local		
dhcp	infra_svm.flexpod.local		

7. Click OK.

Installing SQL Server 2012 SP2

You can install SQL Server 2012 SP1 into the SCVMM server. For deployments of more than 150 hosts, you should consider using a dedicated SQL Server cluster. To install SQL Server onto the SCVMM VM, complete the following steps:

1. From the SQL Server 2012 SP1 installation media source, right-click setup.exe and select Run as Administrator from the context menu to begin setup. The SQL Server Installation Center appears. Select the Installation menu option.
2. From the SQL Server Installation Center, click the New SQL Server standalone installation or add features to an existing installation link.
3. The SQL Server 2012 SP1 setup wizard appears. In the Setup Support Rules dialog box, verify that each rule shows a Passed status. If any rule requires attention, remediate the issue and rerun the validation check. Click OK to continue.
4. In the Product Key dialog box, select the Enter the Product Key option and enter the associated product key in the provided text box. Click Next to continue.

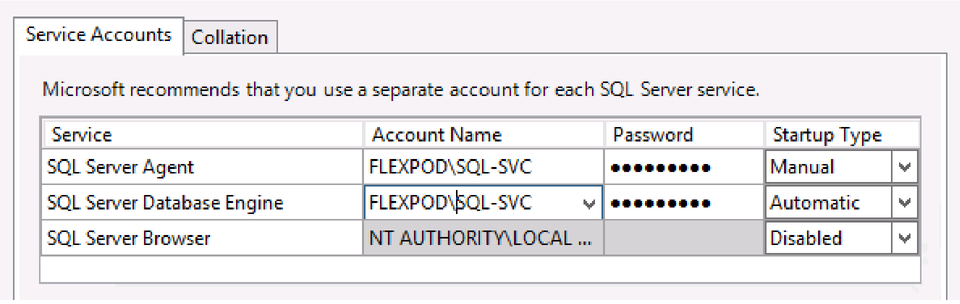
   Note: If you do not have a product key, select the Specify a Free Edition option and select Evaluation from the drop-down menu for a 180-day evaluation period.

5. In the License Terms dialog box, select the I Accept the License Terms checkbox. Select or clear the Send Feature Usage Data to Microsoft checkbox based on your organization’s policies and click Next to continue.

6. In the Product Updates dialog box, select the Include SQL Server Product Updates checkbox and click Next to continue.
7. In the Install Setup Files dialog box, click Install and allow the support files to install.
8. In the Setup Support Rules dialog box, verify that each rule shows a Passed status. If any rule requires attention, remediate the issue and rerun the validation check.

   Note: Common issues include Microsoft Distributed Transaction Coordinator (MSDTC), Microsoft Cluster Service, and Windows Firewall warnings. Note that the use of MSDTC is not required for the System Center 2012 SP1 environment.

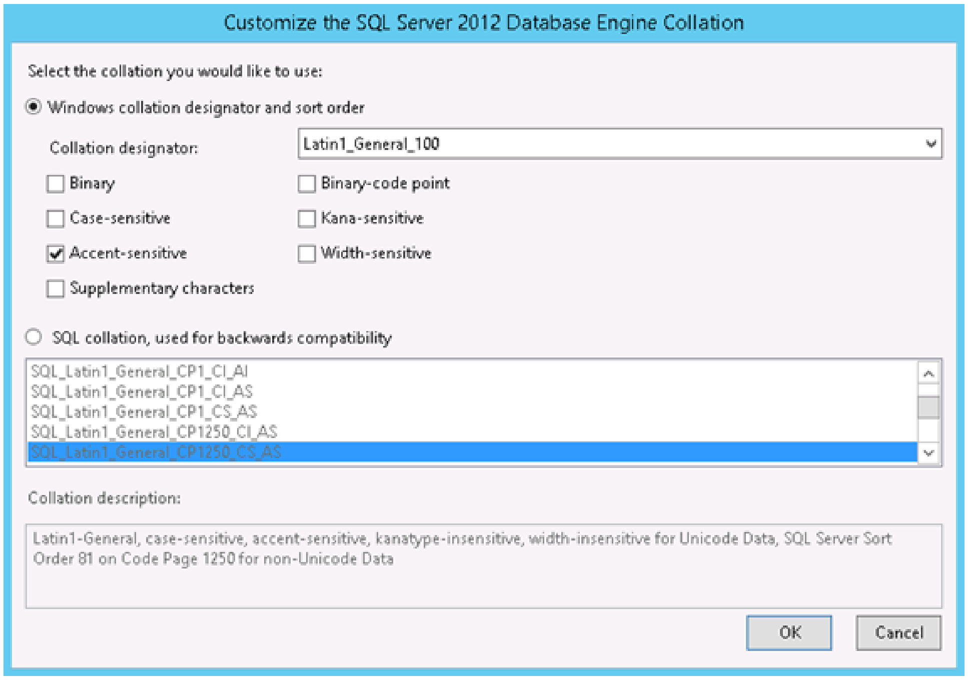
9. Click Next to continue.
10. In the Setup Role dialog box, select the SQL Server Feature Installation button and click Next to continue.
11. In the Feature Selection dialog box, select the following:
    - Database Engine Services
    - Management Tools – Basic
    - Management Tools – Complete
12. In the Installation Rules dialog box, click Next to continue. The Show Details and View Detailed Report can be viewed if required.
13. In the Server Configuration dialog box, select the Service Accounts tab. Specify the SCVMM service account and password for the SQL Server Agent and SQL Server Database Engine services.



