NetApp Verified Architecture

FlexPod Express with Microsoft Windows Server 2012 R2 Hyper-V: Small and Medium Configurations

NVA Deployment Guide

Authors: Karthick Radhakrishnan, Arvind Ramakrishnan, NetApp
Reviewers: Jeffrey Fultz, Chris O’Brien, Cisco

October 2015 | NVA-0021-DEPLOY | Version 1.0

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Solution Overview

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

FlexPod Express:

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

1.1 Solution Technology

The small and medium FlexPod Express configurations use Cisco UCS C-Series rack servers, Cisco Nexus switches(1GbE), and NetApp FAS storage systems (NetApp clustered Data ONTAP: switchless). This document describes the implementation of Microsoft Windows Server 2012 R2 Hyper-V on the small and medium FlexPod Express offerings. The configurations are based on best practices for each component in the solution architecture to enable a reliable, enterprise-class infrastructure.

Figures 1 and 2 depict the topology of the FlexPod Express small and medium offerings.

Figure 1) Physical topology of FlexPod Express small configuration.

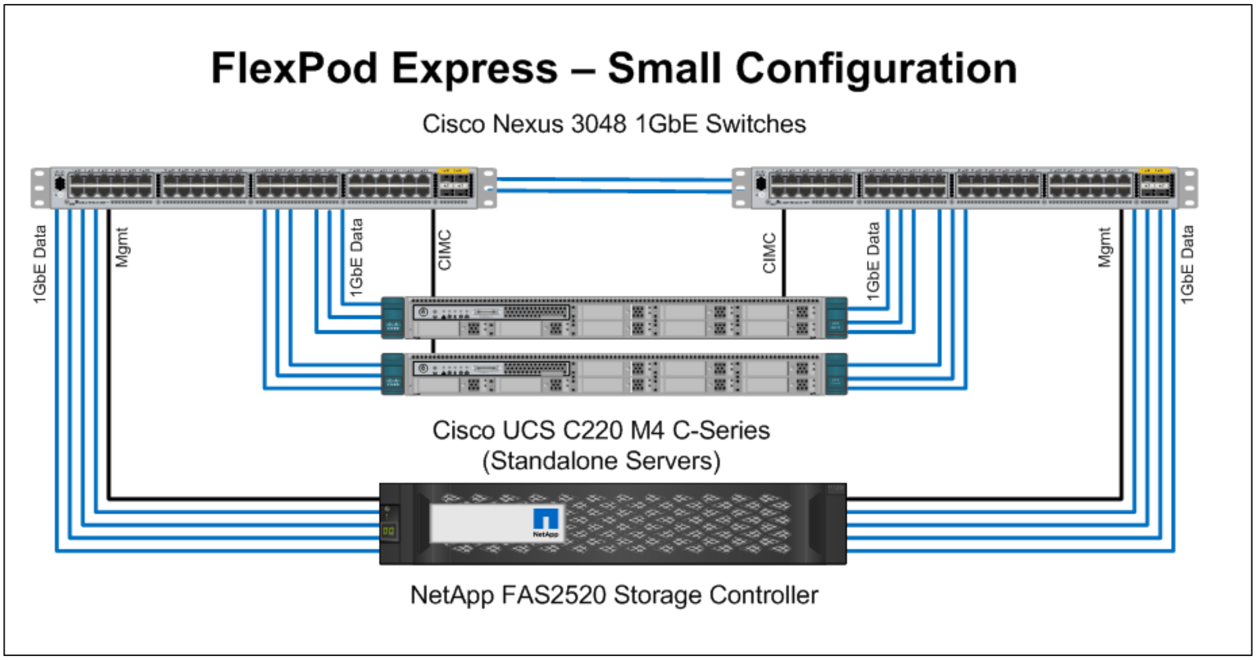
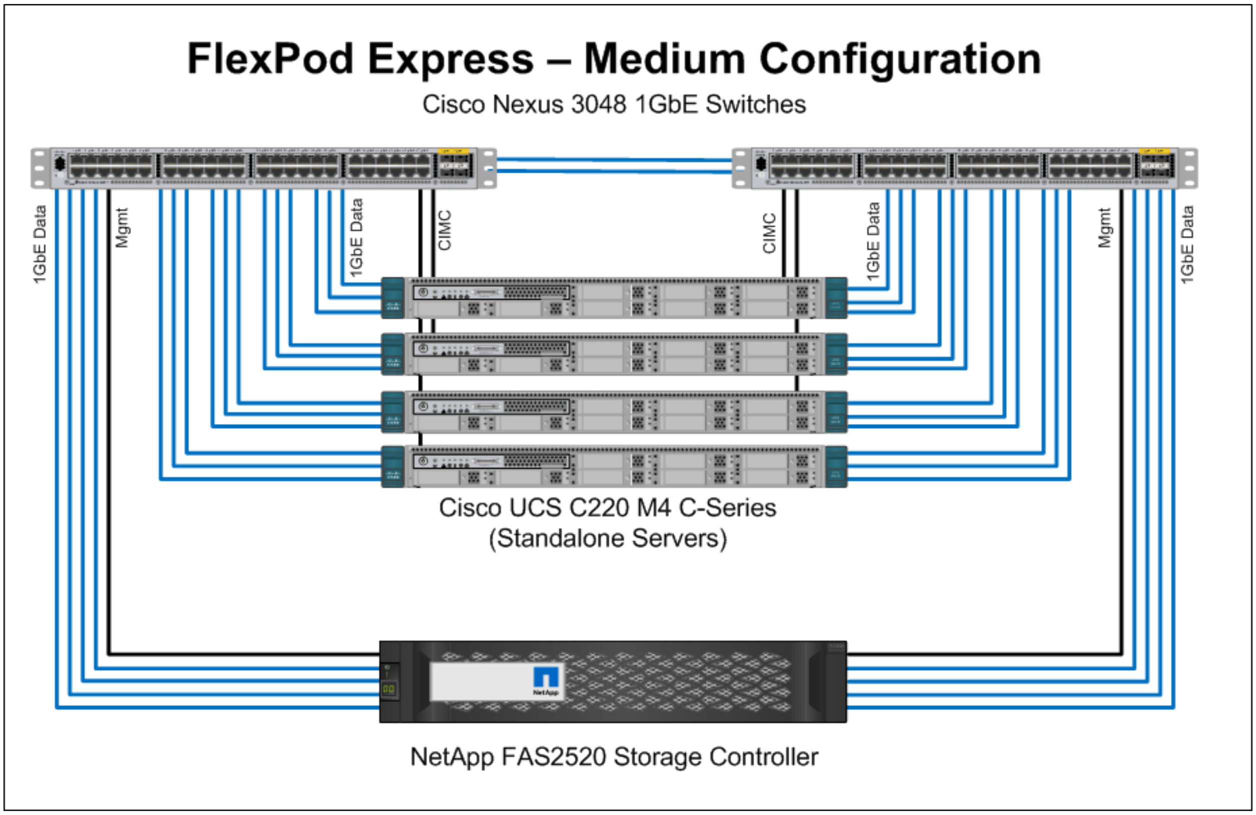

FlexPod Express – Small Configuration
Cisco Nexus 3048 1GbE Switches
1GbE Data
Mgmt
1GbE Data
CIMC
CIMC
1GbE Data
Mgmt
1GbE Data
Cisco UCS C220 M4 C-Series
(Standalone Servers)
NetApp FAS2520 Storage Controller

Figure 2) Physical topology of FlexPod express medium configuration.


FlexPod Express – Medium Configuration
Cisco Nexus 3048 1GbE Switches
1GbE Data
Mgmt
1GbE Data
CIMC
CIMC
1GbE Data
Mgmt
1GbE Data
Cisco UCS C220 M4 C-Series
(Standalone Servers)
NetApp FAS2520 Storage Controller

1.2 Use Case Summary

This document describes the deployment procedures and best practices to set up a FlexPod Express small and/or medium with Microsoft Windows Server 2012 R2 Hyper-V as the workload. The server operating system/hypervisor is Microsoft Windows Server 2012 R2 Hyper-V, and an instance of Microsoft System Center 2012 R2 Virtual Machine Manager is installed to manage the Hyper-V instances. The whole infrastructure is supported by NetApp FAS storage systems that serve data over storage area network (SAN) and network-attached storage (NAS) protocols.

2 Technology Requirements

The hardware and software components required to implement the FlexPod Express small and medium configurations are detailed in this section.

2.1 Hardware Requirements

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

Table 1) FlexPod Express small configuration hardware requirements.

Layer	Hardware	Quantity
Compute	Cisco UCS C220 M4 rack servers (standalone)	2
Network	Cisco Nexus 3048 switches	2

Layer	Hardware	Quantity
Storage	NetApp FAS2520 (high-availability pair)	1
Disks	900GB, 10.000 rpm SAS with Advanced Drive Partitioning	12

Table 2 lists the hardware components required to implement the FlexPod Express medium configuration solution.

Table 2) FlexPod Express medium configuration hardware requirements.

Layer	Hardware	Quantity
Compute	Cisco UCS C220 M4 rack servers (standalone)	4
Network	Cisco Nexus 3048 switches	2
Storage	NetApp FAS2520 (high-availability pair)	1
Disks	900GB, 10,000 rpm SAS with Advanced Drive Partitioning	12

2.2 Software Requirements

Table 3 lists the software components required to implement the FlexPod Express small and medium configurations.

Table 3) Software requirements.

Layer	Component	Version or Release	Details
Compute	Cisco UCS C220 M4 rack servers	2.0(3)	Cisco® Integrated Management Controller (IMC) software
Network	Cisco Nexus 3048 Gigabit Ethernet switches	6.0(2)U6(1)	Cisco NX-OS software
Storage	NetApp FAS2520 high-availability storage	8.3	NetApp Data ONTAP software
Hypervisor	Microsoft Windows Server 2012 R2 Hyper-V	2012 R2	Virtualization hypervisor
Other software	System Center Virtual Machine Manager	2012 R2	Virtualization management
	NetApp Data ONTAP SMI-S Agent	5.1.1	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 NetApp Snapshot management
	NetApp SnapManager for Hyper-V	2.0.3	NetApp plug-in for Hyper-V

3 FlexPod Express Cabling Information

3.1 FlexPod Express Small Configuration

Figure 3 provides a cabling diagram for the FlexPod Express small configuration. Table 4 provides the cabling information.

Figure 3) FlexPod Express small configuration cabling diagram.

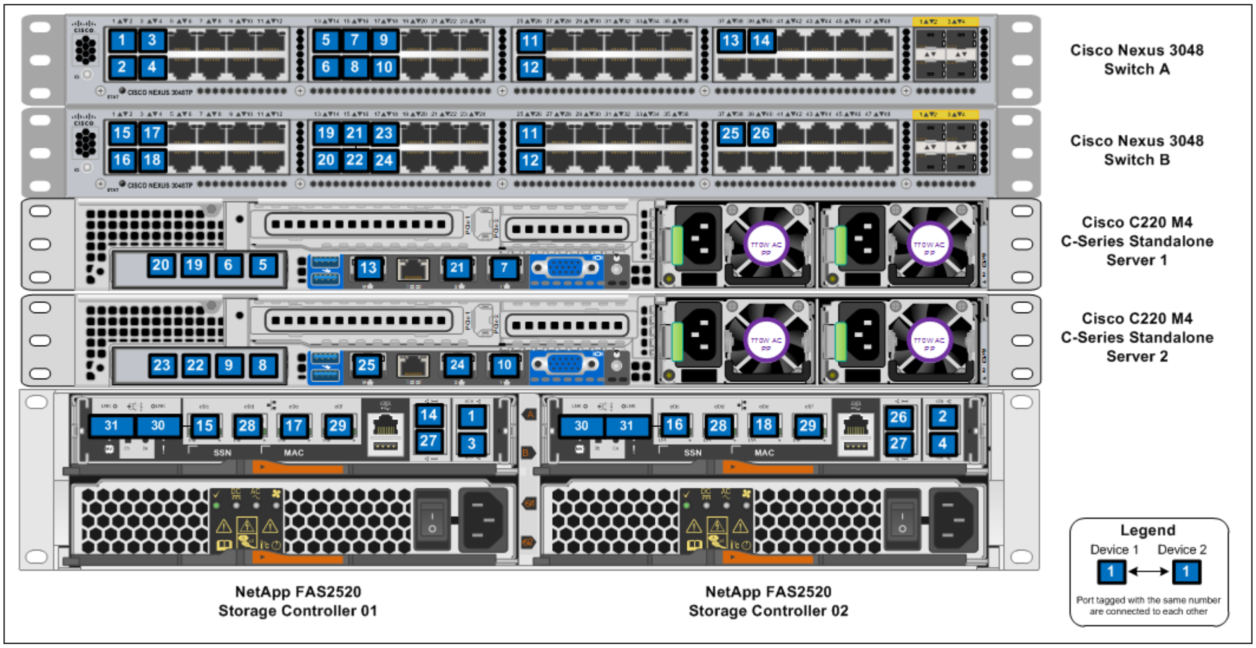

Cisco Nexus 3048 Switch A
1 3 2 4 5 7 9 6 8 10 11 12 13 14
Cisco Nexus 3048 Switch B
15 17 16 18 19 21 23 20 22 24 11 12 25 26
Cisco C220 M4 C-Series Standalone Server 1
20 19 6 5 13 21 7
Cisco C220 M4 C-Series Standalone Server 2
23 22 9 8 25 24 10
31 30 15 28 17 29 14 27 1 3
30 31 16 28 18 29 26 27 2 4
NetApp FAS2520 Storage Controller 01
NetApp FAS2520 Storage Controller 02
Legend
Device 1
Device 2
1
1
Port tagged with the same number are connected to each other

Table 4) Cabling information for the FlexPod Express small configuration.

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
Cisco Nexus 3048 Switch A	Eth1/1	NetApp FAS2520 Storage Controller 01	e0a	1
	Eth1/2	NetApp FAS2520 Storage Controller 02	e0a	2
	Eth1/3	NetApp FAS2520 Storage Controller 01	e0b	3
	Eth1/4	NetApp FAS2520 Storage Controller 02	e0b	4
	Eth1/13	Cisco UCS C220 C-Series Standalone Server 1	MLOM Port 1	5
	Eth1/14	Cisco UCS C220 C-Series Standalone Server 1	MLOM Port 2	6
	Eth1/15	Cisco UCS C220 C-Series Standalone Server 1	LOM1	7
	Eth1/16	Cisco UCS C220 C-Series Standalone Server 2	MLOM Port 1	8

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
	Eth1/17	Cisco UCS C220 C-Series Standalone Server 2	MLOM Port 2	9
	Eth1/18	Cisco UCS C220 C-Series Standalone Server 2	LOM1	10
	Eth1/25	Cisco Nexus 3048 Switch B	Eth1/25	11
	Eth1/26	Cisco Nexus 3048 Switch B	Eth1/26	12
	Eth1/37	Cisco UCS C220 C-Series Standalone Server 1	Cisco IMC	13
	Eth1/39	NetApp FAS2520 Storage Controller 01	e0M	14

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
Cisco Nexus 3048 Switch B	Eth1/1	NetApp FAS2520 Storage Controller 01	e0c	15
	Eth1/2	NetApp FAS2520 Storage Controller 02	e0c	16
	Eth1/3	NetApp FAS2520 Storage Controller 01	e0e	17
	Eth1/4	NetApp FAS2520 Storage Controller 02	e0e	18
	Eth1/13	Cisco UCS C220 C-Series Standalone Server 1	MLOM Port 3	19
	Eth1/14	Cisco UCS C220 C-Series Standalone Server 1	MLOM Port 4	20
	Eth1/15	Cisco UCS C220 C-Series Standalone Server 1	LOM2	21
	Eth1/16	Cisco UCS C220 C-Series Standalone Server 2	MLOM Port 3	22
	Eth1/17	Cisco UCS C220 C-Series Standalone Server 2	MLOM Port 4	23
	Eth1/18	Cisco UCS C220 C-Series Standalone Server 2	LOM2	24
	Eth1/25	Cisco Nexus 3048 Switch A	Eth1/25	11
	Eth1/26	Cisco Nexus 3048 Switch A	Eth1/26	12

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
	Eth1/37	Cisco UCS C220 C-Series Standalone Server 2	Cisco IMC	25
	Eth1/39	NetApp FAS2520 Storage Controller 02	e0M	26

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
NetApp FAS2520 Storage Controller 01	e0d	NetApp FAS2520 Storage Controller 02	e0d	28
	e0f	NetApp FAS2520 Storage Controller 02	e0f	29
	ACP	NetApp FAS2520 Storage Controller 02	ACP	27
	SAS 0a	NetApp FAS2520 Storage Controller 02	SAS 0b	30
	SAS 0b	NetApp FAS2520 Storage Controller 02	SAS 0a	31

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
NetApp FAS2520 Storage Controller 02	e0d	NetApp FAS2520 Storage Controller 01	e0d	28
	e0f	NetApp FAS2520 Storage Controller 01	e0f	29
	ACP	NetApp FAS2520 Storage Controller 01	ACP	27
	SAS 0a	NetApp FAS2520 Storage Controller 01	SAS 0b	31
	SAS 0b	NetApp FAS2520 Storage Controller 01	SAS 0a	30

3.2 FlexPod Express Medium Configuration

Figure 4 provides the cabling diagram for the FlexPod Express small configuration. Table 5 provides the cabling information.

Figure 4) FlexPod Express medium configuration cabling diagram.

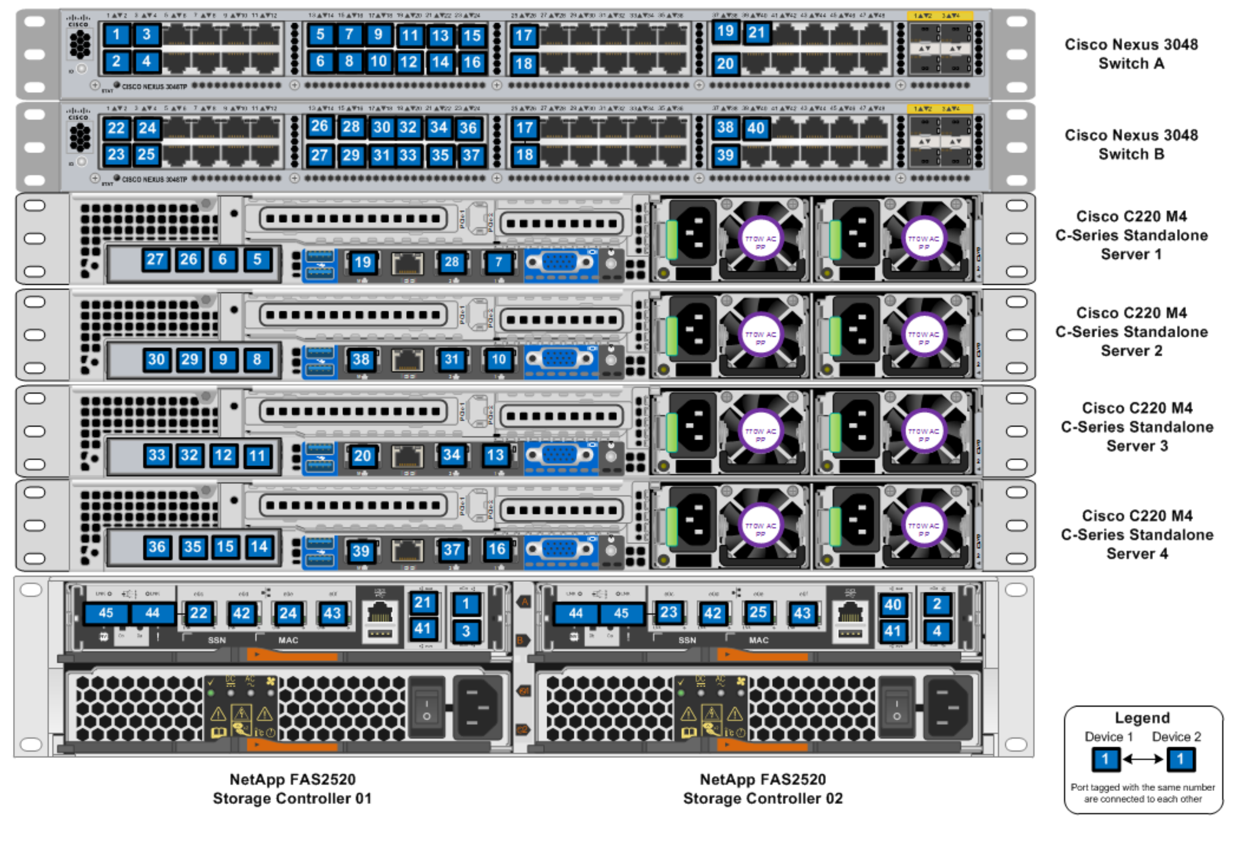


Table 5) Cabling information for the FlexPod Express medium configuration.

