Technical Report

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

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

October 2014 | TR-4339
TABLE OF CONTENTS

1 Overview ................................................................................................................................................. 6

2 Audience .................................................................................................................................................. 6

3 Architecture ............................................................................................................................................. 6
   3.1 Small Configuration .......................................................................................................................... 6
   3.2 Medium Configuration ..................................................................................................................... 7

4 Hardware Details ..................................................................................................................................... 8
   4.1 Small Configuration ........................................................................................................................ 8
   4.2 Medium Configuration ..................................................................................................................... 8

5 Software Details ..................................................................................................................................... 9

6 Configuration Guidelines ........................................................................................................................ 9

7 FlexPod Express Cabling Information .................................................................................................... 16
   7.1 FlexPod Express Small Configuration ........................................................................................... 16
   7.2 FlexPod Express Medium Configuration ....................................................................................... 20

8 Cisco Nexus 3048 Deployment Procedure .............................................................................................. 24
   8.1 Upgrading the Software (Optional) ................................................................................................. 25
   8.2 Enabling Advanced Features ......................................................................................................... 26
   8.3 Performing Global PortChannel Configuration ............................................................................. 26
   8.4 Performing Global Spanning-Tree Configuration .......................................................................... 26
   8.5 Configuring Jumbo Frames .............................................................................................................. 27
   8.6 Defining VLANs .............................................................................................................................. 27
   8.7 Configuring Access and Management Port Descriptions ............................................................. 27
   8.8 Configuring Server and Storage Management Interfaces ............................................................ 28
   8.9 Performing Virtual PortChannel Global Configuration ............................................................... 29
   8.10 Configuring Storage PortChannels ............................................................................................... 30
   8.11 Configuring Server Connections ................................................................................................. 30
   8.12 Performing In-Band Management SVI Configuration ................................................................ 34
   8.13 Saving the Configuration .............................................................................................................. 34
   8.14 Uplinking to Existing Network Infrastructure ............................................................................ 34

9 NetApp FAS Storage Deployment Procedure ......................................................................................... 34
   9.1 Controller FAS25xx Series ............................................................................................................. 34
   9.2 Configuring NetApp Clustered Data ONTAP 8.2.2 ....................................................................... 35
   9.3 Creating Clusters in NetApp Clustered Data ONTAP ................................................................... 39
9.4 Joining Clusters in NetApp Clustered Data ONTAP .......................................................... 41
9.5 Changing the RAID Configuration on Root Aggregates .................................................. 42
9.6 Zeroing All Spare Disks ...................................................................................................... 42
9.7 Configuring ifgrp LACP in NetApp Clustered Data ONTAP ........................................... 42
9.8 Configuring VLANs in Clustered Data ONTAP ................................................................. 43
9.9 Migrating the Cluster Management Interface on Controller 01 ........................................ 43
9.10 Logging in to the Cluster .................................................................................................. 43
9.11 Setting Auto-Revert on Cluster Management ................................................................. 43
9.12 Configuring Failover Group Management in Clustered Data ONTAP ............................ 43
9.13 Assigning the Management Failover Group to the Cluster Management LIF ............... 43
9.14 Configuring Failover Group Node Management in Clustered Data ONTAP .................. 44
9.15 Assigning Node Management Failover Groups to Node Management LIFs .................. 44
9.16 Creating Aggregates ........................................................................................................ 44
9.17 Configuring the Service Processor .................................................................................. 44
9.18 Configuring Jumbo Frames in Clustered Data ONTAP ................................................... 45
9.19 Configuring NTP in Clustered Data ONTAP .................................................................. 45
9.20 Configuring SNMP in Clustered Data ONTAP ............................................................... 46
9.21 Configuring SNMPv1 in Clustered Data ONTAP ............................................................ 46
9.22 Configuring SNMPv3 in Clustered Data ONTAP ............................................................ 46
9.23 Configuring AutoSupport HTTPS in Clustered Data ONTAP ....................................... 46
9.24 Configuring Cisco Discovery Protocol in Clustered Data ONTAP ................................ 47
9.25 Setting Up Vserver .......................................................................................................... 47
9.26 Configuring iSCSI Service in Clustered Data ONTAP .................................................... 48
9.27 Configuring HTTPS Access in Clustered Data ONTAP .................................................. 48
9.28 Configuring FlexVol in Clustered Data ONTAP ............................................................. 49
9.29 Configuring iSCSI LIF in Clustered Data ONTAP ......................................................... 49
9.30 Configuring Failover Group Vserver Management in Clustered Data ONTAP ............ 49
9.31 Adding an Infrastructure Vserver Administrator ............................................................ 50

10 Cisco UCS C-Series Rack Server Deployment Procedure ................................................. 50
    10.1 Performing Initial Cisco UCS C-Series Standalone Server Setup for Cisco IMC ........... 50
    10.2 Configuring Cisco UCS C-Series RAID Configuration ............................................... 53

11 Windows Server 2012 Deployment Procedure .................................................................. 56
    11.1 Logging in to the Cisco UCS C-Series Standalone Server IMC Interface ..................... 56
    11.2 Setting Up the Windows Server 2012 Installation ....................................................... 57
    11.3 Installing Windows Server 2012 .................................................................................. 57
LIST OF FIGURES

Figure 1) Physical topology of FlexPod Express small configuration. .................................................................7
Figure 2) Physical topology of FlexPod Express medium configuration. .............................................................8
Figure 3) FlexPod Express small configuration cabling diagram. ........................................................................17
Figure 4) FlexPod Express medium configuration cabling diagram. ...................................................................20
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, 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 demands of the business.

2 Audience

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

3 Architecture

Both the small and medium FlexPod Express configurations use Cisco Unified Computing System™ C-Series rack servers, Cisco Nexus® switches, and NetApp FAS storage (NetApp clustered Data ONTAP: switchless). Although FlexPod Express supports an open ecosystem of virtualization and management software solutions, the architecture described in this document specifically includes VMware vSphere® virtualization and Cisco UCS® Director software. NetApp strongly recommends virtualization software and infrastructure management software as part of every FlexPod Express deployment. Each configuration uses the best practices for each component to enable a reliable, enterprise-class infrastructure.

3.1 Small Configuration

The small configuration consists of the following components:

- Cisco Nexus 3048 switches
- Cisco UCS C220 M3 rack servers
- NetApp FAS2520 storage controllers
- Microsoft® Windows Server® 2012 R2
- System Center 2012 R2 Virtual Machine Manager
3.2 Medium Configuration

The medium configuration consists of the following components:

- Cisco Nexus 3048 switches
- Cisco UCS C220 M3 rack servers
- NetApp FAS2520 storage controllers
- Windows Server 2012 R2 Hyper-V®
- System Center 2012 R2 Virtual Machine Manager
4 Hardware Details

4.1 Small Configuration
Table 1 details the hardware and software configuration of a small FlexPod Express configuration.

Table 1) Small configuration details.

<table>
<thead>
<tr>
<th>Layer</th>
<th>Component</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute</td>
<td>Cisco UCS C220 M3 servers (Standalone)</td>
<td>2</td>
</tr>
<tr>
<td>Network</td>
<td>Cisco Nexus 3048 switches</td>
<td>2</td>
</tr>
<tr>
<td>Storage</td>
<td>NetApp FAS2520 (high-availability pair)</td>
<td>1</td>
</tr>
<tr>
<td>Disks</td>
<td>900GB 10K SAS</td>
<td>12</td>
</tr>
</tbody>
</table>

4.2 Medium Configuration
Table 2 details the hardware and software configuration of a small FlexPod Express configuration.

Table 2) Medium configuration details.

<table>
<thead>
<tr>
<th>Layer</th>
<th>Component</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute</td>
<td>Cisco UCS C220 M3 servers (standalone)</td>
<td>4</td>
</tr>
<tr>
<td>Network</td>
<td>Cisco Nexus 3048 switches</td>
<td>2</td>
</tr>
<tr>
<td>Storage</td>
<td>NetApp FAS2520 (high-availability pair)</td>
<td>1</td>
</tr>
</tbody>
</table>
5 Software Details

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

Table 3) Software details.

<table>
<thead>
<tr>
<th>Layer</th>
<th>Component</th>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute</td>
<td>Cisco UCS C220 M3 rack servers (Standalone)</td>
<td>2.0(1a)</td>
<td>Cisco® Integrated Management Controller (IMC) software</td>
</tr>
<tr>
<td>Network</td>
<td>Cisco Nexus 3048 Gigabit Ethernet switches</td>
<td>6.0(2)U2(3)</td>
<td>Cisco NX-OS software</td>
</tr>
<tr>
<td>Storage</td>
<td>NetApp FAS2520 HA</td>
<td>8.2.2</td>
<td>Data ONTAP software</td>
</tr>
<tr>
<td>Software</td>
<td>Microsoft Windows Server 2012 R2 Hyper-V</td>
<td>2012 R2</td>
<td>Virtualization hypervisor</td>
</tr>
<tr>
<td></td>
<td>System Center Virtual Machine Manager</td>
<td>2012 R2</td>
<td>Virtualization management</td>
</tr>
<tr>
<td></td>
<td>NetApp Data ONTAP SMI-S Agent</td>
<td>5.1.1</td>
<td>SMI-S Agent</td>
</tr>
<tr>
<td></td>
<td>NetApp Windows® Host Utilities Kit</td>
<td>6.0.2</td>
<td>NetApp plug-in for Windows</td>
</tr>
<tr>
<td></td>
<td>NetApp SnapDrive® for Windows</td>
<td>7.0.3</td>
<td>LUN provisioning and NetApp Snapshot® management</td>
</tr>
<tr>
<td></td>
<td>NetApp SnapManager® for Hyper-V</td>
<td>2.0.3</td>
<td>NetApp plug-in for Hyper-V</td>
</tr>
</tbody>
</table>

6 Configuration Guidelines

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

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

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

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

This document is intended to enable you to fully configure the FlexPod Express environment. In this process, various steps require you to insert customer-specific naming conventions, IP addresses, and VLAN schemes. Table 4 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 4) Required VLANs.

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>VLAN Purpose</th>
<th>ID Used in Validating This Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>VLAN for management interfaces</td>
<td>186</td>
</tr>
<tr>
<td>Native</td>
<td>VLAN to which untagged frames are assigned</td>
<td>2</td>
</tr>
<tr>
<td>iSCSI-A</td>
<td>VLAN for iSCSI traffic</td>
<td>10</td>
</tr>
<tr>
<td>iSCSI-B</td>
<td>VLAN for iSCSI traffic</td>
<td>20</td>
</tr>
<tr>
<td>LiveMigration</td>
<td>VLAN designated for the movement of virtual machines (VMs) from one physical host to another</td>
<td>30</td>
</tr>
<tr>
<td>Cluster</td>
<td>VLAN for cluster communication and CSV traffic</td>
<td>40</td>
</tr>
<tr>
<td>VM Traffic</td>
<td>VLAN for VM application traffic</td>
<td>50</td>
</tr>
</tbody>
</table>

Table 5) Hyper-V virtual machines created.

<table>
<thead>
<tr>
<th>Virtual Machine Description</th>
<th>Host Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Center 2012 R2 Virtual Machine Manager</td>
<td></td>
</tr>
<tr>
<td>NetApp SMI-S Agent</td>
<td></td>
</tr>
</tbody>
</table>