Microsoft recommends that you use a separate account for each SQL Server service.

Service	Account Name	Password	Startup Type
SQL Server Agent	FLEXPOD\SQL-SVC	●●●●●●●●●	Manual
SQL Server Database Engine	FLEXPOD\SQL-SVC	●●●●●●●●●	Automatic
SQL Server Browser	NT AUTHORITY\LOCAL ...		Disabled

14. In the Disk Space Requirements dialog box, verify that you have sufficient disk space and click Next.
15. In the Server Configuration dialog box, select the Collation tab and click Customize.
    a. Select the Windows collation designator and sort order option.
    b. Select Latin1_General_100 from the drop-down menu and the Accent-sensitive checkbox.
    c. Click OK to set the collation to Latin1_General_100_CI_AS.
    d. Click Next.



Customize the SQL Server 2012 Database Engine Collation

Select the collation you would like to use:

● Windows collation designator and sort order

Collation designator: Latin1_General_100

□ Binary	□ Binary-code point
□ Case-sensitive	□ Kana-sensitive
☑ Accent-sensitive	□ Width-sensitive
□ Supplementary characters	

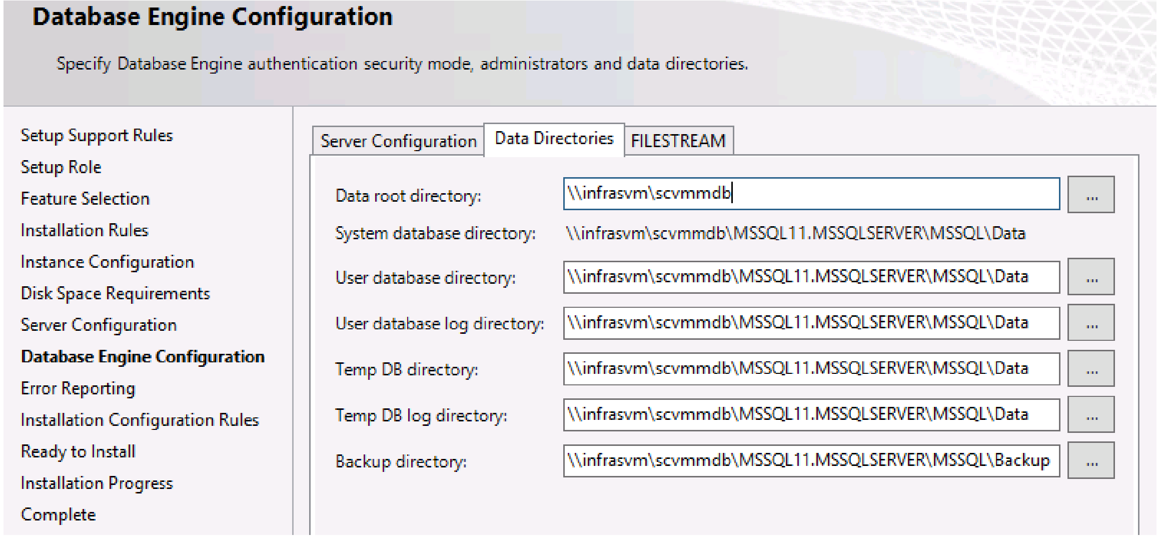
○ SQL collation, used for backwards compatibility

SQL_Latin1_General_CP1_CI_AI
SQL_Latin1_General_CP1_CI_AS
SQL_Latin1_General_CP1_CS_AS
SQL_Latin1_General_CP1250_CI_AS
SQL_Latin1_General_CP1250_CS_AS

Collation description:

Latin1-General, case-sensitive, accent-sensitive, kanatype-insensitive, width-insensitive for Unicode Data, SQL Server Sort Order 81 on Code Page 1250 for non-Unicode Data

16. In the Database Engine Configuration dialog box, select the Server Configuration tab. In the Authentication Mode section, select the Windows authentication mode option. In the Specify SQL Server administrators section, click the Add Current User button to add the current installation user. Click the Add button and add BUILTIN\Administrators and any other groups that should have administrator access to the SQL instance.
17. In the same Database Engine Configuration dialog box, select the Data Directories tab. Under the data root directory field, enter the UNC path to the SCVMM SQL share. Click Next to continue.

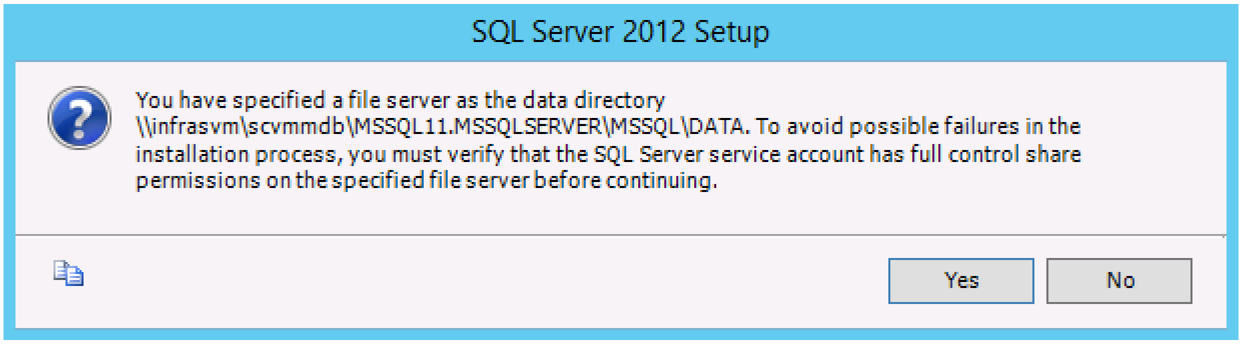


Database Engine Configuration

Specify Database Engine authentication security mode, administrators and data directories.