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
Cisco Nexus 3048 Switch A	Eth1/1	NetApp FAS2520 Storage Controller 01	e0a	1
	Eth1/2	NetApp FAS2520 Storage Controller 02	e0a	2
	Eth1/3	NetApp FAS2520 Storage Controller 01	e0b	3
	Eth1/4	NetApp FAS2520 Storage Controller 02	e0b	4
	Eth1/13	Cisco UCS C220 C-Series Standalone Server 1	MLOM Port 1	5
	Eth1/14	Cisco UCS C220 C-Series Standalone Server 1	MLOM Port 2	6
	Eth1/15	Cisco UCS C220 C-Series Standalone Server 1	LOM1	7
	Eth1/16	Cisco UCS C220 C-Series Standalone Server 2	MLOM Port 1	8

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
	Eth1/17	Cisco UCS C220 C-Series Standalone Server 2	MLOM Port 2	9
	Eth1/18	Cisco UCS C220 C-Series Standalone Server 2	LOM1	10
	Eth1/19	Cisco UCS C220 C-Series Standalone Server 3	MLOM Port 1	11
	Eth1/20	Cisco UCS C220 C-Series Standalone Server 3	MLOM Port 2	12
	Eth1/21	Cisco UCS C220 C-Series Standalone Server 3	LOM1	13
	Eth1/22	Cisco UCS C220 C-Series Standalone Server 4	MLOM Port1	14
	Eth1/23	Cisco UCS C220 C-Series Standalone Server 4	MLOM Port 2	15
	Eth1/24	Cisco UCS C220 C-Series Standalone Server 4	LOM1	16
	Eth1/25	Cisco Nexus 3048 Switch B	Eth1/25	17
	Eth1/26	Cisco Nexus 3048 Switch B	Eth1/26	18
	Eth1/37	Cisco UCS C220 C-Series Standalone Server 1	Cisco IMC	19
	Eth1/38	Cisco UCS C220 C-Series Standalone Server 3	Cisco IMC	20
	Eth1/39	NetApp FAS2520 Storage Controller 01	e0M	21

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
Cisco Nexus 3048 Switch B	Eth1/1	NetApp FAS2520 Storage Controller 01	e0c	22
	Eth1/2	NetApp FAS2520 Storage Controller 02	e0c	23
	Eth1/3	NetApp FAS2520 Storage Controller 01	e0e	24
	Eth1/4	NetApp FAS2520 Storage Controller 02	e0e	25
	Eth1/13	Cisco UCS C220 C-Series Standalone Server 1	MLOM Port 3	26

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
	Eth1/14	Cisco UCS C220 C-Series Standalone Server 1	MLOM Port 4	27
	Eth1/15	Cisco UCS C220 C-Series Standalone Server 1	LOM2	28
	Eth1/16	Cisco UCS C220 C-Series Standalone Server 2	MLOM Port 3	29
	Eth1/17	Cisco UCS C220 C-Series Standalone Server 2	MLOM Port 4	30
	Eth1/18	Cisco UCS C220 C-Series Standalone Server 2	LOM2	31
	Eth1/19	Cisco UCS C220 C-Series Standalone Server 3	MLOM Port 3	32
	Eth1/20	Cisco UCS C220 C-Series Standalone Server 3	MLOM Port 4	33
	Eth1/21	Cisco UCS C220 C-Series Standalone Server 3	LOM2	34
	Eth1/22	Cisco UCS C220 C-Series Standalone Server 4	MLOM Port3	35
	Eth1/23	Cisco UCS C220 C-Series Standalone Server 4	MLOM Port 4	36
	Eth1/24	Cisco UCS C220 C-Series Standalone Server 4	LOM2	37
	Eth1/25	Cisco Nexus 3048 Switch A	Eth1/25	17
	Eth1/26	Cisco Nexus 3048 Switch A	Eth1/26	18
	Eth1/37	Cisco UCS C220 C-Series Standalone Server 2	Cisco IMC	38
	Eth1/38	Cisco UCS C220 C-Series Standalone Server 4	Cisco IMC	39
	Eth1/39	NetApp FAS2520 Storage Controller 02	e0M	40

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
NetApp FAS2520 Storage	e0d	NetApp FAS2520 Storage Controller 02	e0d	42
	e0f	NetApp FAS2520 Storage Controller 02	e0f	43

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
Controller 01	ACP	NetApp FAS2520 Storage Controller 02	ACP	41
	SAS 0a	NetApp FAS2520 Storage Controller 02	SAS 0b	44
	SAS 0b	NetApp FAS2520 Storage Controller 02	SAS 0a	45

Local Device	Local Port	Remote Device	Remote Port	Cabling Code
NetApp FAS2520 Storage Controller 02	e0d	NetApp FAS2520 Storage Controller 01	e0d	42
	e0f	NetApp FAS2520 Storage Controller 01	e0f	43
	ACP	NetApp FAS2520 Storage Controller 01	ACP	41
	SAS 0a	NetApp FAS2520 Storage Controller 01	SAS 0b	45
	SAS 0b	NetApp FAS2520 Storage Controller 01	SAS 0a	44

4 Deployment Procedures

This document provides details for configuring a fully redundant, highly available FlexPod Express system. To reflect this redundancy, the components being configured in each step are referred to as either Component 01 or Component 02. For example, Controller 01 and Controller 02 identify the two NetApp storage controllers that are provisioned in this document, and Switch A and Switch B identify the pair of Cisco Nexus switches that are configured.

Additionally, this document details the 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 6 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 6) Required VLANs.

VLAN Name	VLAN Purpose	ID Used in Validating This Document
Management VLAN	VLAN for management interfaces	186
Native VLAN	VLAN to which untagged frames are assigned	2
iSCSI-A	VLAN for iSCSI traffic	3011
iSCSI-B	VLAN for iSCSI traffic	3012
LiveMigration	VLAN designated for the movement of virtual machines (VMs) from one physical host to another	3013
Cluster	VLAN for cluster communication and CSV traffic	3014
VM Traffic	VLAN for VM application traffic	3015

Table 7 lists Hyper-V virtual machines (VMs) created.

Table 8) Hyper-V virtual machines created.

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

4.1 Cisco Nexus 3048 Deployment Procedure

The following section details the Cisco Nexus 3048 switch configuration for use in a FlexPod Express environment.

Cisco Nexus 3048 Switch Initial 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 3048 switch 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 keepalive 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 onscreen prompts as illustrated here for the initial setup of both switches, substituting the appropriate values for the switch-specific information.

Cisco Nexus Switch A and Switch B

```
Abort Power On Auto Provisioning [yes - continue with normal setup, skip - bypass password and
basic configuration, no - continue with Power On Auto Provisioning] (yes/skip/no)[no]: 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 3000 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]:n
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
no telnet server enable
ssh key rsa 1024 force
ssh server enable
system default switchport
no system default switchport shutdown
policy-map type control-plane copp-system-policy ( default )

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

Upgrading Cisco NX-OS (Optional)

Perform any required software upgrades on the switch at this point in the configuration process. Download and install the latest available Cisco NX-OS software for the Cisco Nexus 3048 switch from the Cisco software download site. There are several 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 3048 switch.

Note: Cisco NX-OS software release 6.0(2)U6(1) is used in this solution.

1. Copy the files to the local bootflash memory and update the switch.

Cisco Nexus Switch A and Switch B

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

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

Enabling Advanced Features

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

Note: The `interface-vlan` feature is required only if you are use the back-to-back mgmt0 option described throughout this document. 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.

Cisco Nexus Switch A and Switch B

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

Performing Global PortChannel Configuration

The default PortChannel load-balancing hash uses the source and destination IP addresses to determine the load-balancing algorithm across the interfaces in the PortChannel. You can achieve better distribution across the members of the PortChannels by providing more inputs to the hash algorithm beyond the source and destination IP addresses. For that reason, NetApp highly recommends adding the source and destination TCP ports to the hash algorithm.

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

Cisco Nexus Switch A and Switch B

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

Performing Global Spanning-Tree Configuration

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

The recommended setting for bridge assurance is to consider all ports to be network ports by default. This setting forces the network administrator to review the configuration of each port and helps reveal the most common configuration errors, such as unidentified edge ports or a neighbor that does not have bridge assurance enabled. Also, it is safer to have spanning tree block too many ports than not enough, enabling 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 might 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.

Cisco Nexus Switch A and Switch B

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

Configuring Jumbo Frames

Jumbo frames should be configured throughout the network to 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.

Cisco Nexus Switch A and Switch B

```
policy-map type network-qos jumbo
  class type network-qos class-default
    mtu 9000
system qos
  service-policy type network-qos jumbo
exit
```

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 troubleshooting in the future.

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

Cisco Nexus Switch A and Switch B

```
vlan <<iscsia_vlan_id>>
  name iSCSIA-VLAN
vlan <<iscsib_vlan_id>>
  name iSCSIB-VLAN
vlan <<lm_vlan_id>>
  name LiveMigration-VLAN
vlan <<csv_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
```

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.

For the small configuration, the descriptions for the management ports and data ports associated with Server-3 and Server-4 is not required because the FlexPod Express small configuration contains only two servers.

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

FlexPod Express Small Configuration

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

Cisco Nexus Switch A

```
int eth1/1
  description Controller-01:e0a
int eth1/2
  description Controller-02:e0a
int eth1/3
  description Controller-01:e0b
int eth1/4
  description Controller-02:e0b
int eth1/13
  description Server-1:MLOM Port1
int eth1/14
  description Server-1:MLOM Port2
int eth1/15
  description Server-1:LOM Port1
int eth1/16
  description Server-2:MLOM Port1
int eth1/17
  description Server-2:MLOM Port2
int eth1/18
  description Server-2:LOM Port1
int eth1/25
  description vPC peer-link NX3048-B:1/25
int eth1/26
  description vPC peer-link NX3048-B:1/26
int eth1/37
  description Server-1:mgmt
int eth1/39
  description Controller-01:mgmt
```

Cisco Nexus Switch B

```
int eth1/1
  description Controller-01:e0c
int eth1/2
  description Controller-02:e0c
int eth1/3
  description Controller-01:e0e
int eth1/4
  description Controller-02:e0e
int eth1/13
  description Server-1: MLOM Port3
int eth1/14
  description Server-1:MLOM Port4
int eth1/15
  description Server-1:LOM Port2
int eth1/16
  description Server-2:MLOM Port3
int eth1/17
  description Server-2:MLOM Port4
int eth1/18
  description Server-2:LOM Port2
int eth1/25
  description vPC peer-link NX3048-A:1/25
int eth1/26
  description vPC peer-link NX3048-A:1/26
int eth1/37
  description Server-2:mgmt
int eth1/39
  description Controller-02:mgmt
```

FlexPod Express Medium Configuration

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

Cisco Nexus Switch A

```
int eth1/19
  description Server-3: MLOM Port1
int eth1/20
  description Server-3: MLOM Port2
int eth1/21
  description Server-3: LOM Port1
int eth1/22
  description Server-4: MLOM Port1
int eth1/23
  description Server-4: MLOM Port2
int eth1/24
  description Server-4: LOM Port1
int eth1/38
  description Server-3:mgmt
```

Cisco Nexus Switch B

```
int eth1/19
  description Server-3: MLOM Port3
int eth1/20
  description Server-3: MLOM Port4
int eth1/21
  description Server-3: LOM Port2
int eth1/22
  description Server-4: MLOM Port3
int eth1/23
  description Server-4: MLOM Port4
int eth1/24
  description Server-4: LOM Port2
int eth1/38
  description Server-4:mgmt
```

Configuring Server and Storage Management Interfaces

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

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

Cisco Nexus Switch A and Switch B

```
int eth1/37-39
  switchport access vlan <<ib_mgmt_vlan_id>>
  spanning-tree port type edge
exit
```

Performing Virtual PortChannel Global Configuration

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

Cisco Nexus Switch A

```
vpc domain 1
  role priority 10
  peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source <<switch_A_mgmt0_ip_addr>> vrf
management
  peer-gateway
  auto-recovery
int eth1/25-26
  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 <<iscsia_vlan_id>>,<<iscsib_vlan_id>>, <<lm_vlan_id>>,
<<csv_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.

Cisco Nexus Switch B

```
vpc domain 1
  role priority 20
  peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source <<switch_B_mgmt0_ip_addr>> vrf
management
int eth1/25-26
  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 <<iscsia_vlan_id>>,<<iscsib_vlan_id>>, <<lm_vlan_id>>,
<<csv_vlan_id>>, << vmtraffic_vlan_id>>, << ib_mgmt_vlan_id>>
  spanning-tree port type network
  vpc peer-link
no shut
exit
copy run start
```

Configuring Storage PortChannels

The NetApp storage controllers allow an active-active connection to the network using Link Aggregation Control Protocol (LACP). The use of LACP is preferred because it adds both negotiation and logging between the switches. Because the network is set up for vPC, this approach 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.

Cisco Nexus Switch A and Switch B and Controller-01 Configuration

```
int eth1/1, eth1/3
  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 <<iscsia_vlan_id>>,<<iscsib_vlan_id>>,<<ib_mgmt_vlan_id>>
  spanning-tree port type edge trunk
  vpc 11
  no shut
```

Cisco Nexus Switch A and Switch B and Controller-02 Configuration

```
int eth1/2, eth1/4
  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 <<iscsia_vlan_id>>,<<iscsib_vlan_id>>,<<ib_mgmt_vlan_id>>
  spanning-tree port type edge trunk
  vpc 12
  no shut
exit
copy run start
```

Configuring Server Connections

The Cisco UCS servers have multiple Ethernet interfaces that can be configured to fail over to one another, providing additional redundancy beyond a single link. Spreading these links across multiple switches enables the server to survive even a complete switch failure.

For the small configuration, you need to configure only Server-1 and Server-2 because only two servers are used in the small FlexPod Express configuration.

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

FlexPod Express Small Configuration

Cisco Nexus Switch A and Switch B, Server-1, and Server-2

```
int eth1/13, eth1/16
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<vmtraffic_vlan_id>>, <<ib_mgmt_vlan_id>>
  spanning-tree port type edge trunk
  no shut
exit

copy run start
```

Cisco Nexus Switch A, Server-1, and Server-2

```
int eth1/14, eth1/17
  switchport
  switchport access vlan <<iscsia_vlan_id>>
  spanning-tree port type edge
  no shut
exit

int eth1/15, eth1/18
  switchport
  switchport access vlan <<lm_vlan_id>>
  spanning-tree port type edge
  no shut
exit

copy run start
```

Cisco Nexus Switch B, Server-1, and Server-2

```
int eth1/13, eth1/16
  vpc orphan-port suspend
  no shut
exit

int eth1/14, eth1/17
  switchport
  switchport access vlan <<iscsib_vlan_id>>
  spanning-tree port type edge
  no shut
exit

int eth1/15, eth1/18
  switchport
  switchport access vlan <<csv_vlan_id>>
  spanning-tree port type edge
  no shut
exit

copy run start
```

FlexPod Express Medium Configuration

Cisco Nexus Switch A and Switch B, Server-3, and Server-4 Configuration

```
int eth1/19, eth1/22
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<vmtraffic_vlan_id>>, <<ib_mgmt_vlan_id>>
  spanning-tree port type edge trunk
  no shut
exit

copy run start
```

Cisco Nexus Switch A, Server-3, and Server-4

```
int eth1/20, eth1/23
  switchport
  switchport access vlan <<iscsia_vlan_id>>
  spanning-tree port type edge
  no shut
exit
int eth1/21, eth1/24
  switchport
  switchport access vlan <<lm_vlan_id>>
  spanning-tree port type edge
  no shut
exit
copy run start
```

Cisco Nexus Switch B, Server-3, and Server-4

```
int eth1/19, eth1/22
  vpc orphan-port suspend
  no shut
exit

int eth1/20, eth1/23
  switchport
  switchport access vlan <<iscsib_vlan_id>>
  spanning-tree port type edge
  no shut
exit
int eth1/21, eth1/24
  switchport
  switchport access vlan <<csv_vlan_id>>
  spanning-tree port type edge
  no shut
exit
copy run start
```

Performing In-Band Management SVI Configuration

In-band management using SSH in the FlexPod Express environment is handled by an SVI. To configure the 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.

Cisco Nexus Switch A

```
int Vlan <<ib_mgmt_vlan_id>>
ip address <<inband_mgmt_ip_address_A>>/<<inband_mgmt_netmask>>
no shut
ip route 0.0.0.0/0 <<inband_mgmt_gateway>>
```

Cisco Nexus Switch B

```
int Vlan <<ib_mgmt_vlan_id>>
ip address <<inband_mgmt_ip_address_B>>/<<inband_mgmt_netmask>>
no shut
ip route 0.0.0.0/0 <<inband_mgmt_gateway>>
```

4.2 NetApp FAS Storage Deployment Procedure

This section describes the NetApp FAS storage deployment procedure.

Controller FAS25xx Series

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 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.”

Table 9) Controller FAS25XX series prerequisites.

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

Storage Controllers

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

NetApp Clustered Data ONTAP 8.3

Complete the Configuration Worksheet

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

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

Table 10) Clustered Data ONTAP software installation prerequisites.