Table 6) Deployment guide variables.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Customer Implementation Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;&lt;admin_password&gt;&gt;</td>
<td>Global default administrative password</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;switch_A_hostname&gt;&gt;</td>
<td>Cisco Nexus A host name</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;switch_A_mgmt0_ip_addr&gt;&gt;</td>
<td>Cisco Nexus A management IP address</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;switch_A_mgmt0_netmask&gt;&gt;</td>
<td>Cisco Nexus A netmask</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;switch_B_hostname&gt;&gt;</td>
<td>Cisco Nexus B host name</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;switch_B_mgmt0_ip_addr&gt;&gt;</td>
<td>Cisco Nexus B management IP address</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;switch_B_mgmt0_netmask&gt;&gt;</td>
<td>Cisco Nexus B netmask</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;iscsia_vlan_id&gt;&gt;</td>
<td>iSCSI-A VLAN ID</td>
<td></td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td>Customer Implementation Value</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>&lt;&lt;iscsib_vlan_id&gt;&gt;</td>
<td>iSCSI-B VLAN ID</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;lm_vlan_id&gt;&gt;</td>
<td>LiveMigration VLAN ID</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;csv_vlan_id&gt;&gt;</td>
<td>Cluster VLAN ID</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;vmtraffic_vlan_id&gt;&gt;</td>
<td>VM traffic VLAN ID</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;ib_mgmt_vlan_id&gt;&gt;</td>
<td>Management VLAN ID</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;native_vlan_id&gt;&gt;</td>
<td>Native VLAN ID</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;inband_mgmt_ip_address&gt;&gt;</td>
<td>In-band management IP address for SVI</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;inband_mgmt_netmask&gt;&gt;</td>
<td>In-band management netmask for SVI</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;inband_mgmt_gateway&gt;&gt;</td>
<td>In-band management gateway for SVI</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller01_mgmt_ip&gt;&gt;</td>
<td>Management IP address for Controller 01</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller01_mgmt_netmask&gt;&gt;</td>
<td>Controller 01 management netmask</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller01_mgmt_gateway&gt;&gt;</td>
<td>Controller 01 management gateway</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller02_mgmt_ip&gt;&gt;</td>
<td>Management IP address for Controller 02</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller02_mgmt_netmask&gt;&gt;</td>
<td>Controller 02 management netmask</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller02_mgmt_gateway&gt;&gt;</td>
<td>Controller 02 management gateway</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;url_boot_software&gt;&gt;</td>
<td>Data ONTAP 8.2.2 URL; format: http://</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;dns_domain_name&gt;&gt;</td>
<td>DNS domain name</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;nameserver_ip&gt;&gt;</td>
<td>DNS server IP(s)</td>
<td></td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td>Customer Implementation Value</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>&lt;&lt;fas_location&gt;&gt;</td>
<td>Physical location for each FAS box</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;#_of_disks&gt;&gt;</td>
<td>Number of disks to assign to each storage controller</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;num_disks&gt;&gt;</td>
<td>Number of disks to assign to storage data aggregate</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller01_sp_ip&gt;&gt;</td>
<td>Controller 01 service processor IP</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller01_sp_netmask&gt;&gt;</td>
<td>Controller 01 service processor netmask</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller01_sp_gateway&gt;&gt;</td>
<td>Controller 01 service processor gateway</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller02_sp_ip&gt;&gt;</td>
<td>Controller 02 service processor IP</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller02_sp_netmask&gt;&gt;</td>
<td>Controller 02 service processor netmask</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller02_sp_gateway&gt;&gt;</td>
<td>Controller 02 service processor gateway</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;timezone&gt;&gt;</td>
<td>FlexPod Express time zone</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;global_ntp_server_ip&gt;&gt;</td>
<td>NTP server IP address</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;snmp_contact&gt;&gt;</td>
<td>Storage administrator e-mail address</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;snmp_location&gt;&gt;</td>
<td>Storage location string</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;snmp_trap_server_fqdn&gt;&gt;</td>
<td>Fully qualified domain name of fault management system or NetApp DFM</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;snmp_community&gt;&gt;</td>
<td>SNMP v1/v2 community name</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;mailhost&gt;&gt;</td>
<td>Mail server host name</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;storage_admin_email&gt;&gt;</td>
<td>Storage administrator e-mail address</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;country_code&gt;&gt;</td>
<td>Two-letter country code</td>
<td></td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td>Customer Implementation Value</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>&lt;&lt;state&gt;&gt;</td>
<td>State or province name</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;city&gt;&gt;</td>
<td>City name</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;org&gt;&gt;</td>
<td>Organization or company name</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;unit&gt;&gt;</td>
<td>Organizational unit name</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;cimc_server1_ip&gt;&gt;</td>
<td>Cisco IMC IP for C 220 M3 Server 1</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;cimc_server2_ip&gt;&gt;</td>
<td>Cisco IMC IP for C 220 M3 Server 2</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;cimc_server3_ip&gt;&gt;</td>
<td>Cisco IMC IP for C 220 M3 Server 3</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;cimc_server4_ip&gt;&gt;</td>
<td>Cisco IMC IP for C 220 M3 Server 4</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;cimc_netmask&gt;&gt;</td>
<td>Cisco IMC netmask for C 220 M3 Servers</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;cimc_gateway&gt;&gt;</td>
<td>Cisco IMC Gateway for C 220 M3 Servers</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;clustername&gt;&gt;</td>
<td>Storage cluster host name</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;cluster_base_license_key&gt;&gt;</td>
<td>Cluster base license key</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;clustermgmt_ip&gt;&gt;</td>
<td>Cluster management IP for the storage cluster</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;clustermgmt_netmask&gt;&gt;</td>
<td>Cluster management netmask for the storage cluster</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;clustermgmt_gateway&gt;&gt;</td>
<td>Cluster management gateway for the storage cluster</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;security_cert_vserver_common_name&gt;&gt;</td>
<td>Infrastructure Vserver FQDN</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;security_cert_cluster_common_name&gt;&gt;</td>
<td>Storage cluster FQDN</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;security_cert_controller01_common&gt;&gt;</td>
<td>Controller 01 FQDN</td>
<td></td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td>Customer Implementation Value</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>n_name&gt;&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;security_cert_controller02_common_name&gt;&gt;</td>
<td>Controller 02 FQDN</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;security_certificate_vserver_authority&gt;&gt;</td>
<td>Infrastructure Vserver security certificate authority</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;security_certificate_vserver_serial_no&gt;&gt;</td>
<td>Infrastructure Vserver security certificate serial number</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;security_certificate_cluster_authority&gt;&gt;</td>
<td>Storage cluster security certificate authority</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;security_certificate_cluster_serial_no&gt;&gt;</td>
<td>Storage cluster security certificate serial number</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;security_certificate_controller01_authority&gt;&gt;</td>
<td>Controller 01 security certificate authority</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;security_certificate_controller01_serial_no&gt;&gt;</td>
<td>Controller 01 security certificate serial number</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;security_certificate_controller02_authority&gt;&gt;</td>
<td>Controller 02 security certificate authority</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;security_certificate_controller02_serial_no&gt;&gt;</td>
<td>Controller 02 security certificate serial number</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller01_iscsia_lif_ip&gt;&gt;</td>
<td>Controller 01 iSCSI-A LIF IP address</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller02_iscsia_lif_ip&gt;&gt;</td>
<td>Controller 02 iSCSI-A LIF IP address</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller01_iscsib_lif_ip&gt;&gt;</td>
<td>Controller 01 iSCSI-B LIF IP address</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller02_iscsib_lif_ip&gt;&gt;</td>
<td>Controller 02 iSCSI-B LIF IP address</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller01_iscsia_lif_netmask&gt;&gt;</td>
<td>Controller 01 iSCSI-A LIF IP netmask</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller02_iscsia_lif_netmask&gt;&gt;</td>
<td>Controller 02 iSCSI-A LIF IP netmask</td>
<td></td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td>Customer Implementation Value</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>&lt;&lt;controller01_iscsib_lif_netmask&gt;&gt;</td>
<td>Controller 01 iSCSI-B LIF IP netmask</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller02_iscsib_lif_netmask&gt;&gt;</td>
<td>Controller 02 iSCSI-B LIF IP netmask</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;vserver_mgmt_netmask&gt;&gt;</td>
<td>Subnet mask for Vserver</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;vsadmin_password&gt;&gt;</td>
<td>Password for VS admin account</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;admin_password&gt;&gt;</td>
<td>Global default administrative password</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;switch_A_hostname&gt;&gt;</td>
<td>Cisco Nexus A host name</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;switch_A_mgmt0_ip_addr&gt;&gt;</td>
<td>Cisco Nexus A management IP address</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;switch_A_mgmt0_netmask&gt;&gt;</td>
<td>Cisco Nexus A netmask</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;switch_B_hostname&gt;&gt;</td>
<td>Cisco Nexus B host name</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;switch_B_mgmt0_ip_addr&gt;&gt;</td>
<td>Cisco Nexus B management IP address</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;switch_B_mgmt0_netmask&gt;&gt;</td>
<td>Cisco Nexus B netmask</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;iscsia_vlan_id&gt;&gt;</td>
<td>iSCSI-A VLAN ID</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;iscsib_vlan_id&gt;&gt;</td>
<td>iSCSI-B VLAN ID</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;lm_vlan_id&gt;&gt;</td>
<td>LiveMigration VLAN ID</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;csv_vlan_id&gt;&gt;</td>
<td>Cluster VLAN ID</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;vmtraffic_vlan_id&gt;&gt;</td>
<td>VM traffic VLAN ID</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;ib_mgmt_vlan_id&gt;&gt;</td>
<td>Management VLAN ID</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;native_vlan_id&gt;&gt;</td>
<td>Native VLAN ID</td>
<td></td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td>Customer Implementation Value</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>&lt;&lt;inband_mgmt_ip_address&gt;&gt;</td>
<td>In-band management IP address for SVI</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;inband_mgmt_netmask&gt;&gt;</td>
<td>In-band management netmask for SVI</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;inband_mgmt_gateway&gt;&gt;</td>
<td>In-band management gateway for SVI</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller01_mgmt_ip&gt;&gt;</td>
<td>Management IP address for Controller 01</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller01_mgmt_netmask&gt;&gt;</td>
<td>Controller 01 management netmask</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller01_mgmt_gateway&gt;&gt;</td>
<td>Controller 01 management gateway</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller02_mgmt_ip&gt;&gt;</td>
<td>Management IP address for Controller 02</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller02_mgmt_netmask&gt;&gt;</td>
<td>Controller 02 management netmask</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;controller02_mgmt_gateway&gt;&gt;</td>
<td>Controller 02 management gateway</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;url_boot_software&gt;&gt;</td>
<td>Data ONTAP 8.2.2 URL; format: http://</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;dns_domain_name&gt;&gt;</td>
<td>DNS domain name</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;nameserver_ip&gt;&gt;</td>
<td>DNS server IP(s)</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;fas_location&gt;&gt;</td>
<td>Physical location for each controller box</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;#_of_disks&gt;&gt;</td>
<td>Number of disks to assign to each storage controller</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;num_disks&gt;&gt;</td>
<td>Number of disks to assign to storage data aggregate</td>
<td></td>
</tr>
</tbody>
</table>

7 FlexPod Express Cabling Information

7.1 FlexPod Express Small Configuration

Figure 3 provides a cabling diagram for the FlexPod Express small configuration, and Table 7 provides cabling information.
Figure 3) FlexPod Express small configuration cabling diagram.

Table 7) Cabling information for the FlexPod Express small configuration.

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Remote Device</th>
<th>Remote Port</th>
<th>Cabling Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Nexus 3048 Switch A</td>
<td>Eth1/1</td>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>e0a</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Eth1/2</td>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>e0a</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Eth1/3</td>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>e0b</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Eth1/4</td>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>e0b</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Eth1/13</td>
<td>Cisco UCS C220 Standalone Server 1</td>
<td>Port 1/1</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Eth1/14</td>
<td>Cisco UCS C220 Standalone Server 1</td>
<td>Port 1/2</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Eth1/15</td>
<td>Cisco UCS C220 Standalone Server 1</td>
<td>Port 1/3</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Eth1/16</td>
<td>Cisco UCS C220 Standalone Server 2</td>
<td>Port 1/1</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Eth1/15</td>
<td>Cisco UCS C220 Standalone Server 2</td>
<td>Port 1/2</td>
<td>9</td>
</tr>
<tr>
<td>Local Device</td>
<td>Local Port</td>
<td>Remote Device</td>
<td>Remote Port</td>
<td>Cabling Code</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>---------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Eth1/16</td>
<td>Cisco UCS C220 Standalone Server 2</td>
<td>Port 1/3</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Eth1/25</td>
<td>Cisco Nexus 3048 Switch B</td>
<td>Eth1/25</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>Eth1/26</td>
<td>Cisco Nexus 3048 Switch B</td>
<td>Eth1/26</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Eth1/37</td>
<td>Cisco UCS C220 Standalone Server 1</td>
<td>CIMC</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>Eth1/39</td>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>e0M</td>
<td>14</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Remote Device</th>
<th>Remote Port</th>
<th>Cabling Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/1</td>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>e0c</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Eth1/2</td>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>e0c</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>Eth1/3</td>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>e0e</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>Eth1/4</td>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>e0e</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>Eth1/13</td>
<td>Cisco UCS C220 Standalone Server 1</td>
<td>Port 0/1</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>Eth1/14</td>
<td>Cisco UCS C220 Standalone Server 1</td>
<td>Port 0/2</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Eth1/15</td>
<td>Cisco UCS C220 Standalone Server 1</td>
<td>Port 1/4</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>Eth1/16</td>
<td>Cisco UCS C220 Standalone Server 2</td>
<td>Port 0/1</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>Eth1/17</td>
<td>Cisco UCS C220 Standalone Server 2</td>
<td>Port 0/2</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td>Eth1/18</td>
<td>Cisco UCS C220 Standalone Server 2</td>
<td>Port 1/4</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>Local Device</td>
<td>Local Port</td>
<td>Remote Device</td>
<td>Remote Port</td>
<td>Cabling Code</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>------------</td>
<td>---------------------------------------------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Eth1/25</td>
<td>Cisco Nexus 3048 Switch A</td>
<td>Eth1/25</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>Eth1/26</td>
<td>Cisco Nexus 3048 Switch A</td>
<td>Eth1/26</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Eth1/37</td>
<td>Cisco UCS C220 Standalone Server 2</td>
<td>CIMC</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Eth1/39</td>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>Management Port</td>
<td>26</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Remote Device</th>
<th>Remote Port</th>
<th>Cabling Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>e0d</td>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>e0d</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>e0f</td>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>e0f</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>ACP</td>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>ACP</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>SAS 0b</td>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>SAS 0a</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>SAS 0a</td>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>SAS 0b</td>
<td>24</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Remote Device</th>
<th>Remote Port</th>
<th>Cabling Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>e0d</td>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>e0d</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>e0f</td>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>e0f</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>ACP</td>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>ACP</td>
<td>27</td>
</tr>
</tbody>
</table>
### 7.2 FlexPod Express Medium Configuration

Figure 4 provides a cabling diagram for the FlexPod Express medium configuration, and Table 8 provides cabling information.

#### Figure 4) FlexPod Express medium configuration cabling diagram.

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Remote Device</th>
<th>Remote Port</th>
<th>Cabling Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>Eth1/1</td>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>e0a</td>
<td>1</td>
</tr>
<tr>
<td>Eth1/2</td>
<td></td>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>e0a</td>
<td>2</td>
</tr>
</tbody>
</table>

