MURAL Hardware Installation Reference Guide

Version 3.6

Published: 2015-10-12
THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. CISCO DOES NOT WARRANT AGAINST INTERFERENCE WITH THE ENJOYMENT OF THE SOFTWARE. CISCO DOES NOT WARRANT THAT THE SOFTWARE FITS THE USER’S PURPOSE, WORKS IN COMBINATION WITH ANY OTHER EQUIPMENT OR SOFTWARE, OR CONFORMS TO ANY SPECIFICATION.

IN NO EVENT SHALL CISCO, ITS SUPPLIERS, OR AGENTS BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING LOSS PROFITS OR LOSSES OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO, ITS SUPPLIERS, OR AGENTS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco’s trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Copyright © 2015, Cisco Systems, Inc. All rights reserved.
# Table of Contents

- Verifying UCS Hardware Configuration for MURAL .......................... 8
  - Preparing for Initial Configuration ........................................ 8
  - Reviewing Hardware Topology ............................................ 8
  - Verifying Slot Assignments for Blades ................................. 9
  - Verifying Physical Connections to the Fabric Interconnects ........ 11
  - Setting the Base Configuration for the UCS System .................. 16

- Configuring Chassis Discovery Policy in Cisco UCS for MURAL .......... 19

- Configuring Ports in Cisco UCS for MURAL ............................... 21
  - Configure a Port as a Server Port or an Uplink Port ............... 21
  - Configure Storage Ports ................................................. 21
  - Create Uplink Port Channels .......................................... 23
  - Create a Fibre Channel Port Channel .................................. 25

- Updating Firmware in Cisco UCS for MURAL .............................. 28
  - Update Firmware on Adapters, CIMC, and IOM ....................... 29
  - Activate the Firmware on Adapters .................................... 30

- Server-Related Configurations in Cisco UCS for MURAL ................ 32
  - Create a KVM IP Pool ..................................................... 32
  - Create a Sub-Organization .............................................. 32
  - Create a Server Pool ................................................... 34
  - Create a UUID Suffix Pool ............................................. 35

- Network-Related Configurations in Cisco UCS for MURAL ............... 37
  - Create MAC Pools ....................................................... 37
  - Create a Network Control Policy ..................................... 38
Create VLANs ............................................................................................................. 38

**Storage-Related Configurations in Cisco UCS for MURAL .................. 40**

Create WWNN Pools ................................................................. 40
Create WWPN Pools ................................................................. 40
Create VSANs .............................................................................. 41

**Configuring Cisco UCS Templates and Policy for MURAL .................. 43**

Create vNIC Templates ............................................................... 43
Create vHBA Templates ............................................................... 45
Create a BIOS policy ................................................................. 46
Create a Host Firmware Policy .................................................. 47
Create Local Disk Configuration Policy ........................................ 48
Create a Maintenance Policy ...................................................... 49
Create a Boot Policy ................................................................. 50
Create a Service Profile Template .............................................. 51
Deploy a Service Profile ............................................................ 57
Configure Call Home ................................................................. 59
Configure NTP ............................................................................. 61

**Configuring Cisco UCS Direct-Attached SAN .............................. 63**

Set Fabric Interconnects to FC Switch Mode .................................. 63
Create VSANs for Zoning ........................................................... 64
Designate Storage Ports ............................................................. 66
Assign the Storage Cloud VSAN to the FC Ports .......................... 68
Confirm Storage Port WWPN is Logged Into the Fabrics ............... 69
Create Storage Connection Policies ............................................. 71
Create SAN Connectivity Policy .................................................................73
Configure SAN Cloud Policy .................................................................74
Create vHBA Initiator Groups .................................................................77
Verifying Service Profile Templates .........................................................77

**Allocating Storage on the EMC** ..............................................................79
Configure the Base IP Addresses to Access the EMC System ..................79
EMC Hardware Installation Prerequisites ...............................................79
Verify Zoning/FLOGI on the Fabric Interconnect .................................80

**Registering MURAL Nodes with EMC** ....................................................83
Before You Begin .........................................................................................83
Create RAID Groups and LUNs ...............................................................87
Create Storage Groups .............................................................................93
Adjust Caching on the EMC ....................................................................96
Verifying UCS Hardware Configuration for MURAL

The Cisco Unified Computing System (UCS) 5108 Blade Server hosts the hardware components (blades) on which the Mobility Unified Reporting and Analytics (MURAL) software components (nodes) run. This topic describes:

- Verifying UCS hardware configuration, such as slot assignments for blades, fabric interconnections, uplinks for UCS SANs, and network uplinks
- Configuring initial UCS settings, such as the admin password, the management port IP address, a cluster for the two fabrics, and the default gateway

Before you begin, verify that you have all items listed in the bill of materials (BOM).

Preparing for Initial Configuration

Before You Begin

Before you begin configuring the fabrics, verify the following physical connections:

- The Management Ethernet port (mgmt0) is connected to an external hub, switch, or router.
- L1 ports on both fabric interconnects are directly connected to each other.
- L2 ports on both fabric interconnects are directly connected to each other.

Set the console port parameters on the computer terminal (or console server) to:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

Reviewing Hardware Topology

MURAL has been tested and validated in the configuration shown in the following figure.
To verify UCS hardware configuration, including slot assignments for blades, connections between Fabric Interconnects, SAN uplinks, and network uplinks, perform the tasks described in the following sections:

- "Verifying UCS Hardware Configuration for MURAL" on the previous page
- "Verifying Physical Connections to the Fabric Interconnects" on page 11

**Verifying Slot Assignments for Blades**

The **IP Survey** worksheet in the Customer Information Questionnaire (CIQ) specifies for your deployment which nodes run on the blades installed in slots on the chassis. The sample slot assignments in the following figures and tables are for illustrative purposes only; refer to your CIQ for the actual assignments.

**Notes:**

- All blades are physically identical, except the UI/Caching blades, which have two to three times more RAM than the others.
The sample slot assignments provide for high availability by placing redundant nodes of each type on different chassis (for example, the Insta 1 node is on Chassis 1 and the Insta 2 node is on Chassis 2). Verify that your slot assignments follow this pattern.

- Slots are numbered 1 through 8 from left to right, top to bottom.

**Double Chassis for a Standard MURAL Deployment**

The following figure and table depict sample slot assignments for Chassis 1.

<table>
<thead>
<tr>
<th>Chassis</th>
<th>Slot</th>
<th>Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Collector 1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>Compute 1</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>Compute 2</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>Insta 1</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>Rubix/UI 1</td>
</tr>
<tr>
<td>1</td>
<td>6</td>
<td>GMS 1</td>
</tr>
</tbody>
</table>

The following figure and table depict sample slot assignments Chassis 2.
<table>
<thead>
<tr>
<th>Chassis</th>
<th>Slot</th>
<th>Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>Collector 2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>Compute 3</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>Compute 4</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>Insta 2</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>Rubix/UI 2</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>GMS 2 (optional)</td>
</tr>
</tbody>
</table>

**Note:** When assigning the blades, ensure that **HA Level** is maintained for Collector, Compute, Insta, Rubix (UI/Caching), and optionally GMS nodes. Ensure that HA nodes are not assigned on same chassis.

**Verifying Physical Connections to the Fabric Interconnects**

Verify the physical connections between the Cisco UCS 6248UP 48-Port Fabric Interconnect and other hardware components.

