



Technical Report

FlexPod Express with Microsoft Windows Server 2012 Hyper-V Implementation Guide

Glenn Sizemore, Michael Zimmerman, David Klem,
Chris Reno, Michael Ansel, NetApp
June 2013 | TR-4137

TABLE OF CONTENTS

1	Overview.....	5
2	Audience.....	5
3	Architecture.....	5
3.1	Small Configuration.....	5
3.2	Medium Configuration.....	6
4	Hardware Details.....	7
4.1	Small Configuration.....	7
4.2	Medium Configuration.....	7
5	Software Details.....	7
6	Configuration Guidelines.....	8
7	FlexPod Express Cabling Information.....	8
7.1	Small Configuration Cabling Diagram.....	8
7.2	Small Configuration Cabling Tables.....	9
7.3	Medium Configuration Cabling Diagram.....	10
7.4	Medium Configuration Cabling Tables.....	11
8	Cisco Nexus 3048 Deployment Procedure	13
8.1	Initial Setup of the Cisco Nexus 3048 Switches.....	13
8.2	Software Upgrade (Optional)	14
8.3	Features.....	14
8.4	Global Port-Channel Configuration	14
8.5	Global Spanning-Tree Configuration.....	15
8.6	Jumbo Frames	15
8.7	VLAN Definitions.....	15
8.8	Access and Management Port Descriptions	16
8.9	Server and Storage Management Interface Configuration.....	17
8.10	Virtual Port Channel (vPC) Global Configuration	17
8.11	Storage Port Channels.....	18
8.12	Server Connections	18
8.13	In-Band Management SVI Configuration	21
8.14	Save Configuration	22
8.15	Uplink into Existing Network Infrastructure.....	22
9	NetApp FAS Storage Deployment Procedure.....	22

9.1	Controller FAS22xx Series	22
9.2	System Configuration Guides	22
9.3	Assign Controller Disk Ownership and Initialize Storage	23
9.4	Run the Setup Process	25
9.5	64-Bit Aggregates	27
9.6	IFGRP LACP	27
9.7	VLAN	28
9.8	IP Config	28
9.9	iSCSI	28
9.10	Install SnapManager Licenses	28
9.11	Storage Controller Active-Active Configuration	29
9.12	Data ONTAP SecureAdmin	29
9.13	Secure Shell	30
9.14	AutoSupport HTTPS	30
9.15	Security Best Practices	30
9.16	Enable NDMP	30
9.17	Create FlexVol Volumes	30
9.18	Enable CDP	31
10	Cisco Unified Computing System C-Series Server Deployment Procedure	31
10.1	Perform Initial Cisco UCS C-Series Standalone Server CIMC Setup	31
10.2	Configure Cisco UCS C-Series RAID Configuration	33
11	Windows Server 2012 Deployment Procedure	36
11.1	Log into the Cisco UCS C-Series Standalone Server CIMC Interface	36
11.2	Set Up the Windows Server 2012 Install	36
11.3	Install Windows Server 2012	36
11.4	Install .NET Framework 3.5 Feature	37
11.5	Configure Windows Networking for FlexPod Express	37
11.6	Install NetApp Windows iSCSI Host Utilities	39
11.7	Configure Windows Host iSCSI Initiator	39
11.8	Install NetApp SnapDrive	40
11.9	Install NetApp SnapManager for Hyper-V	40
11.10	Create a Cluster	41
12	Bill of Materials	43

LIST OF TABLES

Table 1) Small configuration hardware details.....	7
Table 2) Medium configuration hardware details.....	7
Table 3) Software details.....	8
Table 4) Cisco Nexus Switch 1 small configuration cabling.....	9
Table 5) Cisco Nexus Switch 2 small configuration cabling.....	10
Table 6) Cisco Nexus Switch 1 medium configuration cabling.	11
Table 7) Cisco Nexus Switch 2 medium configuration cabling.	12
Table 8) Controller FAS22XX series prerequisites.	22
Table 9) Small configuration components.	43
Table 10) Medium configuration components.....	44

LIST OF FIGURES

Figure 1) FlexPod Express small configuration.	6
Figure 2) FlexPod Express medium configuration.....	7
Figure 3) Small configuration cabling.	Error! Bookmark not defined.
Figure 4) Medium configuration cabling.....	11

1 Overview

The small and medium FlexPod[®] Express configurations are low-cost, standardized infrastructure solutions developed to meet the needs of small and midsize businesses. The configurations have been built and tested to deliver a cost-effective, high-value, and best practice architecture. 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 business demands.

2 Audience

This document describes the architecture and deployment procedures for both small and medium FlexPod Express configurations. The intended audience for this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, partner engineering, and customers who want to deploy FlexPod Express.

3 Architecture

Both the small and medium FlexPod Express configurations leverage Cisco Unified Computing System[™] (Cisco UCS[®]) C-Series servers, Cisco Nexus[®] switches, and NetApp[®] FAS storage. Although FlexPod Express supports an open ecosystem of virtualization and management software solutions, the architecture described in this document specifically includes Microsoft[®] Windows Server[®] 2012. Virtualization software and infrastructure management software are strongly recommended as a part of every FlexPod Express deployment. Each configuration leverages the best practices, and between each component, to enable a reliable, enterprise-class infrastructure.

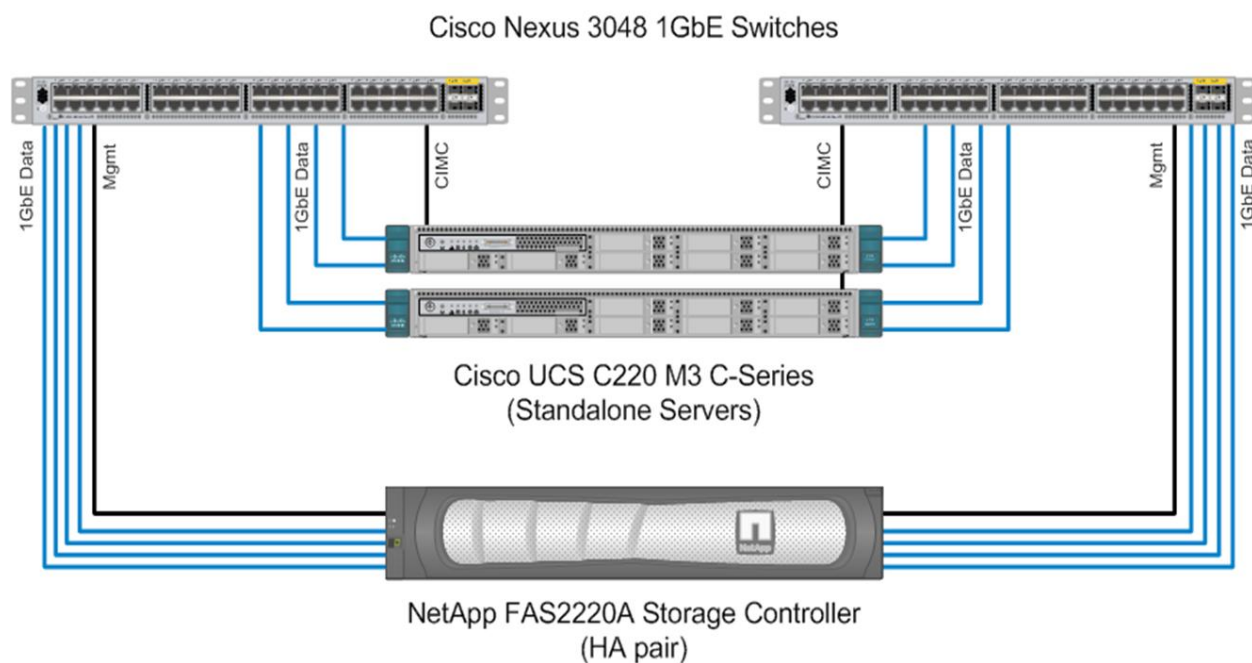
3.1 Small Configuration

The small configuration as validated with Microsoft Windows Server 2012 includes the following components:

- Cisco Nexus 3048 switches
- Cisco UCS C220 M3 servers
- NetApp FAS2220 storage controllers
- Microsoft Windows Server 2012

Figure 1 highlights the physical topology of the small FlexPod Express configuration.

Figure 1) FlexPod Express small configuration.



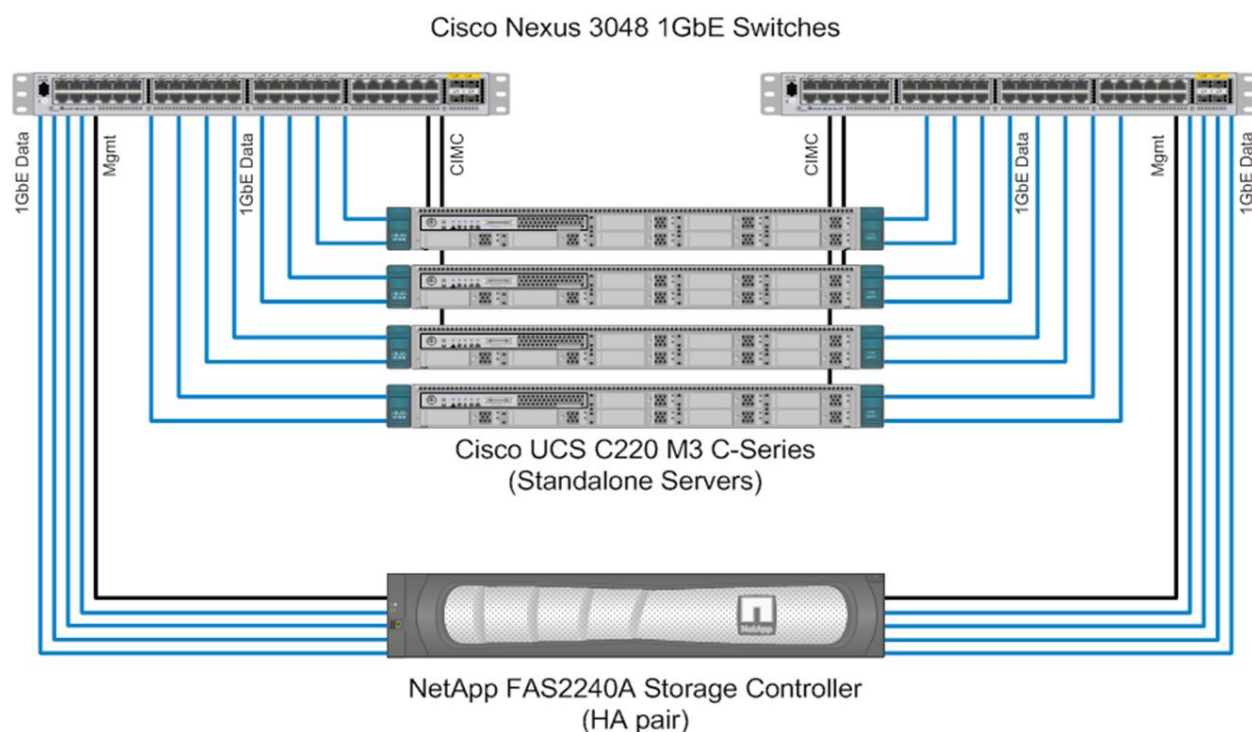
3.2 Medium Configuration

The medium configuration as validated with Microsoft Windows Server 2012 includes the following components:

- Cisco Nexus 3048 switches
- Cisco UCS C220 M3 servers
- NetApp FAS2240 storage controllers
- Microsoft Windows Server 2012

Figure 2 highlights the physical topology of the medium FlexPod Express configuration.