#### Table 8) Cabling information for the FlexPod Express medium configuration.

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Remote Device</th>
<th>Remote Port</th>
<th>Cabling Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Nexus 3048 Switch A</td>
<td>Eth1/1</td>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>e0a</td>
<td>1</td>
</tr>
<tr>
<td>Eth1/2</td>
<td></td>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>e0a</td>
<td>2</td>
</tr>
<tr>
<td>Local Device</td>
<td>Local Port</td>
<td>Remote Device</td>
<td>Remote Port</td>
<td>Cabling Code</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------</td>
<td>---------------------------------------------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Eth1/3</td>
<td>Eth1/3</td>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>e0b</td>
<td>3</td>
</tr>
<tr>
<td>Eth1/4</td>
<td>Eth1/4</td>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>e0b</td>
<td>4</td>
</tr>
<tr>
<td>Eth1/13</td>
<td>Eth1/13</td>
<td>Cisco UCS C220 Standalone Server 1</td>
<td>Port 1/1</td>
<td>5</td>
</tr>
<tr>
<td>Eth1/14</td>
<td>Eth1/14</td>
<td>Cisco UCS C220 Standalone Server 1</td>
<td>Port 1/2</td>
<td>6</td>
</tr>
<tr>
<td>Eth1/15</td>
<td>Eth1/15</td>
<td>Cisco UCS C220 Standalone Server 1</td>
<td>Port 1/3</td>
<td>7</td>
</tr>
<tr>
<td>Eth1/16</td>
<td>Eth1/16</td>
<td>Cisco UCS C220 Standalone Server 2</td>
<td>Port 1/1</td>
<td>8</td>
</tr>
<tr>
<td>Eth1/17</td>
<td>Eth1/17</td>
<td>Cisco UCS C220 Standalone Server 2</td>
<td>Port 1/2</td>
<td>9</td>
</tr>
<tr>
<td>Eth1/18</td>
<td>Eth1/18</td>
<td>Cisco UCS C220 Standalone Server 2</td>
<td>Port 1/3</td>
<td>10</td>
</tr>
<tr>
<td>Eth1/19</td>
<td>Eth1/19</td>
<td>Cisco UCS C220 Standalone Server 3</td>
<td>Port 1/1</td>
<td>11</td>
</tr>
<tr>
<td>Eth1/20</td>
<td>Eth1/20</td>
<td>Cisco UCS C220 Standalone Server 3</td>
<td>Port 1/2</td>
<td>12</td>
</tr>
<tr>
<td>Eth1/21</td>
<td>Eth1/21</td>
<td>Cisco UCS C220 Standalone Server 3</td>
<td>Port 1/3</td>
<td>13</td>
</tr>
<tr>
<td>Eth1/22</td>
<td>Eth1/22</td>
<td>Cisco UCS C220 Standalone Server 4</td>
<td>Port 1/1</td>
<td>14</td>
</tr>
<tr>
<td>Eth1/23</td>
<td>Eth1/23</td>
<td>Cisco UCS C220 Standalone Server 4</td>
<td>Port 1/2</td>
<td>15</td>
</tr>
<tr>
<td>Eth1/24</td>
<td>Eth1/24</td>
<td>Cisco UCS C220 Standalone Server 4</td>
<td>Port 1/3</td>
<td>16</td>
</tr>
<tr>
<td>Eth1/25</td>
<td>Eth1/25</td>
<td>Cisco Nexus 3048 Switch B</td>
<td>Eth1/25</td>
<td>17</td>
</tr>
<tr>
<td>Eth1/26</td>
<td>Eth1/26</td>
<td>Cisco Nexus 3048 Switch B</td>
<td>Eth1/26</td>
<td>18</td>
</tr>
<tr>
<td>Eth1/37</td>
<td>Eth1/37</td>
<td>Cisco UCS C220 Standalone Server 1</td>
<td>CIMC</td>
<td>19</td>
</tr>
<tr>
<td>Local Device</td>
<td>Local Port</td>
<td>Remote Device</td>
<td>Remote Port</td>
<td>Cabling Code</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>---------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Eth1/38</td>
<td>Cisco UCS C220 Standalone Server 3</td>
<td>CIIC</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Eth1/39</td>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>e0M</td>
<td>21</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Remote Device</th>
<th>Remote Port</th>
<th>Cabling Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Nexus 3048 Switch B</td>
<td>Eth1/1</td>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>e0c</td>
<td>22</td>
</tr>
<tr>
<td>Eth1/2</td>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>e0c</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td>Eth1/3</td>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>e0e</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>Eth1/4</td>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>e0e</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Eth1/13</td>
<td>Cisco UCS C220 Standalone Server 1</td>
<td>Port 0/1</td>
<td>26</td>
<td></td>
</tr>
<tr>
<td>Eth1/14</td>
<td>Cisco UCS C220 Standalone Server 1</td>
<td>Port 0/2</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>Eth1/15</td>
<td>Cisco UCS C220 Standalone Server 1</td>
<td>Port 1/4</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>Eth1/16</td>
<td>Cisco UCS C220 Standalone Server 2</td>
<td>Port 0/1</td>
<td>29</td>
<td></td>
</tr>
<tr>
<td>Eth1/17</td>
<td>Cisco UCS C220 Standalone Server 2</td>
<td>Port 0/2</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>Eth1/18</td>
<td>Cisco UCS C220 Standalone Server 2</td>
<td>Port 1/4</td>
<td>31</td>
<td></td>
</tr>
<tr>
<td>Eth1/19</td>
<td>Cisco UCS C220 Standalone Server 3</td>
<td>Port 0/1</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>Eth1/20</td>
<td>Cisco UCS C220 Standalone Server 3</td>
<td>Port 0/2</td>
<td>33</td>
<td></td>
</tr>
<tr>
<td>Eth1/21</td>
<td>Cisco UCS C220 Standalone Server 3</td>
<td>Port 1/4</td>
<td>34</td>
<td></td>
</tr>
<tr>
<td>Local Device</td>
<td>Local Port</td>
<td>Remote Device</td>
<td>Remote Port</td>
<td>Cabling Code</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>---------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Eth1/22</td>
<td>Cisco UCS C220 Standalone Server 4</td>
<td>Port 0/1</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>Eth1/23</td>
<td>Cisco UCS C220 Standalone Server 4</td>
<td>Port 0/2</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>Eth1/24</td>
<td>Cisco UCS C220 Standalone Server 4</td>
<td>Port 1/4</td>
<td>37</td>
<td></td>
</tr>
<tr>
<td>Eth1/25</td>
<td>Cisco Nexus 3048 Switch A</td>
<td>Eth1/25</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>Eth1/26</td>
<td>Cisco Nexus 3048 Switch A</td>
<td>Eth1/26</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>Eth1/37</td>
<td>Cisco UCS C220 Standalone Server 2</td>
<td>CIMC</td>
<td>38</td>
<td></td>
</tr>
<tr>
<td>Eth1/38</td>
<td>Cisco UCS C220 Standalone Server 4</td>
<td>CIMC</td>
<td>39</td>
<td></td>
</tr>
<tr>
<td>Eth1/39</td>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>e0M</td>
<td>40</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Remote Device</th>
<th>Remote Port</th>
<th>Cabling Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>e0d</td>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>e0d</td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>e0f</td>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>e0f</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>ACP</td>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>ACP</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>SAS 0b</td>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>SAS 0a</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>SAS 0a</td>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>SAS 0b</td>
<td>42</td>
</tr>
</tbody>
</table>
8 Cisco Nexus 3048 Deployment Procedure

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 together in a back-to-back configuration. Any valid IP address and netmask can be configured on each mgmt0 interface as long as they are in the same network. Because they are configured back to back with no switch or other device in between, no default gateway configuration is needed, and they should be able to communicate with each other. This link cannot be used for external management access such as SSH access, but it will be used for the virtual PortChannel (vPC) peer keep alive traffic. To enable SSH management access to the switch, you need to configure the in-band interface VLAN IP address on an SVI, as discussed later in this document:

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

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Remote Device</th>
<th>Remote Port</th>
<th>Cabling Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetApp FAS2520 Storage Controller 02</td>
<td>e0d</td>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>e0d</td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>e0f</td>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>e0f</td>
<td>44</td>
</tr>
<tr>
<td>ACP</td>
<td></td>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>ACP</td>
<td>45</td>
</tr>
<tr>
<td>SAS 0b</td>
<td></td>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>SAS 0a</td>
<td>42</td>
</tr>
<tr>
<td>SAS 0a</td>
<td></td>
<td>NetApp FAS2520 Storage Controller 01</td>
<td>SAS 0b</td>
<td>41</td>
</tr>
</tbody>
</table>

Switches A and B

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

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

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

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

This setup utility will guide you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.
Please register Cisco Nexus 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) [n]: Enter
Enable the telnet service? (yes/no) [n]: 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 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

8.1 Upgrading the Software (Optional)

You should perform any required software upgrades on the switch at this point in the configuration process. Download and install the latest available Cisco NX-OS software for the Cisco Nexus 3048 switch from the Cisco software download site. There are multiple ways to transfer both the kickstart and system images for Cisco NX-OS to the switch. The most straightforward procedure uses the on-board 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: The Cisco NX-OS software version used in this solution is 6.0(2)U2(3).

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

Switches A and B

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

The switch will install the updated Cisco NX-OS files and reboot.
8.2 Enabling Advanced Features

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

Note: The `interface-vlan` feature is required only if you are using the back-to-back 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 by using the `(config t)` command and type the following commands to enable the appropriate features on each switch.

**Switches A and B**

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

8.3 Performing Global PortChannel Configuration

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

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

**Switches A and B**

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

8.4 Performing Global Spanning-Tree Configuration

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

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

This setting will force the network administrator to review the configuration of each port and will help reveal the most common configuration 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, allowing the default port state to enhance the overall stability of the network.

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

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

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

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

### 8.5 Configuring Jumbo Frames

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

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

Switches A and B

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

### 8.6 Defining VLANs

Before you configure individual ports with different VLANs, you must define those layer 2 VLANs on the switch. It’s also good practice to name the VLANs to help with any troubleshooting in the future.

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

Switches A and B

```plaintext
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
```

### 8.7 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 are 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.

#### Switch A

- `int eth1/1`
  - Description: Controller-01:e0a
- `int eth1/2`
  - Description: Controller-02:e0a
- `int eth1/3`
  - Description: Controller-01:e0c
- `int eth1/4`
  - Description: Controller-02: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 eth1/25`
  - 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

#### Switch B

- `int eth1/1`
  - Description: Controller-01:e0b
- `int eth1/2`
  - Description: Controller-02:e0b
- `int eth1/3`
  - Description: Controller-01:e0d
- `int eth1/4`
  - Description: Controller-02: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 eth1/25`
  - 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

For the FlexPod Express medium configuration, provide the following port descriptions in addition to the port descriptions for the FlexPod Express Small Configuration provided previously.

#### Switch A

- `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 eth1/38`
  - Description: Server-3:mgmt

#### Switch B

- `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 eth1/38`
  - Description: Server-4:mgmt

### 8.8 Configuring Server and Storage Management Interfaces

The management interfaces for both the server and storage typically use only a single VLAN. Therefore, you must 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.
Switches A and B

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

8.9 Performing Virtual PortChannel Global Configuration

To function properly, the vPC feature requires some initial setup between the two Cisco Nexus switches. If you are using the back-to-back mgmt0 configuration, be sure to use the addresses defined on the interfaces and verify that they can communicate by using the ping <<switch_A/B_mgmr0_ip_addr>>vrf management command.

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

Switch A

```
vpc domain 1
   role priority 10
   peer-keepalive destination <<switch_B_mgmr0_ip_addr>> source <<switch_A_mgmr0_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 <<iscsi_a_vlan_id>>,<<iscsi_b_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.

Switch B

```
vpc domain 1
   role priority 20
   peer-keepalive destination <<switch_A_mgmr0_ip_addr>> source <<switch_B_mgmr0_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 <<iscsi_a_vlan_id>>,<<iscsi_b_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
```
8.10 Configuring Storage PortChannels

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

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

### Switches A and B, 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 <<iscsi_a_vlan_id>>,<<iscsi_b_vlan_id>>, <<ib_mgmt_vlan_id>>
   spanning-tree port type edge trunk
   vpc 11
   no shut
```

### Switches A and 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 <<iscsi_a_vlan_id>>,<<iscsi_b_vlan_id>>, <<ib_mgmt_vlan_id>>
   spanning-tree port type edge trunk
   vpc 12
   no shut
exit
```

8.11 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

#### Switch A, Server 1 Configuration

```
int eth1/13
   channel-group 21 mode active
exit
int Po21
```
description VM traffic
switchport
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmtraffic_vlan_id>>, <<mgmt_vlan_id>>
spanning-tree port type edge trunk
vpc 21
no shut
exit
int eth1/14
  switchport
  switchport access vlan <<iscsia_vlan_id>>
  spanning-tree port type edge
  no shut
  exit
int eth1/15
  switchport
  switchport access vlan <<lm_vlan_id>>
  spanning-tree port type edge
  no shut
  exit
Switch B, Server 1 Configuration

int eth1/13
  channel-group 21 mode active
  exit
int Po21
  description VM traffic
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<vmtraffic_vlan_id>>, <<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  vpc 21
  no shut
  exit
int eth1/14
  switchport
  switchport access vlan <<iscsib_vlan_id>>
  spanning-tree port type edge
  no shut
  exit
int eth1/15
  switchport
  switchport access vlan <<csv_vlan_id>>
  spanning-tree port type edge
  no shut
  exit
Switch A, Server 2 Configuration

int eth1/16
  channel-group 22 mode active
  exit
int Po22
  description VM traffic
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<vmtraffic_vlan_id>>, <<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  vpc 22
  no shut
  exit
int eth1/17
  switchport
  switchport access vlan <<iscsia_vlan_id>>
  spanning-tree port type edge
no shut
exit
int eth1/18
  switchport
  switchport access vlan <<lm_vlan_id>>
  spanning-tree port type edge
  no shut
  exit

Switch B, Server 2 Configuration

int eth1/16
  channel-group 22 mode active
  exit
int Po22
  description VM traffic
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<vmtraffic_vlan_id>>, <<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  vpc 22
  no shut
  exit
int eth1/17
  switchport
  switchport access vlan <<iscsib_vlan_id>>
  spanning-tree port type edge
  no shut
  exit
int eth1/18
  switchport
  switchport access vlan <<csv_vlan_id>>
  spanning-tree port type edge
  no shut
  exit

FlexPod Express Medium Configuration

To set up the FlexPod Express medium configuration, run the following commands in addition to the commands provided for the FlexPod Express small configuration in the previous section.

Switch A, Server 3 Configuration

int eth1/19
  channel-group 23 mode active
  exit
int Po23
  description VM traffic
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<vmtraffic_vlan_id>>, <<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  vpc 23
  no shut
  exit
int eth1/20
  switchport
  switchport access vlan <<iscsia_vlan_id>>
  spanning-tree port type edge
  no shut
  exit
int eth1/21
  switchport
  switchport access vlan <<lm_vlan_id>>
  spanning-tree port type edge
  no shut
exit

**Switch B, Server 3 Configuration**

```bash
int eth1/19
    channel-group 23 mode active
exit
int Po23
    description VM traffic
    switchport
    switchport mode trunk
    switchport trunk native vlan <<native_vlan_id>>
    switchport trunk allowed vlan <<vmtraffic_vlan_id>>, <<mgmt_vlan_id>>
    spanning-tree port type edge trunk
vpc 23
no shut
exit
int eth1/20
    switchport
    switchport access vlan <<iscsib_vlan_id>>
    spanning-tree port type edge
    no shut
exit
int eth1/21
    switchport
    switchport access vlan <<csv_vlan_id>>
    spanning-tree port type edge
    no shut
exit
```

**Switch A, Server 4 Configuration**