Data root directory:	\\infrasvm\scvmmdb
System database directory:	\\infrasvm\scvmmdb\MSSQL11.MSSQLSERVER\MSSQL\Data
User database directory:	\\infrasvm\scvmmdb\MSSQL11.MSSQLSERVER\MSSQL\Data
User database log directory:	\\infrasvm\scvmmdb\MSSQL11.MSSQLSERVER\MSSQL\Data
Temp DB directory:	\\infrasvm\scvmmdb\MSSQL11.MSSQLSERVER\MSSQL\Data
Temp DB log directory:	\\infrasvm\scvmmdb\MSSQL11.MSSQLSERVER\MSSQL\Data
Backup directory:	\\infrasvm\scvmmdb\MSSQL11.MSSQLSERVER\MSSQL\Backup

18. A popup will open warning that if the SQL Service account does not have full control of the share the installation will fail. Click Yes to acknowledge the warning.


SQL Server 2012 Setup

You have specified a file server as the data directory \\infrasvm\scvmmdb\MSSQL11.MSSQLSERVER\MSSQL\DATA. To avoid possible failures in the installation process, you must verify that the SQL Server service account has full control share permissions on the specified file server before continuing.

19. In the Error Reporting dialog box, select or clear the Send Windows and SQL Server Error Reports to Microsoft or Your Corporate Report Server checkbox based on your organization's policies and click Next to continue.
20. In the Installation Rules dialog box, verify that each rule shows a Passed status. If any rule requires attention, remediate the issue and rerun the validation check. Click Next to continue.
21. In the Ready to Install dialog box, verify all the settings that were entered during the setup process and click Install to begin the installation of the SQL Server instance.
22. Monitor installation progress as displayed in the Installation Progress dialog box.
23. When initial installation is complete, the Complete dialog box appears. Click Close to complete the installation of this SQL Server database instance.
24. Verify the installation by inspecting the instances in the Failover Cluster Manager and in SQL Server 2012 Management Studio before you move on to the next step of installation.

Installing Virtual Machine Manager

Perform the following procedure on one of the Virtual Machine Manager VMs:

1. From the VMM installation media source, right-click setup.exe and select Run as Administrator from the context menu to begin setup. If prompted by user account control, select Yes to allow the installation to make changes to the computer.
2. The VMM installation wizard begins. At the splash page, click Install to begin the VMM server installation.
3. In the Select Features to Install dialog box, verify that the Virtual Machine Manager Management Server Installation option checkbox is selected. After selecting it, the Virtual Machine Manager Console Installation option checkbox will be selected by default. Click Next to continue.
4. In the Product Registration Information dialog box, enter the following information in the text boxes and click Next to continue:
   - Name: Specify the name of the primary user or responsible party within your organization.
   - Organization: Specify the name of the licensed organization.
   - Product Key: Provide a product key for installation of VMM. If no key is provided, VMM is installed in evaluation mode.
5. Accept the EULA and click Next to continue.
6. In the Join the Customer Experience Improvement Program (CEIP) dialog box, select the option to either participate or not participate in the CEIP by providing selected system information to Microsoft. Click Next to continue.
7. In the Microsoft Update dialog box, select the option to either allow or not allow VMM to use Microsoft Update to check for and perform automatic updates based on your organization's policies. Click Next to continue.