Cluster Detail	Cluster Detail Value
Cluster node 01 IP address	`<<var_node01_mgmt_ip>>`
Cluster node 01 netmask	`<<var_node01_mgmt_mask>>`
Cluster node 01 gateway	`<<var_node01_mgmt_gateway>>`
Cluster node 02 IP address	`<<var_node02_mgmt_ip>>`
Cluster node 02 netmask	`<<var_node02_mgmt_mask>>`

Cluster Detail	Cluster Detail Value
Cluster node 02 gateway	`<<var_node02_mgmt_gateway>>`
Data ONTAP 8.3 URL	`<<var_url_boot_software>>`

Node 01

To configure node 01, complete the following steps:

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

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

2. Set boot monitor defaults.

```
Set-defaults
```

3. Allow the system to boot.

```
autoboot
```

4. Press Ctrl-C when prompted.

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

5. To install new software, select option 7.

```
7
```

6. Answer `yes` to perform an upgrade.

```
y
```

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

```
e0M
```

8. Select yes to reboot now.

```
y
```

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

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

10. Enter the URL where the software is located.

Note: This web server must be pingable.

```
<<var_url_boot_software>>
```

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

```
Enter
```

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

```
y
```

13. Enter yes to reboot the node.

```
y
```

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

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

```
Ctrl - C
```

15. Select option 5 to enter into maintenance mode.

```
5
```

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

```
disk remove_ownership

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

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

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

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

```
halt
```

18. Start Data ONTAP.

```
autoboot
```

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

```
Ctrl - C
```

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

```
4
```

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

```
y
```

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

```
y
```

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

Node 02

To configure node 02, complete the following steps:

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

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

2. Set the boot monitor defaults.

```
set-defaults
```

3. Allow the system to boot.

```
autoboot
```

4. Press Ctrl-C when prompted.

```
Ctrl-C
```

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

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

```
7
```

6. Answer yes to perform a nondisruptive upgrade.

```
y
```

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

```
e0M
```

8. Select yes to reboot now.

```
y
```

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

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

10. Enter the URL where the software is located.

Note: This web server must be pingable.

```
<<var_url_boot_software>>
```

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

```
Enter
```

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

```
y
```

13. Select yes to reboot the node.

```
y
```

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

14. Press Ctrl-C for the boot menu:

```
Ctrl - C
```

15. Select option 5 to enter maintenance mode.

```
5
```

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

```
disk remove_ownership

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

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

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

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

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

```
halt
```

18. Start Data ONTAP.

```
autoboot
```

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

```
Ctrl – C
```

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

```
4
```

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

```
y
```

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

```
y
```

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

Node Setup in Clustered Data ONTAP

From a console port program attached to the storage controller A (Node 01) console port, execute the node setup script. This script will come up when Data ONTAP 8.3 first boots on a node.

1. Follow the prompts below:

```
Welcome to node setup.

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

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

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

Type yes to confirm and continue {yes}: yes

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


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

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

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

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

2. Press Return and log in to the node using the admin user ID and no password to get a node command prompt.

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

::> system node reboot

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

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

```
Welcome to node setup.

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

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


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


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

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

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

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

4. Log in to the node with the admin user and no password.
5. Repeat this entire procedure for node 2 of the storage cluster.

Cluster Create in Clustered Data ONTAP

Table 11) Cluster create in clustered Data ONTAP prerequisites.

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

Cluster Detail	Cluster Detail Value
Cluster node01 gateway	<<var_node01_mgmt_gateway>>

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

Using the console session to node 01 the Cluster Setup wizard is brought up by typing `cluster setup`.

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

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

To create a new cluster, complete the following steps:

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

```
create
```

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

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

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

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

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

```
Existing cluster interface configuration found:

Port    MTU     IP              Netmask
e0d     9000    169.254.128.103       255.255.0.0
e0f     9000    169.254.52.249 255.255.0.0

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

5. The steps to create a cluster are displayed.

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

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

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

```
Enter the cluster management interface port [e0a]: e0M
Enter the cluster management interface IP address: <<var_clustermgmt_ip>>
Enter the cluster management interface netmask: <<var_clustermgmt_mask>>
Enter the cluster management interface default gateway: <<var_clustermgmt_gateway>>
```

6. Enter the DNS domain name.

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

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

7. Set up the node.

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

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

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

Cluster Join in Clustered Data ONTAP

Table 12) Cluster join in clustered Data ONTAP prerequisites.

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

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

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

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

```
admin
```

2. Start the Cluster Setup wizard by typing `cluster setup`.

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

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

3. Run the following command to join a cluster:

```
join
```

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

```
Existing cluster interface configuration found:

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

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

5. The steps to join a cluster are displayed.

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

```

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

6. Set up the node.

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


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

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

Logging in to the Cluster

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

Zeroing All Spare Disks

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

1. Run the following command:

```
disk zerospares
```

Changing Disk Ownership

Data ONTAP 8.3 has Advanced Drive Partitioning (ADP) feature, which increases storage efficiency. This document covers the creation of one data aggregate in active/passive configuration. However, if desired, there can be multiple data aggregates in active/active configuration. To configure ADP active/passive configuration, complete the following steps:

1. Disable the disk autoassign.

```
storage disk option modify -autoassign off -node <<var_node01>>, <<var_node02>>
```

2. Find all the data partition owned by node02.

```
nbice-fpe1::> storage disk show -data-owner <<var_node02>>
```

```
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name      Owner
---------------- ---------- ----- --- ------- ----------- --------- --------
1.0.0               546.9GB     0   0 SAS     shared      aggr0_nbice_fpe1_02_0
                                                                    nbice-fpe1-02
1.0.2               546.9GB     0   2 SAS     shared      aggr0_nbice_fpe1_02_0
                                                                    nbice-fpe1-02
1.0.4               546.9GB     0   4 SAS     shared      aggr0_nbice_fpe1_02_0
                                                                    nbice-fpe1-02
1.0.6               546.9GB     0   6 SAS     shared      aggr0_nbice_fpe1_02_0
                                                                    nbice-fpe1-02
1.0.8               546.9GB     0   8 SAS     shared      aggr0_nbice_fpe1_02_0
                                                                    nbice-fpe1-02
1.0.10              546.9GB     0  10 SAS     shared      -         nbice-fpe1-02
6 entries were displayed.
```

3. Increase the privilege level.

```
nbice-fpe1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only when directed to do so
by NetApp personnel.
Do you want to continue? {y|n}: y
```

4. Remove the disk ownership for the disks listed in the previous command.

```
storage disk removeowner -data true -disk <Disk Name>

Warning: Disks may be automatically assigned to the node because the disk's auto-assign option is
enabled. If the affected volumes are not offline, the disks may be auto-assigned during the
remove owner operation, which will cause unexpected results. To verify that the volumes are
offline, abort this command and use "volume show".
Do you want to continue? {y|n}: y
6 entries were acted on.
```

Note: To remove the ownership of multiple disks, <Disk Name> can be comma separated in the previous command.

5. Assign all the unassigned data partition disks to node 01.

```
storage disk assign -data true -disk <Disk Name> -owner <<var_node01>>
```

Note: The disk assign command should be executed one at a time for each disk.

6. Decrease the privilege level.

```
set -privilege admin
```

Enabling Cisco Discovery Protocol in Clustered Data ONTAP

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

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

1. Enable CDP on Data ONTAP.

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

Setting Auto-Revert on Cluster Management

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

1. Run the following command:

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

Setting Up Service Processor Network Interface

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

1. Run the following commands:

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

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

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

Enabling Storage Failover in Clustered Data ONTAP

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

1. Verify the status of storage failover.

```
storage failover show
```

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

2. Enable failover on one of the two nodes.

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

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

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

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

```
cluster ha show
```

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

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

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

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

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

Creating Jumbo Frame MTU Broadcast Domain in Clustered Data ONTAP

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

1. Create broadcast domain on Data ONTAP.

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

Removing 1 GE Data Ports From Default Broadcast Domain

To remove a data port from the default broadcast domain, complete the following step:

```
broadcast-domain remove-ports -broadcast-domain Default -ports <<var_node01>>:e0a,
<<var_node01>>:e0b, <<var_node01>>:e0c, <<var_node01>>:e0e, <<var_node02>>:e0a,
<<var_node02>>:e0b, <<var_node02>>:e0c, <<var_node02>>:e0e
```

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. From the cluster prompt, complete the following steps:

```
ifgrp create -node <<controller01>> -ifgrp a0a -distr-func port -mode multimode_lacp
network port ifgrp add-port -node <<var_node01>> -ifgrp a0a -port e0a
network port ifgrp add-port -node <<var_node01>> -ifgrp a0a -port e0b
network port ifgrp add-port -node <<var_node01>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_node01>> -ifgrp a0a -port e0e

ifgrp create -node <<controller02>> -ifgrp a0a -distr-func port -mode multimode_lacp
network port ifgrp add-port -node <<var_node02>> -ifgrp a0a -port e0a
network port ifgrp add-port -node <<var_node02>> -ifgrp a0a -port e0b
network port ifgrp add-port -node <<var_node02>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_node02>> -ifgrp a0a -port e0e
```

Configuring Jumbo Frames in Clustered Data ONTAP

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

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

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

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

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

Creating VLAN in Clustered Data ONTAP

1. Create iSCSI VLAN ports and add to the data broadcast domain.

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

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

2. Create IB-MGMT-VLAN ports and add it to the default broadcast domain.

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

broadcast-domain add-ports -broadcast-domain Default -ports <<var_node01>>: a0a-
<<ib_mgmt_vlan_id>>, <<var_node02>>: a0a-<<ib_mgmt_vlan_id>>
```

Creating Aggregates in Clustered Data ONTAP

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

To create new aggregates, complete the following steps:

1. Run the following commands:

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

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

Note: Start with five disks initially; you can add disks to an aggregate when additional storage is required. Note that in this configuration with a FAS2520, it may be desirable to create an aggregate with all but one remaining disk (spare) assigned to the controller.

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

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

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

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

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

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

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

Configuring NTP in Clustered Data ONTAP

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

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

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

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

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

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

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

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

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

Configuring SNMP in Clustered Data ONTAP

To configure SNMP, complete the following steps:

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

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

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

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

Configuring SNMPv1 in Clustered Data ONTAP

To configure SNMPv1, complete the following step:

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

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

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

Configuring SNMPv3 in Clustered Data ONTAP

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

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

```
security login create -user-or-group-name snmpv3user -authmethod usm -application snmp
```

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

Configuring AutoSupport HTTPS in Clustered Data ONTAP

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

1. Run the following command:

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

Creating Storage Virtual Machine (Vserver)

To create an infrastructure Vserver, complete the following steps:

1. Run the Vserver create command.

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

2. Select the Vserver data protocols to configure, leaving `iscsi`.

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

3. Enable and run the iSCSI protocol in the Infra-SVM Vserver.

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

Configuring HTTPS Access in Clustered Data ONTAP

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

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

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

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

```
security certificate show
```

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

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

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

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

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

5. To obtain the values for the parameters that would be required in the following step, run the `security certificate show` command.

6. Enable each certificate that was just created using the `–server-enabled true` and `–client-enabled false` parameters. Again use TAB completion.

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

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

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

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

8. Revert to normal admin privilege level and set up to allow Vserver logs to be available by web.

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

Creating FlexVol Volume in Clustered Data ONTAP

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

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

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate aggr1_node01 -size 2t -
state online -policy default -space-guarantee none -percent-snapshot-space 0 -junction-path
/infra_datastore_1

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

```
volume create -vserver Infra-SVM -volume quorum -aggregate aggr1_node01 -size 5g -state online -
policy default -space-guarantee none -percent-snapshot-space 0 -junction-path /quorum
```

Creating iSCSI LIF in Clustered Data ONTAP

To create iSCSI LIFs, complete the following step:

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

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

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

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

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

network interface show
```

Adding Infrastructure Vserver Administrator

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

1. Run the following commands:

```
network interface create –vserver Infra-SVM –lif vsmgmt –role data –data-protocol none –home-node
<<var_node01>> -home-port  a0a-<<ib_mgmt_vlan_id>> –address <<var_vserver_mgmt_ip>> -netmask
<<var_vserver_mgmt_mask>> -status-admin up –failover-policy broadcast-domain-wide –firewall-
policy mgmt –auto-revert true

```

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

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

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

network route show
```

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

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

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

4.3 Cisco UCS C-Series Rack Server Deployment Procedure

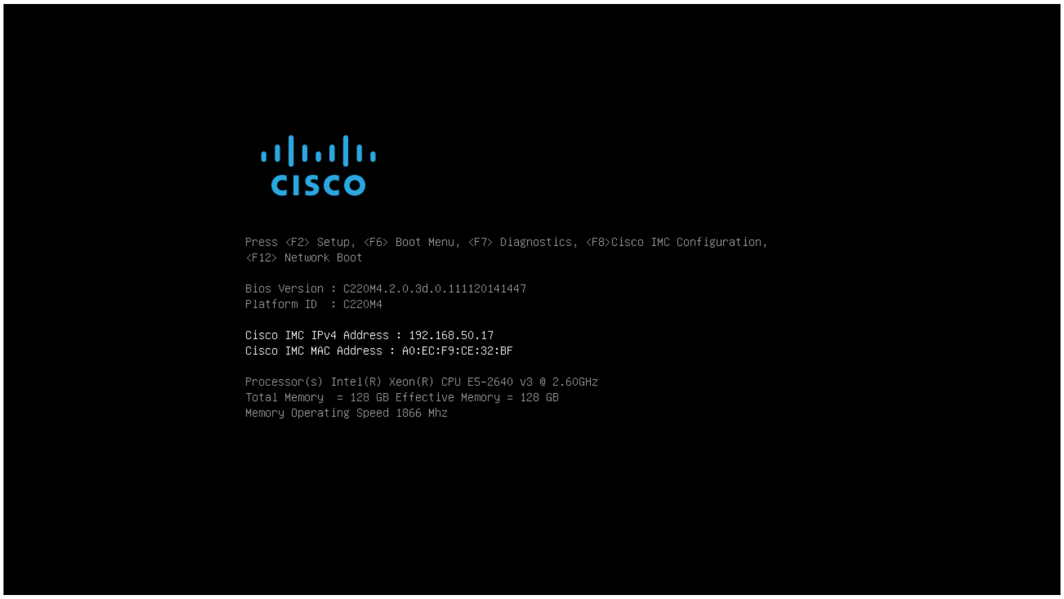
The following section provides a detailed procedure for configuring a Cisco UCS C-Series standalone rack server for use in large FlexPod Express configurations.

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

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

All Servers

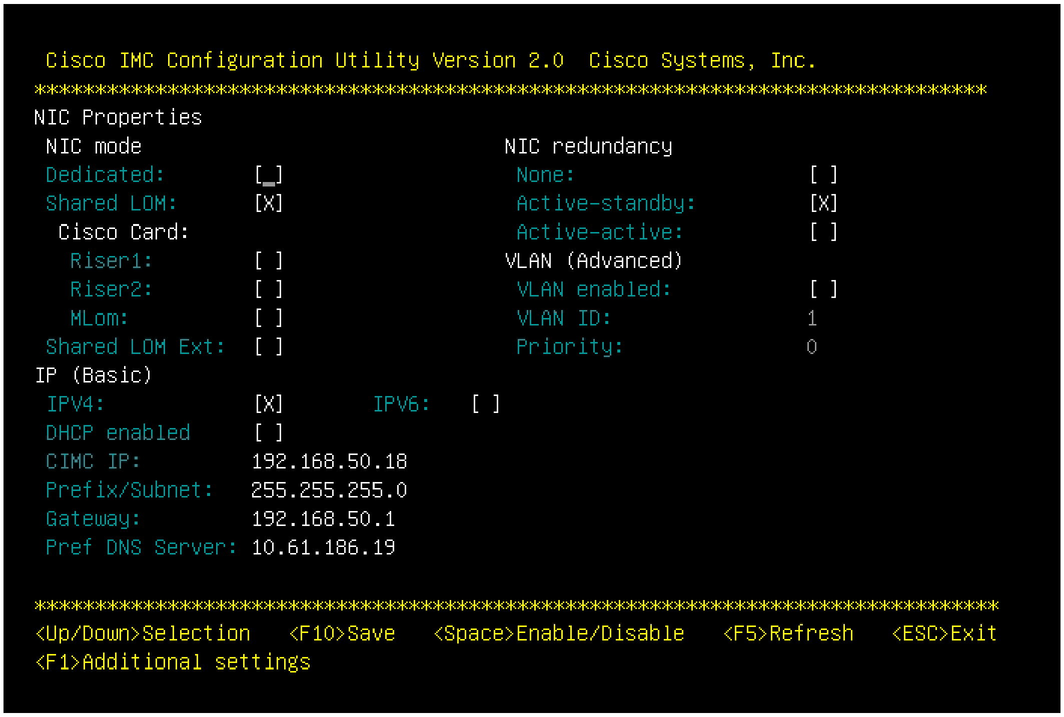
1. Attach the Cisco keyboard, video, and mouse (KVM) dongle (provided with the server) to the KVM 1.port on the front of the server. Plug a VGA monitor and USB keyboard into the appropriate KVM dongle ports.
2. Power on the server and press F8 when prompted to enter the Cisco IMC configuration.