Figure 2) FlexPod Express medium configuration.



4 Hardware Details

4.1 Small Configuration

Table 1) Small configuration hardware details.

Layer	Component	Quantity
Compute	Cisco UCS C-Series C220 M3 servers (standalone)	2
Network	Cisco Nexus 3048 switches	2
Storage	NetApp FAS2220A (HA pair) (w/ qty. 12 x 600GB 10K SAS HDDs)	1

4.2 Medium Configuration

Table 2) Medium configuration hardware details.

Layer	Component	Quantity
Compute	Cisco UCS C-Series C220 M3 servers (standalone)	4
Network	Cisco Nexus 3048 switches	2
Storage	NetApp FAS2240A (HA pair) (w/ qty. 24 x 600GB 10K SAS HDDs)	1

5 Software Details

It is important to note the software versions used in this document. Table 3 details the software revisions used throughout this document.

Table 3) Software details.

Layer	Component	Version or Release	Details
Compute	Cisco UCS C Series C220 M2 standalone servers	1.4(7b)	CIMC software
Network	Cisco Nexus 3048 GbE switches	5.0(3)U4(1)	NX-OS software
Storage (small configuration)	NetApp FAS2220A	8.1.1 operating in 7-Mode	NetApp Data ONTAP® software
Storage (medium configuration)	NetApp FAS2240A	8.1.1 operating in 7-Mode	Data ONTAP software
Software	Microsoft Windows Server 2012	2012	Virtualization hypervisor
	NetApp Windows® Host Utilities Kit	6.0.1	NetApp plug-in for Windows
	SnapDrive® for Windows	6.5	LUN provisioning and Snapshot™ management

6 Configuration Guidelines

This document provides details for configuring a fully redundant, highly available configuration for an FlexPod Express unit. Therefore, reference is made to which component is being configured with each step, either 1 or 2. For example, Controller 1 and Controller 2 are used to identify the two NetApp storage controllers that are provisioned; Switch 1 and Switch 2 identify the pair of Cisco Nexus switches that are configured. Additionally, this document details steps for provisioning multiple Cisco UCS hosts, and these are identified sequentially: Server-1, Server-2, and so on. Finally, to indicate that you should include information pertinent to your environment in a given step, <<var_text>> appears as part of the command structure. See the following example for the `vlan create` command:

```
controller1>vlan create vif0 <<var_mgmt_vlan>>
```

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.

7 FlexPod Express Cabling Information

7.1 Small Configuration Cabling Diagram

Each port used on each component in the small configuration is designated with a box and an associated number. Port connections are defined by matching numbers. For example, Cisco Nexus 3048 Switch 1 port Eth1/1 is labeled with a “1” and is connected to NetApp FAS2240 Storage Controller 1 port e0a, which is also labeled with a “1.”

Figure 3) Small configuration cabling.

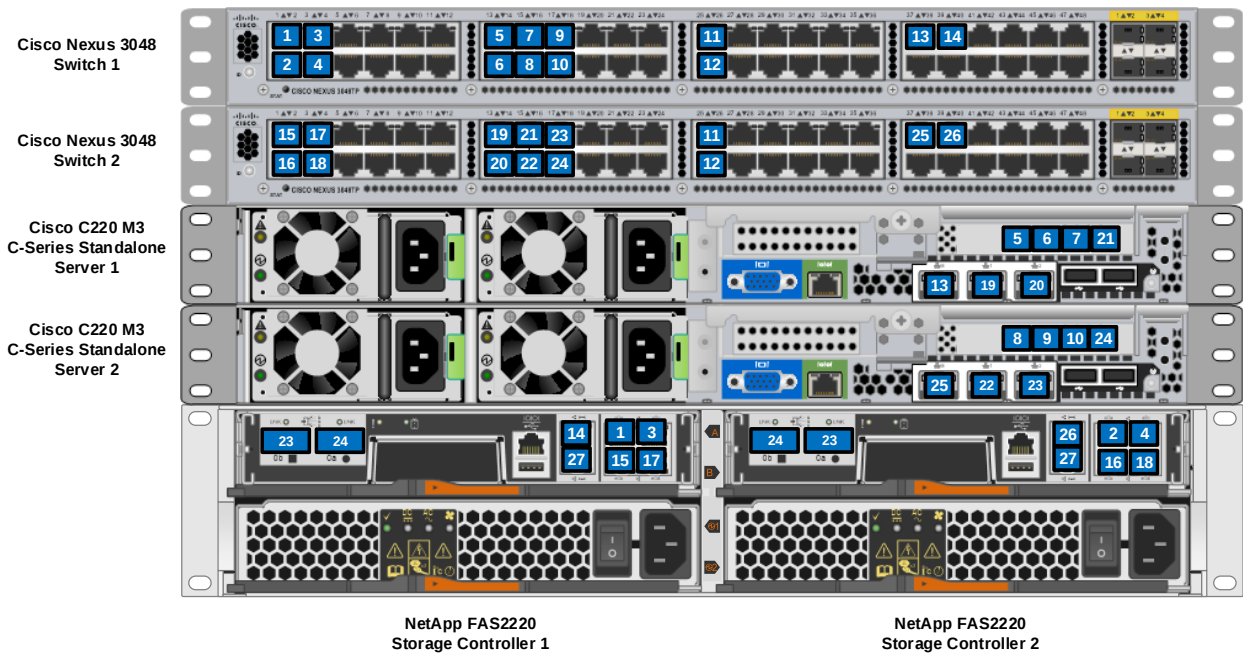


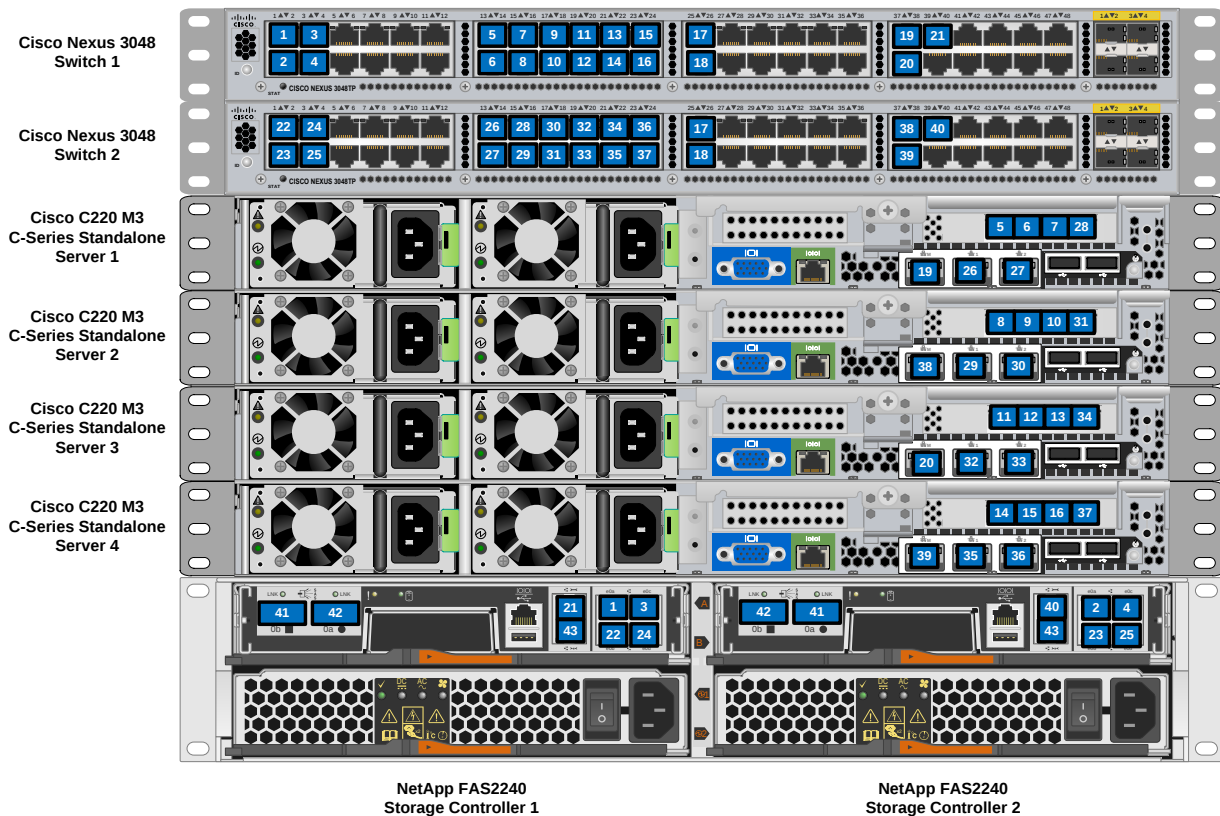
Table 5) Cisco Nexus Switch 2 small configuration cabling.

Local Device	Local Port	Remote Device	Remote Port
Cisco Nexus 3048 Switch 2	Eth1/1	NetApp FAS2220 Storage Controller 1	e0b
	Eth1/2	NetApp FAS2220 Storage Controller 2	e0b
	Eth1/3	NetApp FAS2220 Storage Controller 1	e0d
	Eth1/4	NetApp FAS2220 Storage Controller 2	e0d
	Eth1/13	Cisco UCS C220 C-Series Standalone Server 1	0/1
	Eth1/14	Cisco UCS C220 C-Series Standalone Server 1	0/2
	Eth1/15	Cisco UCS C220 C-Series Standalone Server 1	1/4
	Eth1/16	Cisco UCS C220 C-Series Standalone Server 2	0/1
	Eth1/17	Cisco UCS C220 C-Series Standalone Server 2	0/2
	Eth1/18	Cisco UCS C220 C-Series Standalone Server 2	1/4
	Eth1/25	Cisco Nexus 3048 Switch 1	Eth1/25
	Eth1/26	Cisco Nexus 3048 Switch 1	Eth1/26
	Eth1/37	Cisco UCS C220 C-Series Standalone Server 2	Management port
	Eth1/38	Cisco UCS C220 C-Series Standalone Server 4	Management port

7.3 Medium Configuration Cabling Diagram

Each port used on each component in the medium configuration is designated with a box and an associated number. Port connections are defined by matching numbers. For example, Cisco Nexus 3048 Switch 1 port Eth1/1 is labeled with a “1” and is connected to NetApp FAS2240 Storage Controller 1 port e0a, which is also labeled with a “1.”

Figure 4) Medium configuration cabling.



7.4 Medium Configuration Cabling Tables

Table 6) Cisco Nexus Switch 1 medium configuration cabling.