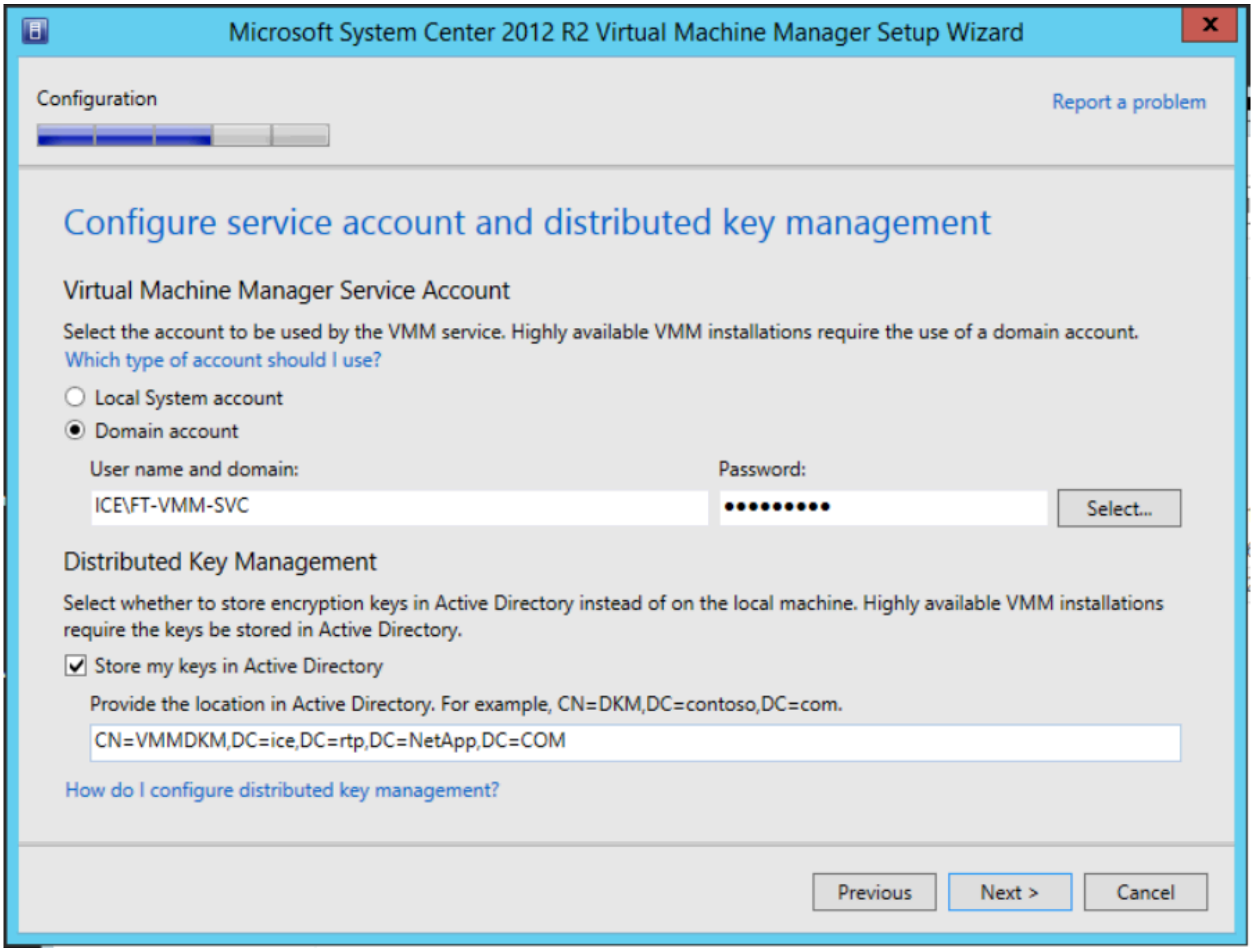
8. In the Select Installation Location dialog box, specify a location or accept the default location of %ProgramFiles%\Microsoft System Center 2012 R2\Virtual Machine Manager for the installation. Click Next to continue.

   Note: The setup wizard has a built-in prerequisite checker. If for any reason a prerequisite is not met, the setup UI notifies you about the discrepancy.

   If the system passes the prerequisite check, no screen is displayed and the setup wizard proceeds to the Database configuration screen.

9. In the Database configuration dialog box, enter the following information in the text boxes and click Next to continue:
   - Server Name: Specify the name of the SQL Server (typically the local machine name).
   - Port: Specify the TCP port used for the SQL Server; leave this blank if you are using a local instance.
   - Verify that the Use the Following Credentials checkbox is not selected. In the Instance Name drop-down menu, select the VMM database instance deployed earlier (for example, MSSQLSERVER).
   - In the Select an Existing Database or Create a New Database option, select the New Database option and accept the default database name of VirtualManagerDB.

10. In the Configure Service Account and Distributed Key Management dialog box, in the Virtual Machine Manager Service Account section, select the Domain Account option. Enter the following information in the text boxes and click Next to continue:
    - User Name and Domain: Specify the VMM service account identified in section “Accounts” in the following format: <DOMAIN>\<USERNAME>.
    - Password: Specify the password for the VMM service account.
    - In the Distributed Key Management section, select the Store My Keys in Active Directory checkbox. In the provided text box, type the distinguished name (DN) location created earlier within Active Directory: CN=VMMDKM,DC=domain, and so on.



Microsoft System Center 2012 R2 Virtual Machine Manager Setup Wizard

Configuration

Report a problem

Configure service account and distributed key management

Virtual Machine Manager Service Account

Select the account to be used by the VMM service. Highly available VMM installations require the use of a domain account.

Which type of account should I use?

○ Local System account

● Domain account

User name and domain: ICE\FT-VMM-SVC

Password: ••••••••••

Distributed Key Management

Select whether to store encryption keys in Active Directory instead of on the local machine. Highly available VMM installations require the keys be stored in Active Directory.