**Verifying Connections to the Management Network**

Verify that the physical connections match the following figure and table which shows a front view of the equipment and illustrates the connections needed.
Verifying Connections to the Chassis

Verify that the physical connections between the Fabric Interconnects and the Blade Server chassis match the following figure and tables.

Connecting First Chassis

The following table indicates how to connect the ports in the Cisco UCS Fabric Extenders for Chassis 1 to the ports on Fabric Interconnects A and B. Consult the bill of materials (BOM) to determine which model of Fabric Extender is specified for your deployment.

<table>
<thead>
<tr>
<th>UCS 2104XP Chassis 1 Fabric</th>
<th>UCS 6248 Fabric Interconnect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extender 1: Slot 1:</td>
<td>Interconnect A:</td>
</tr>
<tr>
<td>Port 1</td>
<td>Port 1</td>
</tr>
<tr>
<td>Port 2</td>
<td>Port 2</td>
</tr>
<tr>
<td>Port 3</td>
<td>Port 3</td>
</tr>
<tr>
<td>Port 4</td>
<td>Port 4</td>
</tr>
</tbody>
</table>
### Connecting Second Chassis

The following table indicates how to connect the ports in the Cisco UCS Fabric Extenders for Chassis 2 to the ports on Fabric Interconnects A and B.

<table>
<thead>
<tr>
<th>UCS 2104XP Chassis 2 Fabric</th>
<th>UCS 6248 Fabric Interconnect</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Extender 1:Slot 1:</strong></td>
<td><strong>Interconnect B:</strong></td>
</tr>
<tr>
<td>Port 1</td>
<td>Port 1</td>
</tr>
<tr>
<td>Port 2</td>
<td>Port 2</td>
</tr>
<tr>
<td>Port 3</td>
<td>Port 3</td>
</tr>
<tr>
<td>Port 4</td>
<td>Port 4</td>
</tr>
<tr>
<td><strong>Extender 2:Slot 2:</strong></td>
<td><strong>Interconnect A:</strong></td>
</tr>
<tr>
<td>Port 1</td>
<td>Port 5</td>
</tr>
<tr>
<td>Port 2</td>
<td>Port 6</td>
</tr>
<tr>
<td>Port 3</td>
<td>Port 7</td>
</tr>
<tr>
<td>Port 4</td>
<td>Port 8</td>
</tr>
</tbody>
</table>
Verifying Connections to the SAN

Verify that the physical connections between the Fabric Interconnects and the UCS storage area network (SAN) uplinks match the following figure and table:

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP-A management port</td>
<td>Customer management switch</td>
</tr>
<tr>
<td>SP-B management port</td>
<td>Customer management switch</td>
</tr>
<tr>
<td>SP-A FC-A</td>
<td>Fabric A—Port 31</td>
</tr>
<tr>
<td>SP-A FC-B</td>
<td>Fabric B—Port 31</td>
</tr>
<tr>
<td>SP-B FC-A</td>
<td>Fabric A—Port 32</td>
</tr>
<tr>
<td>SP-A FC-B</td>
<td>Fabric B—Port 32</td>
</tr>
</tbody>
</table>
Verifying Connections to the UCS Networks

Verify that the physical connections between the Fabric Interconnects and the UCS networks match the following figure and table:

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric A—Port 17</td>
<td>Customer production network</td>
</tr>
<tr>
<td>Fabric B—Port 17</td>
<td>Customer production network</td>
</tr>
<tr>
<td>Fabric A—Port 18</td>
<td>Customer secondary production switch (optional)</td>
</tr>
<tr>
<td>Fabric B—Port 18</td>
<td>Customer secondary production switch (optional)</td>
</tr>
</tbody>
</table>

Setting the Base Configuration for the UCS System

To set the base configuration for the UCS system and enable the fabrics be brought up of the fabrics, complete the following procedure to set the admin password, set up the management port IP address, set up a cluster for the two fabrics, and specify the default gateway.

To set the base UCS configuration, perform the following steps:
1. Connect to the console port of fabric A.

   **Note:** Use these settings for the console port parameters on the computer terminal or console server—9600 baud, 8 data bits, 1 stop bit, and no parity.

2. For fabric A, set the following parameters:

   Configuration method: *console*
   Setup mode: *setup*
   New fabric interconnect: *Y*
   Enforce strong password: *Y*
   Admin password: *admin-password*
   Is this Fabric Interconnect part of a cluster: *Y*
   Switch fabric: *A*
   System Name: *UCS-name*
   Mgmt0 IP address: *Fab-A-mgmt-port-IP-address*
   Mgmt0 Netmask: *mgmt-port-IP-netmask*
   IPv4 default gateway: *gateway-address-in-mgmt-subnet*
   Cluster IPv4 address: *Virtual-IP-for-active-node*

   Where:
   - *UCS-name* does not end with -A or -B.
   - *Virtual-IP-for-active-node* is usually the IP belonging to the management subnet.

   **Note:** You can also configure the DNS server address and the unit’s domain name, but this is not required.

3. Connect to the console port of fabric B, and verify the redundancy cables between the two fabrics are connected. Perform the initial configuration with the following parameters:

   Configuration method: *console*
   This fabric interconnect will be added to the cluster: *Y*
   Admin password of interconnect: *admin-password*
   Mgmt0 IP address: *Fab-B-management-port-IP-address*
Where \textit{admin-password} is the same as what was used for Fabric A.

You can now log in to the management UI from a web browser at \texttt{http://ip-address-of-cluster}. 
Configuring Chassis Discovery Policy in Cisco UCS for MURAL

After the initial configuration and cabling of Fabric Interconnect A and B is complete, open a browser and connect to the cluster IP address and launch Cisco Unified Computing System (UCS) Manager.

Set the number of connections required for a chassis to be discovered and configure the power policy for environments with two power sources.

1. In the **Navigation** pane, click **Equipment** tab.
2. On the **Equipment** tab, click the **Equipment** node.
3. In the **Work** pane, click the **Policies** tab.
4. Click the **Global Policies** subtab, and perform the following steps:

   a. In the **Chassis/FEX Discovery Policy** area, select a policy from the **Action** drop-down list. This selection specifies the minimum number of connections between the I/O modules (IOMs) and the Fabric Interconnects (FIs).

      Each IOM in this setup has four connections to its associated FI, therefore it is recommended to select the 4 link policy.

   b. Set the **Link Grouping Preference** as **Port Channel**.

   c. In the **Power Policy** area, select the **Grid** option. This is required for environments with two power sources. If one source fails (causing a loss of power to one or both power supplies), the surviving power supplies on the other power circuit continues to provide power to the chassis. Both grids in a power redundant system must have the same number of power supplies. Slots 1 and 2 are assigned to grid 1 and slots 3 and 4 are assigned to grid 2.
The following image illustrates the **Global Policies** subtab.
Configuring Ports in Cisco UCS for MURAL

After configuring the chassis discovery policy, configure ports in the Cisco Unified Computing System (UCS) specifically for MURAL.

Configure a Port as a Server Port or an Uplink Port

Configure the connections between IOM and FI as Server ports and connections to network as Uplink ports.

1. In the Navigation pane, click Equipment tab.
2. On the Equipment tab, expand Equipment > Fabric Interconnects > Fabric_Interconnect_Name.
3. Click Fixed Module or Expansion Module node as required.
4. Select a node and right-click in the General pane.
5. To configure the port as Server port, select Configure as Server Port.
   To configure the port as Uplink port, select Configure as Uplink Port.

The following image illustrates the procedure in the UI.