```bash
int eth1/22
    channel-group 24 mode active
exit
int Po24
    description VM traffic
    switchport
    switchport mode trunk
    switchport trunk native vlan <<native_vlan_id>>
    switchport trunk allowed vlan <<vmtraffic_vlan_id>>, <<mgmt_vlan_id>>
    spanning-tree port type edge trunk
vpc 24
no shut
exit
int eth1/23
    switchport
    switchport access vlan <<iscsia_vlan_id>>
    spanning-tree port type edge
    no shut
exit
int eth1/24
    switchport
    switchport access vlan <<lm_vlan_id>>
    spanning-tree port type edge
    no shut
exit
```

**Switch B, Server 4 Configuration**

```bash
int eth1/22
    channel-group 24 mode active
exit
int Po24
    description VM traffic
    switchport
    switchport mode trunk
    switchport trunk native vlan <<native_vlan_id>>
    switchport trunk allowed vlan <<vmtraffic_vlan_id>>, <<mgmt_vlan_id>>
```
8.12 Performing In-Band Management SVI Configuration

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

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

**Switches A and B**

```
int vlan <<ib_mgmt_vlan_id>>
  ip address <<inband_mgmt_ip_address>>/<<inband_mgmt_netmask>>
  no shut
ip route 0.0.0.0/0 <<inband_mgmt_gateway>>
```

8.13 Saving the Configuration

Save the configuration on both switches for configuration persistence.

**Switches A and B**

```
copy run start
```

8.14 Uplinking to Existing Network Infrastructure

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

9 NetApp FAS Storage Deployment Procedure

9.1 Controller FAS25xx Series

Table 9) Controller FAS25xx series prerequisites.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Reference</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical site where storage system needs to be installed must</td>
<td>Site Requirements Guide</td>
<td>Refer to the “Site Preparation” section.</td>
</tr>
</tbody>
</table>
be ready.

<table>
<thead>
<tr>
<th>Storage system connectivity requirements must be met.</th>
<th>Site Requirements Guide</th>
<th>Refer to the “System Connectivity Requirements” section.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage system general power requirements must be met.</td>
<td>Site Requirements Guide</td>
<td>Refer to the “Circuit Breaker, Power Outlet Balancing, System Cabinet Power Cord Plugs, and Console Pinout Requirements” section.</td>
</tr>
<tr>
<td>Storage system model-specific requirements must be met.</td>
<td>Site Requirements Guide</td>
<td>Refer to the “FAS25xx Series Systems” section.</td>
</tr>
</tbody>
</table>

### 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.

### Storage Controllers

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

#### 9.2 Configuring NetApp Clustered Data ONTAP 8.2.2

These steps demonstrate how to assign disk ownership and perform disk initialization and verification.

**Controller 01**

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

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

2. From the Loader-A prompt, enter:

   ```
   printenv
   ```

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

4. Allow the system to boot.

   ```
   boot_ontap
   ```

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

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

6. To install new software, first select option 7.
7. Answer yes to perform a nondisruptive upgrade.
   
   y

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

9. Select yes to reboot now.
   
   y

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

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

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

    <<url_boot_software>>

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

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

    y

14. Enter yes to reboot the node.

    y

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

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

    Starting AUTOBOOT press Ctrl-C to abort..

16. From the Loader-A prompt, enter:

    printenv

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

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

    setenv bootarg.init.boot_clustered true
    setenv bootarg.bsdportname eOM

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

    autoboot

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

    Ctrl - C

20. Select option 5 to enter Maintenance mode.

    5

21. When prompted with Continue with boot?, enter y.

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

23. Use the disk assign -n <<#_of_disks>> command to assign disks to Controller-01.
Note: For the small and medium FlexPod Express configurations, <<#_of_disks>> should equal 9 for Controller 01.

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

```
ha-config show
```

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

25. Reboot the controller by using the `halt` command.

26. At the Loader-A prompt, enter:

```
autoboot
```

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

```
Ctrl - C
```

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

```
4
```

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

```
y
```

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

```
y
```

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

Controller 02

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

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

2. From the Loader-A prompt, enter:

```
printenv
```

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

4. Allow the system to boot up.

```
boot_ontap
```

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

```
Ctrl-C
```

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

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

```
7
```

7. Answer yes to perform a nondisruptive upgrade.

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

9. Select yes to reboot now.
y

10. Enter the IP address, netmask, and default gateway for eOM in their respective places.
<<controller02_mgmt_ip>> <<controller02_mgmt_netmask>> <<controller02_mgmt_gateway>>

11. Enter the URL where the software can be found.
Note: This web server must be pingable.
<<url_boot_software>>

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

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

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

15. Press Ctrl-C to exit autoboot when you see this message:
Starting AUTOBOOT press Ctrl-C to abort…

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

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

17. If the system is not set to boot in clustered Data ONTAP, at the Loader-A prompt, enter the following command to make the system boot in clustered Data ONTAP:
setenv bootarg.init.boot_clustered true
setenv bootarg.bsdportname eOM

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

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

20. Select option 5 to enter Maintenance mode.
5

21. When prompted with Continue with boot?, enter y.

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

23. Use the disk assign -n <<#_of_disks>> command to assign disks to Controller 02.

Note: For the small and medium FlexPod Express configurations, <<#_of_disks>> should equal 3 for Controller 02.
24. To verify the HA status of your environment, run the following command:

```
ha-config show
```

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

25. Reboot the controller by using the `halt` command.

26. At the Loader-A prompt, enter:

```
autoboot
```

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

```
Ctrl - C
```

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

```
4
```

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

```
y
```

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

```
y
```

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

### 9.3 Creating Clusters in NetApp Clustered Data ONTAP

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

**Controller 01**

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

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

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

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

   ```
create
```

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

   Do you intend for this node to be used as a single node cluster? {yes, no} [no]: Enter
   
   Will the cluster network be configured to use network switches? [yes]:no
   
   Non-HA mode, Reboot node to activate HA

© 2014 NetApp, Inc. All rights reserved.
Do you want to reboot now to set storage failover (SFO) to HA mode? {yes, no} [yes]: Enter

4. After the reboot, continue with the cluster create operation.

5. The existing cluster interface configuration is displayed.

<table>
<thead>
<tr>
<th>Port</th>
<th>MTU</th>
<th>IP</th>
<th>Netmask</th>
</tr>
</thead>
<tbody>
<tr>
<td>e0d</td>
<td>9000</td>
<td>169.254.250.41</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>e0f</td>
<td>9000</td>
<td>169.254.175.136</td>
<td>255.255.0.0</td>
</tr>
</tbody>
</table>

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

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

6. Accept the configuration by pressing the Enter key.

7. The steps to create a cluster are displayed.

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

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

Enter an additional license key []:

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

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

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

9. Enter the DNS domain name.

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

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

10. Set up the node.

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

11. Press Enter to accept the NetApp AutoSupport™ message.

12. Log in to the cluster.


storage disk option modify -autoassign off
9.4 Joining Clusters in NetApp Clustered Data ONTAP

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

Controller 02

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

   Welcome to the cluster setup wizard.

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

   You can return to cluster setup at any time by typing "cluster setup".
   To accept a default or omit a question, do not enter a value.

   Do you want to create a new cluster or join an existing cluster?(create, join):

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

2. Enter the following command to join a cluster:

   `join`

3. Enter `yes` to activate HA.

   Non-HA mode, Reboot node to activate HA

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

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

<table>
<thead>
<tr>
<th>Port</th>
<th>MTU</th>
<th>IP</th>
<th>Netmask</th>
</tr>
</thead>
<tbody>
<tr>
<td>e0d</td>
<td>9000</td>
<td>169.254.49.199</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>e0f</td>
<td>9000</td>
<td>169.254.132.123</td>
<td>255.255.0.0</td>
</tr>
</tbody>
</table>

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

   **Note:** Before you accept the preceding configuration, make sure that the correct ports are listed for the cluster interfaces.

5. Accept the configuration by pressing the Enter key.

6. The steps to create a cluster are displayed.

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

   **Note:** The node should find the cluster name automatically.

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

7. Set up the node.

   Enter the node management interface port [e0M]: Enter
   Enter the node management interface IP address: <<controller02_mgmmt_ip>>
   Enter the node management interface netmask: Enter
   Enter the node management interface default gateway: Enter
   Enable IPv4 DHCP on the service processor interface [no]: Enter
   Enter the service processor interface IP address: <<controller02_sp_ip>>
Enter the service processor interface netmask: <<controller02_sp_netmask>>
Enter the service processor interface default gateway: <<controller02_sp_gateway>>

8. Press Enter to accept the AutoSupport message.
9. Log in to the cluster interface with the admin user ID and admin password.
10. Disable disk autoassign by entering:

   ```
   storage disk option modify -autoassign off -node <<clusternname>>-02
   ```

9.5 Changing the RAID Configuration on Root Aggregates

The RAID configuration on the root aggregates of Controller 01 and 02 must be changed from `raid_dp` to `raid4`.

**Controller 01**
1. Connect to the storage system console port to change the RAID configuration.

   ```
   aggr modify -aggregate aggr0 -raidtype raid4
   aggr modify -aggregate aggr0_<<controller01>> -raidtype raid4
   ```

9.6 Zeroing All Spare Disks

**Controller 01**
1. Connect to the storage system console port to zero all spare disks in the cluster.

   ```
   disk zerospares
   ```

9.7 Configuring ifgrp LACP in NetApp Clustered Data ONTAP

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

Connect to the storage system console port of Controller 01 and run the following commands on the command line to create an interface group (ifgrp).

**Controller 01**

```
ifgrp create -node <<clustername>>-01 -ifgrp a0a -distr-func port -mode multimode_lacp
network port ifgrp add-port -node <<clustername>>-01 -ifgrp a0a -port e0b
network port ifgrp add-port -node <<clustername>>-01 -ifgrp a0a -port e0c
network port ifgrp add-port -node <<clustername>>-01 -ifgrp a0a -port e0e
```

**Controller 02**

```
ifgrp create -node <<clustername>>-02 -ifgrp a0a -distr-func port -mode multimode_lacp
network port ifgrp add-port -node <<clustername>>-02 -ifgrp a0a -port e0a
network port ifgrp add-port -node <<clustername>>-02 -ifgrp a0a -port e0b
network port ifgrp add-port -node <<clustername>>-02 -ifgrp a0a -port e0c
network port ifgrp add-port -node <<clustername>>-02 -ifgrp a0a -port e0e
```

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

**Note:** The interface group name must follow the standard naming convention of "a<<number><letter>>", where <number> is an integer in the range [0–999] without leading zeros, and <letter> is a lowercase letter.
9.8 Configuring VLANs in Clustered Data ONTAP

Connect to the storage system console port of Controller 01 and run the following commands on the command line to create VLANs.

**Controller 01 and Controller 02**

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

   ```
   network port vlan create -node <<clusternname>>-01 -vlan-name a0a-<<iscsia_vlan_id>>
   network port vlan create -node <<clusternname>>-02 -vlan-name a0a-<<iscsia_vlan_id>>
   ``

2. Follow these steps to create a VLAN interface for node management failover groups:

   ```
   network port vlan create -node <<clusternname>>-01 -vlan-name a0a-<<ib_mgmt_vlan_id>>
   network port vlan create -node <<clusternname>>-02 -vlan-name a0a-<<ib_mgmt_vlan_id>>
   ``

9.9 Migrating the Cluster Management Interface on Controller 01

Connect to the storage system console port of Controller 01 and run the following commands from the command line:

1. Migrate the `cluster_mgmt` logical interface from `e0a` to `ifgrp a0a-<<ib_mgmt_vlan_id>>` on Controller 01.

   ```
   network interface migrate -vserver <<clusternname>> -lif cluster_mgmt -destination-node <<clusternname>>-01 -destination-port a0a-<<ib_mgmt_vlan_id>>
   ``

2. Set the home port of the `cluster_mgmt` logical interface to the new destination-port.

   ```
   network interface modify -vserver <<clusternname>> -lif cluster_mgmt -home-node <<clusternname>>-01 -home-port a0a-<<ib_mgmt_vlan_id>>
   ``

3. Add the physical port `e0a` to the `ifgrp a0a`.

   ```
   network port ifgrp add-port -node <<clusternname>>-01 -ifgrp a0a -port e0a
   ``