Local Device	Local Port	Remote Device	Remote Port
Cisco Nexus 3048 Switch 1	Eth1/1	NetApp FAS2220 Storage Controller 1	e0a
	Eth1/2	NetApp FAS2220 Storage Controller 2	e0a
	Eth1/3	NetApp FAS2220 Storage Controller 1	e0c
	Eth1/4	NetApp FAS2220 Storage Controller 2	e0c
	Eth1/13	Cisco UCS C220 C-Series Standalone Server 1	1/1
	Eth1/14	Cisco UCS C220 C-Series Standalone Server 1	1/2
	Eth1/15	Cisco UCS C220 C-Series Standalone Server 1	1/3
	Eth1/16	Cisco UCS C220 C-Series Standalone Server 2	1/1
	Eth1/17	Cisco UCS C220 C-Series Standalone Server 2	1/2
	Eth1/18	Cisco UCS C220 C-Series Standalone Server 2	1/3
	Eth1/19	Cisco UCS C220 C-Series Standalone Server 3	1/1
	Eth1/20	Cisco UCS C220 C-Series Standalone Server 3	1/2

Local Device	Local Port	Remote Device	Remote Port
	Eth1/21	Cisco UCS C220 C-Series Standalone Server 3	1/3
	Eth1/22	Cisco UCS C220 C-Series Standalone Server 4	1/1
	Eth1/23	Cisco UCS C220 C-Series Standalone Server 4	1/2
	Eth1/24	Cisco UCS C220 C-Series Standalone Server 4	1/3
	Eth1/25	Cisco Nexus 3048 Switch 2	Eth1/25
	Eth1/26	Cisco Nexus 3048 Switch 2	Eth1/26
	Eth1/37	Cisco UCS C220 C-Series Standalone Server 1	Management port
	Eth1/38	Cisco UCS C220 C-Series Standalone Server 3	Management port
	Eth1/39	NetApp FAS2220 Storage Controller 1	Management port

Table 7) Cisco Nexus Switch 2 medium configuration cabling.

Local Device	Local Port	Remote Device	Remote Port
Cisco Nexus 3048 Switch 2	Eth1/1	NetApp FAS2220 Storage Controller 1	e0b
	Eth1/2	NetApp FAS2220 Storage Controller 2	e0b
	Eth1/3	NetApp FAS2220 Storage Controller 1	e0d
	Eth1/4	NetApp FAS2220 Storage Controller 2	e0d
	Eth1/13	Cisco UCS C220 C-Series Standalone Server 1	0/1
	Eth1/14	Cisco UCS C220 C-Series Standalone Server 1	0/2
	Eth1/15	Cisco UCS C220 C-Series Standalone Server 1	1/4
	Eth1/16	Cisco UCS C220 C-Series Standalone Server 2	0/1
	Eth1/17	Cisco UCS C220 C-Series Standalone Server 2	0/2
	Eth1/18	Cisco UCS C220 C-Series Standalone Server 2	1/4
	Eth1/19	Cisco UCS C220 C-Series Standalone Server 3	0/1
	Eth1/20	Cisco UCS C220 C-Series Standalone Server 3	0/2
	Eth1/21	Cisco UCS C220 C-Series Standalone Server 3	1/4
	Eth1/22	Cisco UCS C220 C-Series Standalone Server 4	0/1
	Eth1/23	Cisco UCS C220 C-Series Standalone Server 4	0/2
	Eth1/24	Cisco UCS C220 C-Series Standalone Server 4	1/4
	Eth1/25	Cisco Nexus 3048 Switch 1	Eth1/25
	Eth1/26	Cisco Nexus 3048 Switch 1	Eth1/26
	Eth1/37	Cisco UCS C220 C-Series Standalone Server 2	Management port
	Eth1/38	Cisco UCS C220 C-Series Standalone Server 4	Management port

Local Device	Local Port	Remote Device	Remote Port
	Eth1/39	NetApp FAS2220 Storage Controller 2	Management port

8 Cisco Nexus 3048 Deployment Procedure

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

8.1 Initial Setup of the Cisco Nexus 3048 Switches

On initial boot and connection to the console port of the switch, the NX-OS setup automatically starts. This initial configuration addresses basic settings such as the switch name, the mgmt0 interface configuration, and SSH setup and defines the control plane policing policy.

The first major decision involves the configuration of the management network for the switches themselves. For FlexPod Express, there are two main options for configuring the mgmt0 interfaces. The first involves configuring and cabling the mgmt0 interfaces into an already existing out-of-band network. In this instance, where a management network already exists, all that are needed are valid IP addresses, the netmask configuration for this network, and a connection from the mgmt0 interfaces into this network.

The other option for installations without a dedicated management network involves cabling the mgmt0 interfaces of each Cisco Nexus 3048 switch together in a back-to-back configuration. Any valid IP address and netmask may be configured on each mgmt0 interface as long as they are on 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, but it will be used for the vPC peer keepalive traffic. To enable SSH management access to the switch, the configuration of the in-band interface-vlan IP address on a switched virtual interface (SVI) is addressed later in this guide.

Power on the switch and follow the onscreen prompts as illustrated in the following code for the initial setup of both switches, substituting the appropriate values for the switch-specific information.

Switch1 and 2

```

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

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

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

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

Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]:
Configure read-only SNMP community string (yes/no) [n]:
Configure read-write SNMP community string (yes/no) [n]:
Enter the switch name : <<var_switch_hostname>>
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:
Mgmt0 IPv4 address : <<var_mgmt0_ip_address>>
Mgmt0 IPv4 netmask : <<var_mgmt0_netmask>>
Configure the default gateway for mgmt? (yes/no) [y]: n
Enable the telnet service? (yes/no) [n]:
Enable the ssh service? (yes/no) [y]:
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]:
Configure CoPP System Policy Profile ( default / 12 / 13 ) [default]:

The following configuration will be applied:

```

```

switchname <<var_switch_hostname>>
interface mgmt0
ip address <<var_mgmt0_ip_address>><<var_mgmt0_netmask>>
no shutdown
no telnet server enable
ssh key rsa 1024 force
ssh server enable
policy-map type control-plane copp-system-policy ( default )

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

```

8.2 Software Upgrade (Optional)

NetApp recommends performing any required software upgrades on the switch at this point in the configuration. Download and install the latest available NX-OS software for the Cisco Nexus 3048 switch from the Cisco® software download site. There are various methods to transfer both the kickstart and system images for NX-OS to the switch. The most straightforward procedure leverages the onboard USB port on the switch. Download the 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.

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

Switch 1 and 2

```

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

```

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

8.3 Features

Certain advanced features need to be enabled within NX-OS to allow for additional configuration options. The interface-vlan feature is only required if using the back-to-back mgmt0 option described in section 8.1. This will allow an IP address to be assigned to the interface VLAN (SVI), which enables in-band management communication to the switch such as ssh.

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

Switch 1 and 2

```

feature interface-vlan
feature lacp
feature vpc

```

8.4 Global Port-Channel Configuration

The default port-channel load-balancing hash uses the source and destination IP to determine the load-balancing algorithm across the interfaces in the port channel. Better distribution across the members of the port channels can be achieved by providing more inputs to the hash algorithm beyond the source and destination IP. For this reason, adding the source and destination TCP port to the hash algorithm is highly recommended.

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

Switch 1 and 2

```

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

```

8.5 Global Spanning-Tree Configuration

The Cisco Nexus platform leverages a new protection feature called bridge assurance. Bridge assurance helps to 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 a few states depending on the platform, including “network” and “edge.”

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

This mode will force the network administrator to visit the configuration of each port and can help reveal the most common configuration errors such as nonidentified edge ports or bridge assurance not enabled on a neighbor. Also, it is safer to have spanning-tree block many ports than not enough, which allows the default port state to enhance the overall stability of the network.

Pay close attention to the spanning-tree state when adding additional servers, storage, or uplink switches, especially if they do not support bridge assurance. In those cases, you might be required to change the port type for the ports to become active.

BPDU guard is enabled on edge ports by default as another layer of protection. This feature will shut down the port if BPDUs from another switch are seen on this interface to prevent loops in the network.

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.

Switch 1 and 2

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

8.6 Jumbo Frames

Jumbo frames should be configured throughout the network to allow for any applications or operating systems to transmit larger frames without fragmentation. Note that both endpoints and all interfaces between the endpoints (L2 and L3) must support and be configured for jumbo frames to realize 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.

Switch 1 and 2

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

8.7 VLAN Definitions

Before individual ports are configured with different VLANs, those L2 VLANs must be defined on the switch. It's also good practice to name the VLANs to help with any troubleshooting in the future.

From configuration mode (`config t`), type the following commands to define and describe the L2 VLANs.

Switch 1 and 2

```
vlan <<var_iscsia_vlan_id>>
  name iSCSIA-VLAN
vlan <<var_iscsib_vlan_id>>
  name iSCSIB-VLAN
```

```

vlan <<var_lm_vlan_id>>
  name LiveMigration-VLAN
vlan <<var_csv_vlan_id>>
  name CSV-VLAN
vlan <<var_vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<var_mgmt_vlan_id>>
  name MGMT-VLAN

```

8.8 Access and Management Port Descriptions

Similar to assigning names to the L2 VLAN, setting proper descriptions on all of the interfaces can help with both provisioning and troubleshooting.

For the small configuration, the descriptions for both the management and data ports associated with Server-3 and Server-4 are not required because the small FlexPod Express configuration only contains two servers. From configuration mode (`config t`) in each switch, type the following commands to set the proper port descriptions.

Switch 1

```

int eth1/1
  description FAS-1:e0a
int eth1/2
  description FAS-2:e0a
int eth1/3
  description FAS-1:e0c
int eth1/4
  description FAS-2:e0c
int eth1/13
  description Server-1:port1/1
int eth1/14
  description Server-1:port1/2
int eth1/15
  description Server-1:port1/3
int eth1/16
  description Server-2:port1/1
int eth1/17
  description Server-2:port1/2
int eth1/18
  description Server-2:port1/3
int eth1/19
  description Server-3:port1/1
int eth1/20
  description Server-3:port1/2
int eth1/21
  description Server-3:port1/3
int eth1/22
  description Server-4:port1/1
int eth1/23
  description Server-4:port1/2
int eth1/24
  description Server-4:port1/3
int eth1/25
  description vPC peer-link SwB:1/25
int eth1/26
  description vPC peer-link SwB:1/26
int eth1/37
  description Server-1:mgmt
int eth1/38
  description Server-3:mgmt
int eth1/39
  description FAS-1:mgmt

```

Switch 2

```

int eth1/1
  description FAS-1:e0b
int eth1/2
  description FAS-2:e0b
int eth1/3
  description FAS-1:e0d
int eth1/4
  description FAS-2:e0d
int eth1/13
  description Server-1:port0/1
int eth1/14
  description Server-1:port0/2
int eth1/15
  description Server-1:port1/4
int eth1/16
  description Server-2:port0/1
int eth1/17
  description Server-2:port0/2
int eth1/18
  description Server-2:port1/4
int eth1/19
  description Server-3:port1/1
int eth1/20
  description Server-3:port0/2
int eth1/21
  description Server-3:port1/4
int eth1/22
  description Server-4:port0/1
int eth1/23
  description Server-4:port0/2
int eth1/24
  description Server-4:port1/4
int eth1/25
  description vPC peer-link:1/25
int eth1/26
  description vPC peer-link:1/26
int eth1/37
  description Server-2:mgmt
int eth1/38
  description Server-4:mgmt
int eth1/39
  description FAS-2:mgmt

```

8.9 Server and Storage Management Interface Configuration

The management interfaces for both the server and storage typically only utilize a single VLAN. Because of this, the management interface ports are configured as access ports. Define the management VLAN for each 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.

Switch 1 and 2

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

8.10 Virtual Port Channel (vPC) Global Configuration

The vPC feature requires an initial setup between the two Cisco Nexus switches to function properly. If using the back-to-back mgmt0 configuration, be sure to use the addresses defined on the interfaces and verify that they can communicate by using the `ping <<var_mgmt0_ip_address>> vrf management` command.