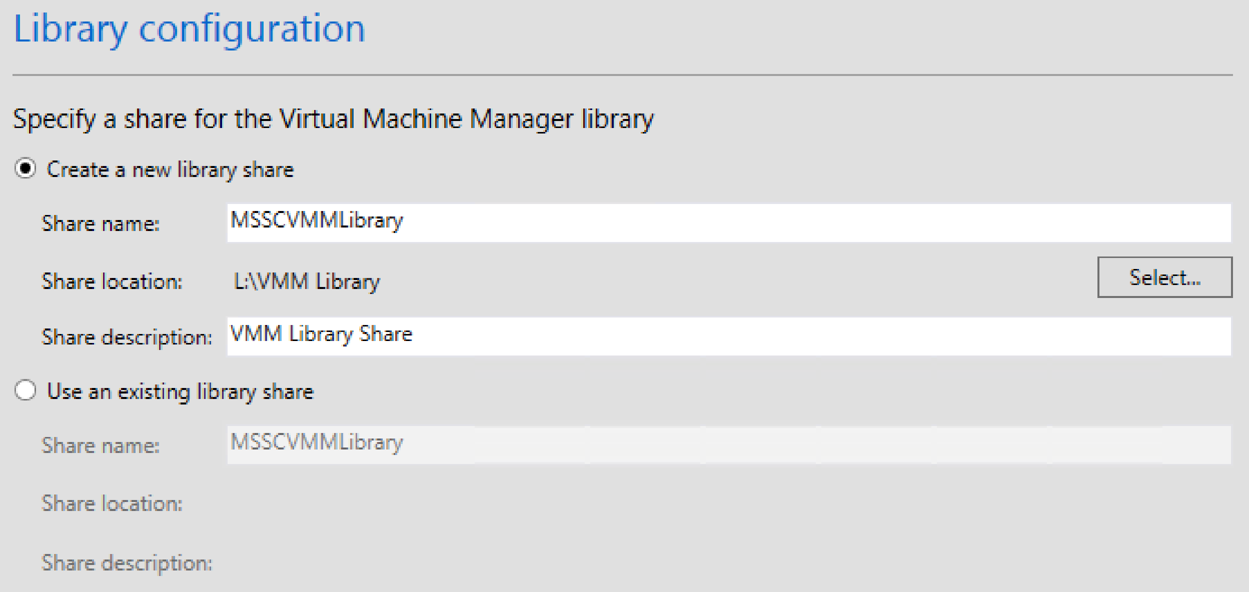
☑ Store my keys in Active Directory

Provide the location in Active Directory. For example, CN=DKM,DC=contoso,DC=com.

CN=VMMDKM,DC=ice,DC=rtp,DC=NetApp,DC=COM

How do I configure distributed key management?

11. In the Port Configuration dialog box, accept the default values in the text boxes and click Next to continue:
    - Communication with the VMM Console: Default: 8100.
    - Communication to Agents on Hosts and Library Servers: Default: 5985.
    - File Transfers to Agents on Hosts and Library Servers: Default: 443.
    - Communication with Windows Deployment Services: Default: 8102.
    - Communication with Windows Preinstallation Environment (Windows PE) Agents: Default: 8101.
    - Communication with Windows PE Agent for Time Synchronization: Default: 8103.
12. In the Library Configuration dialog box, under Share Location, click Select. Browse to the L: drive and click Make New Folder. Rename the new folder as VMM Library and click OK. Click Next to continue.



Library configuration

Specify a share for the Virtual Machine Manager library

● Create a new library share

Share name: MSSCVMMLibrary

Share location: L:\VMM Library

Share description: VMM Library Share

○ Use an existing library share

Share name: MSSCVMMLibrary

Share location:

Share description:

13. The Installation Summary dialog box appears and displays the selections you made during the installation wizard. Review the options selected and click Install to continue.
14. Monitor installation progress. The wizard displays the progress while installing features.
15. When the initial installation is complete, the wizard displays the Setup Completed Successfully dialog box. Click Close to complete the installation.
16. When the final installation is complete, launch the Virtual Machine Manager console to verify that the installation occurred properly. Verify that the console launches and connects to the Virtual Machine Manager instance installed.

Creating VMM Run As Account

Complete the following steps to create the VMM Run as account in SCVMM:

1. In the Virtual Machine Manager console, navigate to the Settings pane, and click Create Run as Account.
2. Name the account. Provide an Active Directory account name and password with administrator rights to all Hyper-V hosts and clusters.
3. Click OK to create the Run as Account.

Registering SMI-S in SCVMM

The following steps needs to be completed to register the NetApp SMI-S provider in SCVMM.

1. In the Virtual Machine Manager console, navigate to the Fabric pane and expand the Storage node. Select the Providers subnode.
2. From the ribbon select Add Resources, and select Storage Devices from the drop-down.
3. On the Add Storage Devices Wizard select Add a Storage device that is managed by a SMI-S provider, and Click Next.
4. Select the SAN and NAS devices discovered and managed by SMI-S provider, and click Next.
5. On the Specify Discovery Scope page:
   a. Select SMI-S CIMXML for the Protocol

b. Enter the IP or FQDN for the SMI-S provider

c. Check the Use Secure Sockets Layer checkbox

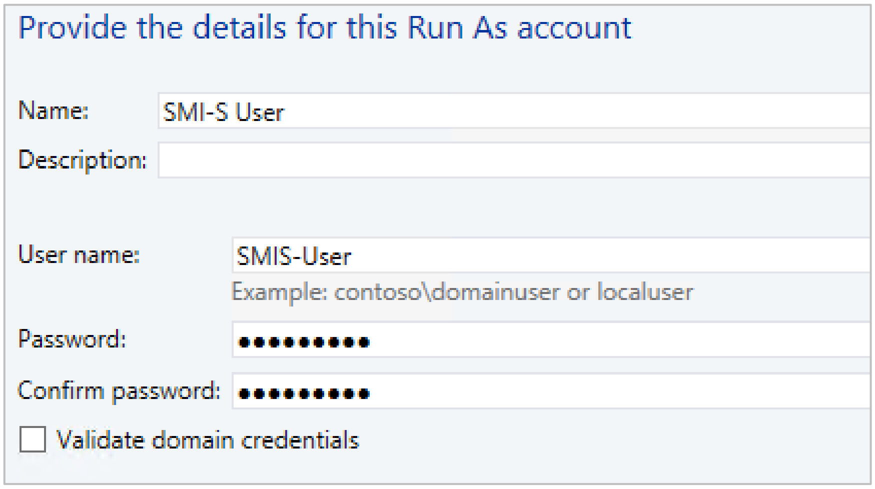
d. Click Browse, and in the resulting popup select Create Run As Account

– Enter a Display Name

– Enter the User Name (for example: SMIS-User)

– Enter the Password

– Click OK.