Configure Storage Ports

1. In the Navigation pane, click the Equipment tab.
2. On the Equipment tab, expand Equipment > Fabric Interconnects >
Fabric_Interconnect_Name.

3. In the Work pane, click the General tab.

4. In the Actions area of the General tab, click Configure Unified Ports.

5. Review the confirmation message and click Yes to acknowledge that a reboot of the module will be necessary to make these changes.

6. Click the Configure Fixed Module option.

7. Use your mouse to drag the slider along the bar until the display shows the ports that you want to configure as storage ports.

8. Click Finish to save your port mode configuration.

The following image illustrates the configuration of storage ports in the UI.
Create Uplink Port Channels

To create port channels on each FI for Uplink ports:

1. In the Navigation pane, click the **LAN** tab.

2. On the **LAN** tab, expand **LAN > LAN Cloud**.

3. Expand the node for the fabric interconnect where you want to add the port channel.

4. Right-click the **Port Channels** node and choose **Create Port Channel**.

5. In the Set Port Channel Name page of the Create Port Channel wizard, specify the ID and name for the port channel.

   The following image illustrates the Set Port Channel Name page.
In the Add Ports page of the Create Port Channel wizard, select the required ports and add them to the **Ports in the port channel** table.

The following image illustrates the Add Ports page.
7. Click **Finish**.

8. Select the Port Channel and enable it. Set the appropriate speed as illustrated in the succeeding image.

Create a Fibre Channel Port Channel

1. In the Navigation pane, click the **SAN** tab.

2. On the **SAN** tab, expand **SAN > SAN Cloud**.

3. Expand the node for the fabric where you want to add the port channel.

4. Right-click the **FC Port Channels** node and choose **Create Port Channel**.

5. In the Set Port Channel Name page of the Create Port Channel wizard, specify the ID and name for the port channel. The following image illustrates the Set Port Channel Name page.
6. In the Add Ports page of the Create Port Channel wizard, select the required ports and add them to the **Ports in the port channel** table.

The following image illustrates the Add Ports page.

7. Click **Finish**.

8. Select the Port Channel and enable it. Set the appropriate speed as illustrated in the succeeding image.
Updating Firmware in Cisco UCS for MURAL

Complete the procedure in this section to manually update the firmware to the release 2.1 on the newly installed system.

**Note:** Refer to the MURAL Release Notes before upgrading to any firmware release as the order of these steps may change over time.

1. Download the following latest firmware packages from [http://www.cisco.com/](http://www.cisco.com/).
   - The “*.A.bin” file contains all the firmware for the Fabric Interconnects, I/O Modules and UCS Manager
   - The “*.B.bin” file contains all of the firmware for the B-Series blades.

The following image illustrates the packages to be downloaded.

For more information, refer to [Obtaining Firmware Packages from Cisco](http://www.cisco.com/).

2. Launch the UCS Manager.

3. In the **Navigation** pane, click the **Equipment** tab.

4. In the **Work** pane, click the **Firmware Management** tab.

5. Click the **Installed Firmware** tab.
6. Click **Download Firmware**.

7. In the Download Firmware dialog box, click the **Local File System** option in the **Location of the Image File** field.

8. In the **Filename** field, type the full path where the firmware packages are saved. Alternatively, click **Browse**.

The following image illustrates the Download Firmware dialog box.

![Download Firmware dialog box](image)

The newly downloaded packages are displayed on the **Equipment > Firmware Management > Packages** tabs.

**Update Firmware on Adapters, CIMC, and IOM**

1. In the **Navigation** pane, click the **Equipment** tab.

2. On the **Equipment** tab, click the **Equipment** node.

3. In the Work pane, click the **Firmware Management** tab.

4. On the **Installed Firmware** tab, click **Update Firmware**.

5. In the Update Firmware dialog box, perform the following steps:

   - From the **Filter** drop-down list on the menu bar, select **Adapters**.
   - Select the **2.1 (1a)** bundle from the **Set Bundle** drop-down list.
   - Click **OK**.
To ensure that the update is successful, note the Update Status column for all updated endpoints. Do not activate the firmware until the status is displayed as Ready.

The following image illustrates the Update Firmware dialog box.

---

Activating the Firmware on Adapters

1. In the Navigation pane, click the Equipment tab.
2. On the Equipment tab, click the Equipment node.
3. In the Work pane, click the Firmware Management tab.
4. On the Installed Firmware tab, click Activate Firmware.
5. To activate the firmware on adapters, perform the following steps in the Activate Firmware dialog box:
   - From the Filter drop-down list on the menu bar, select Adapters.
   - Select the 2.1 (1a) bundle from the Set Bundle drop-down list.
   - Check the Set Startup Version Only check box.
   - Click OK.

To ensure that the activation is successful, note the Activate Status column for all activated endpoints.
The following image illustrates the Activate Firmware dialog box.

To activate the subordinate Fabric Interconnect and then the primary Fabric Interconnect, perform the following steps in the Activate Firmware dialog box.

- From the **Filter** drop-down list on the menu bar, select **Fabric Interconnects**.
- Click **OK**.

To ensure that the activation is successful, note the Activate Status column for all the activated FIs.

The following image illustrates the Activate Firmware dialog box.
Server-Related Configurations in Cisco UCS for MURAL

Create a KVM IP Pool

1. In the Navigation pane, click the LAN tab.


3. Right-click the IP Pool ext-mgmt node and select Create Block of IP addresses.

4. In the Create a Block of IP Addresses dialog box, specify the starting IP address and other IP addresses required, along with the default gateway, primary DNS server and secondary DNS server.

The following image illustrates the Create a Block of IP Addresses dialog box.

Create a Sub-Organization

This is an optional procedure for granularity and organizational purposes and is meant to contain servers/pools/policies of different functions.
1. Right-click any root directory and select \textit{Create Organization}. 

The following image illustrates the navigation to root directory in UI.

![Image of navigation to root directory]

2. Specify the name of the organization and other parameters.

The following image illustrates the Create Organization dialog box.
3. Click **OK**.

The newly created sub-organization is displayed on the relevant tabs.

**Create a Server Pool**

1. In the **Navigation** pane, click the **Servers** tab.
2. On the **Servers** tab, expand **Servers > Pools**.
3. Expand the **root > Sub-Organizations > ESXi_Servers** nodes.
4. Right-click the **Server Pools** node and select **Create Server Pool**.
5. In the Create Server Pool wizard, specify a name for the pool and select the servers to be part of the pool.
The following image illustrates the Add Servers page.

Create a UUID Suffix Pool

1. In the Navigation pane, click the Servers tab.
2. On the Servers tab, expand Servers > Pools.
3. Expand the root > Sub-Organizations nodes.
4. Right-click the UUID Suffix Pool node and select Create UUID Suffix Pool.
5. In the Create UUID Suffix Pool wizard, specify a name for the pool and create a block of UUID Suffixes. For example, create a two letter or numeric code ("11" for production ESXi) that aligns with the MAC/HBA templates. This allows to easily identify a server.
The following image illustrates the Add UUID Blocks page.
Network-Related Configurations in Cisco UCS for MURAL

Create MAC Pools

Create two MAC pools for each group of servers such as ESXi_Servers, and Windows_Servers. One MAC pool goes out of the fabric A and another one goes out of the fabric B.