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

Bios Version : C220M4.2.0.3d.0.111120141447
Platform ID  : C220M4

Cisco IMC IPv4 Address : 192.168.50.17
Cisco IMC MAC Address : A0:EC:F9:CE:32:BF

Processor(s) Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
Total Memory  = 128 GB Effective Memory = 128 GB
Memory Operating Speed 1866 Mhz
```

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

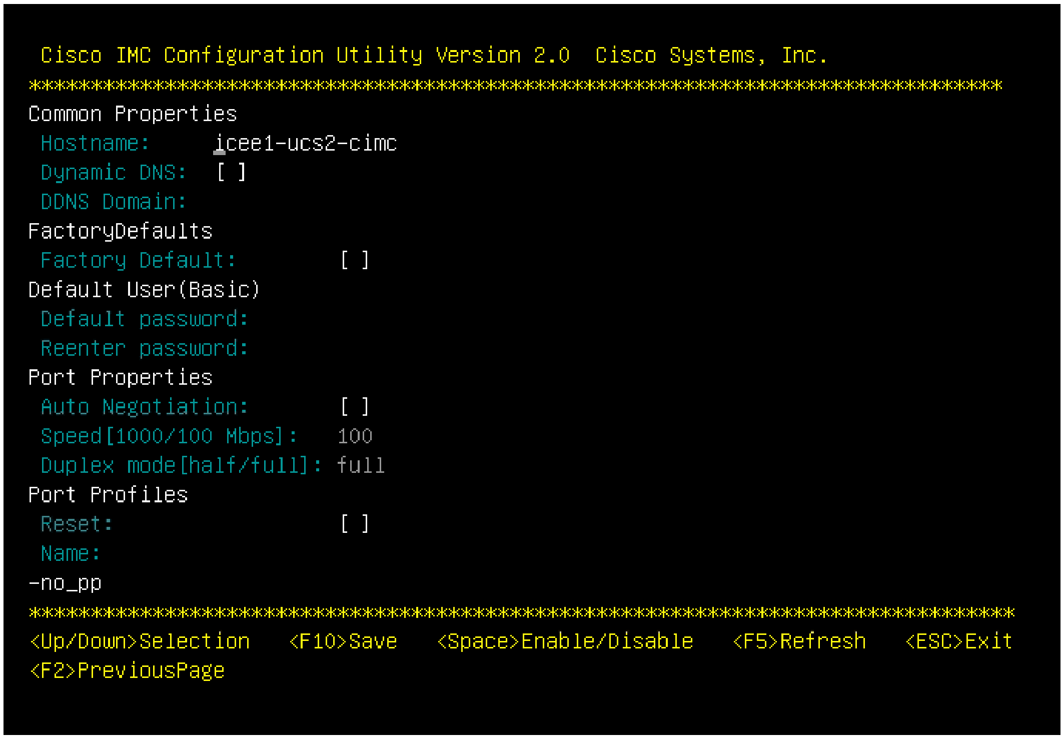
- Network Interface Card (NIC) Mode:
  - Dedicated [X]
- IP (Basic):
  - IPV4: [X]
  - DHCP enabled: [ ]
  - CIMC IP: `<<cimc_ip>>`
  - Prefix/Subnet: `<<cimc_netmask>>`
  - Gateway: `<<cimc_gateway>>`
- VLAN (Advanced): Leave cleared to disable VLAN tagging.
  - NIC Redundancy
  - None: [X]



```
 Cisco IMC Configuration Utility Version 2.0  Cisco Systems, Inc.
*******************************************************************************
NIC Properties
 NIC mode                              NIC redundancy
 Dedicated:       [_]                   None:                   [ ]
 Shared LOM:      [X]                   Active-standby:         [X]
  Cisco Card:                           Active-active:          [ ]
   Riser1:        [ ]                  VLAN (Advanced)
   Riser2:        [ ]                   VLAN enabled:           [ ]
   MLom:          [ ]                   VLAN ID:                1
 Shared LOM Ext:  [ ]                   Priority:               0
IP (Basic)
 IPV4:            [X]        IPV6:    [ ]
 DHCP enabled     [ ]
 CIMC IP:         192.168.50.18
 Prefix/Subnet:   255.255.255.0
 Gateway:         192.168.50.1
 Pref DNS Server: 10.61.186.19

********************************************************************************
<Up/Down>Selection   <F10>Save   <Space>Enable/Disable   <F5>Refresh   <ESC>Exit
<F1>Additional settings
```

4. Press F1 to see additional settings.

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



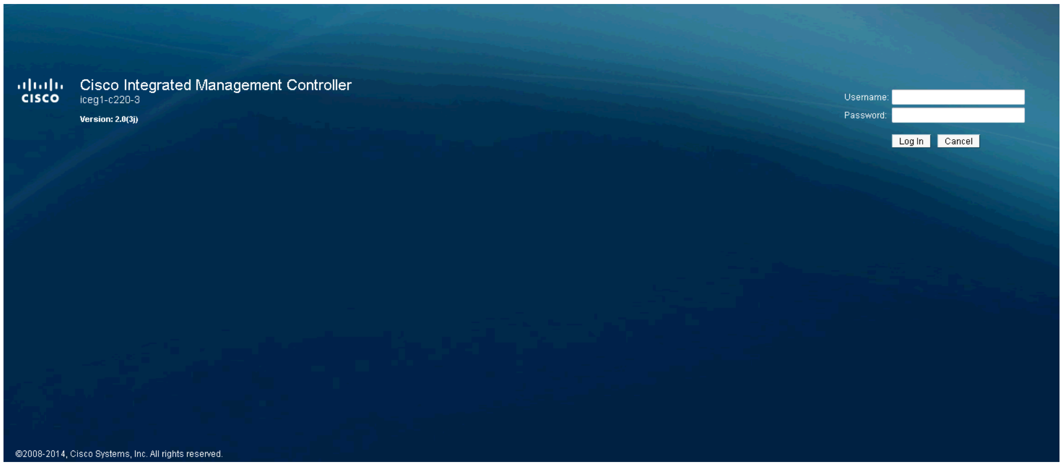
```
 Cisco IMC Configuration Utility Version 2.0  Cisco Systems, Inc.
*******************************************************************************
Common Properties
 Hostname:      icee1-ucs2-cimc
 Dynamic DNS:   [ ]
 DDNS Domain:
FactoryDefaults
 Factory Default:         [ ]
Default User(Basic)
 Default password:
 Reenter password:
Port Properties
 Auto Negotiation:        [ ]
 Speed[1000/100 Mbps]:    100
 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
```

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

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

Configuring Cisco UCS C-Series RAID Configuration

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



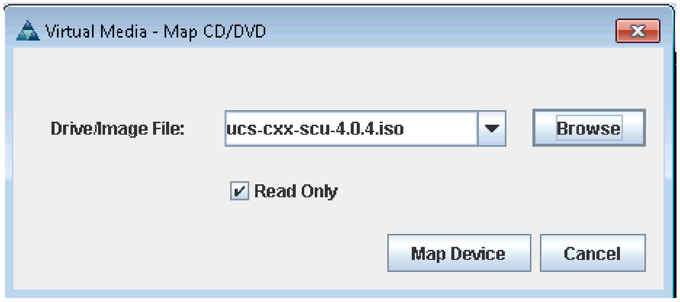
Cisco Integrated Management Controller
iceg1-c220-3
Version: 2.0(3j)

Username:
Password:

©2008-2014, Cisco Systems, Inc. All rights reserved.

3. Click the Server tab and choose Summary. Choose Launch KVM Console.
4. The virtual KVM window will open. 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`.

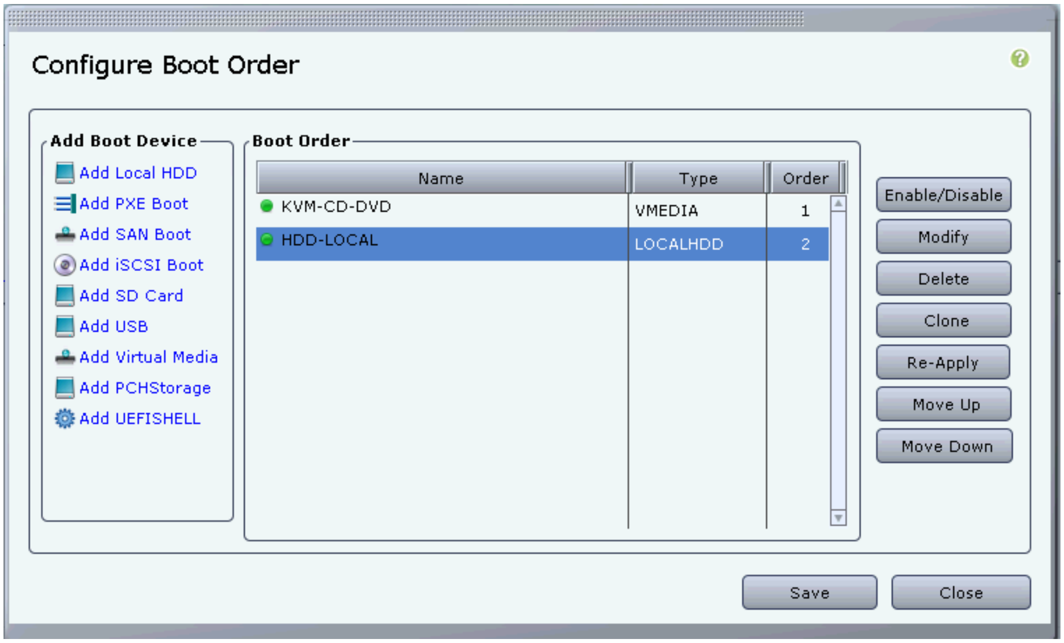


Drive/Image File: ucs-cxx-scu-4.0.4.iso

☑ Read Only

8. Return to the CIMC interface browser window (do not close the virtual KVM window), click the Server tab and select BIOS.
9. Select `Configure Boot Order` and click OK.
10. Verify that the boot options are configured as follows:

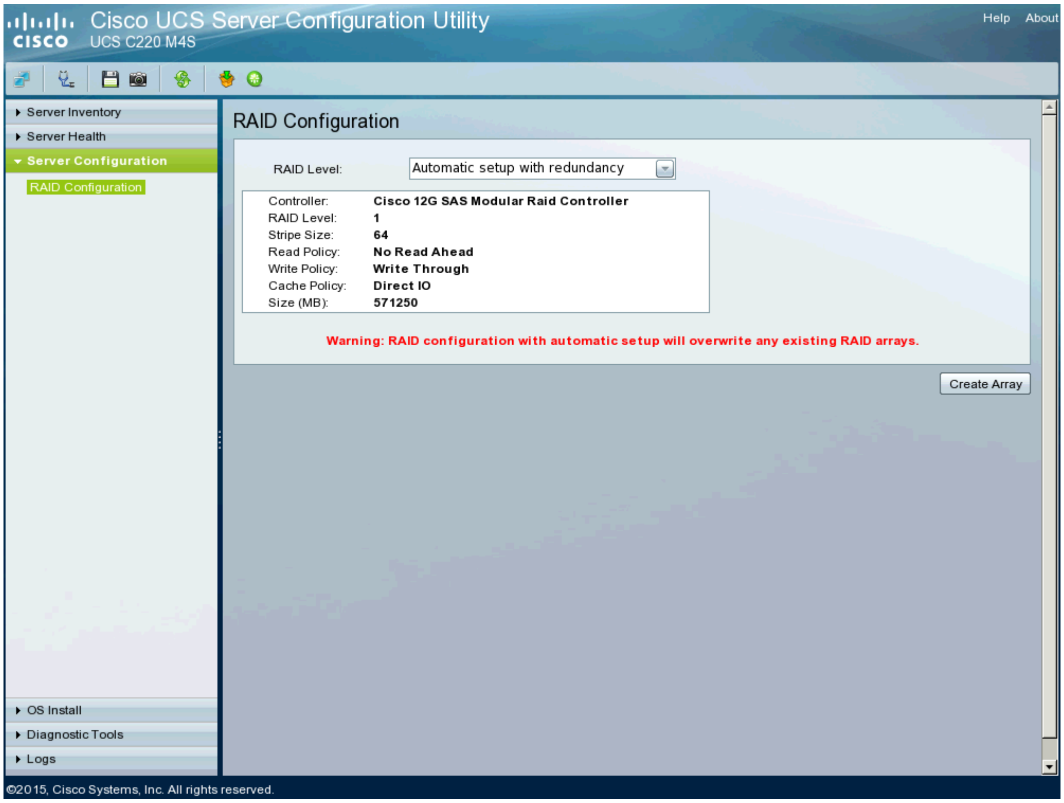
- Add Virtual Media
  - Name: KVM-CD-DVD
  - Sub Type: KVM MAPPED DVD
  - State: Enabled
  - Order: 1
- Add Local HDD
  - Name: HDD-LOCAL
  - State: Enabled
  - Order: 2
  - Slot: HBA



Name	Type	Order
● KVM-CD-DVD	VMEDIA	1
● HDD-LOCAL	LOCALHDD	2

11. Click the `Server` tab and select `Summary`. Select `Power Cycle Server`.
12. Return to the virtual KVM window. Click the `KVM` tab at the top of the window.

    The server should now boot into the Server Configuration Utility.
13. Click the Server Configuration tab in the left pane.
14. Choose RAID Configuration.
15. In the upper-right corner, click the Configure button.
16. 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 12G SAS Modular Raid Controller
RAID Level:	1
Stripe Size:	64
Read Policy:	No Read Ahead
Write Policy:	Write Through
Cache Policy:	Direct IO
Size (MB):	571250

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

17. Click Ok.
18. After the RAID configuration completes, close the virtual KVM window.
19. Return to the CIMC interface browser window, click the Server tab and select Power Off Server.

4.4 Windows Server 2012 Deployment Procedure

This section provides detailed procedures for installing Windows Server 2012 in a FlexPod Express configuration. The deployment procedures that follow are customized to include the environment variables described in previous sections.

Several methods exist for installing Windows Server in such an environment. This procedure highlights using the virtual KVM console and virtual media features within the Cisco UCS C-Series CIMC interface to map remote installation media to each individual server.

Logging into the Cisco UCS C-Series Standalone Server CIMC Interface

The following steps detail the method for logging into the Cisco UCS C-Series standalone server CIMC interface. You must log into the CIMC interface to execute the virtual KVM to begin the installation of the operating system through remote media.

All Hosts

1. Navigate to a web browser and enter the IP address for the Cisco C-Series CIMC interface. This will launch the CIMC GUI application.
2. Log in to the CIMC GUI with admin user name and credentials.
3. In the main menu, click the Server tab.
4. Click Launch KVM Console.

Preparing Windows Server 2012 Install

This section details the steps required to prepare the server for OS installation.

All Hosts

1. From the 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. To boot the server, select the KVM tab.
5. Select `Power On Server` in the CIMC interface Summary tab, and then click OK.

Installing Windows Server 2012

The following steps describe the installation of Windows Server 2012 R2 to each host's local RAID drive.

All Hosts

1. On boot, the machine detects the presence of the Windows installation media.
2. After the installer is finished loading, enter the relevant region information and click Next.
3. Click Install Now.
4. Enter the product key and click Next.
5. Select `Windows Server 2012 R2 Datacenter (Server with a GUI)` and click Next.

   Note: You may optionally remove the GUI after the Hyper-V cluster is operational.
6. Review and accept the EULA, and click Next.
7. Select `Custom: Install Windows only (advanced).`
8. Select the local RAID drive that was set up previously as the installation location for Windows. Click Next.
9. After the install is complete, be sure to unmap the Windows installation image in the Virtual Media tab of the KVM console to make sure that the server reboots into Windows and not the installer.
10. The Virtual Media window might warn you that it is preferable to eject the media from the guest. Because we cannot do this (and the media is read-only) unmap the image anyway by clicking Yes.
11. Back in the KVM tab, press Enter to reboot the server.
12. After installation, enter an administrator password on the settings page and click Finish.

Installing Windows Features

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

All Hosts

1. From the Cisco CIMC 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 into Windows using the administrator password entered during installation.
5. Launch a PowerShell prompt by right-clicking the PowerShell icon in the taskbar, and selecting `Run as Administrator`.
6. Add the .NET 3.5, Hyper-V, MPIO, and clustering features.

```
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:\.

7. Unmap the Windows Server 2012 R2 installation media from the Virtual Media tab.

Configuring Windows Networking for FlexPod Express

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

All Hosts

1. Log in using the administrator password entered previously during installation.
2. Launch a PowerShell prompt by right-clicking the PowerShell icon in the taskbar, and selecting Run as Administrator.
3. One at a time disconnect each network cable by either physically unplugging the Ethernet cable or shutting down the switch port on the switch. Rename the port to match its intended use.

   Example:

```
Rename-NetAdapter -Name “Ethernet 2” -NewName Public0
Rename-NetAdapter -Name "Ethernet 6" -NewName iSCSI-A
Rename-NetAdapter -Name "LOM Port 1" -NewName LM
Rename-NetAdapter -Name "Ethernet 5" -NewName Public1
Rename-NetAdapter -Name "Ethernet 3" -NewName iSCSI-B
Rename-NetAdapter -Name "LOM Port 2" -NewName Cluster
```

Note: Due to how Windows Plug and Play detects hardware, your list will most likely change. You will have to physically identify the ports connected to each server by disconnecting the link.

4. Create a NIC team from a PowerShell prompt.

```
New-NetLbfoTeam -Name TM1 -TeamMembers Public* -TeamingMode SwitchIndependent -LoadBalancing
HyperVPort
```

5. Type `Yes` to confirm the previous action.
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 management VM NIC.

```
Add-VMNetworkAdapter -ManagementOS -Name Mgmt -SwitchName VMComm
```

```
Set-VMNetworkAdapterVlan -ManagementOS -VMNetworkAdapterName Mgmt -Access -AccessVlanId
<<ib_mgmt_vlan_id>>
```

9. Create Hyper-V virtual switches for the iSCSI networks.

```
New-VMSwitch -Name iSCSI-A -NetAdapterName iSCSI-A -AllowManagementOS $true -EnableIov $true
New-VMSwitch -Name iSCSI-B -NetAdapterName iSCSI-B -AllowManagementOS $true -EnableIov $true
```

10. Configure jumbo frames.

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

11. Configure the 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 (iSCSI-A)' -IPAddress <iscsia_ipaddress> -
PrefixLength <iscsia_prefix>
New-NetIPAddress -InterfaceAlias 'vEthernet (iSCSI-B)' -IPAddress <iscsib_ipaddress> -
PrefixLength <iscsib_prefix>
New-NetIPAddress -InterfaceAlias LM -IPAddress <lm_ipaddress> -PrefixLength <lm_prefix>
New-NetIPAddress -InterfaceAlias Cluster -IPAddress <csv_ipaddress> -PrefixLength <csv_prefix>
```

12. Disable DNS registration for all NICs.

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

13. 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>
```

14. Configure Windows Server MSDSM to claim NetApp LUNs.

```
New-MSDSMSupportedHW -VendorId NETAPP -ProductId LUN
New-MSDSMSupportedHW -VendorId NETAPP -ProductId "LUN C-Mode"
Update-MPIOClaimedHW
```

15. Type `Yes` to confirm the previous action.

```
Restart-Computer
```

16. Launch a PowerShell prompt by right-clicking the PowerShell icon in the taskbar, and selecting `Run as Administrator`.
17. Rename the host.

```
Rename-Computer -NewName <hostname> -restart
```

18. Add the host to Active Directory.

```
Add-Computer -DomainName <domain_name> -Restart
```

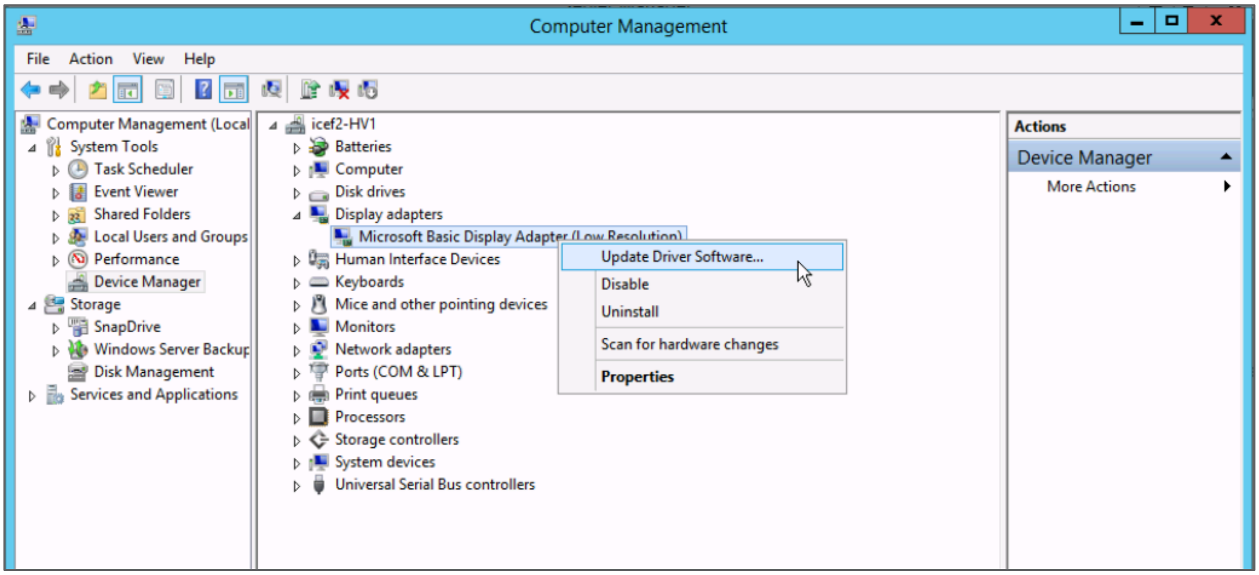
Updating Windows Drivers

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

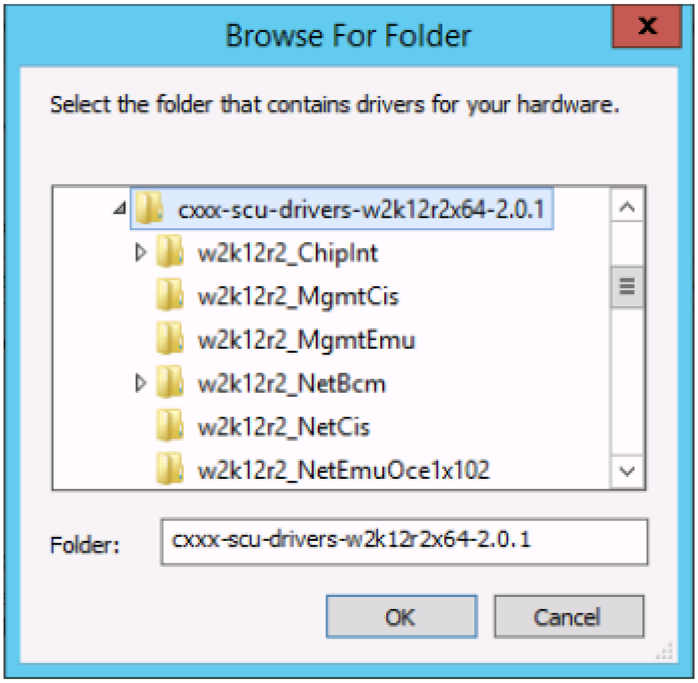
All Hosts

1. Log into Windows with the administrator password entered during installation.
2. Open a web browser and navigate to https://software.cisco.com/download/type.html?mdfid=286281345&flowid=71442&softwareid=283291009.
3. Select Windows 2012r2 64-bit as the platform and download the latest version of the drivers.