Provide the details for this Run As account

Name: SMI-S User

Description:

User name: SMIS-User

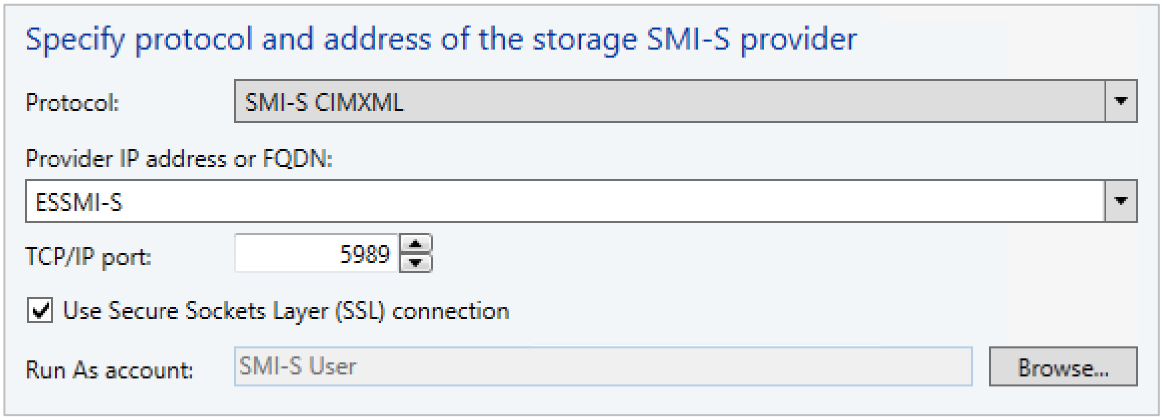
Example: contoso\domainuser or localuser

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

□ Validate domain credentials

– Click Next



Specify protocol and address of the storage SMI-S provider

Protocol: SMI-S CIMXML

Provider IP address or FQDN:

ESSMI-S

TCP/IP port: 5989

☑ Use Secure Sockets Layer (SSL) connection

Run As account: SMI-S User

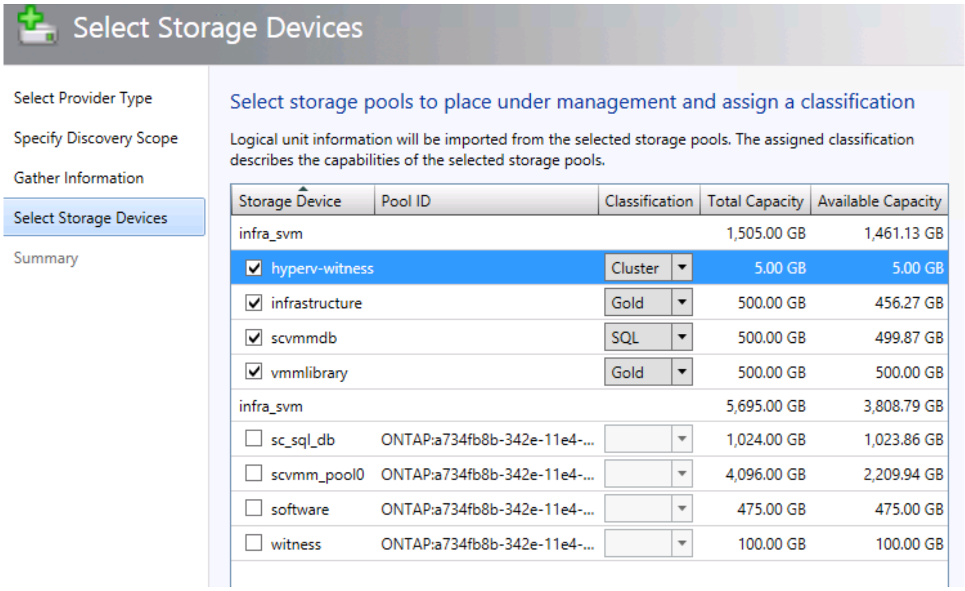
6. During the discovery phase a popup will open asking to Import the SMI-S providers Certificate. Click Import

7. Once Discovery is completed the Wizard will show every storage controller registered with the SMI-S provider, Click Next.

8. On the Select Storage Devices page.

9. Click the Create Classification button. In the resulting popup enter a name for the storage pool.

10. Check the scvmm_pool0 storage pool, and assign a classification. Optionally you may select and assign classifications for all the shares and pools.



Select storage pools to place under management and assign a classification

Logical unit information will be imported from the selected storage pools. The assigned classification describes the capabilities of the selected storage pools.