From configuration mode (`config t`), type the following commands to configure the vPC global configuration for Switch 1.

Switch 1

```
vpc domain 1
  role priority 10
  peer-keepalive destination <<var_mgmt0_ip_address[of switch2]>> source
  <<var_mgmt0_ip_address[of switch1]>>

int eth1/25-26
  channel-group 10 mode active

int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1, <<var_iscsia_vlan_id>>, <<var_iscsib_vlan_id>>,
  <<var_lm_vlan_id>>, <<var_csv_vlan_id>>, <<var_vmtraffic_vlan_id>>, <<var_mgmt_vlan_id>>
  spanning-tree port type network
  vpc peer-link
  no shut
```

From configuration mode (`config t`), type the following commands to configure the vPC global configuration for Switch 2.

Switch 2

```
vpc domain 1
  role priority 10
  peer-keepalive destination <<var_mgmt0_ip_address[of switch1]>> source
  <<var_mgmt0_ip_address[of switch2]>>

int eth1/25-26
  channel-group 10 mode active

int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1, <<var_iscsia_vlan_id>>, <<var_iscsib_vlan_id>>,
  <<var_lm_vlan_id>>, <<var_csv_vlan_id>>, <<var_vmtraffic_vlan_id>>, <<var_mgmt_vlan_id>>
  spanning-tree port type network
```

```
vpc peer-link
no shut
```

8.11 Storage Port Channels

The NetApp storage controllers allow for an active-active connection to the network using LACP. Using LACP is preferred because it adds additional negotiation between the switches in addition to logging. Because the network is set up for vPC, this allows us 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 IFGRP.

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

Switch 1 and 2, FAS-1 Config

```
int eth1/1,eth1/3
  channel-group 11 mode active

int Po11
  description vPC to FAS-1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1, <<var_iscsia_vlan_id>>, <<var_iscsib_vlan_id>>
,<<var_vmtraffic_vlan_id>>
  spanning-tree port type edge trunk
  vpc 11
  no shut
```

Switch 1 and 2, FAS-2 Config

```
int eth1/2,eth1/4
  channel-group 12 mode active

int Po12
  description vPC to FAS-2
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1, <<var_iscsia_vlan_id>>, <<var_iscsib_vlan_id>>
,<<var_vmtraffic_vlan_id>>
  spanning-tree port type edge trunk
  vpc 12
  no shut
```

8.12 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 out across multiple switches enables the server to survive even a complete switch failure.

For the small configuration, you only need to configure `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.

Switch 1, Server-1 Config

```
int eth1/13
  channel-group 21 mode active
exit
int Po21
```

```

description VM traffic
switchport
switchport mode trunk
switchport trunk allowed vlan 1, <<var_vmtraffic_vlan_id>>, <<var_mgmt_vlan_id>>
spanning-tree port type edge
vpc 21
no shut
exit
int eth1/14
switchport
switchport access vlan <<var_iscsia_vlan_id>>
spanning-tree port type edge
no shut
exit
int eth1/15
switchport
switchport access vlan <<var_lm_vlan_id>>
spanning-tree port type edge
no shut
exit

```

Switch 2, Server-1 Config

```

int eth1/13
channel-group 21 mode active
exit
int Po21
description VM traffic
switchport
switchport mode trunk
switchport trunk allowed vlan 1, <<var_vmtraffic_vlan_id>>, <<var_mgmt_vlan_id>>
spanning-tree port type edge
vpc 21
no shut
exit
int eth1/14
switchport
switchport access vlan <<var_iscsib_vlan_id>>
spanning-tree port type edge
no shut
exit
int eth1/15
switchport
switchport access vlan <<var_csv_vlan_id>>
spanning-tree port type edge
no shut
exit

```

Switch 1, Server-2 Config

```

int eth1/16
channel-group 22 mode active
exit
int Po22
description VM traffic
switchport
switchport mode trunk
switchport trunk allowed vlan 1, <<var_vmtraffic_vlan_id>>, <<var_mgmt_vlan_id>>
spanning-tree port type edge
vpc 22
no shut
exit
int eth1/17
switchport
switchport access vlan <<var_iscsia_vlan_id>>
no shut
exit
int eth1/18
switchport

```

```
    switchport access vlan <<var_lm_vlan_id>>
exit
```

Switch 2, Server-2 Config

```
int eth1/16
    channel-group 22 mode active
exit
int Po22
    description VM traffic
    switchport
    switchport mode trunk
    switchport trunk allowed vlan 1, <<var_vmtraffic_vlan_id>>, <<var_mgmt_vlan_id>>
    spanning-tree port type edge
    vpc 22
    no shut
exit
int eth1/17
    switchport
    switchport access vlan <<var_iscsib_vlan_id>>
    no shut
exit
int eth1/18
    switchport
    switchport access vlan <<var_csv_vlan_id>>
exit
```

Switch 1, Server-3 Config

```
int eth1/19
    channel-group 23 mode active
exit
int Po23
    description VM traffic
    switchport
    switchport mode trunk
    switchport trunk allowed vlan 1, <<var_vmtraffic_vlan_id>>, <<var_mgmt_vlan_id>>
    spanning-tree port type edge
    vpc 23
    no shut
exit
int eth1/20
    switchport
    switchport access vlan <<var_iscsia_vlan_id>>
    no shut
exit
int eth1/21
    switchport
    switchport access vlan <<var_lm_vlan_id>>
exit
```

Switch 2, Server-3 Config

```
int eth1/19
    channel-group 23 mode active
exit
int Po23
    description VM traffic
    switchport
    switchport mode trunk
    switchport trunk allowed vlan 1, <<var_vmtraffic_vlan_id>>, <<var_mgmt_vlan_id>>
    spanning-tree port type edge
    vpc 23
    no shut
exit
int eth1/20
    switchport
    switchport access vlan <<var_iscsib_vlan_id>>
```

```

    no shut
exit
int eth1/21
    switchport
    switchport access vlan <<var_csv_vlan_id>>
exit

```

Switch 1, Server-4 Config

```

int eth1/22
    channel-group 24 mode active
exit
int Po24
    description VM traffic
    switchport
    switchport mode trunk
    switchport trunk allowed vlan 1, <<var_vmtraffic_vlan_id>>, <<var_mgmt_vlan_id>>
    spanning-tree port type edge
    vpc 24
    no shut
exit
int eth1/23
    switchport
    switchport access vlan <<var_iscsia_vlan_id>>
    no shut
exit
int eth1/24
    switchport
    switchport access vlan <<var_lm_vlan_id>>
exit

```

Switch 2, Server-4 Config

```

int eth1/22
    channel-group 24 mode active
exit
int Po24
    description VM traffic
    switchport
    switchport mode trunk
    switchport trunk allowed vlan 1, <<var_vmtraffic_vlan_id>>, <<var_mgmt_vlan_id>>
    spanning-tree port type edge
    vpc 24
    no shut
exit
int eth1/23
    switchport
    switchport access vlan <<var_iscsib_vlan_id>>
    no shut
exit
int eth1/24
    switchport
    switchport access vlan <<var_csv_vlan_id>>
exit

```

8.13 In-Band Management SVI Configuration

In-band management through SSH in the FlexPod Express environment is handled by an SVI. To configure the in-band management on each of the switches, an IP address must be configured on the interface-vlan, and a default gateway must be set up.

From configuration mode (`config t`), type the following commands to configure the SVI L3 interface for management purposes.

Switch 1 and 2

```
int Vlan <<var_mgmt_vlan_id>>
  ip address <<var_inband_mgmt_ip_address>>/<<var_inband_mgmt_netmask>>
  no shut

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

8.14 Save Configuration

Save the configuration on both switches for configuration persistence.

Switch 1 and 2

```
copy run start
```

8.15 Uplink into Existing Network Infrastructure

Depending on the available network infrastructure, several methods and features can be used to uplink the FlexPod Express environment. If an existing Cisco Nexus environment is present, it is recommended to use virtual port channels to uplink the Cisco Nexus 3048 switches included in the FlexPod Express environment into the infrastructure. Make sure to type `copy run start` to save the configuration on each switch after the configuration is completed.

9 NetApp FAS Storage Deployment Procedure

9.1 Controller FAS22xx Series

Table 8) Controller FAS22XX series prerequisites.

Requirement	Reference	Comments
Physical site where storage system needs to be installed must be ready	Site Requirements Guide	Refer to the “Site Preparation” section.
Storage system connectivity requirements	Site Requirements Guide	Refer to the “System Connectivity Requirements” section.
Storage system general power requirements	Site Requirements Guide	Refer to the “Circuit Breaker, Power Outlet Balancing, System Cabinet Power Cord Plugs, and Console Pinout Requirements” section.
Storage system model-specific requirements	Site Requirements Guide	Refer to the “FAS22xx Series Systems” section.

9.2 System Configuration Guides

System configuration guides provide supported hardware and software components for the specific Data ONTAP version. These online guides provide configuration information for all NetApp storage appliances that are currently supported by the Data ONTAP software. They also provide 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 [System Configuration Guides](#) at the NetApp [Support](#) site.
2. Click the appropriate NetApp storage appliance and then click the component you want to view. Alternatively, to compare components by storage appliance, click a component and then click the NetApp storage appliance you want to view.

Controller 1 and 2

Follow the physical installation procedures for the controllers in the [FAS22xx documentation](#) at the NetApp [Support](#) site.

9.3 Assign Controller Disk Ownership and Initialize Storage

These steps provide details for assigning disk ownership, and disk initialization and verification.

Controller 1

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

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

2. If the system is at the LOADER prompt, enter the autoboot command to boot Data ONTAP.
3. During system boot, press Ctrl + C when prompted for the boot menu.

```
Press Ctrl-C for Boot Menu...
```

Note: If 8.1.1 is not the version of software being booted, proceed with the following steps to install new software. If 8.1.1 is the version being booted, go to step 13, maintenance mode boot.

4. To install new software, first select option 7.
5. Answer *yes* for performing a nondisruptive upgrade.
6. Select *e0M* for the network port you want to use for the download.
7. Select *yes* to reboot now.
8. Enter the IP address: <<var_controller1_e0m_ip>>, Netmask: <<var_controller1_e0m_mask>>, and Default gateway: <<var_controller1_e0m_gateway>> for *e0M* in their respective places.
9. Enter the URL: <<var_url_boot_software>> where the software can be found.

Note: This Web server must be pingable.

10. Press Enter for the user name, indicating no user name.
11. Select *yes* to set the newly installed software as the default to be used for subsequent reboots.
12. Select *yes* to reboot the node.
13. Press Ctrl-C when you see Press Ctrl-C for Boot Menu.
14. To enter maintenance mode boot, select option 5.
15. When prompted "Continue to Boot?" answer *yes*.
16. To verify the HA status of your environment, use the command `ha-config show`.

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

```
ha-config modify controller ha
ha-config modify chassis ha
```

17. Use the `disk show -n` command to view how many disks are unowned.

Note: The remaining number of disks should be shown.

18. Use the `disk assign -n<<var_#_of_disks>>` command to assign disks to controller 1.

Note: For the small FlexPod Express configuration, <<var_#_of_disks>> should equal 9 for controller1.

Note: For the medium FlexPod Express configuration, <<var_#_of_disks>> should equal 21 for controller1.

19. Reboot the controller by using the `halt` command.
20. At the LOADER prompt type `autoboot`.
21. Press Ctrl-C for boot menu when prompted.
22. Select option 4) `Clean configuration and initialize all disks`.
23. Answer yes to zero disks, reset config, and install a new file system.
24. Enter `yes` to erase all the data on the disks.

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

Controller 2

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

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

2. If the system is at the LOADER prompt, enter the `autoboot` command to boot Data ONTAP.
3. During system boot, press Ctrl-C when prompted for the boot menu.