1. In the Navigation pane, click the **LAN** tab.
2. On the **LAN** tab, expand **LAN > Pools**.
3. Expand the **root > Sub-Organizations** nodes.
4. Right-click the **MAC Pools** node and select **Create MAC Pool**.
5. In the Create MAC Pool wizard, specify a name for the pool and a MAC address range. For easy identification, you can specify “11” for production ESXi and “A” or “B” for the fabric through which the traffic is routed. If you have multiple UCS pods and multiple sites, consider creating a slightly more complex naming convention that will allow you to easily identify exactly where traffic is coming from by simply reviewing the MAC address information.

The following image illustrates the newly added MAC pools.
Create a Network Control Policy

1. In the Navigation pane, click the LAN tab.
2. On the LAN tab, expand LAN > Policies.
3. Expand the root > Sub-Organizations nodes.
4. Right-click the Network Control Policy node and select Create Network Control Policy.
5. In the Create Network Control Policy dialog box, specify a name of the policy and enable Cisco Discovery Protocol (CDP).

The following image illustrates the enabling of CDP in UI.

Create VLANs

1. In the Navigation pane, click the LAN tab.
2. On the LAN tab, expand LAN Cloud.
3. Right-click the VLANs node and select Create VLANs.
4. In the Create VLANs dialog box, specify a name and an identifier of the VLAN.
The following image illustrates the Create VLANs dialog box.
Storage-Related Configurations in Cisco UCS for MURAL

Create WWNN Pools

1. In the Navigation pane, click the SAN tab.
2. On the SAN tab, expand SAN > Pools.
3. Expand the root > Sub-Organizations nodes.
4. Right-click the WWNN Pools node and select Create WWNN Pool.
5. In the Create WWNN Pool wizard, specify a name for the pool and select a WWNN pool range. Each server must have two HBAs and therefore two WWNNs. Therefore, the number of WWNNs must be equal to twice the number of servers in the pool.

The following image illustrates the newly added WWNN pool.

Create WWPN Pools

1. In the Navigation pane, click the SAN tab.
2. On the SAN tab, expand SAN > Pools.
3. Expand the root > Sub-Organizations nodes.
4. Right-click the WWPN Pools node and select Create WWPN Pool.
5. In the Create WWPN Pool wizard, specify a name for the pool and select a WWPN pool range.
The following image illustrates the newly added WWPN pool.

Create VSANs

1. In the Navigation pane, click the SAN tab.
2. On the SAN tab, expand SAN Cloud.
3. Right-click the VSANs node and select Create VSANs.
4. In the Create VSAN dialog box, perform the following steps:
   - In the Name box, enter a name for the VSAN.
   - Select the Both Fabrics Configured Differently check box.
   - Specify the VSAN ID and FCoE ID for both the fabrics, A and B.

The following image illustrates the Create VSAN dialog box.

After creating the VSAN, perform the following procedure:
1. In the Navigation pane, click the **SAN** tab.

2. On the **SAN** tab, click **SAN Cloud**.

3. Expand **Fabric A > FC Port Channels** and select the appropriate VSAN.

   Expand **Fabric B > FC Port Channels** and select the appropriate VSAN.

4. Repeat steps 2 through 3 for each FC port channel.

5. Click **Save Changes**.

The following image illustrates selection of the newly created VSAN for a FC port channel.
Configuring Cisco UCS Templates and Policy for MURAL

This chapter includes the following sections:

- "Create vNIC Templates" below
- "Create vHBA Templates" on page 45
- "Create a BIOS policy" on page 46
- "Create a Host Firmware Policy" on page 47
- "Create Local Disk Configuration Policy" on page 48
- "Create a Maintenance Policy" on page 49
- "Create a Boot Policy" on page 50
- "Create a Service Profile Template" on page 51
- "Deploy a Service Profile" on page 57
- "Configure Call Home" on page 59
- "Configure NTP" on page 61

Create vNIC Templates

Create two vNIC templates for each group of servers. One going out the “A” side of the fabric and one going out the “B” side.

Prerequisites

Ensure that you have configured the following before creating a vNIC template:

- VLAN
- MAC pool
- Network Control policy

To create a vNIC template:

1. In the Navigation pane, click LAN tab.
2. On the LAN tab, expand LAN > Policies > root > Sub-Organization.
3. Right-click the **vNIC Templates** node, and select Create vNIC Templates.

4. In the Create vNIC Template dialog box, perform the following steps:

   - In the **Name** box, enter a name for the template.
   - Select the **Fabric ID** option. The selection will be based on the Fabric for which you are creating this template.
   - Select the **Updating Template** option.
   - In the **VLANs** area, select the check box next to the appropriate VLANs.
   - From the **MAC Pool** drop-down list, select a MAC pool.
   - From the **Network Control Policy** drop-down list, select the policy.

The following table illustrates the Create vNIC Template dialog box.

The following image illustrates the UI after creating both the vNIC templates.
Create vHBA Templates

Create two vHBA templates for each group of servers. One template goes out of the “A” side of the fabric and another one goes out of the “B” side of the fabric.

Prerequisites

Ensure that you have configured the following before creating a vHBA template:

- VSAN
- WWPN pool

To create a vHBA template:

1. In the Navigation pane, click SAN tab.
2. On the SAN tab, expand SAN > Policies > root > Sub-O rganizations.
3. Right-click the vHBA Templates node, and select Create vHBA Templates.
4. In the Create vHBA Template dialog box, perform the following steps:
• In the **Name** box, enter a name for the template.

• Select the **Fabric ID** option.

  The selection will be based on the Fabric for which you are creating this template.

• Select the **Updating Template** option.

• In the **VSANs** area, select the check box next to the appropriate VSANs.

• From the **WWPN Pool** drop-down list, select a WWPN pool.

The following table illustrates the Create vHBA Template dialog box.

---

### Create a BIOS policy

1. In the Navigation pane, click the **Servers** tab.

2. On the **Servers** tab, expand **Servers > Policies > root > Sub-Organizations**.

3. Right-click **BIOS Policies** and select **Create BIOS Policy**.

4. Perform the following steps in the Create BIOS Policy wizard that is displayed:
• On the Main page, enter a name for the BIOS policy.

• On the Processor page, disable **Turbo Boost** and **Enhanced Intel Speedstep**. This is required for hypervisors.

The following image illustrates the Processor Page of the Create BIOS Policy wizard.

Create a Host Firmware Policy

1. In the Navigation pane, click the **Servers** tab.

2. On the **Servers** tab, expand **Servers > Policies > root > Sub-O rganizations**.

3. Right-click **Host Firmware Packages** and select **Create Host Firmware Package**.

4. In the Create Host Firmware Package dialog box, enter a name for the policy and select the appropriate package.

The following image illustrates the Create Host Firmware Package dialog.
box.

Create Local Disk Configuration Policy

Go to the “Servers” tab, then “Policies->root->Sub-Organizations->Local Disk Config Policies”. Right-click “Local Disk Config Policies” and select “Create Local Disk Configuration Policy”. Give the policy a name and under “Mode:” select “No Local Storage” (assuming you are booting from SAN)

1. In the Navigation pane, click the **Servers** tab.

2. On the **Servers** tab, expand **Servers > Policies > root > Sub-Organizations**.

3. Right-click **Local Disk Config Policies** and select **Create Local Disk Configuration Policy**.

4. In the Create Local Disk Configuration Policy dialog box, enter a name for the policy and select the **No Local Storage** option (assuming the system boots from SAN) from the **Mode** drop-down list.