Storage Device	Pool ID	Classification	Total Capacity	Available Capacity
infra_svm			1,505.00 GB	1,461.13 GB
☑ hyperv-witness		Cluster	5.00 GB	5.00 GB
☑ infrastructure		Gold	500.00 GB	456.27 GB
☑ scvmmdb		SQL	500.00 GB	499.87 GB
☑ vmmlibrary		Gold	500.00 GB	500.00 GB
infra_svm			5,695.00 GB	3,808.79 GB
☐ sc_sql_db	ONTAP:a734fb8b-342e-11e4-...		1,024.00 GB	1,023.86 GB
☐ scvmm_pool0	ONTAP:a734fb8b-342e-11e4-...		4,096.00 GB	2,209.94 GB
☐ software	ONTAP:a734fb8b-342e-11e4-...		475.00 GB	475.00 GB
☐ witness	ONTAP:a734fb8b-342e-11e4-...		100.00 GB	100.00 GB

11. Click Next, and Finish to close out the wizard.

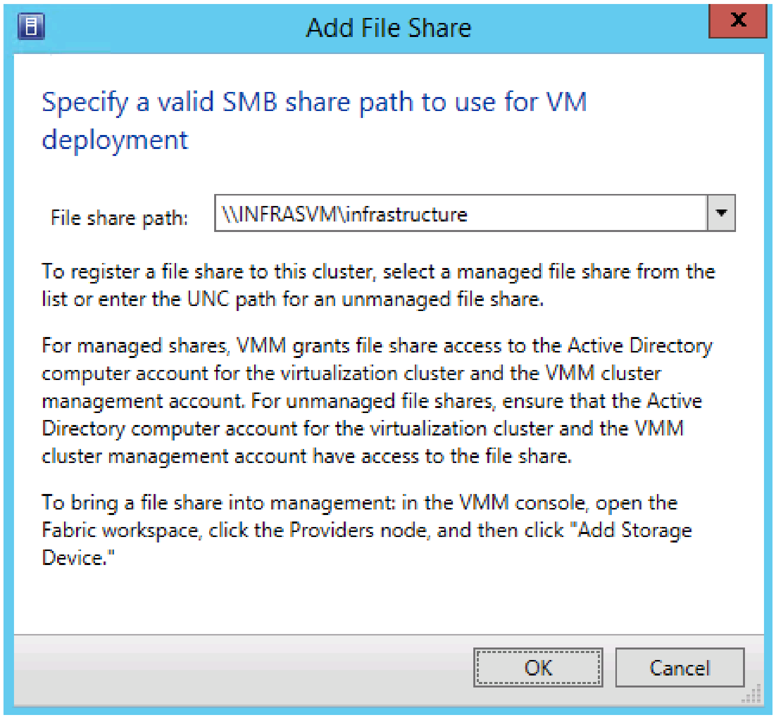
Adding Fabric Management Resources to Virtual Machine Manager

1. In the Virtual Machine Manager console, navigate to the Fabric pane in the left tree view and right-click All Hosts under the Servers section. Select Create Host Group. Name the new host group.
2. Select Fabric and All Hosts. Click Add Resources, Hyper-V Hosts, and Clusters.
3. In the Indicate the Windows Computer location, select Windows Server Computers in a Trusted Active Directory Domain.
4. Select Use an Existing Run as Account and click Browse.
5. Select the VMM Run as Account created in the section “Accounts” and click OK.
6. Click Next to proceed to the next screen.
7. Enter the cluster name and click Next.
8. Click Select All and click Next.
9. Select the Host Group created in step 1 and click Next.
10. Click Finish.
11. k

Registering File Share to Management Cluster

If the infrastructure VMs were provisioned onto an SMB share, complete the following steps to register the file share to the management cluster.

1. Click Fabric in the left-tree view.
2. Expand Servers, All Hosts, and Management Fabric.
3. Right-click the management cluster and select Properties.
4. Select File Share Storage and click Add.
5. From the drop-down menu, select the infrastructure share and click OK.



Add File Share

Specify a valid SMB share path to use for VM deployment

File share path: \\INFRASVM\infrastructure

To register a file share to this cluster, select a managed file share from the list or enter the UNC path for an unmanaged file share.

For managed shares, VMM grants file share access to the Active Directory computer account for the virtualization cluster and the VMM cluster management account. For unmanaged file shares, ensure that the Active Directory computer account for the virtualization cluster and the VMM cluster management account have access to the file share.

To bring a file share into management: in the VMM console, open the Fabric workspace, click the Providers node, and then click "Add Storage Device."