```
Press Ctrl-C for Boot Menu...
```

Note: If 8.1.1 is not the version of software being booted, proceed with the following steps to install new software. If 8.1.1 is the version being booted, then proceed with step 13, maintenance mode boot.

4. To install the new software first, select option 7.
5. Answer `yes` for performing a nondisruptive upgrade.
6. Select `e0M` for the network port you want to use for the download.
7. Select `yes` to reboot now.
8. Enter the IP address: <<var_controller2_e0m_ip>>, netmask: <<var_controller2_e0m_mask>>, and default gateway: <<var_controller2_e0m_gateway>> for e0M in their respective places.
9. Enter the URL: <<var_url_boot_software>> where the software can be found.

Note: This Web server must be pingable.

10. Press Enter for the user name, indicating no user name.
11. Select `yes` to set the newly installed software as the default to be used for subsequent reboots.
12. Select `yes` to reboot the node.
13. Press Ctrl-C when you see `Press Ctrl-C for Boot Menu`.
14. To enter maintenance mode boot, select option 5.
15. When prompted “Continue to Boot?” answer `yes`.
16. To verify the HA status of your environment, use the `ha-config show` command.

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

```
ha-config modify controller ha
ha-config modify chassis ha
```

17. Use the `disk show -a` command to view the number of unowned disks.

Note: The remaining disks should be shown.

18. Use the `disk assign -n<<var_#_of_disks>>` command to assign disks to controller 2.

Note: For both the small and medium FlexPod Express configurations, `<<var_#_of_disks>>` should equal 3 for controller2.

19. Reboot the controller using the `halt` command.

20. At the LOADER prompt type `autoboot`.

21. Press Ctrl-C for boot menu when prompted.

22. Select option 4) Clean configuration and initialize all disks.

23. Answer `yes` to zero disks, reset configuration, and install a new file system.

24. Enter `yes` to erase all the data on the disks.

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

9.4 Run the Setup Process

When Data ONTAP is installed on your new storage system, the following files are not populated:

- `/etc/rc`
- `/etc/exports`
- `/etc/hosts`
- `/etc/hosts.equiv`

Controller 1

1. Enter the configuration values the first time you power on the new system. The configuration values populate these files and configure the installed functionality of the system.

2. Enter the following information:

```
Please enter the new hostname []:<<var_controller1>>

Do you want to enable IPv6? [n]:

Do you want to configure interface groups? [n]:
Please enter the IP address for Network Interface e0a []:
```

Note: Press Enter to accept the blank IP address.

```
Should interface e0a take over a partner IP address during failover? [n]:
Please enter the IP address for the Network Interface e0b []:
Should interface e0b take over a partner IP address during failover? [n]:
Please enter the IP address for the Network Interface e0c []:
Should interface e1a take over a partner IP address during failover? [n]:
Please enter the IP address for the Network Interface e0c []:
Should interface e1b take over a partner IP address during failover? [n]:

Please enter the IP address for Network Interface e0M []: <<var_controller1_e0m_ip>>
Please enter the netmask for the Network Interface e0M
[255.255.255.0]:<<var_controller1_e0m_mask>>

Should interface e0M take over a partner IP address during failover? [n]: y
Please enter the IPv4 address or interface name to be taken over by e0M []: e0M
```

3. Enter the following information:

```
Would you like to continue setup through the Web interface? [n]:

Please enter the name or IP address of the IPv4 default gateway: <<var_controller1_e0m_gateway>>

The administration host is given root access to the storage system's / etc files for system
administration. To allow /etc root access to all NFS clients enter RETURN below.
Please enter the name or IP address for administrative host: <<var_adminhost_ip>>

Please enter timezone [GMT]: <<var_timezone>>
```

Note: Example time zone: America/New_York.

```
Where is the filer located?<<var_location>>
Enter the root directory for HTTP files [home/http]:
Do you want to run DNS resolver? [n]: y
Please enter DNS domain name []: <<var_dns_domain_name>>
Please enter the IP address for first nameserver []:<<var_nameserver_ip>>
Do you want another nameserver? [n]:
```

Note: Optionally enter up to three name server IP addresses.

```
Do you want to run NIS client? [n]:
Press the Return key to continue through AutoSupport message
would you like to configure SP LAN interface [y]:
Would you like to enable DHCP on the SP LAN interface [y]: n
Please enter the IP address for the SP: <<var_controller1_sp_ip>>
Please enter the netmask for the SP []: <<var_controller1_sp_mask>>
Please enter the IP address for the SP gateway: <<var_controller1_sp_gateway>>
Please enter the name or IP address of the mail host [mailhost]: <<var_mailhost>>
Please enter the IP address for <<var_mailhost>> []: <<var_mailhost_ip>>
New password: <<var_admin_passwd>>
Retype new password <<var_admin_passwd>>
```

4. Enter the admin password to log in to Controller 1.

Controller 2

1. Enter the configuration values the first time you power on the new system. The configuration values populate these files and configure the installed functionality of the system.
2. Enter the following information:

```
Please enter the new hostname []:<<var_controller2>>

Do you want to enable IPv6? [n]:

Do you want to configure interface groups? [n]:
Please enter the IP address for Network Interface e0a []:
```

Note: Press Enter to accept the blank IP address.

```
Should interface e0a take over a partner IP address during failover? [n]:
Please enter the IP address for the Network Interface e0b []:
Should interface e0b take over a partner IP address during failover? [n]:
Please enter the IP address for the Network Interface e0c []:
Should interface e0c take over a partner IP address during failover? [n]:
Please enter the IP address for the Network Interface e0d []:
Should interface e0d take over a partner IP address during failover? [n]:

Please enter the IP address for Network Interface e0M []: <<var_controller2_e0m_ip>>
Please enter the netmask for the Network Interface e0M [255.255.255.0]:
<<var_controller2_e0m_mask>>

Should interface e0M take over a partner IP address during failover? [n]: y
Please enter the IPv4 address or interface name to be taken over by e0M []: e0M
```

3. Enter the following information:

```
Would you like to continue setup through the Web interface? [n]:

Please enter the name or IP address of the IPv4 default gateway: <<var_controller2_e0m_gateway>>

The administration host is given root access to the storage system's / etc files for system
administration. To allow /etc root access to all NFS clients enter RETURN below.
Please enter the name or IP address for administrative host: <<var_adminhost_ip>>

Please enter timezone [GMT]: <<var_timezone>>
```

Note: Example time zone: America/New York.

```
Where is the filer located? <<var_location>>
Enter the root directory for HTTP files [home/http]:
Do you want to run DNS resolver? [n]: y
Please enter DNS domain name []: <<var_dns_domain_name>>
Please enter the IP address for first nameserver []: <<var_nameserver_ip>>
Do you want another nameserver? [n]:
```

Note: Optionally enter up to three name server IP addresses.

```
Do you want to run NIS client? [n]:
Press the Return key to continue through AutoSupport message
would you like to configure SP LAN interface [y]: enter
Would you like to enable DHCP on the SP LAN interface [y]: n
Please enter the IP address for the SP: <<var_sp_ip>>
Please enter the netmask for the SP []: <<var_sp_mask>>
Please enter the IP address for the SP gateway: <<var_sp_gateway>>
Please enter the name or IP address of the mail host [mailhost]: <<var_mailhost>>
Please enter the IP address for <<var_mailhost>> []: <<var_mailhost_ip>>
New password: <<var_admin_passwd>>
Retype new password <<var_admin_passwd>>
```

4. Enter the admin password to log in to Controller 2.

9.5 64-Bit Aggregates

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

Controller 1

1. Execute the following command to create a new aggregate:

```
aggr create aggr1 -B 64 <<var##_of_disks>>
```

Note: For the small FlexPod Express configuration, <<var##_of_disks>> should equal 5.

Note: For the medium FlexPod Express configuration, <<var##_of_disks>> should equal 17.

Note: aggr1 is not required on Controller 2 because it is set up as an HA pair.

9.6 IFGRP LACP

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

Controller 1 and Controller 2

1. Run the following command on the command line and also add it to the `/etc/rc` file, so it is activated upon boot.

```
ifgrp create lacp ifgrp0 -b ip e0a e0b e0c e0d
wrf file -a /etc/rc "ifgrp create lacp ifgrp0 -b ip e0a e0b e0c e0d"
```

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

9.7 VLAN

Controller 1 and Controller 2

1. Run the following commands to create a VLAN interface for iSCSI data traffic.

```
vlan create ifgrp0 <<var_iscsia_vlan_id>>, <<var_iscsib_vlan_id>>
wrfile -a /etc/rc "vlan create ifgrp0 <<var_iscsia_vlan_id>>, <<var_iscsib_vlan_id>>"
```

9.8 IP Config

Controller 1

1. Run the following commands from the command line:

```
ifconfig ifgrp0-<<var_iscsia_vlan_id>> <<var_controller1_iscsia_ip>> netmask
<<var_controller1_iscsia_mask>> mtusize 9000 partner ifgrp0-<<var_iscsia_vlan_id>>
wrfile -a /etc/rc " ifconfig ifgrp0-<<var_iscsia_vlan_id>> <<var_controller1_iscsia_ip>> netmask
<<var_controller1_iscsia_mask>> mtusize 9000 partner ifgrp0-<<var_iscsia_vlan_id>>"
ifconfig ifgrp0-<<var_iscsib_vlan_id>> <<var_controller1_iscsib_ip>> netmask
<<var_controller1_iscsib_mask>> mtusize 9000 partner ifgrp0-<<var_iscsib_vlan_id>>
wrfile -a /etc/rc " ifconfig ifgrp0-<<var_iscsib_vlan_id>> <<var_controller1_iscsib_ip>> netmask
<<var_controller1_iscsib_mask>> mtusize 9000 partner ifgrp0-<<var_iscsib_vlan_id>>"
```

Controller 2

1. Run the following commands from the command line:

```
ifconfig ifgrp0-<<var_iscsia_vlan_id>> <<var_controller2_iscsia_ip>> netmask
<<var_controller2_iscsia_mask>> mtusize 9000 partner ifgrp0-<<var_iscsia_vlan_id>>
wrfile -a /etc/rc " ifconfig ifgrp0-<<var_iscsia_vlan_id>> <<var_controller2_iscsia_ip>> netmask
<<var_controller2_iscsia_mask>> mtusize 9000 partner ifgrp0-<<var_iscsia_vlan_id>>"
ifconfig ifgrp0-<<var_iscsib_vlan_id>> <<var_controller2_iscsib_ip>> netmask
<<var_controller2_iscsib_mask>> mtusize 9000 partner ifgrp0-<<var_iscsib_vlan_id>>
wrfile -a /etc/rc " ifconfig ifgrp0-<<var_iscsib_vlan_id>> <<var_controller2_iscsib_ip>> netmask
<<var_controller2_iscsib_mask>> mtusize 9000 partner ifgrp0-<<var_iscsib_vlan_id>>"
```

9.9 iSCSI

Controller 1 and Controller 2

1. Add a license for iSCSI.

```
license add <<var_nfs_license>>
```

2. Start iSCSI.