4. Extract the downloaded the 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. Browse to the root folder of the extracted driver's package and click OK.


Browse For Folder

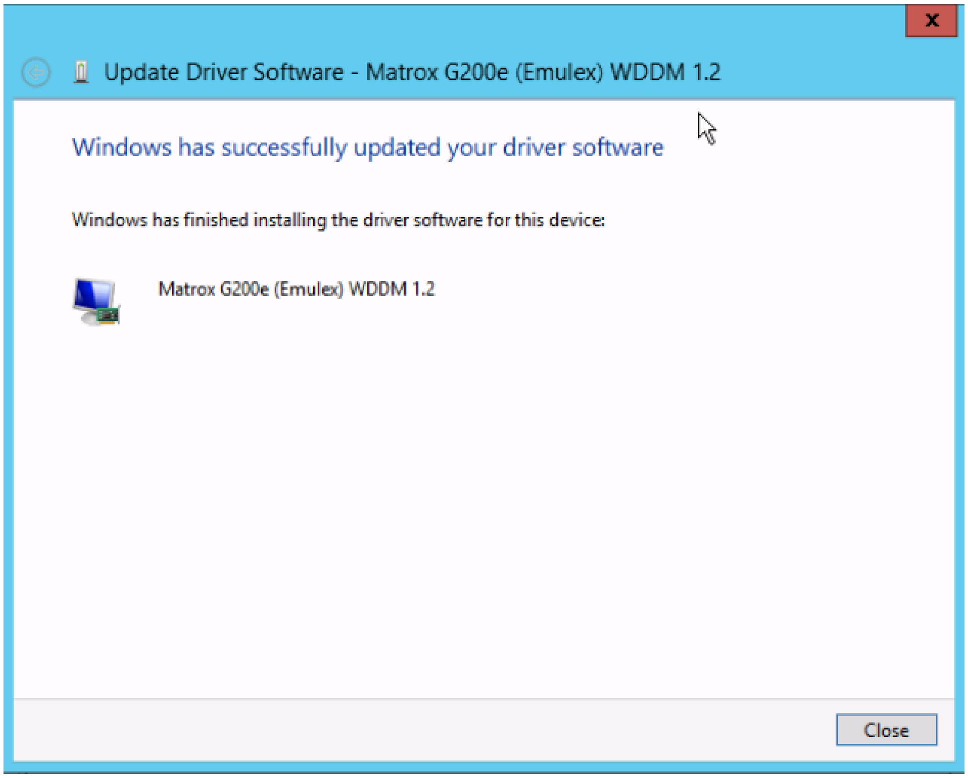
Select the folder that contains drivers for your hardware.

Folder: cxxx-scu-drivers-w2k12r2x64-2.0.1

10. Click Next and the Windows display driver is installed.

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

11. Click Close after the driver update is completed.



Windows has successfully updated your driver software

Windows has finished installing the driver software for this device:

Matrox G200e (Emulex) WDDM 1.2

12. Repeat the previous steps to update the drivers on any other devices required.

Note: It is recommended to update the drivers on the network adapters and storage controllers. You may need to restart the system while updating the drivers on some devices.

13. If applicable, update the drivers on the chipset.
    a. Navigate to the root folder of the extracted driver’s 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 click Next.
    e. Accept the license agreement.
    f. Click Next after viewing the readme file information.
    g. Click Finish after the setup is complete.

Installing NetApp Windows iSCSI Host Utilities

The following section describes how to perform an unattended installation of the NetApp Windows iSCSI Host Utilities. For detailed information regarding the installation see the Windows Host Utilities 6.0.2 Installation and Setup Guide.

All Hosts

1. Download Windows iSCSI Host Utilities from http://mysupport.netapp.com/NOW/download/software/sanhost_win/6.0.2/netapp_windows_host_utilities_6.0.2_x64.msi.

2. Unblock the downloaded file.

```
Unblock-file ~\Downloads\netapp_windows_host_utilities_6.0.2_x64.msi
```

3. Install the Host Utilities.

```
~\Downloads\netapp_windows_host_utilities_6.0.2_x64.msi /qn "MULTIPATHING=1"
```

Note: The system will reboot during this process.

Configuring Windows Host iSCSI initiator

The following steps describe how to configure the built in Microsoft iSCSI initiator.

All Hosts

1. Launch a PowerShell prompt by right-clicking the PowerShell icon in the taskbar, and selecting Run as Administrator.
2. Configure the iSCSI service to start automatically.

```
Set-Service -Name MSiSCSI -StartupType Automatic
```

3. Start the iSCSI service.

```
Start-Service -Name MSiSCSI
```

4. Configure MPIO to claim any iSCSI device.

```
Enable-MSDSMAutomaticClaim -BusType iSCSI
```

5. Set the default load balance policy of all newly claimed devices to round robin.

```
Set-MSDSMGlobalDefaultLoadBalancePolicy -Policy LQD
```

6. Configure an iSCSI target for each controller.

```
New-IscsiTargetPortal -TargetPortalAddress <<fas01_iscsia_lif01_ip>> -InitiatorPortalAddress
<iscsia_ipaddress>
New-IscsiTargetPortal -TargetPortalAddress <<fas01_iscsib_lif01_ip>> -InitiatorPortalAddress
<iscsib_ipaddress>
New-IscsiTargetPortal -TargetPortalAddress <<fas02_iscsia_lif02_ip>> -InitiatorPortalAddress
<iscsia_ipaddress>
New-IscsiTargetPortal -TargetPortalAddress <<fas02_iscsib_lif02_ip>> -InitiatorPortalAddress
<iscsib_ipaddress>
```

7. Connect a session for each iSCSI network to each target.

```
Get-IscsiTarget | Connect-IscsiTarget -IsPersistent $true -IsMultipathEnabled $true -InitiatorPo
rtalAddress <iscsia_ipaddress>
Get-IscsiTarget | Connect-IscsiTarget -IsPersistent $true -IsMultipathEnabled $true -InitiatorPo
rtalAddress <iscsib_ipaddress>
```

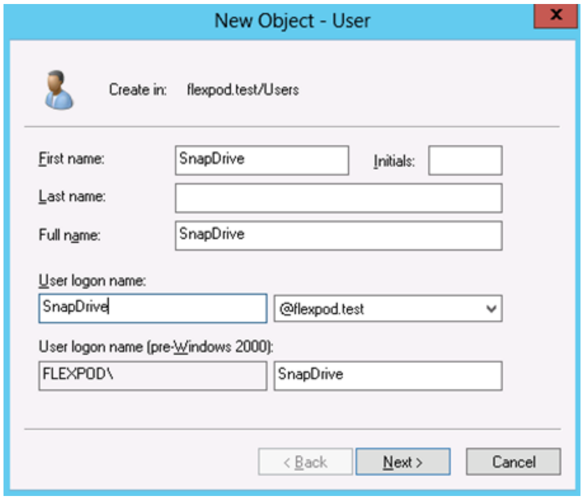
Installing NetApp SnapDrive

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

All Hosts

1. In AD, 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:

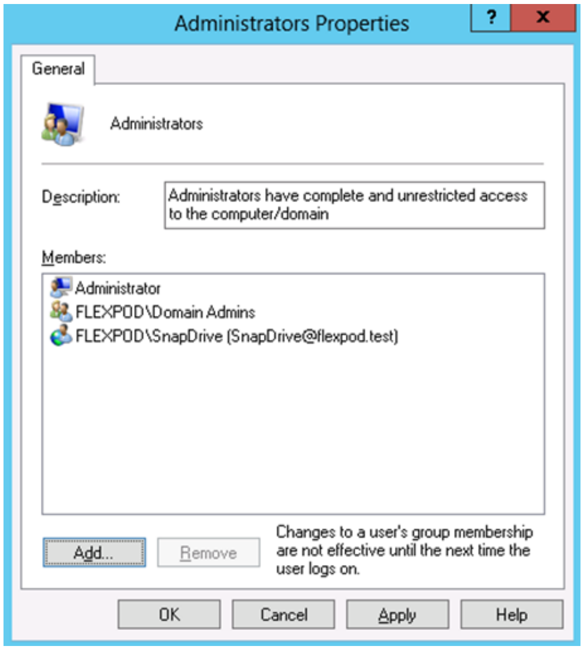
Last name:

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

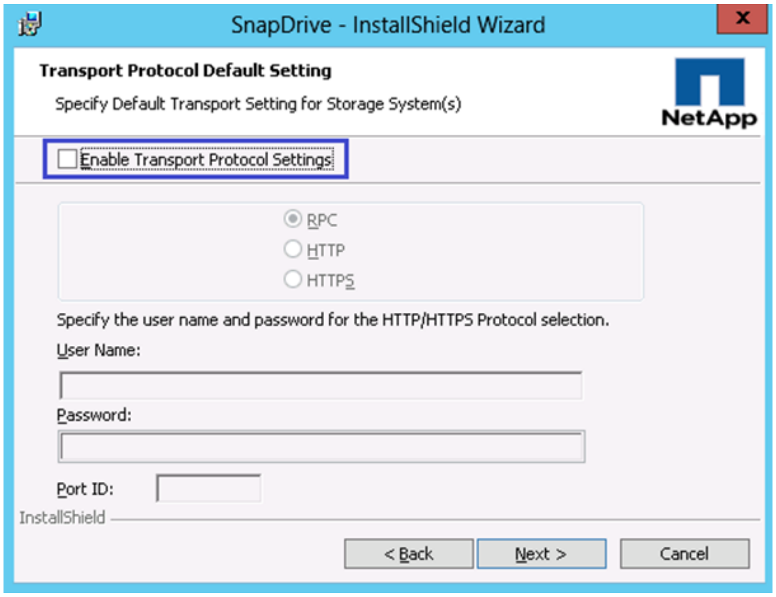
Description: Administrators have complete and unrestricted access to the computer/domain

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 `Enable SnapDrive to Communicate Through the Windows Firewall` 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.



Transport Protocol Default Setting

Specify Default Transport Setting for Storage System(s)

□ Enable Transport Protocol Settings

● RPC
○ HTTP
○ HTTPS

Specify the user name and password for the HTTP/HTTPS Protocol selection.

User Name:

Password:

Port ID:

13. Leave `Enable Unified Manager Configuration` unchecked, and click Next.
14. Click Install.
15. After the installation is 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 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_ip>> -protocol https -credential 
vsadmin
```

Installing NetApp SnapManager for Hyper-V

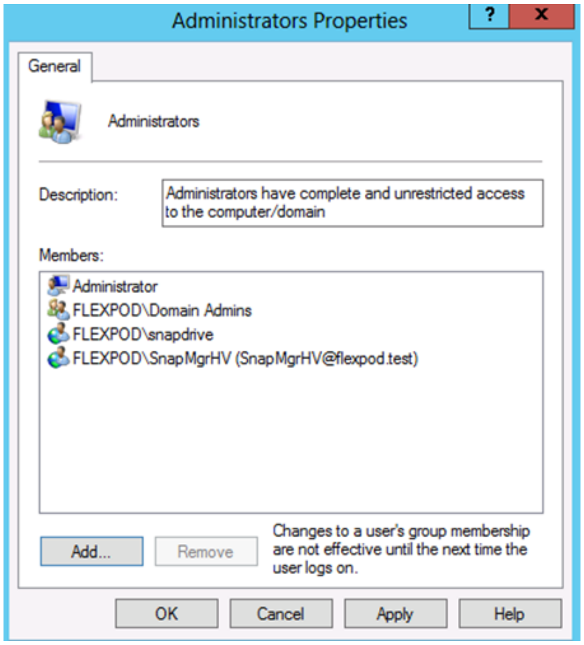
The following section describes how to install NetApp SnapManager for Hyper-V (SMHV). For detailed installation procedures, refer to the Administration and Installation Guide.

All Hosts

1. In AD, create a 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

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.

Creating a Cluster

One Server Only

1. Launch a PowerShell prompt with administrative permissions, by right-clicking the PowerShell icon and selecting `Run as Administrator`.
2. Create a new cluster.

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

3. Rename the cluster 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 *iSCSI-A* | Group Network| %{ (Get-ClusterNetwork
$_.Name).Name = 'iSCSI-A'}
Get-ClusterNetworkInterface | ? Name -like *iSCSI-B* | Group Network| %{ (Get-ClusterNetwork
$_.Name).Name = 'iSCSI-B'}
Get-ClusterNetworkInterface | ? Name -like *Mgmt* | Group Network| %{ (Get-ClusterNetwork
$_.Name).Name = 'Mgmt'}
```

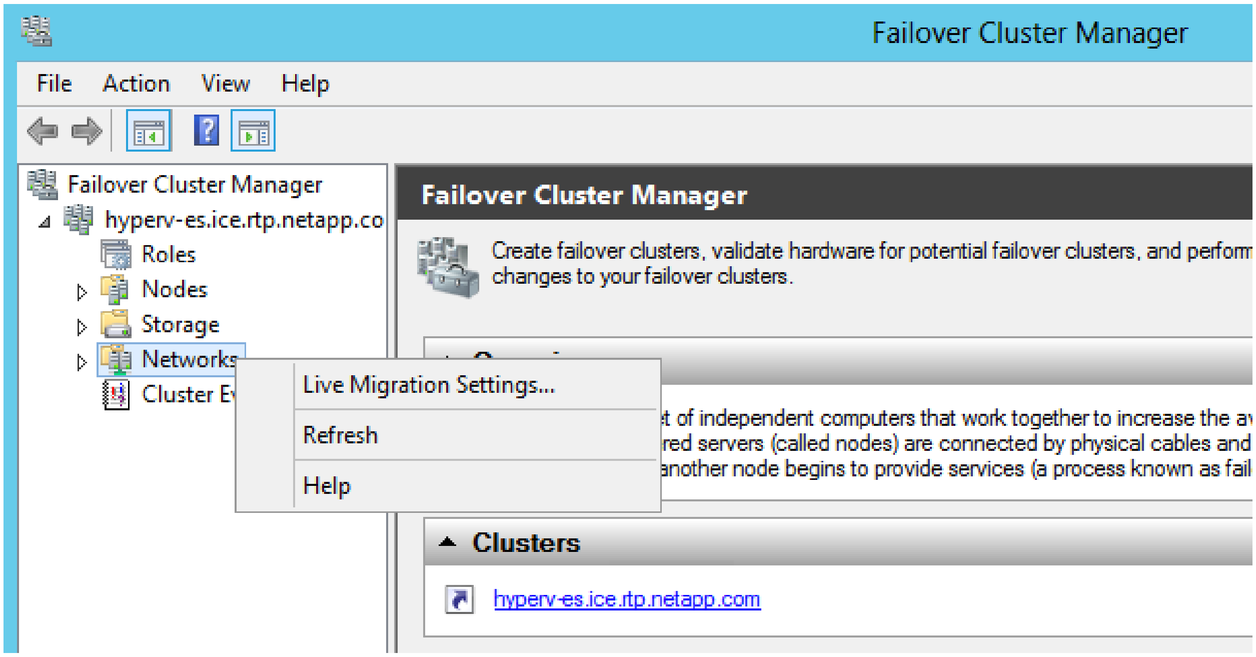
4. Designate the CSV network.

```
(Get-ClusterNetwork -Name Cluster).Metric = 900
```

5. Configure the live migration network.

a. From Server Manager, select Tools > Failover Cluster Manager.

b. 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

c. Deselect all but the LM network and click OK.

6. Change the cluster to use a quorum disk.

a. Launch a PowerShell prompt with administrative permissions by right-clicking the PowerShell icon and selecting Run as Administrator.

```
start-ClusterGroup "Available Storage"| Move-ClusterGroup -Node $env:COMPUTERNAME
```

b. Open SnapDrive from the Start page to configure cluster storage.

c. From SnapDrive, open the server name.

d. Right-click the Disks icon and select the option to create a disk.

e. Select Shared (Microsoft Cluster Services only) and click Next.

f. Type the IP address of the `Infra_SVM` and click Add.

g. Once connected, open the controller tree and select the quorum volume.

h. Type the name of the LUN in the LUN NAME field and click Next.

i. Validate that all nodes of the cluster are shown and click Next.

j. Change the drive letter to W:, set the LUN size to 1GB, and click Next.

k. Click Next through the Volume Properties confirmation.

l. Select the iSCSI initiators to which to map the LUN and click Next.