The following image illustrates the Create Local Disk Configuration Policy
Create a Maintenance Policy

1. In the Navigation pane, click the Servers tab.

2. On the Servers tab, expand Servers > Policies > root > Sub-O rganizations.

3. Right-click Maintenance Policies and select Create MaintenancePolicy.

4. In the Create Maintenance Policy dialog box, enter a name for the policy and select the User ack option. This is required so the administrator must acknowledge any maintenance tasks that require a reboot of the server.

The following image illustrates the Create Maintenance Policy dialog box.
Create a Boot Policy

1. In the Navigation pane, click the Servers tab.

2. On the Servers tab, expand Servers > Policies > root > Sub-Organizations.

3. Right-click Boot Policy and select Create Boot Policy.

4. In the Create Boot Policy dialog box, enter a name for the policy and add a CD-ROM as the first device in the boot order.

5. Click the down arrows to expand the vHBAs area and click Add SAN Boot link.

6. In the Add SAN Boot dialog box, enter the name of your vhBA template. the same as your vhBA template.

Each SAN Boot vhBA has two SAN Boot Targets that needs to be added. The WWNs you enter must match the cabling configuration of your FIs. For example, use the cabling configuration as illustrated in the following image:

The following image illustrates the recommended boot policy configuration
Create a Service Profile Template

Prerequisites

Before building the service profile, ensure that you have configured the following:

- Policies
- Pools
- Interface templates

To create a service profile:

1. In the Navigation pane, click the Servers tab.
2. On the Servers tab, expand Servers > Service Profile Templates > root > Sub-Organizations.
3. Right-click the required Sub-Organization and select Create Service.
Profile Template.

4. In the Identify Service Profile Template page, perform the following steps:
   
   - In the **Name** box, enter a name for the template.
   
   - Select the **Updating Template** option. This will allow you to modify the template at a later time and have those modifications propagate to any service profiles that were deployed using that template.
   
   - From the **UUID Assignment** drop-down list, select the UUID pool that you created earlier.

   The following table illustrates the Identify Service Profile Template page.

   ![Identify Service Profile Template](image)

5. Click **Next** and perform the following steps in the Networking page:
   
   - Select the **Expert** radio button to configure LAN connectivity.
   
   - Click **Add** to add six NICS for ESXi hosts, two for MGMT, two for VMs, and two for vMotion. In the Create vNIC dialog box, select the **Use vNIC Template** checkbox, vNIC Template A/B and the VMware adapter policy. Alternate between the “A” and “B” templates on each vNIC.
The following image illustrates the Networking page.

![Networking Page](image)

6. Click **Next** and perform the following steps in the Storage page:

   - From the **Local Storage** drop-down list, select the local storage policy created earlier.
   - Select the **Expert** option.
   - Click **Add** to add two vHBAs. In the Create vHBA dialog box, select the **Use vHBA Template** checkbox and specify a name for the vHBA.
   - Select the appropriate vHBA Template (For example, vHBA_A > ESXi_HBA_A) and an adapter policy.
The following image illustrates the Storage page.

![Unified Computing System Manager](image)

7. Click **Next** to skip the Zoning and vNIC/vHBA Placement pages. In the Server Boot Order page, select the appropriate boot policy.

The following image illustrates the Server Boot Order page.

![Unified Computing System Manager](image)

8. Click **Next**. In the Maintenance Policy page, select the appropriate
maintenance policy.

The following image illustrates the Maintenance Policy page.

9. Click **Next**. In the Server Assignment page, ensure that default values are selected in the **Pool Assignment** and **Power State** fields. From the **Firmware Management** drop-down list, select the appropriate firmware management policy.

   The following image illustrates the Server Assignment page.
10. Click **Next**. In the Operational Policies page, select the BIOS policy created earlier.

The following image illustrates the Operational Policies page.
11. Click **Finish**.

**Deploy a Service Profile**

1. In the Navigation pane, click the **Servers** tab.

2. On the **Servers** tab, expand **Servers > Service Profile Templates > root > Sub-O rganizations**.

3. Right-click the appropriate service profile template and select **Create service profiles from template**.

4. In the Create service profiles from template dialog box, select a naming prefix and the amount of service profiles to be created.

   The following image illustrates the Create service profiles from template dialog box.
5. To associate a physical server with the newly created profile, right-click the service profile and select **Change service profile association**.

6. In the Associate Service Profile dialog box, choose **Select existing server** from the **Server Assignment** drop-down list. Select the appropriate blade and click **OK**.

   The following image illustrates the Associate Service Profile dialog box.
Note: You can also have the UCS Manager automatically assign a service profile to a physical blade by associating the service profile template to a server pool. However, the way in which UCS automatically assigns a profile to a blade is not recommended. The manual assigning of a service profile allows you to assign profiles to specific slots for better organization.

Configure Call Home

1. In the Navigation pane, click the Admin tab.
2. On the Admin tab, expand Communication Management.
3. Click Call Home.
4. In the Work pane, click the General tab.
5. On the General tab, select the On option in the State field. Specify the required values as illustrated in the following image.

6. Click the Profiles tab and perform the following steps:
   - Expand Profile CiscoTAC-1 and add callhome@cisco.com.
   - Expand Profile full_txt and add the internal email address.

   The following image illustrates the Profile tab.

7. Click the Call Home Policies tab, and add the required policies.

   The following image illustrates the selection of policies that will alert you to any major equipment problems.
8. Click the **System Inventory** tab, and perform the following steps:

   - Select the **On** option in the **Send Periodically** field.
   - In the **Send Interval (days)** box, enter a required interval in days.
   - Click **Save Changes**.

   The following image illustrates the **System Inventory** tab.

9. Click **Finish**.

**Configure NTP**

1. In the Navigation pane, click the **Admin** tab.

2. On the **Admin** tab, expand **Time Zone Management**.

3. Click **Add NTP Server** and add an NTP server.

4. Click **Save Changes**.
The following image illustrates the Add NTP Server page.
Configuring Cisco UCS Direct-Attached SAN

This section describes how to set up Cisco UCS Direct-Attached SAN, which enables you to directly-attach a fiber-channel SAN to the Fabric Interconnects (FIs).

Set Fabric Interconnects to FC Switch Mode

To set the Fabric Interconnects into FC Switch Mode:

1. In the Navigation pane, click the Equipment tab.
2. Expand Equipment > Fabric Interconnect A/B nodes.
3. In the Work pane, click the General tab.
4. Select both Set FC Switching Mode and Set Ethernet Switching Mode.
5. Click Save Changes.
6. If FC Mode is not shown as Switch, reboot the system.
7. Repeat steps 1 through 5 for the other FIs.
Create VSANs for Zoning

Create one virtual storage area network (VSAN) for each FI.

Follow these guidelines and recommendations when naming VSANs, including storage VSANs:

- Do not configure a VSAN as 4079. This VSAN is reserved and cannot be used in either FC switch mode or FC end-host mode.
- Do not configure VSANs with an ID in the range from 3040 to 4078 if you plan to use FC switch mode in a Cisco UCS domain. In FC switch mode, VSANs in that range are not operational and the Cisco UCS Manager marks them with an error and raises a fault.

To create a VSAN for a Fabric Interconnect:

1. In the Navigation pane, click the the SAN tab.
2. Expand **SAN Cloud > Fabric A/B.**
3. Right-click **VSANs** and click **Create VSAN.**
4. In the **Name** box, enter a name for the VSAN. For naming convention, refer to the succeeding image.