6. Click OK to register the file share.

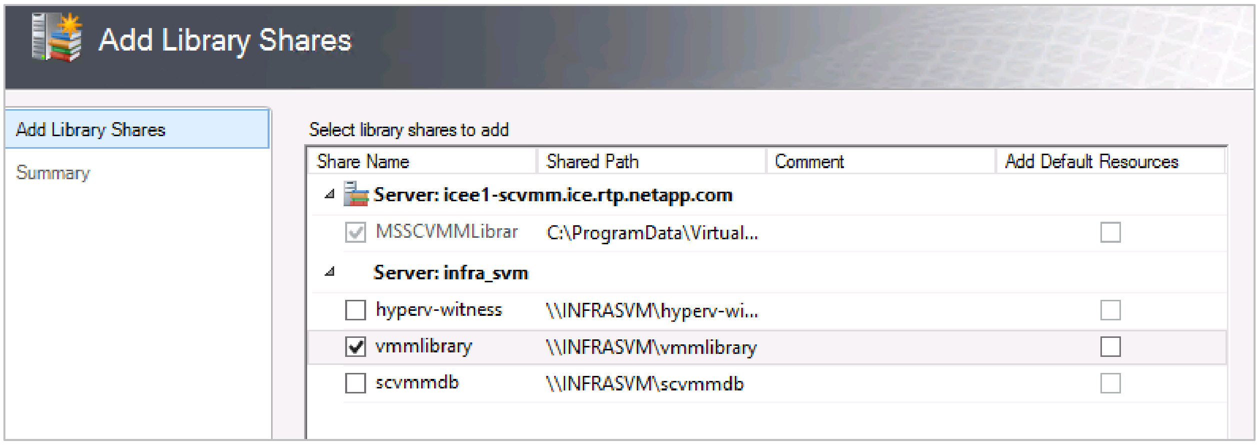
Assigning Permissions

1. Open an SSH connection to cluster IP or host name and log in to the admin user with the password you provided earlier.
2. Add permissions for the following accounts with NTFS full control permissions over the share:
   - VMM service account
   - VMM admins group
   - VMM computer accounts

```
share access-control create -share vmmlibrary -user-or-group FLEXPOD\SCVMM01$ -permission
full_Control -vserver infra_svm
share access-control create -share vmmlibrary -user-or-group FLEXPOD\SCVMM-Admins -permission
full_Control -vserver infra_svm
share access-control create -share vmmlibrary -user-or-group FLEXPOD\VMM-SVC -permission
full_Control -vserver infra_svm
```

Adding Library Shares to SCVMM Library Server

1. In the SCVMM management console, select Library.
2. Browse to Library Servers, right-click the SCVMM library, and select Properties.
3. In the SCVMM Properties window, find the Library Management Credentials entry and click Browse.
4. Select the Action account created in the section “Creating VMM Run As Account” and click OK.
5. Click OK to save the account selection.
6. Right-click the SCVMM library and select Add Library Shares.
7. In the Add Library Server wizard, select the vmmlibrary share configured previously.



Add Library Shares

- Add Library Shares
- Summary

Select library shares to add

Share Name	Shared Path	Comment	Add Default Resources
Server: icee1-scvmm.ice.rtp.netapp.com			
☑ MSSCVMMLibrar	C:\ProgramData\Virtual...		□
Server: infra_svm			
□ hyperv-witness	\\INFRASVM\hyperv-wi...		□
☑ vmmlibrary	\\INFRASVM\vmmlibrary		□
□ scvmmdb	\\INFRASVM\scvmmdb		□

8. Click Next, then Review the Summary page, and click Add Library Shares.

12 Bill of Materials

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

Table 9 lists the components for the large configuration.

Table 9) 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	Cisco 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-M3S	Cisco UCS C220 M3 SFF w/o CPU mem HDD PCIe PSU w/ rail kit	4
UCS-CPU-E52650B	2.60 GHz E5-2650 v2/95W 8C/20MB Cache/DDR3 1866MHz	8
UCS-MR-1X162RY-A	16GB DDR3-1600-MHz RDIMM/PC3-12800/dual rank/1.35v	32

A03-D600GA2	600GB 6Gb SAS 10K RPM SFF HDD/hot plug/drive sled mounted	8
CAB-C13-C14-AC	Power cord, C13 to C14 (recessed receptacle), 10A	8
UCSC-PSU-450W	450W power supply for C-series rack servers	8
UCSC-PCIE-CSC-02	Cisco VIC 1225 Dual Port 10Gb SFP+ CNA	4
N20-BBLKD	Cisco UCS 2.5 inch HDD blanking panel	24
UCS-M3-V2-LBL	Cisco M3 - v2 CPU asset tab ID label (Auto-Expand)	4
UCSC-HS-C220M3	Heat Sink for Cisco UCS C220 M3 Rack Server	8
UCSC-PCIF-01H	Half height PCIe filler for UCS	4
UCSC-RAID-11-C220	Cisco UCS RAID SAS 2008M-8i Mezz Card for C220 (0/1/10/5/50)	4
UCSC-RAIL1	Rail Kit for C220, C22, C24 rack servers	4
CON-SNT-C220M3SF	SMARTnet 8X5XNBD Cisco UCS C220 M3 SFF w/o	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
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
X5527A-R6-C	Rackmount Kit,2-Post,DS2246,-C	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-2-2552A-FCP-C	SW-2,FCP,2552A,-C	2

NetApp Components		
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

13 Conclusion

FlexPod Express is the optimal shared infrastructure foundation to deploy a variety of IT workloads. This platform is both flexible and scalable for multiple use cases and applications. Windows Server 2012 R2 Hyper-V is one common use case as the virtualization solution, which is described in this document. The flexibility and scalability of FlexPod Express enables customers to start out with a right-sized infrastructure that can ultimately grow with and adapt to their evolving business requirements.

14 References

- NetApp FAS25XX Series Storage Controllers:
  http://www.netapp.com/in/products/storage-systems/fas2500/
- Cisco UCS C-Series Servers:
  www.cisco.com/c/en/us/products/servers-unified-computing/ucs-c-series-rack-servers/index.html
- Cisco Nexus 3524 Switches:
  http://www.cisco.com/c/en/us/products/switches/nexus-3524-switch/index.html
- Cisco Nexus 9000 Switches:
  http://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/index.html
- Microsoft Hyper-V:
  http://www.microsoft.com/en-us/server-cloud/solutions/virtualization.aspx

[1] SupportEdge Premium is required for cooperative support.

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.

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

www.netapp.com