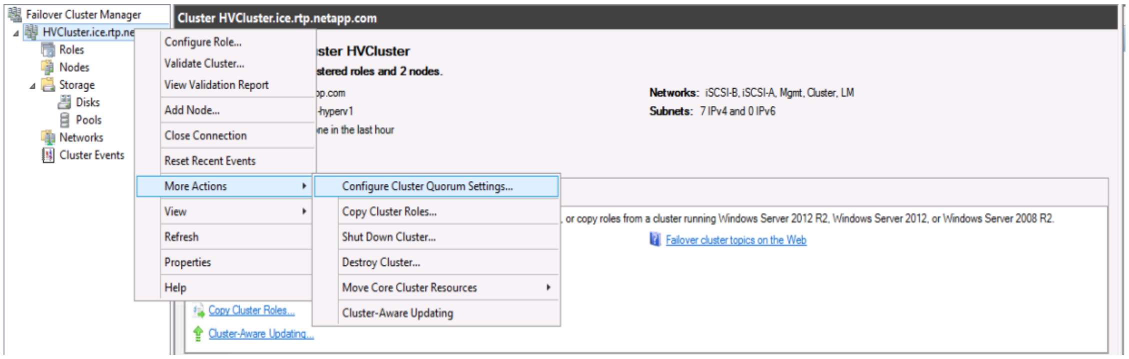
m. Select `Automatic igroup management` and click Next.

n. Select the available storage cluster group and click Next.

o. Click Finish.

p. Make sure that the W: drive is accessible on all of the nodes.

q. In Failover Cluster Manager, select `Configure Cluster Quorum Settings`.



r. Click Next through the Welcome page.

s. Select the quorum witness and click Next.

t. Select `Configure a disk witness`, and click Next.

u. Select Disk W: from the available storage and click Next.

v. Click Next through the confirmation page and Finish on the summary page.

7. Create CSV LUN for VM storage.

   a. Open SnapDrive from the start page.

   b. From SnapDrive, open the server name.

   c. Right-click the Disks icon and select the option to create a disk.

   d. Select Shared (Microsoft Cluster Services only) and click Next.

   e. Type the IP address of `Infra_SVM`.

   f. Once connected, open the controller tree and select the `infra_datastore_1` volume.

   g. Type the name of the LUN in the LUN NAME field and click Next.

   h. Validate that all nodes of the cluster are shown and click Next.

   i. Select `Do not assign a Drive letter or Volume Mount Point`. Set the LUN size to be 1TB and click Next.

   j. Click Next through the Volume Properties confirmation.

   k. Select the iSCSI initiators to which to map the LUN and click Next.

   l. Select Automatic igroup management and click Next.

   m. Select Add to cluster shared volumes and click Next.

   n. Click Finish.

8. Run the Cluster Validation wizard from Failover Cluster Manager to validate deployment.

5 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 in a FlexPod environment.

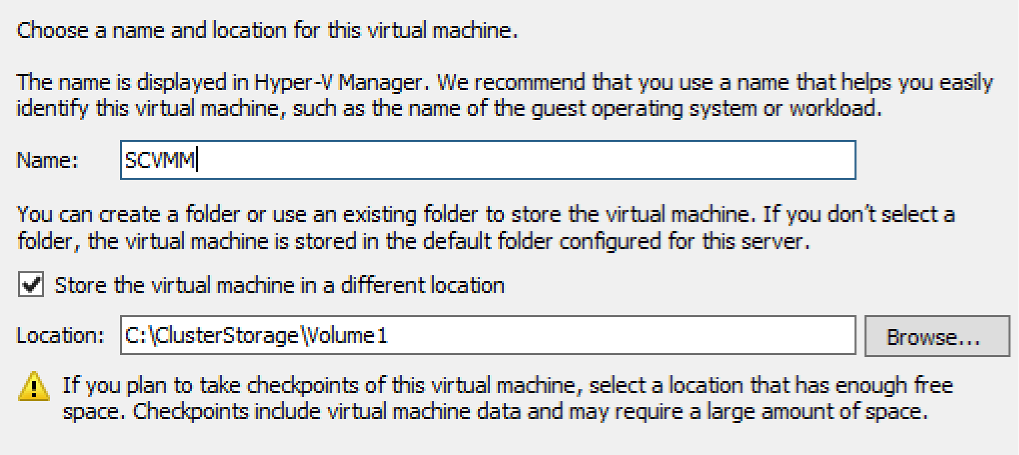
Table 13) VM requirements.

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

5.1 Build the SMI-S and SCVMM VMs

One Server Only

1. In Failover Cluster Manager, right-click Roles and select Virtual Machine. Select New Virtual Machine.
2. Select the host for the new virtual machine and click OK.
3. On the New Virtual Machine welcome page, 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

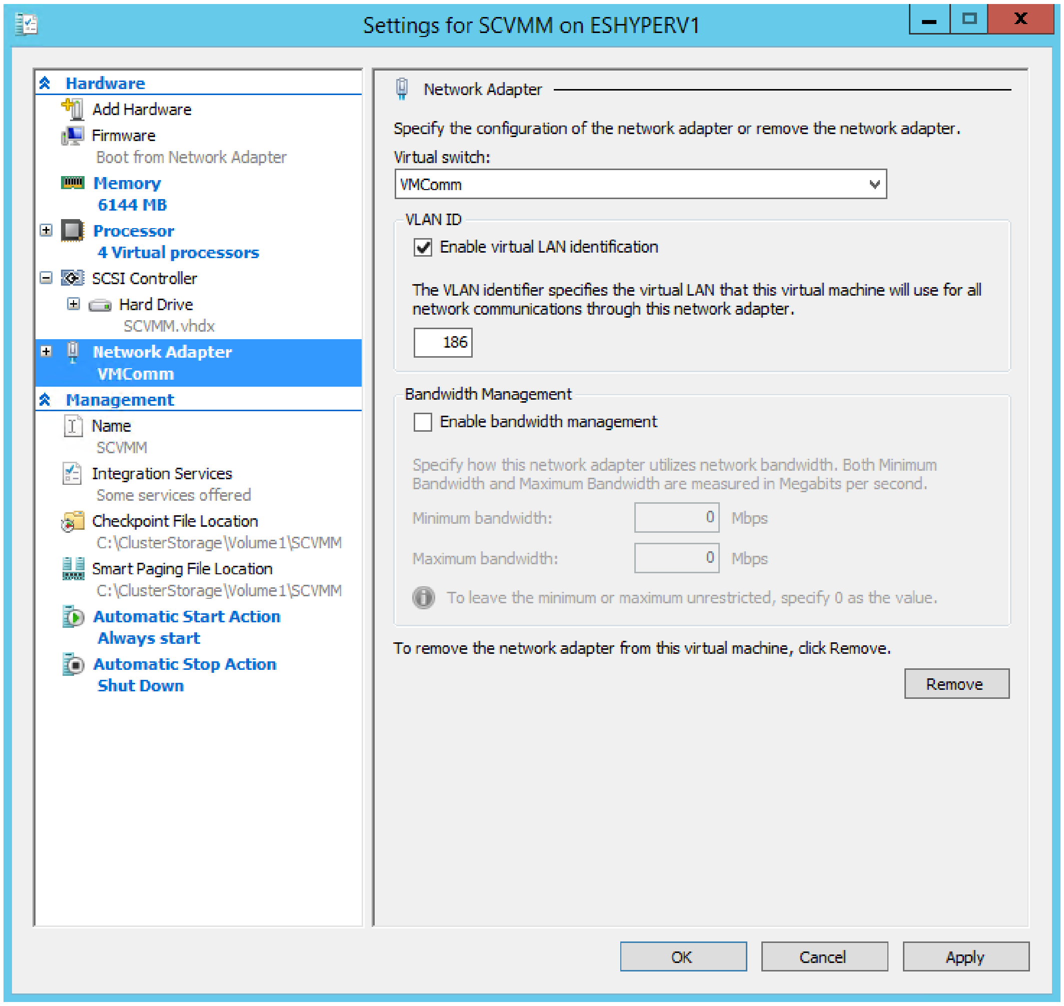
Location: C:\ClusterStorage\Volume1

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 form a bootable image file`, and provide the path to the Windows Server 2012 R2 ISO.
10. Click Finish.
11. Repeat steps 1 through 10 for the remaining VMs.

5.2 SMI-S and SCVMM VMs Configuration

1. In 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 value outlined in Table 13.
4. Select Network Adapter, select Enable Virtual LAN Identification, and enter the `<<ib_mgmt_vlan_id>>`.
5. Select Automatic Start Action and select Always Start This Virtual Machine Automatically.
6. Select `Automatic Stop Action` and select `Shut Down the Guest Operating System`.
7. Click OK to save the modifications.
8. Repeat steps 1 through 7 for the remaining VMs.



Settings for SCVMM on ESHYPERV1

Hardware
- Add Hardware
- Firmware
  Boot from Network Adapter
- Memory
  6144 MB
- Processor
  4 Virtual processors
- SCSI Controller
  - Hard Drive
    SCVMM.vhdx
- Network Adapter
  VMComm

Management
- Name
  SCVMM
- Integration Services
  Some services offered
- Checkpoint File Location
  C:\ClusterStorage\Volume1\SCVMM
- Smart Paging File Location
  C:\ClusterStorage\Volume1\SCVMM
- Automatic Start Action
  Always start
- Automatic Stop Action
  Shut Down

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

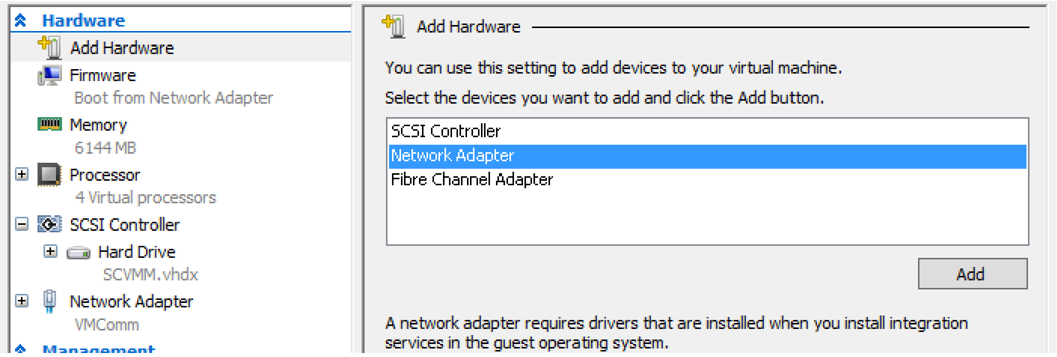
Maximum bandwidth: 0 Mbps

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

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

5.3 SCVMM iSCSI Network Adapters Addition

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.



Hardware
- Add Hardware
- Firmware
  Boot from Network Adapter
- Memory
  6144 MB
- Processor
  4 Virtual processors
- SCSI Controller
  - Hard Drive
    SCVMM.vhdx
- Network Adapter
  VMComm

Management

Add Hardware

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

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

- SCSI Controller
- Network Adapter
- Fibre Channel Adapter

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

3. Select the iSCSI-A virtual switch.
4. From the Add hardware section, select Network Adapter and click Add.
5. Select the iSCSI-B virtual switch.
6. Click Ok to save the modifications.

5.4 Windows Server 2012 R2 on the VMs Installation

1. In 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 is finished loading, enter the 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. Review and accept the EULA and click Next.
8. Select `Custom: Install Windows only (advanced)`.
9. Select Drive 0, and click Next to continue with the install.
10. After Windows has finished installing, enter an administrator password in 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 the important and recommended Windows updates and reboot.
13. Configure the network adapter settings if using static IPs.

Note: The SCVMM virtual machine 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.

5.5 NetApp SMI-S Agent Installation

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

Prerequisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following local account has been created:

User name	Purpose	Permissions
SMIS-User	SMI-S access account	This account will not need any special delegation. Note this is NOT a domain account it must be a local account in Windows.

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

Installing the SMI-S Agent

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

1. Download the Data ONTAP SMI-S Agent installer from http://mysupport.netapp.com/NOW/download/software/smis/Windows/5.1.2/smisagent-5-1-2.msi.
2. Unblock the downloaded file.

```
Unblock-file ~\Downloads\smisagent-5-1-2.msi
```

3. Install the Agent by running the following command:

```
~\Downloads\smisagent-5-1-2.msi /qb
```

Configuring the SMI-S Provider

To configure the NetApp SMI-S provider, complete the following steps:

1. Open the App page, right-click Data ONTAP SMI-S Agent, and select `Run as Administrator` at the bottom of the page.
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.

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

5. Restart the Agent/cimserver.

```
Smis cimserver restart
```

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

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

5.6 System Center Virtual Machine Manager Installation

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

Prerequisites

The following environment prerequisites must be met before proceeding.

Accounts

Verify that the following accounts have been created:

User Name	Purpose	Permissions
<DOMAIN>\FT-VMM-SVC	Virtual Machine Manager Service Account	This account will need full admin permissions on the Virtual Machine Manager server virtual machine and runs the Virtual Machine Manager service.
<DOMAIN>\SnapDrive	SnapDrive for Windows	This account needs to be an administrator on the SCVMM virtual machine.

Groups

Verify that the following security groups have been created:

Security Group Name	Group Scope	Members
<DOMAIN>\FT-SCVMM-Admins	Global	FT-VMM-SVC
<DOMAIN>\FT-SCVMM-FabricAdmins	Global	Virtual Machine Manager delegated

Security Group Name	Group Scope	Members
		administrators
<DOMAIN>\FT-SCVMM-ROAdmins	Global	Virtual Machine Manager read-only admins
<DOMAIN>\FT-SCVMM-TenantAdmins	Global	Virtual Machine Manager tenant administrators who manage self-service users
<DOMAIN>\FT-VMM-AppAdmins	Global	Virtual Machine Manager self-service users

Verify the following accounts and/or groups are members of the local administrator's group on the Virtual Machine Manager virtual machine:

- SnapDrive
- Virtual Machine Manager Admins group.
- Virtual Machine Manager service account.

Install the Windows Assessment and Deployment Kit

The SCVMM installation requires that the Windows Assessment and Deployment Kit (ADK) be installed on the Virtual Machine Manager management server. You can download the Windows ADK 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, an offline installation can be performed.

The following steps outline how to install the Windows ADK on the SCVMM management server.

1. From the Windows ADK installation media source, right-click `adksetup.exe` and select Run as Administrator. If prompted by User Account Control, click Yes to allow the installation to make changes to the computer.
2. In the Specify Location page, accept the default folder location of %ProgramFiles%\Windows Kits\8.1 and click Next.
3. In the Join the Customer Experience Improvement Program (CEIP) page, select the option to either participate or not participate in the CEIP by providing selected system information to Microsoft. Click Next.
4. In the License Agreement page, click Accept.
5. In the Select the features you want to install page, select the following checkboxes:
   - Deployment Tools
   - Windows Preinstallation Environment (Windows PE)
6. Make sure that all other option checkboxes are cleared. Click Install to begin the installation.
7. After installation is complete, clear the `Launch the Getting Started Guide` checkbox and click Close to exit the installation wizard.

Install the WSUS RSAT Tools

The Virtual Machine Manager installation requires the WSUS Administration Tools to be installed on the Virtual Machine Manager management server.

1. Launch a PowerShell prompt by right-clicking the PowerShell icon in the taskbar, and selecting Run as Administrator.

2. Add the failover cluster, multipath-IO, and WSUS console.

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

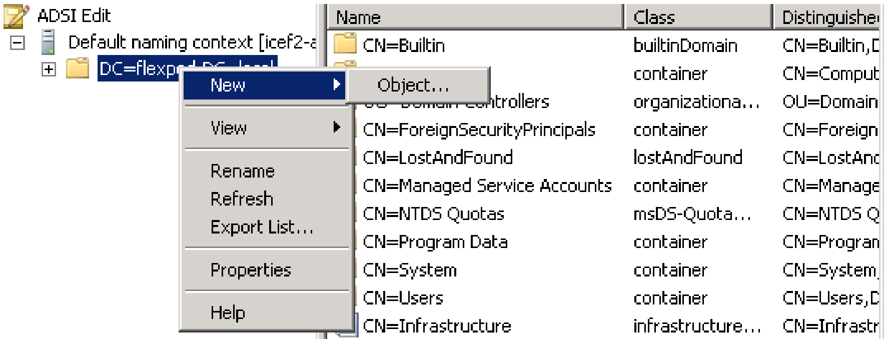
Create the Virtual Machine Manager Distributed Key Management Container in Active Directory Domain Services

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

Note: If Virtual Machine Manager will be deployed using an account with rights to create containers in AD DS, you can skip this step.

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

1. Log in to a domain controller with a user that has domain admin privileges and run `adsiedit.msc`.
2. Right-click the ADSI Edit node and select Connect to.
3. In the Connections Settings page, from 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>] and expand <distinguished name of domain>. Right-click the root node and select New – Object.



Name	Class	Distinguishe
CN=Builtin	builtinDomain	CN=Builtin,D
	container	CN=Comput
ntrollers	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 page, 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 the VMM Admins group. Grant the security principles Full Control permissions.
10. Click OK three times and close ADSI Edit.

Configuring Windows MPIO

The following section describes how to configure Windows MPIO to claim NetApp LUNs.

1. Open a PowerShell prompt by right-clicking and selecting Run as Administrator. Enter the following commands to install the MPIO feature.

```
Add-WindowsFeature Multipath-IO –IncludeManagementTools
```

2. Configure Windows Server 2012 R2 MSDSM to claim any NetApp LUNs.

```
New-MSDSMSupportedHW -VendorId NETAPP -ProductId LUN
```

```
New-MSDSMSupportedHW -VendorId NETAPP -ProductId "LUN C-Mode"
Update-MPIOClaimedHW -confirm:$false
Restart-Computer
```

Installing NetApp Windows iSCSI Host Utilities

The following section describes how to perform an unattended installation of the NetApp Windows iSCSI Host Utilities. For detailed information regarding the installation see the Windows Host Utilities 6.0.2 Installation and Setup Guide.

1. Download Windows iSCSI Host Utilities: http://mysupport.netapp.com/NOW/download/software/sanhost_win/6.0.2/netapp_windows_host_utilities_6.0.2_x64.msi.
2. Open a PowerShell prompt by right-clicking and selecting `Run as Administrator`. Enter the following commands:

```
Unblock-file ~\Downloads\netapp_windows_host_utilities_6.0.2_x64.msi
```

3. Install the Host Utilities.

```
~\Downloads\netapp_windows_host_utilities_6.0.2_x64.msi /qn "MULTIPATHING=1"
```

The virtual machine restarts after installation.

Configuring Windows Host iSCSI initiator

The following steps describe how to configure the built in Microsoft iSCSI initiator.