5. Select the FC Zoning Enabled, Fabric A/B, VSAN ID, and FCoE VLAN, as illustrated in the following image.

![Image of FC Zoning Configuration](image.png)

**Notes:** Ensure that the FCoE VLAN ID is same as the VSAN ID. You can use the values 3010 and 3020 for the VSANs. Ensure that these values are not used in the network.

6. Repeat steps 1 through 5 for other FIs.

7. Click **Save Changes**.

VSANs are required under both SAN and Storage clouds, as illustrated in the following image.
Designate Storage Ports

For each FI, configure the ports connecting to the storage array as FC, reboot, and then designate the FC Ports as FC Storage Ports.

To designate storage ports:

1. In the Navigation pane, click the Equipment tab.
2. Expand Fabric Interconnect A/B > Configure Unified Ports.
The following image illustrates the Configure Fixed Module Ports dialog box is displayed.

3. Use the slider to configure the ports connecting to the storage array as FC.

4. Repeat steps 1 through 3 for the other FI. Wait until the FIs have rebooted.

5. On the **Equipment** tab, expand **Fiber Interconnect** > **Fiber Interconnect A/B** > **Fixed Module** > **FC Ports** > **FC Port 31 /32**.

6. In the Work pane, select **Configure as FC Storage Port** on the **General** tab.

   The following image illustrates the **General** tab.
Assign the Storage Cloud VSAN to the FC Ports

To assign the Storage Cloud VSAN to the FC ports:

1. On the Equipment tab, expand Fabric Interconnect > Fabric Interconnect A/B > Fixed Module > FC Ports > FC Port 31/32.

2. Select the required VSAN (for example, VSAN3010 for Fabric Interconnect A, as illustrated in the following image).
3. Click **Save Changes**.

4. Repeat steps 1 through 3 for the other Fabric Interconnects, ensuring that correct VSANs are selected.

**Confirm Storage Port WWPN is Logged Into the Fabrics**

Zoning enables access control between storage devices and user groups. Creating zones increases network security and prevents data loss or corruption. A zone set consists of one or more zones in a VSAN.

To confirm the storage port is logged into the fabrics:

1. Using SSH, log in as admin to the virtual IP address for the UCS Fabric Interconnect.

2. Run the connect command to enter the NX-OS CLI:

```bash
cisco-lab-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2013, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
cisco-lab-A(nxos)#
Note: You can use the ? option at the prompt to get help.View
the active zonesets:cisco-lab-A(nxos)# show zoneset
activezoneset name ucs-cisco-lab-vsan-3010-zoneset vsan 3010
zone name ucs_cisco-lab_A_8_UI1_vHBA-A vsan 3010
  * fcid 0x6c0000 [pwnn 20:00:00:05:ad:1e:11:2f]
  * fcid 0x6c00ef [pwnn 50:06:01:68:3e:e0:0a:6b]
  * fcid 0x6c01ef [pwnn 50:06:01:60:3e:e0:0a:6b]

zone name ucs_cisco-lab_A_7_GMS1_vHBA-A vsan 3010
pwnn 20:00:00:05:ad:1e:11:4f
  * fcid 0x6c00ef [pwnn 50:06:01:68:3e:e0:0a:6b]
  * fcid 0x6c01ef [pwnn 50:06:01:60:3e:e0:0a:6b]

zone name ucs_cisco-lab_A_6_INSTA1_vHBA-A vsan 3010
  * fcid 0x6c0004 [pwnn 20:00:00:05:ad:1e:11:7f]
  * fcid 0x6c00ef [pwnn 50:06:01:68:3e:e0:0a:6b]
  * fcid 0x6c01ef [pwnn 50:06:01:60:3e:e0:0a:6b]

zone name ucs_cisco-lab_A_5_INSTA2_vHBA-A vsan 3010
  * fcid 0x6c0005 [pwnn 20:00:00:05:ad:1e:11:5f]
  * fcid 0x6c00ef [pwnn 50:06:01:68:3e:e0:0a:6b]
  * fcid 0x6c01ef [pwnn 50:06:01:60:3e:e0:0a:6b]

3. Run the show flogi database vsan vsan-ID command, where vsan-ID is
the identifier for the VSAN. In this example, 3010 is used for VSAN Fabric Interconnect A.

Make a note of the WWPNs as in this example. These WWPNs will be required when creating storage connection policies.

```
mural-norse-lab-B (nxos)# show flogi database vsan 3010
INTERFACE  VSAN   FCID        PORT   NAME           NODE NAME
---------------------------------------------------------------
fc1/31   3010 0x1000ef 50:06:01:60:3e:a0:28:d2 50:06:01:60:be:a0:28:d2
fc1/32   3010 0x1001ef 50:06:01:69:3e:a0:28:d2 50:06:01:60:be:a0:28:d2
```

4. Run the `exit` command.

5. Enter the `connect nxos B` command, where B is for Fabric Interconnect B.

6. Enter the `show flogi database vsan vsan-ID` command, where `vsan-ID` is the identifier for the VSAN. In this example, we use 3020 for VSAN on Fabric Interconnect B.

   Make a note of the WWPN.