9.10 Logging in to the Cluster

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

9.11 Setting Auto-Revert on Cluster Management

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

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

9.12 Configuring Failover Group Management in Clustered Data ONTAP

1. Create a cluster management port failover group.

   ```
   network interface failover-groups create -failover-group fg-clus-mgmt -node <<clusternname>>-01 -port a0a-<<ib_mgmt_vlan_id>>
   network interface failover-groups create -failover-group fg-clus-mgmt -node <<clusternname>>-02 -port a0a-<<ib_mgmt_vlan_id>>
   ``

9.13 Assigning the Management Failover Group to the Cluster Management LIF

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

   ```
   network interface modify -vserver <<clusternname>> -lif cluster_mgmt -failover-group fg-clus-mgmt
   ```
9.14 Configuring Failover Group Node Management in Clustered Data ONTAP

1. Create node management port failover groups.

   network interface failover-groups create -failover-group fg-node-mgmt01 -node <<clustername>>-01 -port a0a-<ib_mgmt_vlan_id>
   network interface failover-groups create -failover-group fg-node-mgmt01 -node <<clustername>>-01 -port e0M
   network interface failover-groups create -failover-group fg-node-mgmt02 -node <<clustername>>-02 -port a0a-<ib_mgmt_vlan_id>
   network interface failover-groups create -failover-group fg-node-mgmt02 -node <<clustername>>-02 -port e0M

9.15 Assigning Node Management Failover Groups to Node Management LIFs

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

   network interface modify -vserver <<clustername>>-01 -lif mgmt1 -auto-revert true -failover-group fg-node-mgmt01
   network interface modify -vserver <<clustername>>-02 -lif mgmt1 -auto-revert true -failover-group fg-node-mgmt02

9.16 Creating Aggregates

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

1. Execute the following command to create new aggregates:

   aggr create -aggregate aggr1_controller01 -nodes <<clustername>>-01 -diskcount <<num_disks>> -raidtype raid4

   Note: For the small and medium FlexPod Express configurations, <<num_disks>> should equal 6.

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

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

   node run <<clustername>>-01 aggr options aggr1_controller01 nosnap on

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

   node run <<clustername>>-01 snap delete -A -a -f aggr1_controller01

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

   aggr show
   aggr rename -aggregate aggr0 -newname aggr0_controller01
   aggr rename -aggregate aggr0_<<clustername>>_02_0 -newname aggr0_controller02

9.17 Configuring the Service Processor

Gather information about the network and the AutoSupport settings before you configure the service processor.

Configure the service processor by using the Dynamic Host Configuration Protocol (DHCP) or static addressing. If the service processor uses a static IP address, verify that the following service processor prerequisites have been met:

- An available static IP address
- The network netmask
- The network gateway IP
- AutoSupport information

A best practice is to configure the AutoSupport recipients and mail host before configuring the service processor. Data ONTAP automatically sends AutoSupport configuration to the service processor, allowing the service processor to send alerts and notifications through an AutoSupport message to the system administrative recipients specified in AutoSupport. When configuring the service processor, enter the name or the IP address of the AutoSupport mail host when prompted.

A service processor must be set up on each node.

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

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

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

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

2. Using a web browser, connect to `http://support.netapp.com/NOW/cgi-bin/fw`.
3. Select the storage platform.
4. Select Service Process Image for installation from the Data ONTAP prompt.
5. Check the latest firmware version that is available for your storage platform. If your storage system is not running the latest version, proceed to the download page for the latest release of the service processor firmware for your storage platform.
6. Using the instructions on this page, update the service processors on both nodes in your cluster. You must download the .zip file to a web server that is reachable from the cluster management interface. In step 2 of the instructions, substitute the following command: `system node image get -node * -package http://web_server_name/path/SP_FW.zip -replace-package true`.
7. Execute step 3 on each node if the service processor automatic update is not enabled.
8. View the status of the service processor upgrade by using steps 4 and 5.

**9.18 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:

   ```bash
   network port modify -node * -port a0a -mtu 9000
   ```

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

   ```bash
   network port modify -node * -port a0a--<<iscsia_vlan_id>> -mtu 9000
   ```

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

   ```bash
   network port modify -node * -port a0a--<<iscsib_vlan_id>> -mtu 9000
   ```

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

**9.19 Configuring NTP in Clustered Data ONTAP**

To configure time synchronization on the cluster, complete the following steps.
1. Set the time zone for the cluster.
   `timezone <<timezone>>`
   **Note:** For example, in the eastern United States, the time zone is America/New_York.

2. Set the date for the cluster.
   `date <ccymmdhmm.ss>`
   **Note:** The format for the date is `<[Century][Year][Month][Day][Hour][Minute][Second]>`; for example, 201309231128.50.

3. Configure the Network Time Protocol (NTP) for each node in the cluster.
   ```
   system services ntp server create -node <<clustername>>-01 -server <<global_ntp_server_ip>>
   system services ntp server create -node <<clustername>>-02 -server <<global_ntp_server_ip>>
   ```

### 9.20 Configuring SNMP in Clustered Data ONTAP

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 <<snmp_contact>>
   snmp location "<<snmp_location>>"%
   snmp init 1
   options snmp.enable on
   ```

2. Configure SNMP traps to send to remote hosts, such as a DFM server or another fault management system.
   ```
   snmp traphost add <<snmp_trap_server_fqdn>>
   ```

### 9.21 Configuring SNMPv1 in Clustered Data ONTAP

1. Set the shared secret plaintext password, which is called a community.
   ```
   snmp community delete all
   snmp community add ro <<snmp_community>>
   ```
   **Note:** Use the `delete all` command with caution. If community strings are used for other monitoring products, the `delete all` command removes them.

### 9.22 Configuring SNMPv3 in Clustered Data ONTAP

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

1. Create a user called `snmpv3user`.
   ```
   security login create -username snmpv3user -authmethod usm -application snmp
   ```

2. Enter the authoritative entity’s engine ID and select MD5 as the authentication protocol. Use the command `security snmpusers` to view the engine ID.

3. When prompted, enter a password with a minimum length of eight characters for the authentication protocol.

4. Confirm the authentication protocol password.

5. Select DES as the privacy protocol.

6. When prompted, enter a password with a minimum length of eight characters for the privacy protocol.

7. Confirm the privacy protocol password.

### 9.23 Configuring AutoSupport HTTPS in Clustered Data ONTAP

AutoSupport sends support summary information to NetApp through HTTPS.
1. Run the following command to configure AutoSupport:

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

### 9.24 Configuring Cisco Discovery Protocol in Clustered Data ONTAP

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

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

1. To enable CDP on the NetApp storage controllers, enable CDP on Data ONTAP.

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

### 9.25 Setting Up Vserver

To create an infrastructure Vserver, complete the following steps:

1. Run the Vserver setup wizard.

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

You can enter the following commands at any time:
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the Vserver Setup Wizard. Any changes you made before typing "exit" will be applied.

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

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

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

2. Enter the Vserver name.

```
Enter the Vserver name: Infra_SVM
```

3. Select the Vserver data protocols to configure.

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

4. Select the Vserver client services to configure.

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

5. Enter the Vserver's root volume aggregate.

```
Enter the Vserver's root volume aggregate [aggr1_controller01]: aggr1_controller01
```

6. Enter the Vserver language setting. English is the default, [C].

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

7. Enter the Vserver's security style.

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

8. Do not create the data volume.
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.</td>
<td>Do you want to create a data volume? {yes, no} [yes]: no</td>
</tr>
<tr>
<td>10.</td>
<td>Do you want to create a logical interface? {yes, no} [yes]: no</td>
</tr>
<tr>
<td>11.</td>
<td>Add the data aggregate to the Infra_SVM aggregate list.</td>
</tr>
<tr>
<td>9.26</td>
<td>Configuring iSCSI Service in Clustered Data ONTAP</td>
</tr>
<tr>
<td>1.</td>
<td>Create the iSCSI service on each Vserver.</td>
</tr>
<tr>
<td>9.27</td>
<td>Configuring HTTPS Access in Clustered Data ONTAP</td>
</tr>
<tr>
<td>1.</td>
<td>Increase the privilege level to access the certificate commands.</td>
</tr>
<tr>
<td>2.</td>
<td>Generally, a self-signed certificate is already in place. Check it with the following command:</td>
</tr>
<tr>
<td>3.</td>
<td>Run the following commands as one-time commands to generate and install self-signed certificates. <strong>Note:</strong> You can also use the <code>security certificate delete</code> command to delete expired certificates.</td>
</tr>
<tr>
<td>4.</td>
<td>Configure and enable SSL and HTTPS access and disable telnet access.</td>
</tr>
</tbody>
</table>
network interface failover-groups create -failover-group vs_mgmt01 -node <<clusternname>>-01 -port a0a-<<ib_mgmt_vlan_id>>
network Interface failover-groups create -failover-group vs_mgmt01 -node <<clusternname>>-02 -port a0a-<<ib_mgmt_vlan_id>>

9.28 Configuring FlexVol in Clustered Data ONTAP

1. The following information is required to create a NetApp FlexVol® volume: the volume’s name and size, and the aggregate on which it will exist.

volume create -vserver Infra_SVM -volume infra_datastore_1 -aggregate aggr1_controller01 -size 2t
   -state online -junction-path /infra_datastore_1 -space-guarantee none -percent-snapshot-space 0

volume create -vserver Infra_SVM -volume infra_sql -aggregate aggr1_controller01 -size 500g -
   state online -junction-path /infra_sql -space-guarantee none -percent-snapshot-space 0 -snapshot-
   policy none

volume create -vserver Infra_SVM -volume quorum -aggregate aggr1_controller01 -size 5g -state
   online -junction-path /quorum -space-guarantee none -percent-snapshot-space 0 -snapshot-policy
   none

9.29 Configuring iSCSI LIF in Clustered Data ONTAP

1. Create an iSCSI logical interface (LIF).

network interface create -vserver Infra_SVM -lif iscsia_lif01 -role data -data-protocol iscsi -
   home-node <<clustername>>-01 -home-port a0a-<<iscsia_vlan_id>> -address
   <<controller01_iscsia_lif_ip>> -netmask <<controller01_iscsia_lif_netmask>>

network interface create -vserver Infra_SVM -lif iscsib_lif01 -role data -data-protocol iscsi -
   home-node <<clusternames>>-01 -home-port a0a-<<iscsib_vlan_id>> -address
   <<controller01_iscsib_lif_ip>> -netmask <<controller01_iscsib_lif_netmask>>

network interface create -vserver Infra_SVM -lif iscsia_lif02 -role data -data-protocol iscsi -
   home-node <<clusternames>>-02 -home-port a0a-<<iscsia_vlan_id>> -address
   <<controller02_iscsia_lif_ip>> -netmask <<controller02_iscsia_lif_netmask>>

network interface create -vserver Infra_SVM -lif iscsib_lif02 -role data -data-protocol iscsi -
   home-node <<clusternames>>-02 -home-port a0a-<<iscsib_vlan_id>> -address
   <<controller02_iscsib_lif_ip>> -netmask <<controller02_iscsib_lif_netmask>>

9.30 Configuring Failover Group Vserver Management in Clustered Data ONTAP

1. Create a management port failover group.

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

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

security ssl modify -vserver <<clustername>>-01 -common-name
   <<security_cert_controller01_common_name>> -server-enabled true -client-enabled false -ca
   <<security_certificate_controller01_authority>> -serial
   <<security_certificate_controller01_serial_no>>

security ssl modify -vserver <<clustername>>-02 -common-name
   <<security_cert_controller02_common_name>> -server-enabled true -client-enabled false -ca
   <<security_certificate_controller02_authority>> -serial
   <<security_certificate_controller02_serial_no>>

set -privilege admin
9.31 Adding an Infrastructure Vserver Administrator

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

```plaintext
network interface create -vserver Infra_SVM -lif Mgmt -role data -data-protocol none -home-node <<clusternode>>-02 -home-port a0a-<<ib_mgmt_vlan_id>> -address <<vserver_mgmt_ip>> -netmask <<vserver_mgmt_netmask>> -failover-group vs_mgmt01 -firewall-policy mgmt -auto-revert true

network routing-groups route create -vserver Infra_SVM -routing-group d<<clustermgmt_ip>>/<<vserver_mgmt_netmask>> -destination 0.0.0.0/0 -gateway <<clustermgmt_gateway>>

security login password -vserver Infra_SVM -username vsadmin
Enter a new password: <<vsadmin_password>>
Enter it again: <<vsadmin_password>>

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

10 Cisco UCS C-Series Rack Server Deployment Procedure

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

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

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

**All Servers**

1. Attach the Cisco KVM dongle (provided with the server) to the KVM port on the front of the server.
   Plug a VGA monitor and USB keyboard into the appropriate KVM dongle ports.
2. Power on the server and press F8 when prompted to enter the Cisco IMC configuration.
3. When you are in the Cisco IMC configuration utility, set the following options:

- **Network Interface Card (NIC) mode:**
  - Dedicated [X]

- **IP (Basic):**
  - IPV4: [X]
  - DHCP enabled: [ ]
  - CIMC IP: <<cimc_ip>>
  - Prefix/Subnet: <<cimc_netmask>>
  - Gateway: <<cimc_gateway>>

- **VLAN (Advanced):** Leave unchecked to disable VLAN tagging.
  - NIC redundancy:
    - None: [X]
Note: Press F1 to see additional settings.

- Common Properties:
  - Hostname: <<host_name>>
  - Dynamic DNS: [
- Factory Defaults: Leave unchecked.
- Default User (Basic):
  - Default password: <<admin_password>>
  - Reenter password: <<admin_password>>
- Port Properties: Use default values.
- Port Profiles: Leave unchecked.
4. Press F10 to save the Cisco IMC interface configuration.
5. When the configuration is saved, press ESC to exit.

10.2 Configuring Cisco UCS C-Series RAID Configuration
1. Open a web browser and browse to the Cisco IMC interface IP address.
2. Log in to the Cisco IMC interface. The default user name is admin. Use the admin password, <<admin_password>>, which was set in the Cisco IMC interface setup.
3. After logging in, click the Server tab and then choose Summary. Choose Launch KVM Console.
4. The virtual KVM window opens. Choose Virtual Media at the top of the window.
5. Click Activate Virtual Devices.
6. Click Map CD/DVD.
7. Browse to the location of the Server Configuration Utility ISO image and select it. Click Map Device.

8. Return to the Cisco IMC interface browser window (do not close the virtual KVM window), click the Server tab, and choose BIOS.
9. Choose Configure Boot Order and click OK.
10. Make sure the boot options are configured as follows:
12. Return to the virtual KVM window. Click the KVM tab at the top of the window.
13. The server should now boot into the Server Configuration Utility.
14. Click the Server Configuration tab in the left pane.
15. Choose RAID Configuration.
16. In the upper-right corner, click the Configure button.
17. In the RAID Level drop-down box, choose Automatic Setup with Redundancy. Click Create Array.
18. When the RAID configuration is complete, close the virtual KVM window.
19. Return to the Cisco IMC interface browser window, click the Server tab and then choose 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 Cisco IMC interface to map remote installation media to each individual server.

11.1 Logging in to the Cisco UCS C-Series Standalone Server IMC Interface

The following steps detail the method for logging in to the Cisco UCS C-Series standalone server IMC interface. Administrators must log in to the Cisco IMC interface to execute the virtual KVM, which allows them to begin installing the operating system through remote media.
All Hosts
1. Navigate to a web browser and enter the IP address for the Cisco C-Series IMC interface. This launches the IMC GUI application.
2. Log in to the IMC GUI with the admin user name and credentials.
3. In the main menu, select the Server tab.
4. Click Launch KVM Console.

11.2 Setting Up the Windows Server 2012 Installation
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.
4. To boot the server, select the KVM tab.
5. Select Power On Server in the IMC interface Summary tab, and then click OK.

11.3 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 has 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. After reviewing the end-user license agreement (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 to continue with the installation.
9. After the installation is complete, unmap the Windows installation image in the Virtual Media tab of the KVM Console. This step makes the server reboot into Windows and not the installer by unmapping the Windows image from the virtual media.
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 has finished installing, enter an administrator password on the Settings page and click Finish.
11.4 Updating Windows Drivers

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

All Hosts

1. Log in to Windows with the administrator password entered previously during installation.
3. Select Windows 2012r2 64-bit as the platform and download the latest version of the drivers package.
4. Extract the downloaded drivers package.
5. Launch the Windows Server Manager utility, select Tools on the top right of the window, and select Computer Management.
6. From the Computer Management window, under System Tools, select Device Manager.
7. Expand Display Adapters and right-click Microsoft Basic Display Adapter (Low Resolution).
8. Select Update Driver Software.

9. Click Browse My Computer for Driver Software.
10. Using the Browse button, navigate to the root folder of the extracted drivers package and click OK.
11. Click Next, and the Windows display driver is installed.

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

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

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

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

11.5 Installing Windows Features

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

All Hosts

1. From the Cisco IMC virtual KVM console, select the Virtual Media tab.
2. Click Map CD/DVD.
4. Log in to Windows with the administrator password previously entered during installation.
5. Launch a Microsoft Windows PowerShell® prompt by right-clicking the PowerShell icon in the taskbar and selecting Run as Administrator.
6. Add the .NET 3.5, Hyper-V, Multipath I/O (MPIO), and clustering features by entering the following command:

   Add-WindowsFeature Hyper-V, NET-Framework-Core, Failover-Clustering, Multipath-I0 ` -IncludeManagementTools -Source E:\sources\sxs -Restart

   Note: This command assumes that the ISO image is mounted to drive E:.
7. Unmap the Server 2012 R2 Installation media from the Virtual Media tab.

11.6 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 with the administrator password previously entered during installation.
2. Launch a PowerShell prompt by right-clicking the PowerShell icon in the taskbar and selecting Run as Administrator.
3. Disconnect each network cable one at a time 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 -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 Cluster
Note: Because of the way that Windows Plug and Play detects hardware, your list will most likely change. You must physically identify which port is connected to each server by disconnecting the link.

4. Create a NIC team. From a PowerShell prompt, enter:

```
New-NICfoTeam -Name TM1 -TeamMembers Public* -TeamingMode lacp -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 a Hyper-V virtual switch for the management and VM traffic.