1. Launch a PowerShell prompt by right-clicking the PowerShell icon in the taskbar, and selecting Run as Administrator.
2. Configure the iSCSI service to start automatically.

```
Set-Service -Name MSiSCSI -StartupType Automatic
```

3. Start the iSCSI service.

```
Start-Service -Name MSiSCSI
```

4. Configure MPIO to claim any iSCSI device.

```
Enable-MSDSMAutomaticClaim -BusType iSCSI
```

5. Set the default load balance policy of all newly claimed devices to round robin.

```
Set-MSDSMGlobalDefaultLoadBalancePolicy -Policy LQD
```

6. Configure an iSCSI target for each controller.

```
New-IscsiTargetPortal -TargetPortalAddress <<fas01_iscsia_lif_ip>> -InitiatorPortalAddress
<iscsia_ipaddress>
New-IscsiTargetPortal -TargetPortalAddress <<fas01_iscsib_lif_ip>> -InitiatorPortalAddress
<iscsib_ipaddress>
New-IscsiTargetPortal -TargetPortalAddress <<fas02_iscsia_lif_ip>> -InitiatorPortalAddress
<iscsia_ipaddress>
New-IscsiTargetPortal -TargetPortalAddress <<fas02_iscsib_lif_ip>> -InitiatorPortalAddress
<iscsib_ipaddress>
```

7. Connect a session for each iSCSI network to each target.

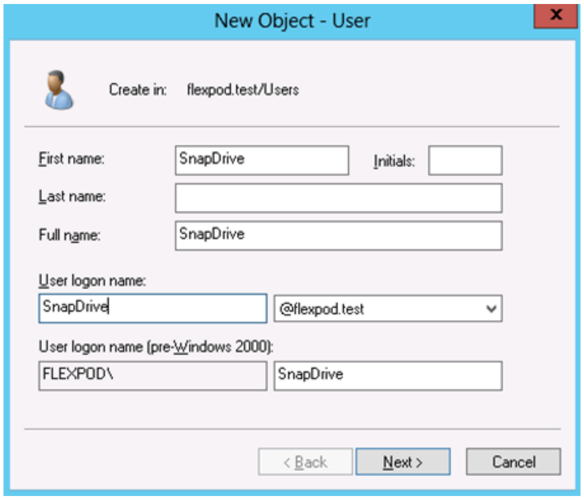
```
Get-IscsiTarget | Connect-IscsiTarget -IsPersistent $true -IsMultipathEnabled $true -InitiatorPo
rtalAddress <iscsia_ipaddress>
Get-IscsiTarget | Connect-IscsiTarget -IsPersistent $true -IsMultipathEnabled $true -InitiatorPo
rtalAddress <iscsib_ipaddress>
```

Installing NetApp SnapDrive

The following section describes how to perform an unattended installation of the NetApp SnapDrive Windows. For detailed information regarding the installation see the Administration and Installation Guide.

1. In AD, create a SnapDrive service account.

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



New Object - User

Create in: flexpod.test/Users

First name: SnapDrive

Initials:

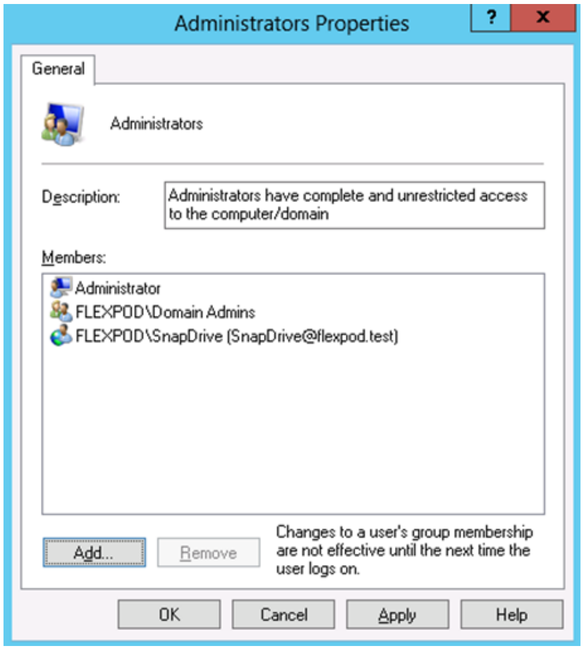
Last name:

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 Administrators group in Windows.



Administrators Properties

General

Administrators

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

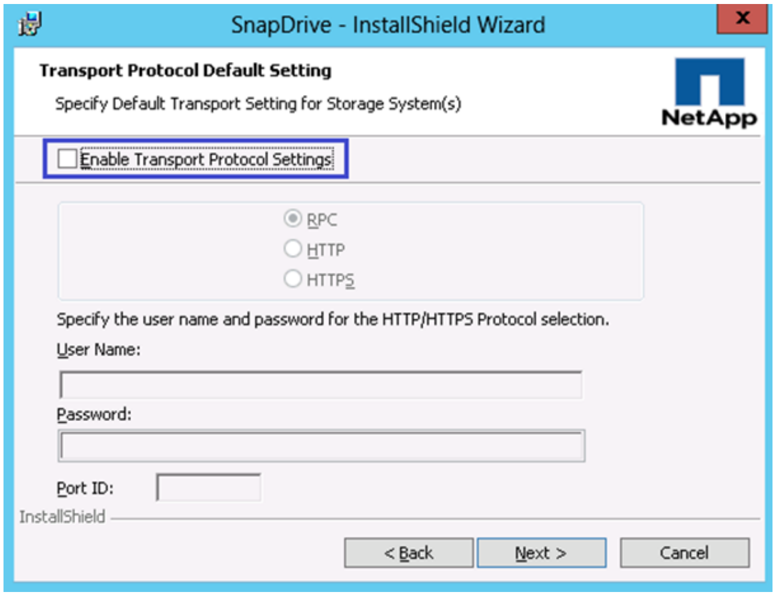
Members:

- Administrator
- FLEXPOD\Domain Admins
- FLEXPOD\SnapDrive (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 `Enable SnapDrive to Communicate Through the Windows Firewall` 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.



SnapDrive - InstallShield Wizard

Transport Protocol Default Setting

Specify Default Transport Setting for Storage System(s)

□ Enable Transport Protocol Settings

● RPC
○ HTTP
○ HTTPS

Specify the user name and password for the HTTP/HTTPS Protocol selection.

User Name:

Password:

Port ID:

13. Leave `Enable Unified Manager Configuration` cleared and click Next.
14. Leave `Enable Hyper-V Server pass-through disk cleared` and click Next.
15. Click Install.
16. After the installation is 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 executable.

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

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

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

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

Creating and Mapping LUNs for SCVMM

Create SQL Server database LUNs using SnapDrive. The LUN sizes and purpose are listed in Table 14.

Table 14) SCVMM LUN requirements.

LUN	Component(s)	NetApp Volume	Purpose	Drive Letter	Size
LUN_1	SQL Server	infra_sql	Database	M	60GB
LUN_2	SQL Server	infra_sql	Logs	N	30GB

LUN	Component(s)	NetApp Volume	Purpose	Drive Letter	Size
LUN_3	VMM Library	infra_datastore_1	Library	L	500GB

1. Open SnapDrive from the start page to configure the LUN.
2. From SnapDrive, open the server name.
3. Right-click the Disks icon and select `Create Disk`.
4. Click Next.
5. Select `Dedicated` and click Next.
6. Type the IP address of the `Infra_SVM` and click Add.
7. Once connected, open the controller tree and select the volume listed in Table 14.
8. Type in the name of the LUN in the LUN NAME field and click Next.
9. Change the drive letter and size to the values from Table 14, and click Next.
10. Select the iSCSI initiator to map the LUN to click Next.
11. Select Automatic igroup management and click Next.
12. Click Finish.
13. Repeat steps 3 through 12 for each remaining LUN in Table 14.

Installing SQL Server 2012 SP1

Install SQL Server 2012 SP1 into the SCVMM server. Deployments of more than 150 hosts should consider using a dedicated SQL cluster. To install SQL on 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. The SQL Server Installation Center will appear. Select the Installation menu option.
2. From the SQL Server Installation Center, click the New SQL Server stand-alone installation or add features to an existing installation link.

   The SQL Server 2012 SP1 Setup wizard will appear.
3. In the Setup Support Rules page, verify that each rule shows a Passed status. If any rule requires attention, remediate the issue and rerun the validation check. Click OK.
4. In the Product Key page, select the Enter the product key option and enter the associated product key in the provided text box. Click Next.

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 page, accept the EULA. Select or clear the Send feature usage data to Microsoft checkbox based on your organization’s policies and click Next.
6. In the Product Updates page, select the Include SQL Server product updates checkbox and click Next.
7. In the Install Setup Files page, click Install and allow the support files to install.
8. In the Setup Support Rules page, verify that each rule shows a Passed status. If any rule requires attention, remediate the issue and rerun the validation check.

Note: The common issues include MSDTC, MSCS, and Windows Firewall warnings. Note that the use of MSDTC is not required for the System Center 2012 SP1 environment.

9. Click Next.
10. In the Setup Role page, select the SQL Server Feature Installation button and click Next.
11. In the Feature Selection page, select the following:

- Database Engine Services

- Management Tools – Basic
  - Management Tools – Complete

12. In the Installation Rules page, click Next. The Show details and View detailed report can be viewed if required.
13. In the Instance Configuration page, click Next.
14. In the Disk Space Requirements page, verify that you have sufficient disk space and click Next.
15. In the Server Configuration page, select the Collation tab, and click Customize.

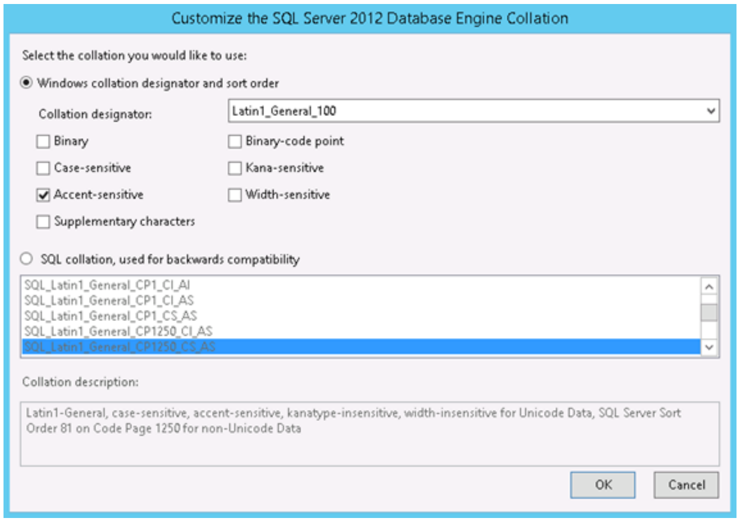
    In the Customize the SQL Server 2012 Database Engine Collation page:

    a. Select the Windows collation designator and sort order option.

    b. Select `Latin1_General_100`, and select 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

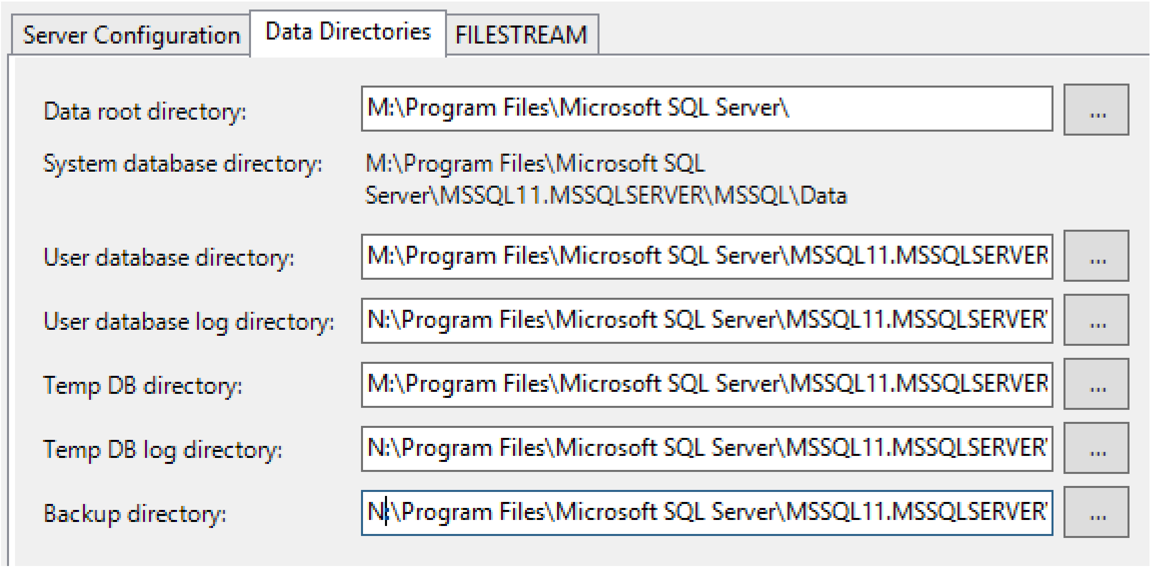
○ SQL collation, used for backwards compatibility

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 page, 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 the BUILTIN\Administrators, and any other groups who should have administrator access to the SQL instance.
17. In the same Database Engine Configuration page, select the Data Directories tab. The correct drive letter for SQL Server data should be specified. If not, enter the proper drive letter in the Data root directory text box. To redirect log files by default to the second drive, change the drive letter in the User databaselog directory and Temp DB log directory text boxes. It is also recommended to change the backup directory to a separate drive such as the log drive. Do not change the folder structure unless your organization has specific standards for this. Click Next.



Data root directory: M:\Program Files\Microsoft SQL Server\

System database directory: M:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Data

User database directory: M:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER

User database log directory: N:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\

Temp DB directory: M:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER

Temp DB log directory: N:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\

Backup directory: N:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\

Note: It may be necessary to relocate the Temp DB files to a dedicated LUN if performance is not adequate using the two primary SQL LUNs.

18. In the Error Reporting page, 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.
19. In the Installation Rules page, verify that each rule shows a Passed status. If any rule requires attention, remediate the issue and rerun the validation check. Click Next.
20. In the Ready to Install page, verify all of the settings that were entered during the setup process and click Install to begin the installation of the SQL Server instance.

    In the Installation Progress page, the installation progress will be displayed.
21. Click Close to complete the installation of this SQL Server database instance.
22. Verify the installation by inspecting the instances in Failover Cluster Manager and in SQL Server 2012 Management Studio (SSMS) prior to moving to the next step of installation.

Installing Virtual Machine Manager

Perform the following procedure on one of the Virtual Machine Manager virtual machines.

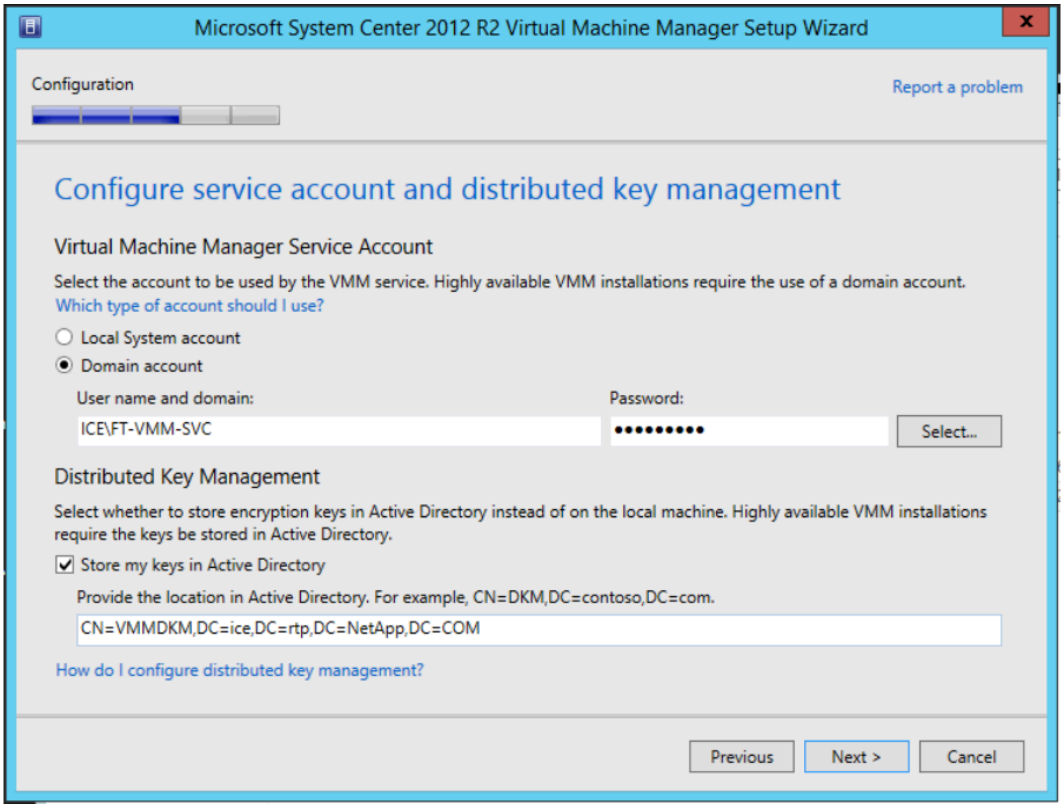
1. From the System Center 2012 R2 Virtual Machine Manager installation media source, right-click setup.exe and select Run as administrator to begin setup. If prompted by user account control, click Yes to allow the installation to make changes to the computer.

   The Virtual Machine Manager Installation wizard will begin.
2. At the splash page, click Install to begin the Virtual Machine Manager Server installation.
3. In the Select features to install page, select the VMM management server installation checkbox. After selecting it, the VMM console installation checkbox will be selected by default. Click Next.
4. In the product registration information page, enter the following information and click Next.
   - 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 valid product key for installation of Virtual Machine Manager. If no key is provided, Virtual Machine Manager will be installed in evaluation mode.
5. Accept the license agreement and click Next.

6. In the Join the Customer Experience Improvement Program (CEIP) page, select the option to either participate or not participate in the CEIP by providing selected system information to Microsoft. Click Next.
7. In the Microsoft Update page, select the option to either allow or not allow Virtual Machine Manager to use Microsoft Update to check for and perform Automatic Updates based on your organization's policies. Click Next.
8. In the Select installation location dialog, specify a location or accept the default location of %ProgramFiles%\Microsoft System Center 2012 R2\Virtual Machine Manager for the installation. Click Next.

Note: The setup wizard has a prerequisite checker built in. If for any reason a prerequisite is not met, the setup UI will notify you of the discrepancy. If the system passes the prerequisite check, no page is displayed and the setup wizard proceeds to the Database configuration page.

9. In the Database configuration page, enter the following information and click Next.
   - Server name. Specify the name of the SQL Server. Should be the local machine.
   - Port. Specify the TCP port used for the SQL Server. Leave blank if using a local instance.
   - Verify that the Use the following credentials checkbox is cleared. In the Instance name drop-down menu, select the Virtual Machine Manager database instance deployed previously (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 page, in the Virtual Machine Manager Service account section, select the Domain account option. Enter the following information and click Next.
    - User name and domain. Specify the Virtual Machine Manager service account identified in the previous section in the following format: <DOMAIN>\<USERNAME>.
    - Password. Specify the password for the Virtual Machine Manager service account identified previously.
    - 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 previously created within Active Directory: cn=VMMDKM,DC=domain,…
    - Click Next.


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.