```
iscsi start
```

9.10 Install SnapManager Licenses

Controller 1 and Controller 2

1. Add a license for SnapManager® for Hyper-V™.

```
license add <<var_snapmanager_hyperv_license>>
```

2. Add a license for SnapDrive for Windows.

```
license add <<var_snapdrive_windows_license>>
```

9.11 Storage Controller Active-Active Configuration

Controller 1 and Controller 2

Enable two storage controllers in an active-active configuration.

1. Enter the cluster license on both nodes.

```
license add <<var_cf_license>>
```

2. Reboot each storage controller.

```
reboot
```

3. Log back into both controllers

Controller 1

1. Enable failover on Controller 1, if it is not already enabled.

```
cf enable
```

9.12 Data ONTAP SecureAdmin

Secure API access to the storage controller must be configured.

Controller 1

1. Issue the following as a one-time command to generate the certificates used by the Web services for the API.

```
secureadmin setup -f -q ssl t US "<<var_state>>"  
<<var_city>><<var_org>><<var_unit>><<var_controller1_fqdn>><<var_admin_email>><<var_key_length>>
```

Note: The format for this command is `secureadmin setup -q ssl domestic<t/f> country state locality org unit fqdn email [keylen] [days until expires]`.

Note: Parameters that need more than one word should be placed in quotation marks (").

After the initialization, the CSR is available in the file `/etc/keymgr/csr/secureadmin_tmp.pem`.

2. Configure and enable SSL and HTTPS for API access using the following options:

```
optionshttpd.access none  
optionshttpd.admin.enable on  
optionshttpd.admin.ssl.enable on  
optionsssl.enable on
```

Controller 2

1. Issue the following as a one-time command to generate the certificates used by the Web services for the API.

```
secureadmin setup -f -q ssl t US "<<var_state>>"  
<<var_city>><<var_org>><<var_unit>><<var_controller2_fqdn>><<var_admin_email>><<var_key_length>>
```

The format for this command is:

```
secureadmin setup -q ssl domestic<t/f> country state locality org unit fqdn email [keylen] [days  
until expires]
```

Parameters that need more than one word should be placed in quotation marks (").

After the initialization, the CSR is available in the file `/etc/keymgr/csr/secureadmin_tmp.pem`.

2. Configure and enable SSL and HTTPS for API access using the following options:

```
options httpd.access none
options httpd.admin.enable on
options httpd.admin.ssl.enable on
options ssl.enable on
```

9.13 Secure Shell

SSH must be configured and enabled.

Controller 1 and Controller 2

1. Use the following one-time command to generate host keys.

```
secureadmin disable ssh
secureadmin setup -f -q ssh 768 512 1024
```

2. Use the following options to configure and enable SSH.

```
options ssh.idle.timeout 60
options autologout.telnet.timeout 5
```

9.14 AutoSupport HTTPS

AutoSupport™ sends the support summary information to NetApp through HTTPS.

Controller 1 and Controller 2

1. Execute the following commands to configure AutoSupport:

```
options autosupport.noteto <<var_admin_email>>
```

9.15 Security Best Practices

Note: Apply the following commands according to local security policies.

Controller 1 and Controller 2

1. Run the following commands to enhance security on the storage controller:

```
options rsh.access none
options webdav.enable off
options security.passwd.rules.maximum 14
options security.passwd.rules.minimum.symbol 1
options security.passwd.lockout.numtries 6
options autologout.console.timeout 5
```

9.16 Enable NDMP

Run the following command to enable NDMP.

Controller 1 and Controller 2

```
options ndmpd.enable on
```

9.17 Create FlexVol Volumes

Controller 1

1. Create two FlexVol® volumes on Controller 1 using the following commands:

```
vol create hyperv_quorum -s none aggr1 10g
snap reserve hyperv_quorum 0
```

```
snap sched hyperv_quorum 0 0 0

vol create infra_datastore_1 -s none aggr1 500g
snap reserve infra_datastore_1 0
sis on /vol/infra_datastore_1
```

9.18 Enable CDP

Use the following step to enable CDP on Controller 1 and Controller 2.

Controller 1 and Controller 2

1. Enable CDP.

```
options cdpd.enable on
```

10 Cisco Unified Computing System C-Series Server Deployment Procedure

This section provides the detailed procedure for configuring a Cisco Unified Computing System C-Series standalone server for use in either small or medium FlexPod Express configurations.

10.1 Perform Initial Cisco UCS C-Series Standalone Server CIMC Setup

These steps describe the setup of the initial Cisco UCS C-Series standalone server.

All Servers

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



Press <F2> to enter setup, <F6> Boot Menu, <F8> CIMC Config, <F12> Network Boot

Bios Version: C220M3.1.4.4c.0.022220121951
Platform ID: C220M3

CIMC IP Address : 10.61.186.94
CIMC MAC Address : 50:3D:E5:9E:32:C2

Processor(s) Intel(R) Xeon(R) CPU E5-2609 0 @ 2.40GHz
Total Memory = 64 GB Effective Memory = 64 GB
Memory Operating Speed 1066 Mhz

92

3. In the CIMC Configuration Utility, set the following options:
 - a. NIC mode:
 - Dedicated ☒ [X]
 - b. IPV4 (Basic):
 - DHCP enabled: ☐ []
 - CIMC IP: <<var_cimc_ip>>
 - Subnet mask: <<var_cimc_mask>>
 - Gateway: <<var_cimc_mask>>
 - c. VLAN (Advanced): Leave this option cleared to disable VLAN tagging.
 - d. NIC redundancy: None.
 - e. Factory Defaults: Leave this option cleared.
 - f. Default User (Basic):
 - Default password: <<var_admin_passwd>>
 - Reenter password: <<var_password>>

```
CIMC Configuration Utility  Version 1.5  Cisco Systems, Inc.
*****
NIC Properties
NIC mode
Dedicated:      [X]
Shared LOM:     [ ]
Shared LOM 10G: [ ]
Cisco Card:     [ ]
NIC redundancy
None:           [X]
Active-standby: [ ]
Active-active:  [ ]
IPV4 (Basic)
DHCP enabled:   [ ]
CIMC IP:        10.61.186.94
Subnetmask:     255.255.255.0
Gateway:        10.61.186.1
Factory Defaults
CIMC Factory Default:[ ]
Default User (Basic)
Default password:
Reenter password:
VLAN (Advanced)
VLAN enabled:   [ ]
VLAN ID:        1
Priority:        0
*****
<Up/Down arrow> Select items    <F10> Save    <Space bar> Enable/Disable
<F5> Refresh                    <ESC> Exit
```

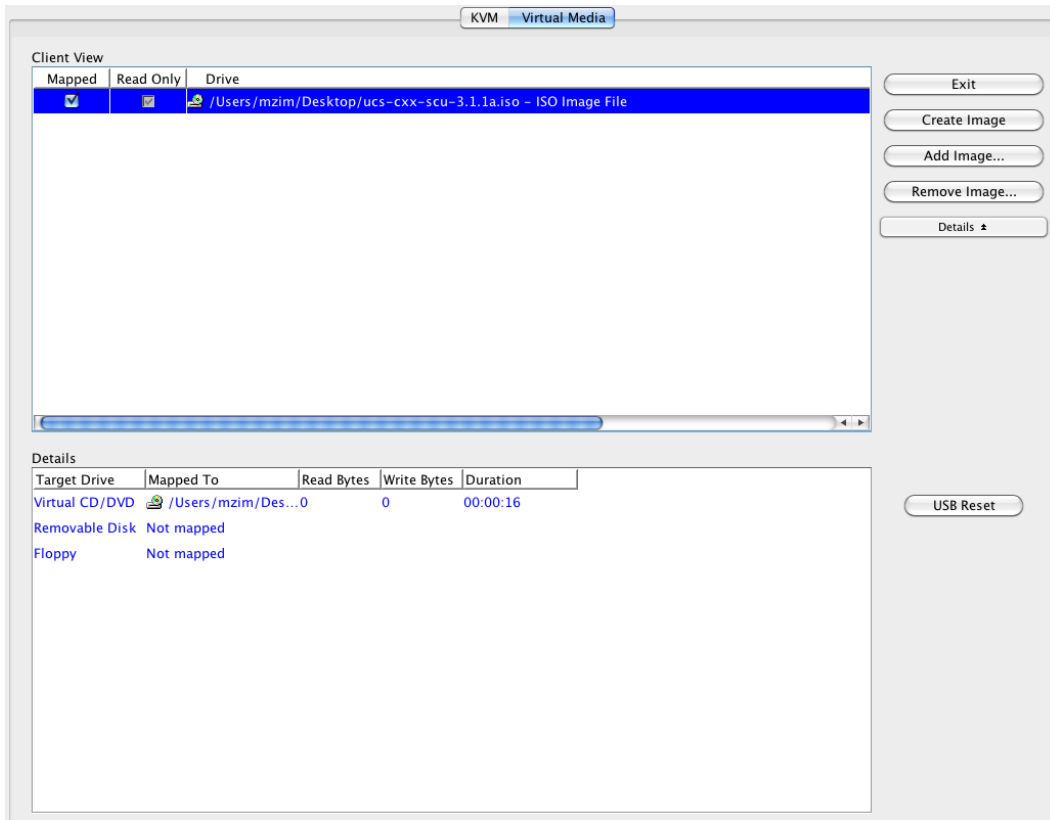
4. Press F10 to save the CIMC interface configuration.
5. After the configuration is saved, press Esc to exit.

10.2 Configure Cisco UCS C-Series RAID Configuration

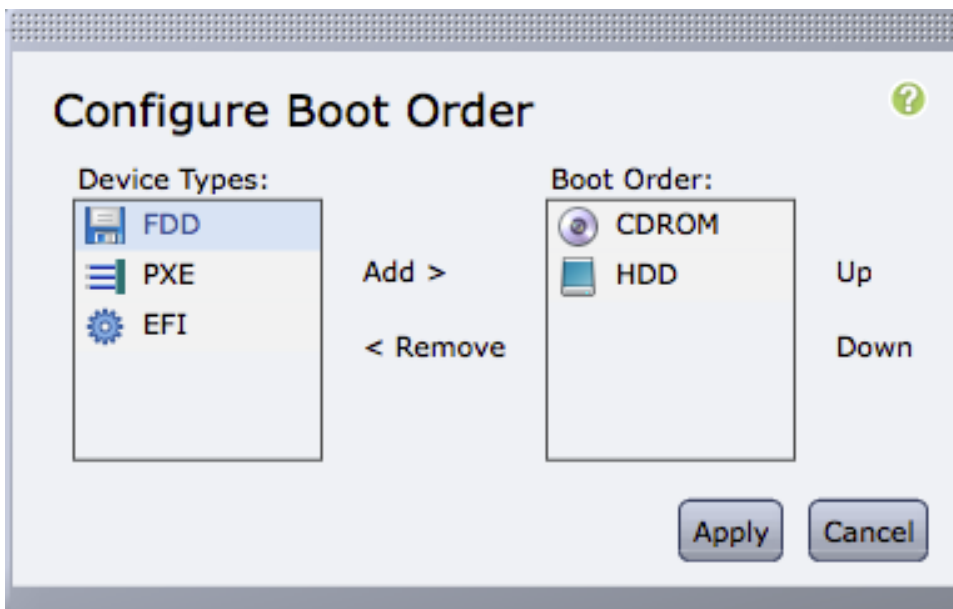
1. Open a Web browser and browse to the CIMC interface IP address.
2. Log in to the CIMC interface using the default user name `admin` and the admin password: `<<var_admin_passwd>>` set in the CIMC interface setup.



3. Once successfully logged in, click the Server tab and choose Summary. Select Launch KVM Console.
4. The virtual KVM window will open. Select Virtual Media at the top of the window.
5. Click Add Image....
6. Browse to the location of the Server Configuration Utility ISO image and select it. Click Open.
7. Select the Mapped checkbox next to the selected ISO image to map the image to the server.



8. Return to the CIMC interface browser page (do not close the virtual KVM window), click the Server tab, and choose BIOS.
9. Select Configure Boot Order and click OK.
10. Add both the CDROM and HDD options to the Boot Order field. Click Apply.



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.
13. The server should now boot into the Server Configuration utility.
14. Click the Server Configuration tab in the left pane.
15. Select RAID Configuration.
16. In the upper-right corner, click the Configure button. 
17. From the RAID Level drop-down menu, select Automatic setup with redundancy. Click Create Array.
18. After the RAID configuration completes, close the virtual KVM window.
25. Return to the CIMC interface browser window. Click the Server tab and then select 0. Select Power Off Server.

11 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.

Multiple 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.

11.1 Log 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. One must log in to the CIMC interface to execute the virtual KVM, which enables the administrator to begin installation of the operating system through remote media.

All Hosts

1. Navigate to a Web browser and enter the IP address for the Cisco 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, select the Server tab.
4. Click Launch KVM Console.

11.2 Set Up the 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. Select Add Image in the right pane.
3. Browse to the Windows Server 2012 installer ISO image file and click Open.
4. Map the image that you just added by selecting Mapped.
5. To boot the server, select the KVM tab.
6. Select Power On Server in the CIMC interface Summary tab, and then click OK.

11.3 Install Windows Server 2012

The following steps describe the installation of Windows Server 2012 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 Datacenter (Server with a GUI) and click Next.
Note: You may optionally remove the GUI after the Hyper-V cluster is operational.
6. After reviewing the EULA, select "I accept the license terms" 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 by clearing the Mapped checkbox.
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. When Windows is finished installing, enter an administrator password on the settings page and click Finish.

11.4 Install .NET Framework 3.5 Feature

The following steps describe how to install the .NET Framework 3.5 feature from Windows Server 2012 Installation media.

All Hosts

1. From the Cisco CIMC virtual KVM Console, select the Virtual Media tab.
2. Select Add Image in the right pane.
3. Browse to the Windows Server 2012 installer ISO image file and click Open.
4. Map the image that you just added by selecting Mapped.
5. Log in to Windows with the administrator password previously entered during installation.
6. Launch a Windows PowerShell™ prompt by right-clicking the PowerShell icon in the taskbar and selecting Run as Administrator.
7. Add the .NET 3.5 feature by entering the following command:

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

Note: The preceding command assumes that the ISO image is mounted to drive E:\.

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

11.5 Configure Windows Networking for FlexPod Express

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

All Hosts

1. Log in with the administrator password previously entered during installation.
2. Launch a Windows 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 switchport on the switch. Rename the port to match its intended use.

Example:

```
Rename-NetAdapter -Name Ethernet -NewName Public0
Rename-NetAdapter -Name "Ethernet 2" -NewName iSCSI-A
Rename-NetAdapter -Name "Ethernet 3" -NewName LM
Rename-NetAdapter -Name "Ethernet 4" -NewName Public1
Rename-NetAdapter -Name "Ethernet 5" -NewName iSCSI-B
Rename-NetAdapter -Name "Ethernet 6" -NewName CSV
```

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

4. Configure jumbo frames.

```
Set-NetAdapterAdvancedProperty -Name iSCSI-A, iSCSI-B, CSV, LM -DisplayName "Jumbo Packet" -
DisplayValue "9014 Bytes" -EA SilentlyContinue
Set-NetAdapterAdvancedProperty -Name iSCSI-A, iSCSI-B, CSV, LM -DisplayName "Jumbo Packet" -
DisplayValue "9014" -EA SilentlyContinue
```

5. Create a NIC team from a Windows PowerShell prompt.

```
New-NetLbfoTeam -Name TM1 -TeamMembers VMComm* -TeamingMode lacp
```

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

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

7. Create team NICs for the VM traffic and management VLANs.

```
Add-NetLbfoTeamNic -Team TM1 -VlanID <<var_vmtraffic_vlan_id>> -Name VMComm
Add-NetLbfoTeamNic -Team TM1 -VlanID <<var_mgmt_vlan_id>> -Name Mgmt
```

8. Set IP address information for each host NIC.

```
New-NetIPAddress -InterfaceAlias Mgmt -IPAddress <Mgmt_Ipaddress> -DefaultGateway
<<Mgmt_gateway>> -PrefixLength <Mgmt_network_prefix>
New-NetIPAddress -InterfaceAlias iSCSI-A -IPAddress <iscsia_ipaddress> -Prefix <iscsia_prefix>
New-NetIPAddress -InterfaceAlias iSCSI-B -IPAddress <iscsib_ipaddress> -Prefix <iscsib_prefix>
New-NetIPAddress -InterfaceAlias LM -IPAddress <lm_ipaddress> -Prefix <lm_prefix>
New-NetIPAddress -InterfaceAlias CSV -IPAddress <csv_ipaddress> -Prefix <csv_prefix>
```

9. Disable DNS registration for all NICs.

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

10. Turn registration back on and configure DNS for the management NIC.

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

11. Rename the host.

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

12. Add the host to Active Directory®.

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

13. Add the Hyper-V, failover clustering, and multipath I/O features.

```
Add-WindowsFeature Hyper-V, Failover-Clustering, Multipath-IO -IncludeManagementTools -Restart
```

14. Configure Windows Server 2012 MSDSM to claim any NetApp LUNs.

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

15. Create Hyper-V virtual switch for the VM traffic NIC.

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

16. 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
```

17. Configure jumbo frames.

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

11.6 Install 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 about the installation, see the Administration and Installation Guide.

All Hosts

1. Download Windows iSCSI Host Utilities from http://support.netapp.com/NOW/download/software/kit_iscsi/microsoft/6.0.1/netapp_windows_host_utilities_6.0.1_x64.msi.
2. Unblock the downloaded file.

```
Unblock-file ~\Downloads\netapp_windows_host_utilities_6.0.1_x64.msi
```

3. Install the Host Utilities.

```
~\Downloads\netapp_windows_host_utilities_6.0.1_x64.msi /qn "MULTIPATHING=1"
```

11.7 Configure Windows Host iSCSI Initiator

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

All Hosts

1. Launch a Windows 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 RR
```

6. Configure an iSCSI target for each controller.

```
New-IscsiTargetPortal -TargetPortalAddress <<var_controller1_iscsia_ip>> -InitiatorPortalAddress  
<iscsia_ipaddress>  
New-IscsiTargetPortal -TargetPortalAddress <<var_controller2_iscsia_ip>> -InitiatorPortalAddress  
<iscsia_ipaddress>
```

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

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

11.8 Install NetApp SnapDrive

This 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.

All Hosts

1. Download SnapDrive installer from http://support.netapp.com/NOW/download/software/snapdrive_win/6.5/SnapDrive6.5_x64.exe.
2. Unblock the downloaded file from Windows PowerShell.

```
Unblock-file ~\Downloads\SnapDrive6.5_x64.exe
```

3. Change directory to the Downloads folder.

```
cd ~\Downloads
```

4. Launch a Windows cmd shell.

```
Cmd
```

5. Install SnapDrive utilizing the noninteractive installation.

```
SnapDrive6.5_x64.exe /s /v"/qb SILENT_MODE=1 /Li <<var_sdw_install_log>>
INSTALLDIR="<<var_sdw_install_path>>" SVCUSERNAME=<<var_sdw_install_username>>
SVCUSERPASSWORD=<<var_sdw_install_password>> SVCCONFIRMUSERPASSWORD=<<var_sdw_install_password>>
SDW_WEBSRV_TCP_PORT=808 SDW_WEBSRV_HTTP_PORT=4098 TRANSPORT_SETTING_ENABLE=0
IGNORE_COMPMGMT_RUNNING=1 ADD_WINDOWS_FIREWALL=1"
```

6. After the installation is finished, launch a new Windows 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.

7. Configure SnapDrive preferred IP settings for each controller.

```
sdcli preferredIP set -f <<var_controller1>> -IP <<var_controller1_e0m_ip>>
sdcli preferredIP set -f <<var_controller2>> -IP <<var_controller2_e0m_ip>>
```

8. Configure SnapDrive transport protocol authentication configuration for each controller.

```
sdcli transport_protocol set -f <<var_controller1>> -type https -user root -pwd
<<var_admin_passwd>>
sdcli transport_protocol set -f <<var_controller2>> -type https -user root -pwd
<<var_admin_passwd>>
```

11.9 Install NetApp SnapManager for Hyper-V

All Hosts

1. Download the SnapManager for Hyper-V installer from http://support.netapp.com/NOW/download/software/snapmanager_hyperv_win/1.2/SMHV1.2_NetApp_x64.exe.
2. Unblock the downloaded file.

```
Unblock-file ~\Downloads\SMHV1.2_NetApp_x64.exe
```

3. Install SnapManager for Hyper-V.

```
~\Downloads\SMHV1.2_NetApp_x64.exe /s /v"/qn SILENT MODE=1 /Li <<var_smhv_install_log>>
SVCUSERNAME=<<var_smhv_install_username>> SMHVSrv_PASSWORD=<<var_smhv_install_password>>
SMHVSrv_CONFIRMUSERPASSWORD=<<var_smhv_install_password>>"
```

11.10 Create a Cluster

One Server Only

1. Launch a Windows 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>
```

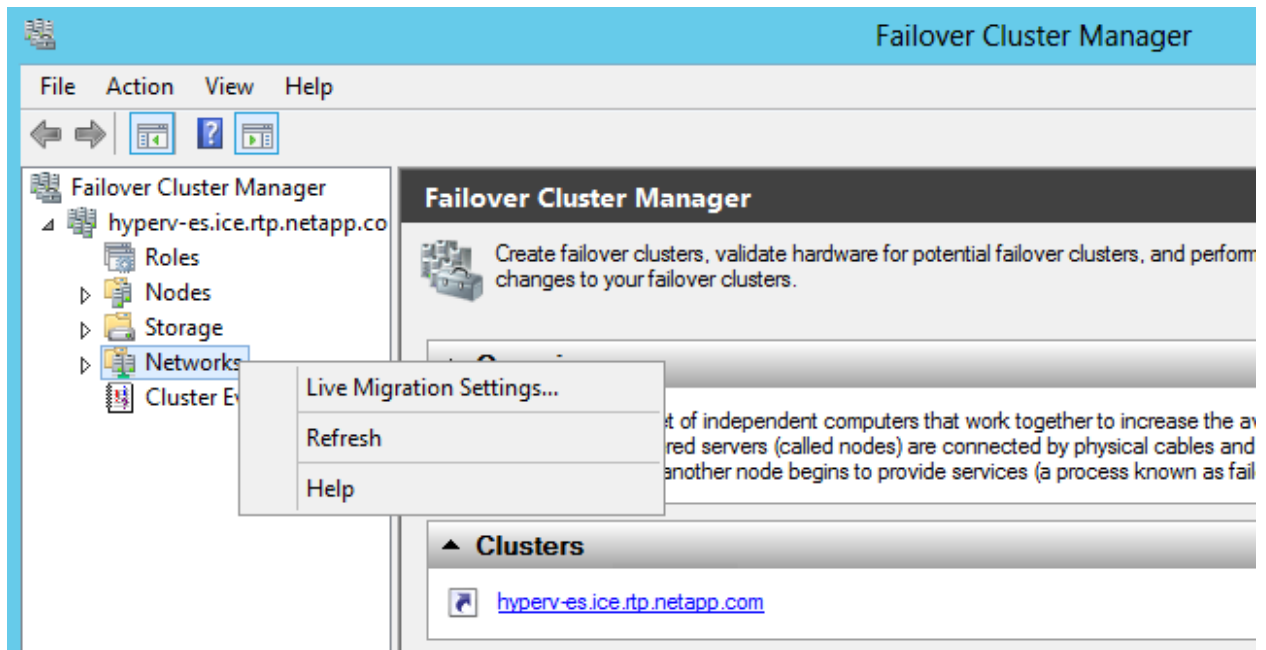
3. Rename cluster networks.