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

8. Create a management VM NIC.

```
Add-VMM NetworkAdapter -ManagementOS -Name Mgmt -SwitchName VMComm
Set-VMM NetworkAdapterVlan -ManagementOS -VMM NetworkAdapterName 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 -DisplayValue "Jumbo Packet" -DisplayValue "9014 Bytes" -EA SilentlyContinue
```

11. Set IP address information for each host NIC.

```
New-NetIPAddress -InterfaceAlias 'vEthernet (Mgmt)' -IPAddress <Mgmt_Ipaddress> -DefaultGateway <<Mgmt_gateway>> -PrefixLength <<Mgmt_network_prefix>>
New-NetIPAddress -InterfaceAlias 'vEthernet (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>>
```


```
New-MSDMSupportedHW -VendorID NETAPP -ProductId LUN
New-MSDMSupportedHW -VendorID NETAPP -ProductId "LUN C-Mode"
Update-MPIOClaimedHW
```

15. Type Yes to confirm the preceding 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 Microsoft Active Directory®.
11.7 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 about 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/kit_iscsi/microsoft/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 reboots during this process.

11.8 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 the 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 <<controller01_iscsia_lif01_ip>> -InitiatorPortalAddress <iscsia_ipaddress>
   New-IscsiTargetPortal -TargetPortalAddress <<controller01_iscsib_lif01_ip>> -InitiatorPortalAddress <iscsia_ipaddress>
   New-IscsiTargetPortal -TargetPortalAddress <<controller02_iscsia_lif02_ip>> -InitiatorPortalAddress <iscsia_ipaddress>
   New-IscsiTargetPortal -TargetPortalAddress <<controller02_iscsib_lif02_ip>> -InitiatorPortalAddress <iscsia_ipaddress>

7. Connect a session for each iSCSI network to each target.
   Get-IscsiTarget | Connect-IscsiTarget -IsPersistent $true -IsMultipathEnabled $true -InitiatorPortalAddress <iscsia_ipaddress>
   Get-IscsiTarget | Connect-IscsiTarget -IsPersistent $true -IsMultipathEnabled $true -InitiatorPortalAddress <iscsia_ipaddress>
11.9 Installing NetApp SnapDrive

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

All Hosts

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

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

   ![New Object - User](image1)

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

   ![Administrators Properties](image2)

3. Download the SnapDrive installer from the NetApp Support site.
4. Launch the installer and click Next.
5. Select the Storage Based Licensing method and click Next.
6. Enter your user name and organization information, and click Next.
7. Validate the installation path and click Next.
8. Select the Enable SnapDrive to Communicate Through the Windows Firewall checkbox and click Next.
9. Enter the information for the SnapDrive service account and click Next.
10. On the SnapDrive Web Service Configuration page, click Next.
11. Clear the Enable Preferred Storage System IP Address checkbox and click Next.

![SnapDrive InstallShield Wizard](image)

13. Leave Enable Unified Manager Configuration unchecked and click Next.
14. Click Install.
15. After the installation has finished, launch a new PowerShell prompt by right-clicking the PowerShell icon in the taskbar and selecting Run as Administrator.

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

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

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

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

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

### 11.10 Installing NetApp SnapManager for Hyper-V

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

1. In Active Directory, create an SMHV service account.
   
   Note: This account requires no special delegation, and the same account can be used for multiple hosts.

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

   ![Administrators Properties](image)

3. Download the SMHV installer from the [NetApp Support site](https://www.netapp.com/support).
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.

### 11.11 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>
   ```


   ```
   Get-ClusterNetworkInterface | ? Name -like 'Cluster*' | Group Network | %{ (Get-ClusterNetwork $_.Name).Name = 'Cluster'}
   Get-ClusterNetworkInterface | ? Name -like 'LM*' | Group Network | %{ (Get-ClusterNetwork $_.Name).Name = 'LM'}
   ```
4. Designate the Cluster Shared Volumes (CSV) network.

\[
\text{Get-ClusterNetworkInterface | ? Name -like "^iSCSI-A\^" | Group Network} \%\{ (Get-ClusterNetwork \$_.Name).Name = 'iSCSI-A' \}
\]

\[
\text{Get-ClusterNetworkInterface | ? Name -like "^iSCSI-B\^" | Group Network} \%\{ (Get-ClusterNetwork \$_.Name).Name = 'iSCSI-B' \}
\]

\[
\text{Get-ClusterNetworkInterface | ? Name -like "^Mgmt\^" | Group Network} \%\{ (Get-ClusterNetwork \$_.Name).Name = 'Mgmt' \}
\]

5. Configure the live migration network:
   a. Open the Failover Cluster Manager from the Server Manager, select Tools > Failover Cluster Manager.
   b. Expand the cluster tree on the left and right-click Networks. Select Live Migration Settings.
   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.
   b. Open SnapDrive from the Start screen to configure cluster storage.
   c. From SnapDrive, select the server name, then click the Open the Disks icon.
   d. Right-click the Disks icon and select Create Disk.
   e. Type in the IP address of Infra_SVM.
   f. When you are connected, open the controller tree and select the quorum volume.
   g. Type in the name of the LUN in the LUN Name box and click Next.
   h. Select Shared (Microsoft Cluster Services Only) 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 map the LUN to 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 the nodes.
q. In the Failover Cluster Manager, select Configure Cluster Quorum Settings.

r. Click Next through the Welcome screen.
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 screen and click Finish on the Summary screen.

7. Create a CSV LUN for VM storage:
   a. Open SnapDrive from the Start screen to configure cluster storage.
   b. From SnapDrive, select the server name, then click the Disks icon.
   c. Right-click the Disks icon and select Create Disk.
   d. Type the IP address of Infra_SVM.
   e. When you are connected, open the controller tree and select the *infra_datastore_1* volume.
   f. Type in 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 1TB, and click Next.
   j. Click Next through the volume properties confirmation.
k. Select the iSCSI initiators to map the LUN to and click Next.
l. Select Automatic igroup Management and click Next.
m. Select Add to Cluster Shared Volumes and click Next.
8. Run the Cluster Validation wizard from the Failover Cluster Manager to validate the deployment.

### 12 System Center 2012 R2 Virtual Machine Manager

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

#### Table 10) VM requirements.

<table>
<thead>
<tr>
<th>Role</th>
<th>Virtual CPU</th>
<th>RAM (GB)</th>
<th>Virtual Hard Disk (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Machine Manager</td>
<td>4</td>
<td>8</td>
<td>60</td>
</tr>
<tr>
<td>SMI-S Agent</td>
<td>1</td>
<td>4</td>
<td>60</td>
</tr>
</tbody>
</table>

#### 12.1 Building the SMI-S and SCVMM VMs

**One Server Only**

1. In the Failover Cluster Manager, right-click Roles, select Virtual Machines, and then select New Virtual Machine.
2. Select the host for the new VM and click OK.
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]

   ![Warning](https://example.com/warning.png)

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

5. Select Generation 2 and click Next.
6. Enter the startup memory for the VM and select the Use Dynamic Memory for This Virtual Machine checkbox. Click Next.
7. Select VMComm Network and click Next.
8. Set the size for the new VHDX and click Next.
9. Select Install an Operating System from a Bootable Image File and provide the path to the Windows Server 2012 R2 ISO. Click Finish.
10. Click Finish in the High Availability Wizard Summary.
11. Repeat steps 1 through 10 for each remaining VM.
12.2 Configuring SMI-S and SCVMM VMs
1. In the Failover Cluster Manager, select Roles, right-click the VM to be modified, and select Settings.
2. Select Memory and set the Dynamic Memory Maximum RAM to the Startup RAM.
3. Select CPU and set the CPU to the desired amount outlined in Table 10.
4. Select Network Adapter, select the Enable Virtual LAN Identification checkbox, and enter the value for `<<ib_mgmt_vlan_id>>`.
5. Select Automatic Start Action and choose the Always Start This Virtual Machine Automatically option.
6. Select Automatic Stop Action and choose the Shut Down the Guest Operating System option.
7. Click OK to save the modifications.
8. Repeat steps 1 through 7 for each remaining VM.

![Settings for SCVMM on EHYPERV1](image)

12.3 Adding SCVMM iSCSI Network Adapters
1. In the 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.
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.

### 12.4 Installing Windows Server 2012 R2 on the VMs

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

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

12. Install important and recommended Windows updates and reboot.
13. Configure network adapter settings if you are using static IPs.
   
   **Note:** The SCVMM VM has three network adapters. Look for the MAC address of the adapters in the VM Settings menu and assign the IP addresses appropriately.

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

### 12.5 Installing the NetApp SMI-S Agent

To install the NetApp SMI-S Agent, complete the following procedures.
Prerequisites
The following environment prerequisites must be met before you proceed.

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

<table>
<thead>
<tr>
<th>User Name</th>
<th>Purpose</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMIS-User</td>
<td>SMI-S access account</td>
<td>Note: This account does not need any special delegation. This is not a domain account. It must be a local account in Windows.</td>
</tr>
</tbody>
</table>

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

Installing the SMI-S Agent
You must complete the following steps to install the NetApp SMI-S Agent:
2. Unblock the downloaded file.
   Unblock-file ~\Downloads\smisagent-5-1-1.msi
3. Install the agent by running the following command:
   ~\Downloads\smisagent-5-1-1.msi /qb

Configuring the SMI-S Agent
You must complete the following steps to configure the NetApp SMI-S Agent:
1. In the Open App screen, right-click the Data ONTAP SMI-S Agent and select Run as Administrator at the bottom of the screen.
2. Change the directory into the SMI-S program files.
   cd %ProgramFiles(x86)%%\ONTAP\smis\pegasus\bin
3. Add the SVM credentials to the SMI-S Agent.
   Smis addsecure <VserverIpAddress> <VserverAdmin> <VserverAdminPassword>
4. Enable user authentication with the Cimconfig command.
   Cimconfig -p -s enableAuthentication=true
5. Restart the agent/cimserver.
   Smis cimserver restart
6. Add the SMI-S Run As account to the SMI-S configuration.
   cimuser -a -u SMIS-User -w <password>

12.6 Installing System Center Virtual Machine Manager
To install SCVMM in a minimal configuration, complete the following steps.
Prerequisites
The following environment prerequisites must be met before you proceed.

Accounts
Verify that the following accounts have been created:

<table>
<thead>
<tr>
<th>User Name</th>
<th>Purpose</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;DOMAIN&gt;\FT-VMM-SVC</td>
<td>Virtual Machine Manager Service Account</td>
<td>This account needs full administrator permissions on the VMM server virtual machine. It runs the VMM service.</td>
</tr>
<tr>
<td>&lt;DOMAIN&gt;\SnapDrive</td>
<td>SnapDrive for Windows</td>
<td>This account needs to be an administrator on the SCVMM VM.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Security Group Name</th>
<th>Group Scope</th>
<th>Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;DOMAIN&gt;\FT-SCVMM-Admins</td>
<td>Global</td>
<td>FT-VMM-SVC</td>
</tr>
<tr>
<td>&lt;DOMAIN&gt;\FT-SCVMM-FabricAdmins</td>
<td>Global</td>
<td>VMM delegated administrators</td>
</tr>
<tr>
<td>&lt;DOMAIN&gt;\FT-SCVMM-ROAdmins</td>
<td>Global</td>
<td>VMM read-only administrators</td>
</tr>
<tr>
<td>&lt;DOMAIN&gt;\FT-SCVMM-TenantAdmins</td>
<td>Global</td>
<td>VMM tenant administrators who manage self-service users</td>
</tr>
<tr>
<td>&lt;DOMAIN&gt;\FT-VMM-AppAdmins</td>
<td>Global</td>
<td>VMM self-service users</td>
</tr>
</tbody>
</table>

2. Verify that the following accounts and groups are members of the local administrator's group on the Virtual Machine Manager VM:
   - SnapDrive
   - Virtual Machine Manager Admins Group
   - Virtual Machine Manager Service Account

Installing the Windows Assessment and Deployment Kit

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

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

1. From the Windows ADK installation media source, right-click adksetup.exe and select Run as Administrator from the context menu to begin setup. If prompted by user account control, select Yes to allow the installation to make changes to the computer.
2. A splash screen appears. In the Specify Location dialog box, accept the default folder location of %ProgramFiles%\Windows Kits\8.1 and click Next to continue.
3. In the Join the Customer Experience Improvement Program (CEIP) dialog box, select the option to either participate or not participate in the CEIP by providing selected system information to Microsoft. Click Next to continue.

4. In the License Agreement dialog box, click Accept to continue.

5. In the Select the Features You Want to Install dialog box, select the following option checkboxes:
   - Deployment Tools
   - Windows Preinstallation Environment (Windows PE)

6. Make sure all other option checkboxes are deselected. Click Install to begin the installation.

7. When installation is complete, deselect the Launch the Getting Started Guide checkbox and click Close to exit the installation wizard.

**Installing the WSUS RSAT Tools**

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

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

2. Add Failover Cluster, Multipath-IO, and the WSUS console by entering the following command:

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

**Creating the VMM Distributed Key Management Container Active Directory Domain Services**

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

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

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

1. Log in to a domain controller with a user that has domain administrator privileges and run `adsiedit.msc`.

2. Right-click the ADSI Edit node and select Connect to... from the context menu.

3. In the Connections Settings dialog box in the Connection Point section, select the Select a Well-Known Naming Context option. Select Default Naming Context from the drop-down menu and click OK.

4. Expand Domain Default Naming Context [<computer fully qualified domain name>], expand <distinguished name of domain>, right-click the root node, and select New > Object from the Context menu.
5. In the Create Object dialog box, select Container and then click Next.
6. In the Value text box, type VMMDKM and then click Next.
7. Click Finish to create the container object.
8. Within ADSI Edit, right-click the new VMMDKM object and then click Properties.
9. In the VMMDKM Properties dialog box, click the Security tab. Click Add to add the VMM Service Account and VMM Admins Group. Grant the security principals full control permissions.
10. Click OK three times and close ADSI Edit.

Configuring Windows MPIO

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

1. Launch a PowerShell prompt by right-clicking the PowerShell icon in the taskbar, select Run as Administrator, and enter the following commands to install the MPIO feature.