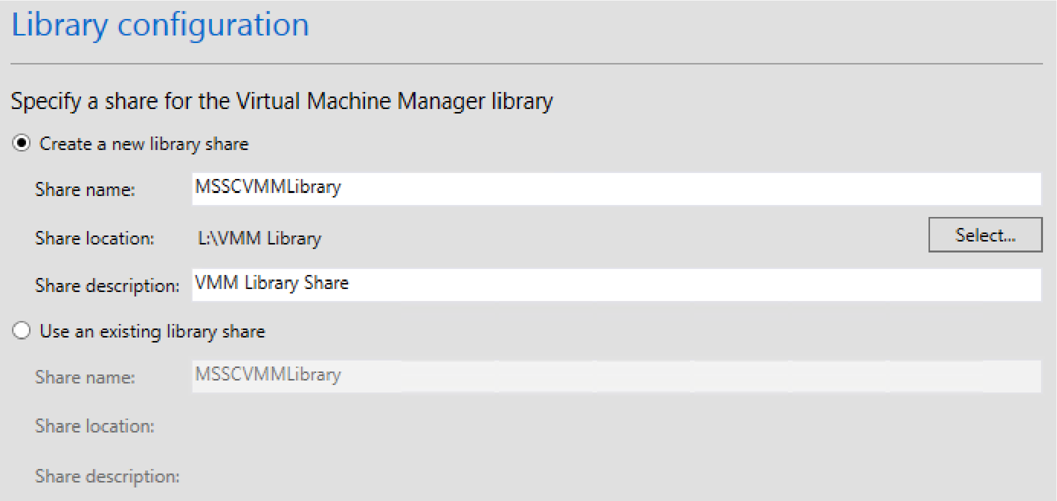
☑ Store my keys in Active Directory

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 page, accept the default values in the provided text boxes and click Next:
    - 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
    - Click Next.
12. In the Library configuration page, under Share Location, click Select. Browse to the L: drive. Click Make New Folder. Rename the new folder as VMM Library and click OK. Click Next.



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 page appears and displays the selections made during the installation wizard. Review the options selected and click Install.

    The wizard will display the progress while installing features.

14. After the installation completes, the wizard indicates that the setup was successful. Click Close to complete the installation.
15. 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 on the local host.

Creating VMM Run as Account

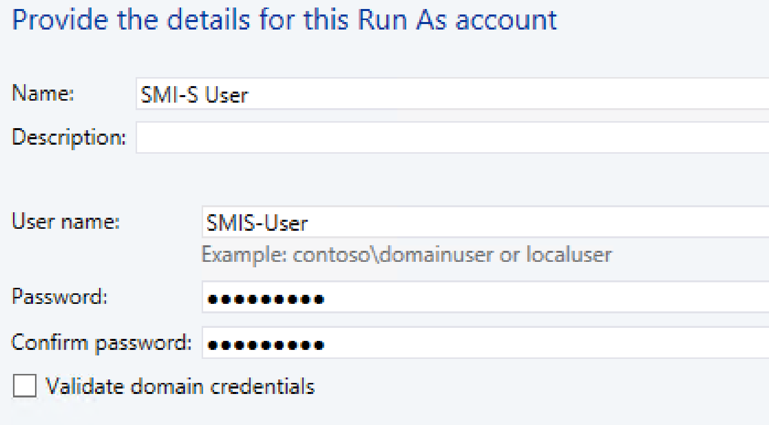
1. From the Virtual Machine Manager console, click Settings in the left tree view and click Create Run As Account.
2. Name the account. Provide the Active Directory account name and password with administrator rights to all Hyper-V hosts and clusters.
3. Click OK to create the Run-As Account.

Registering SMI-S in SCVMM

To register the NetApp SMI-S provider in SCVMM, complete the following steps:

1. In the Virtual Machine Manager console, navigate to the Fabric pane and expand the Storage node. Select the Providers subnode.
2. Click Add Resources and select Storage Devices from the drop-down menu.
3. In 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 the 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. Select the Use Secure Sockets Layer checkbox.
    d. Click Browse and, in the resulting pop-up, select Create Run As Account.
    - Enter a display name.
    - Enter the user name (for example, SMI-S User).

- Enter the password.
- Clear the Validate domain credentials option.
- Click OK.



Provide the details for this Run As account

Name: SMI-S User

Description:

User name: SMIS-User

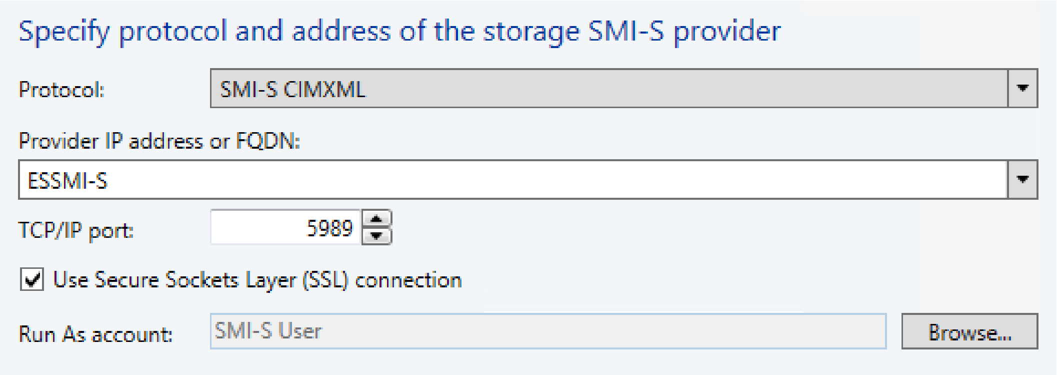
Example: contoso\domainuser or localuser

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

☐ Validate domain credentials

- Click Next



Specify protocol and address of the storage SMI-S provider

Protocol: SMI-S CIMXML

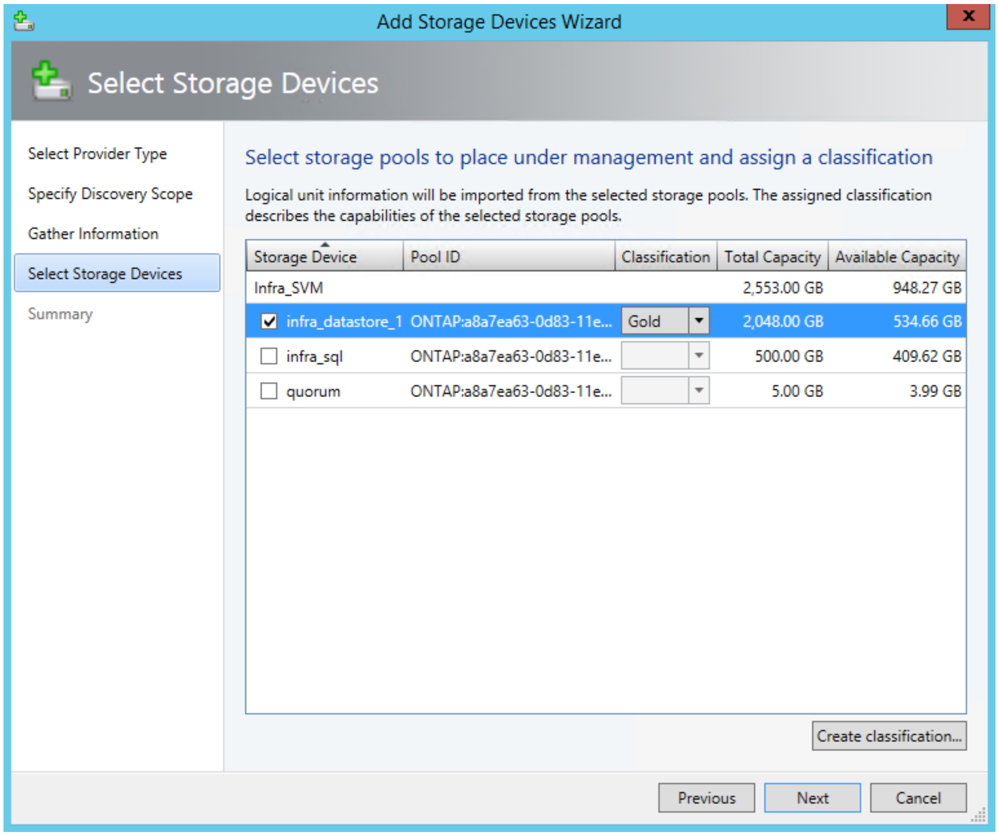
Provider IP address or FQDN: ESSMI-S

TCP/IP port: 5989

☑ Use Secure Sockets Layer (SSL) connection

Run As account: SMI-S User

6. During the discovery phase a pop-up opens prompting you to import the SMI-S provider's certificate. Click Import.
7. After the discovery is complete, the wizard shows all the storage controllers registered with the SMI-S provider. Click Next.
8. On the Select Storage Devices page, click Create Classification. Enter a name for the storage pool.
9. Check the `infra_datastore_1` storage pool, and assign a classification.



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			2,553.00 GB	948.27 GB
☑ infra_datastore_1	ONTAP:a8a7ea63-0d83-11e...	Gold	2,048.00 GB	534.66 GB
□ infra_sql	ONTAP:a8a7ea63-0d83-11e...		500.00 GB	409.62 GB
□ quorum	ONTAP:a8a7ea63-0d83-11e...		5.00 GB	3.99 GB

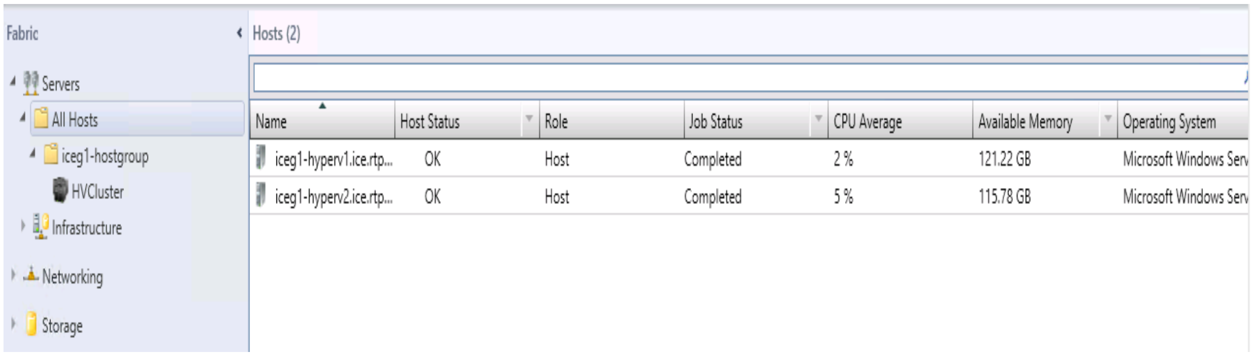
10. Click Next and Finish to close the wizard.

Adding Fabric Management Resources Virtual Machine Manager

1. Click Fabric in the left tree view and right-click All Hosts under the Servers section. Select Create Host Group and provide a name for the host group.
2. Select Fabric and All Hosts. Click `Add Resources, Hyper-V Hosts and Clusters`.
3. In the Indicate the Windows computer location window, select Windows server computers in a trusted Active Directory domain. Click Next.
4. Select `Use an Existing Run As` account and click Browse.
5. Select the previously created account and click OK.
6. Click Next.
7. Enter the cluster name and click Next.
8. Click Select All and click Next.
9. Select the Host Group created earlier and click Next.

Note: Sometimes the process might fail and the wizard would recommend you to restart the host servers. In such a case, reboot the Hyper-V hosts and repeat the procedure from step 1.

10. Verify job completion.
11. Verify that the hosts are added.



Name	Host Status	Role	Job Status	CPU Average	Available Memory	Operating System
iceg1-hyperv1.ice.rtp...	OK	Host	Completed	2 %	121.22 GB	Microsoft Windows Serv
iceg1-hyperv2.ice.rtp...	OK	Host	Completed	5 %	115.78 GB	Microsoft Windows Serv

6 Bill of Materials

This section details the hardware and software components used in validating both the small and medium FlexPod Express configurations included in this document.

6.1 Small Configuration

Table 15) Small configuration components.

Part Number	Product Description	Quantity Required
Cisco Components		
Network Switches		
N3K-C3048-FA-L3	Cisco Nexus 3048 Std Airflow (port side exhaust) AC P/S LAN Ent	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
N3K-C3048-BAS1K9	Cisco Nexus 3048 Base License	2
N3K-C3048-LAN1K9	Cisco Nexus 3048 LAN Enterprise License	2
N3K-C3048-FAN	Cisco Nexus 3048 Fan Module Port-side Exhaust	2
N3K-C3064-ACC-KIT	Cisco Nexus 3064PQ Accessory Kit	2
N3KUK9-602U2.3	Cisco NX-OS Release 6.0(2)U2(3)	2
CON-SNT-48FAL3	Cisco SMARTNET 8X5XNBD Nexus 3048 Std Airflow AC P/S LAN Ent	2
Cisco UCS Compute		
UCSC-C220-M4L	UCS C220 M4 LFF w/o CPU mem HD PCIe PSU rail kit	2
UCS-CPU-E52640D	2.60 GHz E5-2640 v3/90W 8C/20MB Cache/DDR4 1866MHz	4
UCS-MR-1X162RU-A	16GB DDR4-2133-MHz RDIMM/PC4-17000/dual rank/x4/1.2v	16

Part Number	Product Description	Quantity Required
UCSC-MLOM-IRJ45	Intel i350 quad-port MLOM NIC	2
CAB-N5K6A-NA	Power Cord, 200/240V 6A North America	4
UCSC-PSU1-770W	770W AC Hot-Plug Power Supply for 1U C-Series Rack Server	4
UCSC-BBLKD-L	3.5-inch HDD Blanking Panel	16
UCSC-HS-C220M4	Heat sink for UCS C220 M4 rack servers	4
UCSC-RAILB-M4	Ball Bearing Rail Kit for C220 M4 and C240 M4 rack servers	2
UCS-HDD1TI2F212	1TB SAS 7.2K RPM 3.5 inch HDD/hot plug/drive sled mounted	4
UCSC-SAS12GHBA	Cisco 12Gbps Modular SAS HBA	2
C1UCS-OPT-OUT	Cisco ONE Data Center Compute Opt Out Option	2
CON-OSP-C220M4L	SNTC-24X7X4OS UCS C220 M4 LFF w/o CPU, mem, HD (Service Duration: 36 months)	2
NetApp Components		
FAS2520A-001-R6	FAS2520 High Availability System	2
X80102A-R6-C	Bezel,FAS2520,R6,-C	1
FAS2520-111-R6-C	FAS2520,12x900GB,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
X6561-R6	Cable,Ethernet,2m RJ45 CAT6	2
X6557-EN-R6-C	Cbl,SAS Cntlr-Shelf/Shelf-Shelf/HA,0.5m,EN,-C	2
DOC-2520-C	Documents,2520,-C	1
X5518A-R6-C	Kit,FAS2XXX,-C,R6	1
OS-ONTAP-CAP2-1P-C	OS Enable,Per-0.1TB,ONTAP,Perf-Stor,1P,-C	108
SWITCHLESS	2-Node Switchless Cluster	1
SW-2-2520A-SMGR-C	SW-2,SnapManager Suite,2520A,-C	2
SW-2-2520A-SRESTORE-C	SW-2,SnapRestore,2520A,-C	2
SW-2-2520A-FLEXCLN-C	SW-2,FlexClone,2520A,-C	2
SW-2-2520A-ISCSI-C	SW-2,iSCSI,2520A,-C	2
SW-ONTAP8.2.2-CLM	SW,Data ONTAP 8.2.2,Cluster-Mode	2

[1] SupportEdge Premium required for cooperative support.

6.2 Medium Configuration

Table 16) Medium configuration components.

Part Number	Product Description	Quantity Required
Cisco Components		
Network Switches		
N3K-C3048-FA-L3	Cisco Nexus 3048 Std Airflow (port side exhaust) AC P/S LAN Ent	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
N3K-C3048-BAS1K9	Cisco Nexus 3048 Base License	2
N3K-C3048-LAN1K9	Cisco Nexus 3048 LAN Enterprise License	2
N3K-C3048-FAN	Cisco Nexus 3048 Fan Module Port-side Exhaust	2
N3K-C3064-ACC-KIT	Cisco Nexus 3064PQ Accessory Kit	2
N3KUK9-602U2.3	Cisco NX-OS Release 6.0(2)U2(3)	2
CON-SNT-48FAL3	Cisco SMARTNET®8X5XNBD Nexus 3048 Std Airflow AC P/S LAN Ent	2
Cisco UCS Compute		
UCSC-C220-M4L	UCS C220 M4 LFF w/o CPU mem HD PCIe PSU rail kit	4
UCS-CPU-E52640D	2.60 GHz E5-2640 v3/90W 8C/20MB Cache/DDR4 1866MHz	8
UCS-MR-1X162RU-A	16GB DDR4-2133-MHz RDIMM/PC4-17000/dual rank/x4/1.2v	32
UCSC-MLOM-IRJ45	Intel i350 quad-port MLOM NIC	4
CAB-N5K6A-NA	Power Cord, 200/240V 6A North America	8
UCSC-PSU1-770W	770W AC Hot-Plug Power Supply for 1U C-Series Rack Server	8
UCSC-BBLKD-L	3.5-inch HDD Blanking Panel	16
UCS-HDD1TI2F212	1TB SAS 7.2K RPM 3.5 inch HDD/hot plug/drive sled mounted	8
UCSC-SAS12GHBA	Cisco 12Gbps Modular SAS HBA	4
UCSC-HS-C220M4	Heat sink for UCS C220 M4 rack servers	8
UCSC-RAILB-M4	Ball Bearing Rail Kit for C220 M4 and C240 M4 rack servers	4

Part Number	Product Description	Quantity Required
C1UCS-OPT-OUT	Cisco ONE Data Center Compute Opt Out Option	4
CON-OSP-C220M4L	SNTC-24X7X4OS UCS C220 M4 LFF w/o CPU, mem, HD (Service Duration: 36 months)	4
NetApp Components		
FAS2520A-001-R6	FAS2520 High Availability System	2
X80102A-R6-C	Bezel,FAS2520,R6,-C	1
FAS2520-111-R6-C	FAS2520,12x900GB,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
X6561-R6	Cable,Ethernet,2m RJ45 CAT6	2
X6557-EN-R6-C	Cbl,SAS Cntlr-Shelf/Shelf-Shelf/HA,0.5m,EN,-C	2
DOC-2520-C	Documents,2520,-C	1
X5518A-R6-C	Kit,FAS2XXX,-C,R6	1
OS-ONTAP-CAP2-1P-C	OS Enable,Per-0.1TB,ONTAP,Perf-Stor,1P,-C	108
SWITCHLESS	2-Node Switchless Cluster	1
SW-2-2520A-SMGR-C	SW-2,SnapManager Suite,2520A,-C	2
SW-2-2520A-SRESTORE-C	SW-2,SnapRestore,2520A,-C	2
SW-2-2520A-FLEXCLN-C	SW-2,FlexClone,2520A,-C	2
SW-2-2520A-ISCSI-C	SW-2,iSCSI,2520A,-C	2
SW-ONTAP8.2.2-CLM	SW,Data ONTAP 8.2.2,Cluster-Mode	2

[1] SupportEdge Premium required for cooperative support.

7 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 a virtualization solution, which is described in this document. The flexibility and scalability of FlexPod Express enable customers to start out with a right-sized infrastructure that can ultimately grow with and adapt to their evolving business requirements.

References

This report refers to the following documents and resources:

- NetApp FAS2500 Storage
  http://www.netapp.com/in/products/storage-systems/fas2500/

- Cisco UCS C-Series Rack Servers
  http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-c-series-rack-servers/index.html
- Microsoft Hyper-V
  http://www.microsoft.com/en-us/server-cloud/solutions/virtualization.aspx

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

Copyright Information

Trademark Information

NVA-0021-DEPLOY