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

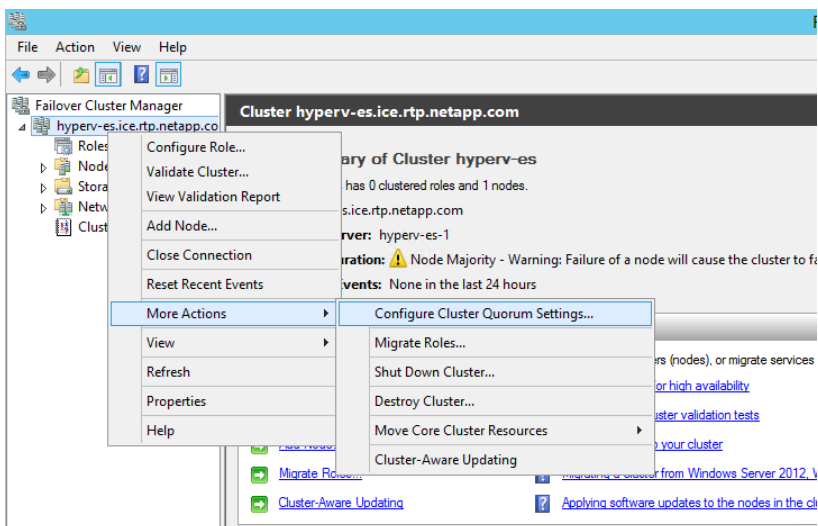
```
(Get-ClusterNetwork -Name CSV).Metric = 900
```

5. Configure Live Migration network.
 - a. Open Failover Cluster Manager from Server Manager, select Tools > Failover Cluster Manager.
 - b. Expand the Cluster tree on the left. Right-click Networks and select Live Migration Settings...



- c. Clear all but the LM network settings and click OK.
6. Change the cluster to use a Quorum Disk.

- a. Open SnapDrive from the start screen to configure cluster storage.
- b. In the SnapDrive main page, open the Server name, and then select the Disks icon.
- c. Right-click the Disks Icon and choose to Create Disk.
- d. Type the IP Address of the controller that contains the Cluster Quorum Volume.
- e. Once connected, open the controller tree and select the Cluster Quorum Volume.
- f. Type the name of the LUN in the LUN NAME box and click Next.
- g. Select Shared (Microsoft Cluster Services only) and click Next.
- h. Validate that all nodes of the cluster are shown and click Next.
- i. Change the drive letter to Q:, set the LUN size to be 5GB, and click Next.
- j. Click Next through the Volume properties confirmation.
- k. Select the iSCSI initiators to map the LUN and click Next.
- l. Select Automatic igroup management and click Next.
- m. Select the Available Storage cluster group, and click Next.
- n. Click Finish.
- o. Make sure that the Q: drive is accessible on all of the nodes.
- p. In failover cluster manager, select Configure Cluster Quorum Settings...



- q. Select Add or Change the quorum witness, and click Next.
 - r. Select Configure a disk witness, and click Next.
 - s. Select Disk Q: from available storage and click Next.
 - t. Click Next through the confirmation screen and Finish on the summary screen.
7. Create CSV LUN for VM storage.
- a. Open SnapDrive from the start screen to configure cluster storage.
 - b. From SnapDrive, open the Server name, and then select the Disks icon.
 - c. Right-click the Disks Icon and choose to Create Disk.
 - d. Type the IP Address of the controller that contains the infra CSV Volume.
 - e. Once connected, open the controller tree and select the infra CSV Volume.
 - f. Type the name of the LUN in the LUN NAME box and click Next.
 - g. Select Shared (Microsoft Cluster Services only) 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 500GB, and click Next.
 - j. Click Next through the Volume properties confirmation.
 - k. Select the iSCSI initiators 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.

12 Bill of Materials

The following information details the hardware and software components used in validating both the small and medium FlexPod Express configurations included in this document.

Small Configuration

Table 9) Small configuration components.

Part Number	Product Description	Quantity Required
Cisco Components		
UCSC-EPOD-C220E-S	Cisco UCS Smart Play Bundle – FlexPod Express Small	1
N3K-UCS3048-F	Cisco Nexus 3048 for Cisco UCS Smart Play	2
N3KUK9-503U3.2	NX-OS Release 5.0(3)U3(2)	2
N2200-PAC-400W	N2K/N3K AC Power Supply, Std airflow (port side exhaust)	4
N3K-C3048-FAN	Cisco Nexus 3048 Fan Module, Port-side Exhaust	2
N3K-C3064-ACC-KIT	Cisco Nexus 3064PQ Accessory Kit	2
UCS-SP5-C220E	Cisco UCS C220 M3 SFF w/ 2650 8x8GB 5709 1Gb 2PS	2
N20-BBLKD	Cisco UCS 2.5 inch HDD blanking panel	16
N2XX-ABPCI03-M3	Broadcom 5709 Quad Port 1Gb w/TOE iSCSI for M3 Servers	2
UCS-CPU-E5-2650	2.00 GHz E5-2650/95W 8C/20MB Cache/DDR3 1600MHz	4
UCS-MR-1X082RY-A	8GB DDR3-1600-MHz RDIMM/PC3-12800/dual rank/1.35v	16
UCSC-HS-C220M3	Heat Sink for Cisco UCS C220 M3 Rack Server	4
UCSC-PCIF-01H	Half height PCIe filler for Cisco UCS	2
UCSC-PSU-650W	650W power supply for C-series rack servers	4
UCSC-RAID-11-C220	Cisco UCS RAID SAS 2008M-8i Mezz Card for C220 (0/1/10/5/50)	2
UCSC-RAIL1	Rail Kit for C220 C22 C24 rack servers	2
UCS-SP-600GB-HDD	600GB 6Gb SAS 10K RPM SFF HDD	4
CON-UCW5-SP5C220E	Cisco UCS HW 8X5XNBDOS Cisco UCS C220 M3 Rack Server	2
CON-SNTP-UCS3048F	Cisco SMARTnet® 24X7X4 Cisco Nexus 3048 for Cisco UCS Smart Play	2
NetApp Components		
FAS2220-R6		1

Part Number	Product Description	Quantity Required
FAS2220A-12X600-R6	FAS2220,HA,12x600GB,10k,Dual CNTLR	1
FAS2220A-HA-SW-R6	FAS2220A,HA CFO Software	2
SW-2220A-ONTAP8-P	SW, Data ONTAP Essentials,2220A,-P	2
SW-CIFS-C	SW,CIFS,-C	2
SW-FCP-C	SW,FCP,-C	2
SW-ISCSI-C	SW, iSCSI,-C	2
SW-NFS-C	SW,NFS,-C	2
X5518A-R6	Rack Mount Kit,FAS2020/40,R6	1
X800-42U-R6	Cabinet Component Power Cable,R6	2
Use NetApp QuoteEdge to determine part number	SupportEdge Standard, Premium or equivalent service from an authorized support services partner ¹	1

Medium Configuration

Table 10) Medium configuration components.

Part Number	Product Description	Quantity Required
Cisco Components		
UCSC-EPOD-C220E-M	Cisco UCS Smart Play Bundle - FlexPod Express Medium	1
N3K-UCS3048-F	Cisco Nexus 3048 for Cisco UCS Smart Play	2
N3KUK9-503U3.2	NX-OS Release 5.0(3)U3(2)	2
N2200-PAC-400W	N2K/N3K AC Power Supply, Std airflow (port side exhaust)	4
N3K-C3048-FAN	Cisco Nexus 3048 Fan Module, Port-side Exhaust	2
N3K-C3064-ACC-KIT	Cisco Nexus 3064PQ Accessory Kit	2
UCS-SP5-C220E	Cisco UCS C220 M3 SFF w/ 2650 8x8GB 5709 1Gb 2PS	4
N20-BBLKD	Cisco UCS 2.5 inch HDD blanking panel	32
N2XX-ABPCI03-M3	Broadcom 5709 Quad Port 1Gb w/TOE iSCSI for M3 Servers	4
UCS-CPU-E5-2650	2.00 GHz E5-2650/95W 8C/20MB Cache/DDR3 1600MHz	8
UCS-MR-1X082RY-A	8GB DDR3-1600-MHz RDIMM/PC3-12800/dual rank/1.35v	32
UCSC-HS-C220M3	Heat Sink for Cisco UCS C220 M3 Rack Server	8
UCSC-PCIF-01H	Half height PCIe filler for Cisco UCS	4
UCSC-PSU-650W	650W power supply for C-series rack servers	8
UCSC-RAID-11-C220	Cisco UCS RAID SAS 2008M-8i Mezz Card for C220 (0/1/10/5/50)	4
UCSC-RAIL1	Rail Kit for C220 C22 C24 rack servers	4
UCS-SP-600GB-HDD	600GB 6Gb SAS 10K RPM SFF HDD	8

¹ SupportEdge Premium required for Cooperative Support

Part Number	Product Description	Quantity Required
CON-UCW5-SP5C220E	Cisco UCS HW 8X5XNBDOS Cisco UCS C220 M3 Rack Server	4
CON-SNTP-UCS3048F	Cisco SMARTnet 24X7X4 Cisco Nexus 3048 for Cisco UCS Smart Play	2
NetApp Components		
FAS2240-2-R5		1
F2240A-2-24X600-R5	FAS2240-2,HA,24x600GB,Dual CTL	1
FAS2240A-HA-SW-R5	FAS2240A, HA CFO Software, R5	2
SW-2240A-ONTAP8-P	SW, Data ONTAP Essentials, 2240A,-P	2
SW-CIFS-C	SW,CIFS,-C	2
SW-FCP-C	SW,FCP,-C	2
SW-ISCSI-C	SW, iSCSI,-C	2
SW-NFS-C	SW,NFS,-C	2
X5526A-R6	Rackmount Kit,4-Post,Universal,R6	1
X6557-R6	Cable, SASCntlr-Shelf/Shelf-Shelf/HA,0.5m	2
X6560-R6	Cable,Ethernet,0.5m RJ45 CAT6	1
X800-42U-R6	Cabinet Component Power Cable,R6	2
Use NetApp QuoteEdge to determine part number	SupportEdge Standard, Premium or equivalent service from an authorized support services partner ²	1

² SupportEdge Premium required for Cooperative Support

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

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

Go further, faster®