```powershell
Add-WindowsFeature Multipath-IO -IncludeManagementTools
```

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

```powershell
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 about the installation, see the Windows Host Utilities 6.0.2 Administration Installation and Installation Setup Guide.

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

2. Launch a PowerShell prompt by right-clicking the PowerShell icon in the taskbar, select Run as Administrator, and enter the following commands to unblock the downloaded file:

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

3. Install the Host Utilities.

```powershell
~\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.

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

2. Configure the iSCSI service to start automatically.

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

3. Start the iSCSI service.

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

4. Configure MPIO to claim any iSCSI device.

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

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

   ```powershell
   Set-MSDSSMGlobalDefaultLoadBalancePolicy -Policy LQD
   ```

6. Configure an iSCSI target for each controller.

   ```powershell
   New-IscsiTargetPortal -TargetPortalAddress <<controller01_iscsia_lif_ip>> -InitiatorPortalAddress <iscsia_ipaddress>
   New-IscsiTargetPortal -TargetPortalAddress <<controller01_iscsib_lif_ip>> -InitiatorPortalAddress <iscsib_ipaddress>
   New-IscsiTargetPortal -TargetPortalAddress <<controller02_iscsia_lif_ip>> -InitiatorPortalAddress <iscsia_ipaddress>
   New-IscsiTargetPortal -TargetPortalAddress <<controller02_iscsib_lif_ip>> -InitiatorPortalAddress <iscsib_ipaddress>
   ```

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

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

### Installing NetApp SnapDrive

The following section describes how to perform an unattended installation of NetApp SnapDrive for Windows. For detailed information about the installation, refer to the SnapDrive Installation Guide.

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

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

   ![New Object - User](image)

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

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

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

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

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

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

**Creating and Mapping LUNs for SCVMM**

You can create Microsoft SQL Server® database LUNs by using SnapDrive. The LUN sizes and the purpose for each are listed in Table 11.

<table>
<thead>
<tr>
<th>LUN</th>
<th>Components</th>
<th>NetApp Volume</th>
<th>Purpose</th>
<th>Drive Letter</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>LUN_1</td>
<td>SQL Server</td>
<td>infra_sql</td>
<td>Database</td>
<td>M</td>
<td>60GB</td>
</tr>
<tr>
<td>LUN_2</td>
<td>SQL Server</td>
<td>infra_sql</td>
<td>Logs</td>
<td>N</td>
<td>30GB</td>
</tr>
<tr>
<td>LUN_3</td>
<td>VMM Library</td>
<td>infra_datastore_1</td>
<td>Library</td>
<td>L</td>
<td>500GB</td>
</tr>
</tbody>
</table>

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

**Installing SQL Server 2012 SP1**

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

1. From the SQL Server 2012 SP1 installation media source, right-click setup.exe and select Run as Administrator from the context menu to begin setup. The SQL Server Installation Center appears. Select the Installation menu option.
2. From the SQL Server Installation Center, click the New SQL Server standalone installation or add features to an existing installation link.

3. The SQL Server 2012 SP1 setup wizard appears. In the Setup Support Rules dialog box, verify that each rule shows a Passed status. If any rule requires attention, remediate the issue and rerun the validation check. Click OK to continue.

4. In the Product Key dialog box, select the Enter the Product Key option and enter the associated product key in the provided text box. Click Next to continue.
   
   **Note:** If you do not have a product key, select the Specify a Free Edition option and select Evaluation from the drop-down menu for a 180-day evaluation period.

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

6. In the Product Updates dialog box, select the Include SQL Server Product Updates checkbox and click Next to continue.

7. In the Install Setup Files dialog box, click Install and allow the support files to install.

8. In the Setup Support Rules dialog box, verify that each rule shows a Passed status. If any rule requires attention, remediate the issue and rerun the validation check.
   
   **Note:** Common issues include Microsoft Distributed Transaction Coordinator (MSDTC), Microsoft Cluster Service, and Windows Firewall warnings. Note that the use of MSDTC is not required for the System Center 2012 SP1 environment.

9. Click Next to continue.

10. In the Setup Role dialog box, select the SQL Server Feature Installation button and click Next to continue.

11. In the Feature Selection dialog box, select the following:
   - Database Engine Services
   - Management Tools – Basic
   - Management Tools – Complete

12. In the Installation Rules dialog box, click Next to continue. The Show Details and View Detailed Report can be viewed if required.

13. In the Instance Configuration dialog box, click Next to continue.

14. In the Disk Space Requirements dialog box, verify that you have sufficient disk space and click Next to continue.

15. In the Server Configuration dialog box, select the Collation tab. Click Customize.

16. In the Customize the SQL Server 2012 Database Engine Collation dialog box:
   a. Select the Windows Collation Designator and Sort Order button.
   b. Select Latin1_General_100 and click the Accent-sensitive checkbox.
   c. Click OK to set the collation to Latin1_General_100_CI_AS.
   d. Click Next to continue.
17. In the Database Engine Configuration dialog box, select the Server Configuration tab. In the Authentication Mode section, select the Windows Authentication Mode option. In the Specify SQL Server Administrators section, click the Add Current User button to add the current installation user. Click the Add button, and add the BUILTIN\Administrators and any other groups who should have administrator access to the SQL Server instance.

18. In the same Database Engine Configuration dialog box, select the Data Directories tab. The proper 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 Database Log Directory and Temp DB log Directory text boxes. NetApp also recommends changing 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. After completion, click Next to continue.
Note: If performance is not adequate, it may be necessary to relocate the temp DB files to a dedicated LUN by using the two primary SQL Server LUNs.

19. In the Error Reporting dialog box, select or clear the Send Windows and SQL Server Error Reports to Microsoft or Your Corporate Report Server checkbox based on your organization’s policies and click Next to continue.

20. In the Installation Rules dialog box, verify that each rule shows a Passed status. If any rule requires attention, remediate the issue and rerun the validation check. Click Next to continue.

21. In the Ready to Install dialog box, verify all the settings that were entered during the setup process and click Install to begin the installation of the SQL Server instance.

22. Monitor installation progress as displayed in the Installation Progress dialog box.

23. When initial installation is complete, the Complete dialog box appears. Click Close to complete the installation of this SQL Server database instance.

24. Verify the installation by inspecting the instances in the Failover Cluster Manager and in SQL Server 2012 Management Studio before you move on to the next step of installation.

Installing Virtual Machine Manager

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

1. From the VMM installation media source, right-click setup.exe and select Run as Administrator from the context menu to begin setup. If prompted by user account control, select Yes to allow the installation to make changes to the computer.

2. The VMM installation wizard begins. At the splash page, click Install to begin the VMM server installation.

3. In the Select Features to Install dialog box, verify that the Virtual Machine Manager Management Server Installation option checkbox is selected. After selecting it, the Virtual Machine Manager Console Installation option checkbox will be selected by default. Click Next to continue.

4. In the Product Registration Information dialog box, enter the following information in the text boxes and click Next to continue:
   - Name: Specify the name of the primary user or responsible party within your organization.
   - Organization: Specify the name of the licensed organization.
   - Product Key: Provide a product key for installation of VMM. If no key is provided, VMM is installed in evaluation mode.

5. Accept the EULA and click Next to continue.

6. In the Join the Customer Experience Improvement Program (CEIP) dialog box, select the option to either participate or not participate in the CEIP by providing selected system information to Microsoft. Click Next to continue.

7. In the Microsoft Update dialog box, select the option to either allow or not allow VMM to use Microsoft Update to check for and perform automatic updates based on your organization’s policies. Click Next to continue.

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

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

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

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

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

11. In the Port Configuration dialog box, accept the default values in the text boxes and click Next to continue:
   - Communication with the VMM Console: Default: 8100.
− Communication to Agents on Hosts and Library Servers: Default: 5985.
− File Transfers to Agents on Hosts and Library Servers: Default: 443.
− Communication with Windows Deployment Services: Default: 8102.
− Communication with Windows PE Agent for Time Synchronization: Default: 8103.

12. In the Library Configuration dialog box, under Share Location, click Select. Browse to the L: drive and click Make New Folder. Rename the new folder as VMM Library and click OK. Click Next to continue.

**Library configuration**

![Library configuration dialog box](image)

13. The Installation Summary dialog box appears and displays the selections you made during the installation wizard. Review the options selected and click Install to continue.

14. Monitor installation progress. The wizard displays the progress while installing the features.

15. When the initial installation is complete, the wizard displays the Setup Completed Successfully dialog box. Click Close to complete the installation.

16. When the final installation is complete, launch the Virtual Machine Manager console to verify that the installation occurred properly. Verify that the console launches and connects to the Virtual Machine Manager instance installed.

**Creating VMM Run as Account**

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

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

**Registering SMI-S in SCVMM**

Complete the following steps to register the NetApp SMI-S provider in SCVMM:

1. In the Virtual Machine Manager console, navigate to the Fabric pane and expand the Storage node. Select the Providers subnode.
2. From the ribbon, select Add Resources. Select Storage Devices from the drop-down menu.
3. In the Add Storage Devices wizard, select Add a Storage Device That Is Managed by an SMI-S Provider and then 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 window, select Create Run as Account:
      - Enter a display name.
      - Enter the user name (for example, SMIS-User).
      - Enter the password.
      - Click OK.
   e. Click Next.
6. During the discovery phase, a pop-up window opens, prompting to import the SMI-S provider’s Certificate. Click Import.
7. After the discovery operation has completed, the wizard displays the storage controllers registered with the SMI-S provider. Click Next.
8. On the Select Storage Devices page, click the Create Classification button. In the resulting pop-up window, enter a name for the storage pool.

9. Select the `infra_datastore_1` storage pool and assign a classification.

![Add Storage Devices Wizard](image)

10. Click Next and then Finish to close out the wizard.

**Adding Fabric Management Resources to Virtual Machine Manager**

1. In the Virtual Machine Manager console, navigate to the Fabric pane in the left tree view and right-click All Hosts under the Servers section. Select Create Host Group. Name the new host group.

2. Select Fabric and All Hosts. Click Add Resources, Hyper-V Hosts, and Clusters.


4. Select Use an Existing Run as Account and click Browse.

5. Select the VMM Run as Account created in section "Accounts " and click OK.

6. Click Next to proceed to the next screen.

7. Enter the cluster name and click Next.

8. Click Select All and click Next.

9. Select the Host Group created in step1 and click Next.

10. Click Finish.
11. Verify job completion.
12. Verify that the hosts have been added.

13 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.

13.1 Small Configuration

Table 12 lists the components of the small configuration.

Table 12) FlexPod Express small configuration components.

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Product Description</th>
<th>Quantity Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>N3K-C3048-FA-L3</td>
<td>Cisco Nexus 3048 Std Airflow (port side exhaust) AC P/S LAN Ent</td>
<td>2</td>
</tr>
<tr>
<td>N2200-PAC-400W</td>
<td>N2K/N3K AC Power Supply Std airflow (port side exhaust)</td>
<td>4</td>
</tr>
<tr>
<td>CAB-C13-C14-AC</td>
<td>Power cord C13 to C14 (recessed receptacle) 10A</td>
<td>4</td>
</tr>
<tr>
<td>N3K-C3048-BAS1K9</td>
<td>Cisco Nexus 3048 Base License</td>
<td>2</td>
</tr>
<tr>
<td>N3K-C3048-LAN1K9</td>
<td>Cisco Nexus 3048 LAN Enterprise License</td>
<td>2</td>
</tr>
<tr>
<td>N3K-C3048-FAN</td>
<td>Cisco Nexus 3048 Fan Module Port-side Exhaust</td>
<td>2</td>
</tr>
<tr>
<td>N3K-C3064-ACC-KIT</td>
<td>Cisco Nexus 3064PQ Accessory Kit</td>
<td>2</td>
</tr>
<tr>
<td>N3KUK9-602U2.3</td>
<td>Cisco NX-OS Release 6.0(2)U2(3)</td>
<td>2</td>
</tr>
<tr>
<td>CON-SNT-48FAL3</td>
<td>Cisco SMARTnet™ 8X5XNBD Cisco Nexus 3048 Std Airflow AC P/S LAN Ent</td>
<td>2</td>
</tr>
<tr>
<td>UCSC-C220-M3S</td>
<td>Cisco UCS C220 M3 SFF w/o CPU mem HDD PCIe PSU w/rail kit</td>
<td>2</td>
</tr>
<tr>
<td>UCS-CPU-E52650B</td>
<td>2.60 GHz E5-2650 v2/95W 8C/20MB Cache/DDR3 1866MHz</td>
<td>4</td>
</tr>
<tr>
<td>UCS-MR-1X162RY-A</td>
<td>16GB DDR3-1600-MHz RDIMM/PC3-12800/dual rank/1.35v</td>
<td>16</td>
</tr>
<tr>
<td>UCSC-RAID-MZ-220</td>
<td>Cisco UCS RAID SAS 2008M-8i Mezz Card for C220 (0/10/10)</td>
<td>2</td>
</tr>
<tr>
<td>A03-D600GA2</td>
<td>600GB 6Gb SAS 10K RPM SFF HDD/hot plug/drive sled mounted</td>
<td>4</td>
</tr>
<tr>
<td>CAB-C13-C14-AC</td>
<td>Power cord, C13 to C14 (recessed receptacle), 10A</td>
<td>4</td>
</tr>
<tr>
<td>UCSC-PSU-450W</td>
<td>450W power supply for C-Series rack servers</td>
<td>4</td>
</tr>
<tr>
<td>N2XX-ABPCI03-M3</td>
<td>Broadcom 5709 Quad Port 1Gb w/TOE iSCSI for M3 &amp; later</td>
<td>2</td>
</tr>
<tr>
<td>Part Number</td>
<td>Description</td>
<td>Quantity</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>N20-BBLKD</td>
<td>Cisco UCS 2.5 inch HDD blanking panel</td>
<td>12</td>
</tr>
<tr>
<td>UCS-M3-V2-LBL</td>
<td>Cisco M3 - v2 CPU asset tab ID label (Auto-Expand)</td>
<td>2</td>
</tr>
<tr>
<td>UCSC-HS-C220M3</td>
<td>Heat Sink for Cisco UCS C220 M3 rack server</td>
<td>4</td>
</tr>
<tr>
<td>UCSC-PCIF-01F</td>
<td>Full height PCIe filler for C-Series</td>
<td>2</td>
</tr>
<tr>
<td>UCSC-RAIL1</td>
<td>Rail Kit for C220, C22, C24 rack servers</td>
<td>2</td>
</tr>
<tr>
<td>CON-SNT-C220M3SF</td>
<td>Cisco SMARTnet 8X5XNBD UCS C220 M3 SFF w/o</td>
<td>2</td>
</tr>
</tbody>
</table>

**NetApp Components**

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAS2520A-001-R6</td>
<td>FAS2520 High Availability System</td>
<td>2</td>
</tr>
<tr>
<td>X80102A-R6-C</td>
<td>Bezel,FAS2520,R6,-C</td>
<td>1</td>
</tr>
<tr>
<td>FAS2520-111-R6-C</td>
<td>FAS2520,12x900GB,10K,-C</td>
<td>1</td>
</tr>
<tr>
<td>X1558A-R6-C</td>
<td>Power Cable,In-Cabinet,48-IN,C13-C14,-C</td>
<td>2</td>
</tr>
<tr>
<td>SVC-FLEXPOD-SYSTEMS</td>
<td>Systems Used in FlexPod Solution, Attach PN</td>
<td>1</td>
</tr>
<tr>
<td>X6560-R6-C</td>
<td>Cable,Ethernet,0.5m RJ45 CAT6,-C</td>
<td>1</td>
</tr>
<tr>
<td>X6561-R6</td>
<td>Cable,Ethernet,2m RJ45 CAT6</td>
<td>2</td>
</tr>
<tr>
<td>X6557-EN-R6-C</td>
<td>Cbl,SASCntl-Shelf/Shelf-Shelf/HA,0.5m,EN,-C</td>
<td>2</td>
</tr>
<tr>
<td>DOC-2520-C</td>
<td>Documents,2520,-C</td>
<td>1</td>
</tr>
<tr>
<td>X5518A-R6-C</td>
<td>Kit,FAS2XXX,-C,R6</td>
<td>1</td>
</tr>
<tr>
<td>OS-ONTAP-CAP2-1P-C</td>
<td>OS Enable,Per-0.1TB,ONTAP,Perf-Stor,1P,-C</td>
<td>108</td>
</tr>
<tr>
<td>SWITCHLESS</td>
<td>2-Node Switchless Cluster</td>
<td>1</td>
</tr>
<tr>
<td>SW-2-2520A-SMGR-C</td>
<td>SW-2,SnapManager Suite,2520A,-C</td>
<td>2</td>
</tr>
<tr>
<td>SW-2-2520A-SRESTORE-C</td>
<td>SW-2,SnapRestore,2520A,-C</td>
<td>2</td>
</tr>
<tr>
<td>SW-2-2520A-FLEXCLN-C</td>
<td>SW-2,FlexClone,2520A,-C</td>
<td>2</td>
</tr>
<tr>
<td>SW-2-2520A-ISCSI-C</td>
<td>SW-2,ISCSI,2520A,-C</td>
<td>2</td>
</tr>
<tr>
<td>SW-ONTAP8.2.2-CLM</td>
<td>SW,DataONTAP8.2.2,Cluster-Mode</td>
<td>2</td>
</tr>
<tr>
<td>SW-2-2520A-CIFS-C</td>
<td>SW-2,CIFS,2520A,-C</td>
<td>2</td>
</tr>
<tr>
<td>SW-2-2520A-NFS-C</td>
<td>SW-2,NFS,2520A,-C</td>
<td>2</td>
</tr>
<tr>
<td>SVC-A2-IN-NBR-E</td>
<td>HW Support,Standard2 Replace,Inst,NBD,e</td>
<td>1</td>
</tr>
<tr>
<td>SW-SSP-A2-IN-NBR-E</td>
<td>SW Subs,Standard2 Replace,Inst,NBD,e</td>
<td>1</td>
</tr>
<tr>
<td>SVC-INST-A2-IN1-NBR-E</td>
<td>Initial Install,Standard2 Replace,Inst,NBD,e</td>
<td>1</td>
</tr>
<tr>
<td>CS-OS-SUPPORT-ONTAP</td>
<td>OS Support Entitlement,ONTAP</td>
<td>1</td>
</tr>
</tbody>
</table>
### 13.2 Medium Configuration

Table 13 lists the components for the medium configuration.

**Table 13) FlexPod Express medium configuration components.**

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Product Description</th>
<th>Quantity Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco Components</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>N3K-C3048-FA-L3</td>
<td>Cisco Nexus 3048 Std Airflow (port side exhaust) AC P/S LAN Ent</td>
<td>2</td>
</tr>
<tr>
<td>N2200-PAC-400W</td>
<td>N2K/N3K AC Power Supply Std airflow (port side exhaust)</td>
<td>4</td>
</tr>
<tr>
<td>CAB-C13-C14-AC</td>
<td>Power cord C13 to C14 (recessed receptacle) 10A</td>
<td>4</td>
</tr>
<tr>
<td>N3K-C3048-BAS1K9</td>
<td>Cisco Nexus 3048 Base License</td>
<td>2</td>
</tr>
<tr>
<td>N3K-C3048-LAN1K9</td>
<td>Cisco Nexus 3048 LAN Enterprise License</td>
<td>2</td>
</tr>
<tr>
<td>N3K-C3048-FAN</td>
<td>Cisco Nexus 3048 Fan Module Port-side Exhaust</td>
<td>2</td>
</tr>
<tr>
<td>N3K-C3064-ACC-KIT</td>
<td>Cisco Nexus 3064PQ Accessory Kit</td>
<td>2</td>
</tr>
<tr>
<td>N3KUK9-602U2.3</td>
<td>Cisco NX-OS Release 6.0(2)U2(3)</td>
<td>2</td>
</tr>
<tr>
<td>CON-SNT-48FAL3</td>
<td>Cisco SMARTnet 8X5XNBD Nexus 3048 Std Airflow AC P/S LAN Ent</td>
<td>2</td>
</tr>
<tr>
<td><strong>Cisco UCS Compute</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UCSC-C220-M3S</td>
<td>Cisco UCS C220 M3 SFF w/o CPU mem HDD PCIe PSU w/ rail kit</td>
<td>4</td>
</tr>
<tr>
<td>UCS-CPU-E52650B</td>
<td>2.60 GHz E5-2650 v2/95W 8C/20MB Cache/DDR3 1866MHz</td>
<td>8</td>
</tr>
<tr>
<td>UCS-MR-1X162RY-A</td>
<td>16GB DDR3-1600-MHz RDIMM/PC3-12800/dual rank/1.35v</td>
<td>32</td>
</tr>
<tr>
<td>UCSC-RAID-MZ-220</td>
<td>Cisco UCS RAID SAS 2008M-8i Mezz Card for C220 (0/10/10)</td>
<td>4</td>
</tr>
<tr>
<td>A03-D600GA2</td>
<td>600GB 6Gb SAS 10K RPM SFF HDD/hot plug/drive sled mounted</td>
<td>8</td>
</tr>
<tr>
<td>CAB-C13-C14-AC</td>
<td>Power cord, C13 to C14 (recessed receptacle), 10A</td>
<td>8</td>
</tr>
<tr>
<td>UCSC-PSU-450W</td>
<td>450W power supply for C-series rack servers</td>
<td>8</td>
</tr>
<tr>
<td>N2XX-ABPCI03-M3</td>
<td>Broadcom 5709 Quad Port 1Gb w/TOE iSCSI for M3 &amp; later</td>
<td>4</td>
</tr>
</tbody>
</table>

1 SupportEdge Premium is required for cooperative support.
<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>N20-BBLKD</td>
<td>Cisco UCS 2.5 inch HDD blanking panel</td>
<td>24</td>
</tr>
<tr>
<td>UCS-M3-V2-LBL</td>
<td>Cisco M3 - v2 CPU asset tab ID label (Auto-Expand)</td>
<td>4</td>
</tr>
<tr>
<td>UCSC-HS-C220M3</td>
<td>Heat Sink for Cisco UCS C220 M3 Rack Server</td>
<td>8</td>
</tr>
<tr>
<td>UCSC-PCIF-01F</td>
<td>Full height PCIe filler for C-Series</td>
<td>4</td>
</tr>
<tr>
<td>UCSC-RAIL1</td>
<td>Rail Kit for C220, C22, C24 rack servers</td>
<td>4</td>
</tr>
<tr>
<td>CON-SNT-C220M3SF</td>
<td>Cisco SMARTnet 8x5xNBD Cisco UCS C220 M3 SFF w/o</td>
<td>4</td>
</tr>
</tbody>
</table>

**NetApp Components**

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAS2520A-001-R6</td>
<td>FAS2520 High Availability System</td>
<td>2</td>
</tr>
<tr>
<td>X80102A-R6-C</td>
<td>Bezel,FAS2520,R6,-C</td>
<td>1</td>
</tr>
<tr>
<td>FAS2520-111-R6-C</td>
<td>FAS2520,12x900GB,10K,-C</td>
<td>1</td>
</tr>
<tr>
<td>X1558A-R6-C</td>
<td>Power Cable,In-Cabinet,48-IN,C13-C14,-C</td>
<td>2</td>
</tr>
<tr>
<td>SVC-FLEXPOD-SYSTEMS</td>
<td>Systems Used in FlexPod Solution, Attach PN</td>
<td>1</td>
</tr>
<tr>
<td>X6560-R6-C</td>
<td>Cable,Ethernet,0.5m RJ45 CAT6,-C</td>
<td>1</td>
</tr>
<tr>
<td>X6561-R6</td>
<td>Cable,Ethernet,2m RJ45 CAT6</td>
<td>2</td>
</tr>
<tr>
<td>X6557-EN-R6-C</td>
<td>Cbl,SAS Cntl-Shelf/Shelf/Shelf/HA,0.5m,EN,-C</td>
<td>2</td>
</tr>
<tr>
<td>DOC-2520-C</td>
<td>Documents,2520,-C</td>
<td>1</td>
</tr>
<tr>
<td>X5518A-R6-C</td>
<td>Kit,FAS2XXX,-C,R6</td>
<td>1</td>
</tr>
<tr>
<td>OS-ONTAP-CAP2-1P-C</td>
<td>OS Enable,Per-0.1TB,ONTAP,Perf-Stor,1P,-C</td>
<td>108</td>
</tr>
<tr>
<td>SWITCHLESS</td>
<td>2-Node Switchless Cluster</td>
<td>1</td>
</tr>
<tr>
<td>SW-2-2520A-SMGR-C</td>
<td>SW-2,SnapManager Suite,2520A,-C</td>
<td>2</td>
</tr>
<tr>
<td>SW-2-2520A-SRESTORE-C</td>
<td>SW-2,SnapRestore,2520A,-C</td>
<td>2</td>
</tr>
<tr>
<td>SW-2-2520A-FLEXCLN-C</td>
<td>SW-2,FlexClone,2520A,-C</td>
<td>2</td>
</tr>
<tr>
<td>SW-2-2520A-ISCSCI-C</td>
<td>SW-2,iscsi,2520A,-C</td>
<td>2</td>
</tr>
<tr>
<td>SW-ONTAP8.2.2-CLM</td>
<td>SW,Data ONTAP8.2.2,Cluster-Mode</td>
<td>2</td>
</tr>
<tr>
<td>SW-2-2520A-CIFS-C</td>
<td>SW-2,CIFS,2520A,-C</td>
<td>2</td>
</tr>
<tr>
<td>SW-2-2520A-NFS-C</td>
<td>SW-2,NFS,2520A,-C</td>
<td>2</td>
</tr>
<tr>
<td>SVC-A2-IN-NBR-E</td>
<td>HW Support,Standard2 Replace,Inst,NBD,e</td>
<td>1</td>
</tr>
<tr>
<td>SW-SSP-A2-IN-NBR-E</td>
<td>SW Subs,Standard2 Replace,Inst,NBD,e</td>
<td>1</td>
</tr>
<tr>
<td>SVC-INST-A2-IN1-NBR-E</td>
<td>Initial Install,Standard2 Replace,Inst,NBD,e</td>
<td>1</td>
</tr>
<tr>
<td>CS-OS-SUPPORT-ONTAP</td>
<td>OS Support Entitlement,ONTAP</td>
<td>1</td>
</tr>
</tbody>
</table>
14 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.

15 References

This report references the following documents and resources:


---

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

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

© 2014 NetApp, Inc. All rights reserved. No portions of this document may be reproduced without prior written consent of NetApp, Inc. Specifications are subject to change without notice. NetApp, the NetApp logo, AutoSupport, Data ONTAP, FlexClone, FlexPod, FlexVol, SnapDrive, SnapManager, SnapRestore, and Snapshot are trademarks or registered trademarks of NetApp, Inc. in the United States and/or other countries. Cisco, Cisco Nexus, and Cisco UCS are registered trademarks and Cisco SMARTnet and Cisco Unified Computing System are trademarks of Cisco Systems, Inc. Microsoft, Active Directory, Hyper-V, SQL Server, Windows, Windows PowerShell, and Windows Server are registered trademarks of Microsoft Corporation. VMware and VMware vSphere are registered trademarks of VMware, Inc. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. TR-4339-1014