```
mural-norse-lab-B(nxos)# show flogi database vsan 3020
--- INTERFACE  VSAN   FCID        PORT   NAME           NODE NAME
--- ---------------------------------------------------------------
fc1/31   3020 0x4200ef 50:06:01:61:3e:a0:28:d2 50:06:01:60:be:a0:28:d2
fc1/32   3020 0x4201ef 50:06:01:69:3e:a0:28:d2 50:06:01:60:be:a0:28:d2
```

### Create Storage Connection Policies

Create a storage connection policy for each Fabric Interconnect.

To create storage connection policies:

1. On the SAN tab, expand Policies > root.

2. Right-click Storage Connection Policies, and select Create Storage Connection Policies.
3. Enter a name that complies with local naming conventions and the values. For example, **storage-conn-polA Zoning = Single Initiator Multiple Target**.

4. In the **FC Target Endpoints**, enter WWPN printed in the last section for the related VSAN.

5. Repeat step 4 for the other WWPN. Another FC Target Point is created.

6. Repeat steps 1 through 5 to create storage connection policies for the other Fabric Interconnect.

The following images illustrate two Fabric Interconnects, FI-A and FI-B, each with two Target Endpoints.
Create SAN Connectivity Policy

A virtual host bus adapter (vHBA) logically connects a virtual machine to a virtual interface on the UCS 6100 series Fabric Interconnect and allows the virtual machine to send and receive traffic through that interface. You must create a vHBA initiator group for each vHBA.

Connectivity policies determine the connections and the network communication resources between the server and the LAN or SAN on the network. These policies use pools to assign MAC addresses, WWNs, and WWPNs to servers and to identify the vNICS and vHBAs that the servers use to communicate with the network.

If you want to support any VSAN, it needs to be configured globally into Cisco UCS Manager, and then it can be associated with a particular vHBA.

To create a vHBA initiator group for the storage connectivity policy:

1. In the Navigation pane, click the SAN tab.
2. On the SAN tab, click Policies > root.
3. Right-click SAN Connectivity Policies and select Create SAN Connectivity Policy.
4. Click **Add**. Enter the values as described in the following example, ensuring that the name complies with local naming conventions.

- **Name**— vHBA-A
- **WWNN Assignment**— wwnn-pool1(768/784)
- **Fabric ID**— A
- **Select VSAN**— VSAN3010
- **Adaptor Policy**— VMWare

5. Repeat steps 1 through 4 for the other vHBA.

**Configure SAN Cloud Policy**

The SAN cloud policy San Con Pol A shows two vHBAs, vHBA-A and vHBA-b, as illustrated in the following image:
The following screen illustrates an example of two vHBAs initiator groups within one SAN connection policy. The section after the screen details the steps for creating a vHBA initiator group.
Create vHBA Initiator Groups

To create a vHBA initiator group for the storage connectivity policy:

1. From the **SAN** tab, navigate to **Policies > Root > SAN Connectivity Policies**.
2. Add SAN Connectivity Policies for F1 A/B (above example shows SAN-con-pol-A).
4. Add values as follows:
   - Name: vHBA-init-grp-A
   - Select vHBA Initiators (for example, vHBA-B)
   - Storage Connection Policy (for example, Storage-con-polB)
5. Click **OK** to save changes.
6. Repeat steps 1 through 5 for the other Fabric Interconnect.

Verifying Service Profile Templates

When vHBA initiator groups are created, vHBAs are updated into service profile templates.

To verify service profile templates:

1. From the **Servers** tab, navigate to **Service Profile Templates > root > Service Template** (for example, Mural-service-template) > **VHB**.
2. From the **SAN Connectivity Policy** drop-down list, select a policy.

   The following image illustrates the selection of the SAN connectivity policy.
3. Verify that vHBAs have been applied to a service profile template, and that all details are correct.

4. Click **Save Changes**.

5. Repeat steps 1 through 4 for the second vHBA.

The following image illustrates vHBA configuration within a service template.
Allocating Storage on the EMC

This section describes how to allocate data storage to each node in the MURAL system. EMC is used to manage the storage environment for MURAL. Storage includes the HDFS connected to the Collector and Compute nodes and the columnar database used by the Insta nodes.

Configure the Base IP Addresses to Access the EMC System

The default IP addresses for the EMC system are **1.1.1.1** and **1.1.1.2**. Perform the following steps to configure the IP address of your laptop to a value in the same range, connect to **1.1.1.1** using a web browser, and set the IP address information:

1. Configure your laptop's IP address to **1.1.1.4/24**.
2. Connect a cable to Service Processor A.
3. Use a web browser to access **http://1.1.1.1/setup**.
4. Reconfigure the IP addresses for the EMC system to the range specified in the CIQ.

**Note:** If you need to restart EMC manually during the set-up procedure, use a web browser to access **http://1.1.1.1/setup**, log in as **admin**, and select the **restart** option.

EMC Hardware Installation Prerequisites

Before beginning, verify that the following EMC hardware installation tasks are completed:

- The EMC VNX chassis and standby power supply (SPS) chassis are installed in the rack according to the instructions in the EMC Unisphere installation guide (EMC P/N 300-012-924) included with the hardware.

- The SPS is connected to the storage processor (SP) management ports according to the instructions in the EMC Unisphere installation guide, using the cables provided with the product.
• Power cords are connected for the following components according to the instructions provided in the EMC Unisphere installation guide.
  o From SPS A and SPS B to SP A and SP B
  o From SPS A and SPS B to power distribution units (PDUs)
• The Fibre Channel SFP+ transceiver, included with the hardware, is installed in ports 4 and 5 of both SP A and SP B.

**Note:** Do not attach the cables between the storage system and the server array until after initialization is complete.

In the following table, make a record of the values provided in your Customer Information Questionnaire (CIQ) for the indicated items.

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP A management port IP</td>
<td></td>
</tr>
<tr>
<td>SP B management port IP</td>
<td></td>
</tr>
<tr>
<td>Subnet mask and gateway for above</td>
<td></td>
</tr>
<tr>
<td>Admin name/password</td>
<td></td>
</tr>
<tr>
<td>Storage system serial number</td>
<td></td>
</tr>
<tr>
<td>Scope</td>
<td></td>
</tr>
<tr>
<td>DNS server address (optional)</td>
<td></td>
</tr>
<tr>
<td>Time server address</td>
<td></td>
</tr>
<tr>
<td>Inbound email address</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The following IP addresses cannot be used: 128.121.1.56 through 128.121.1.248, 192.168.1.1, and 192.168.1.2.

**Verify Zoning/FLOGI on the Fabric Interconnect**

To verify zoning and the fabric login (FLOGI) on the fabric interconnect (FI), perform the following steps:

1. Use SSH to log in to the FI.
2. Run the `connect nxos A` command to connect to the FI.
3. Run the `show zoneset active` command and verify that its output reports
the fiber channel ID (FCID) for all world wide port names (WWPNs) and hosts, as shown for **FI A** and **FI B** in the following examples.

**Note:** In the following output and figures, the identifiers are examples only and are different in your deployment. Also, the term **pwwn** in the output refers to WWPNs.

```bash
hostname-A(nxos)# show zoneset active
```

The resulting output may resemble:

<table>
<thead>
<tr>
<th>zoneset name</th>
<th>hostname-vsan-3010-zoneset vsan 3010</th>
</tr>
</thead>
<tbody>
<tr>
<td>zone name</td>
<td>hostname_A_12_UI1_vHBA-A vsan 3010</td>
</tr>
<tr>
<td></td>
<td>fcid 0x100003 [pwwn 20:00:00:00:05:ad:1e:11:df]</td>
</tr>
<tr>
<td></td>
<td>fcid 0x1000ef [pwwn 50:06:01:60:3e:a0:28:d2]</td>
</tr>
<tr>
<td></td>
<td>fcid 0x1001ef [pwwn 50:06:01:69:3e:a0:28:d2]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>zone name</th>
<th>hostname_A_11_UI2_vHBA-A vsan 3010</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>fcid 0x100006 [pwwn 20:00:00:00:05:ad:1e:11:ff]</td>
</tr>
<tr>
<td></td>
<td>fcid 0x1000ef [pwwn 50:06:01:60:3e:a0:28:d2]</td>
</tr>
<tr>
<td></td>
<td>fcid 0x1001ef [pwwn 50:06:01:69:3e:a0:28:d2]</td>
</tr>
</tbody>
</table>

Run the **show zoneset active** command again for the other Fabric Interconnect:

```bash
hostname-B(nxos)# show zoneset active
```

The resulting output may resemble:

<table>
<thead>
<tr>
<th>zoneset name</th>
<th>hostname-vsan-3020-zoneset vsan 3020</th>
</tr>
</thead>
<tbody>
<tr>
<td>zone name</td>
<td>hostname_B_24_UI1_vHBA-B vsan 3020</td>
</tr>
<tr>
<td></td>
<td>fcid 0x420007 [pwwn 20:00:00:00:05:ad:1e:11:2e]</td>
</tr>
<tr>
<td></td>
<td>fcid 0x4200ef [pwwn 50:06:01:61:3e:a0:28:d2]</td>
</tr>
<tr>
<td></td>
<td>fcid 0x4201ef [pwwn 50:06:01:68:3e:a0:28:d2]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>zone name</th>
<th>hostname_B_23_UI2_vHBA-B vsan 3020</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>fcid 0x420009 [pwwn 20:00:00:00:05:ad:1e:11:5e]</td>
</tr>
<tr>
<td></td>
<td>fcid 0x4200ef [pwwn 50:06:01:61:3e:a0:28:d2]</td>
</tr>
<tr>
<td></td>
<td>fcid 0x4201ef [pwwn 50:06:01:68:3e:a0:28:d2]</td>
</tr>
</tbody>
</table>
4. Verify the zoning using UCS Manager.

   Log in to the UCS Manager and navigate to Servers > Service Profiles > root > Service Profile profile-name (in the following figure, the profile name is HS-ESX01).

5. Go to the FC Zones tab and in each FC Target row, verify that the WWPNs in the Name and Target WWPN fields are the same.

   **Note:** WWPNs on the UCS Manager are on SAN > Pools > WWPN Pools > WWPN Pool (the ID used in this installation is wwpn-ppoll/Initiator).

6. Hosts are ready to be registered, as in the following example, which shows hosts on EMC. On the EMC in the following figure, the Initiator Name format is WWNNWWPN (where WWNN is first, then WWPN).
Registering MURAL Nodes with EMC

Next you associate all MURAL nodes with the world wide port name (WWPN) of the appropriate fibre channel port on the storage arrays. As the term suggests, a WWPN is the unique identifier for a fibre channel port, in this case on the storage arrays. A world wide name node (WWNN) is a unique identifier assigned to a node in a fibre channel fabric, in this case a MURAL node.

You also need to allocate storage to all MURAL nodes, ensuring that its definition in the EMC Unisphere interface matches its definition in the Unified Computing System (UCS). If EMC has been previously configured with MURAL, you still need to verify that the existing definition in EMC exactly matches the definition in the UCS.

**Note:** Alerts might be generated during the set-up process indicating that nodes are not registered (Alert 0x721c). You can ignore them until provisioning is complete, after which point they need to be investigated.

Before You Begin

In the following table, record the WWPNs specified in the UCS Manager for the master GMS node. Typically the last two digits of the WWPN are enough to identify the node on the EMC interface.

<table>
<thead>
<tr>
<th>Node</th>
<th>WWPN</th>
<th>WWNN</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMS1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GMS2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collector1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collector2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rubix1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rubix2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compute1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compute2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compute3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compute4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To register all MURAL nodes with EMC:

1. In the EMC Unisphere interface, mouse over (do not click) the **Hosts** icon in the title bar, then select **Connectivity Status**. A window pops up as shown in the following figure.

2. If the correct WWPN for the master GMS node appears in the **Initiator Name** column, then the storage unit is already configured. If the master GMS node is not yet configured, click **Register** as shown in the preceding figure.
The **Register Initiator Record** window pops up.

![Register Initiator Record Window](image)

3. The world wide name (WWN) of the fibre channel (FC) port on the storage partition appears in the **WWN/IQN** field. The WWN is a unique 16-digit hexadecimal number, such as 20:00:00:25:B5:68:00:08, and is hard-coded into every FC host bus adapter (HBA). Each device must be registered with the storage area network (SAN) by its WWN before the SAN will recognize it.

**Note:** The WWN/IQN shown above is the same Initiator Name that you would find from the UCS Manager, as follows:

- From the UCS Manager, go to **SAN > Pools > wwnn-pool-wwnn-pool1**. The **Initiator** tab shows the WWNN as 20:00:00:05:AD:1E:10:6F. Note the related node from the **Assigned to** column. **Wwnn-pool1** is the name used during initial configuration using the UCS configuration script.

- Go to **SAN > Pools > wwpn-pool-wwpn-pool1**. The Initiator tab shows the WWPN for the same node as 20:00:00:05:AD:1E:11:1F. Again **wwpn-pool1** is the name used during initial configuration using the UCS configuration script.

In other words, on the EMC WWNN and WWPN are shown as WWNNWWPN for the node.
4. On the **Register Initiator Record** screen, perform the following steps:

   a. Enter the MURAL nodes' hostname and IP address in the **Host Name** and **IP Address** fields.

   b. Verify that the value in the **Initiator Type** field is **SGI**.

   c. Verify that the value in the **Failover Mode** field is **ALUA–mode 4** (the default as shown in the figure).
5. Navigate to **Dashboard > Hosts > Host List** in the EMC Unisphere interface and verify that the master GMS node is correctly configured.

A list of hosts similar to the following is displayed:

Create RAID Groups and LUNs

Create RAID groups before creating the logical unit numbers (LUNs) and assign them to the associated RAID group.

The following table specifies the parameters to use when creating RAID groups.

<table>
<thead>
<tr>
<th>RAID Group</th>
<th>Storage Pool ID</th>
<th>RAID Configuration</th>
<th>Disks</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4, 5, 6, 7, 8, 9</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10, 11, 12, 13</td>
</tr>
<tr>
<td>100 (not used)</td>
<td>100</td>
<td>Unbound</td>
<td>0, 1, 2, 3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RAID Group</th>
<th>RAID Type</th>
<th>Storage Pool ID</th>
<th>Disks</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4, 5, 6, 7, 8</td>
</tr>
</tbody>
</table>
MURAL Hardware Installation Reference Guide

<table>
<thead>
<tr>
<th>RAID Group</th>
<th>RAID Type</th>
<th>Storage Pool ID</th>
<th>Disks</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10, 11, 12, 13</td>
</tr>
<tr>
<td>100 (not used)</td>
<td>Unbound</td>
<td>100</td>
<td>0, 1, 2, 3</td>
</tr>
</tbody>
</table>

**Note:** Add any spare disks to RAID Group 5 or 100 depending on the hardware.

The following table specifies the parameters to use when creating the LUNs. Although at this point you are creating only the LUN for the master GMS node, before doing so it is important to review the table and verify that disks of the required sizes have been allocated for all nodes. (The remaining LUNs are created in "Creating RAID Groups and LUNs for the Remaining Nodes").

**Note:** Contact Technical Support now to consult about the following issues:

- The appropriate disk sizes depend on the throughput capacity required by your deployment. Do not simply use the sizes in the **Disk Size (GB)** column, which are examples only.

- The 50 gigabytes (GB) specified for the Insta-1-PGSQL and Insta-2-PGSQL disks is the minimum size in a production environment. The size for a lab environment might be different.

<table>
<thead>
<tr>
<th>RAID</th>
<th>RAID Group Name</th>
<th>LUN Name</th>
<th>LUN ID</th>
<th>Disk Size (GB)</th>
<th>Controller</th>
<th>Storage Pool</th>
<th>Host - MAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>RAID Group 10</td>
<td>INSTA-1</td>
<td>0</td>
<td>1945</td>
<td>FAB-A</td>
<td>INSTA-STR-1</td>
<td>INSTA NODE-1</td>
</tr>
<tr>
<td>10</td>
<td>RAID Group 10</td>
<td>INSTA-2</td>
<td>1</td>
<td>1945</td>
<td>FAB-A</td>
<td>INSTA-STR-2</td>
<td>INSTA NODE-2</td>
</tr>
<tr>
<td>10</td>
<td>RAID Group 10</td>
<td>INSTA-1</td>
<td>2</td>
<td>1945</td>
<td>FAB-B</td>
<td>INSTA-STR-1</td>
<td>INSTA NODE-1</td>
</tr>
<tr>
<td>10</td>
<td>RAID Group 10</td>
<td>INSTA-2</td>
<td>3</td>
<td>1945</td>
<td>FAB-B</td>
<td>INSTA-STR-2</td>
<td>INSTA NODE-1</td>
</tr>
<tr>
<td>5</td>
<td>RAID Group 5</td>
<td>COL-1</td>
<td>4</td>
<td>1024</td>
<td>FAB-A</td>
<td>COL-STR-1</td>
<td>COL NODE-1</td>
</tr>
<tr>
<td>5</td>
<td>RAID Group 5</td>
<td>COL-2</td>
<td>5</td>
<td>1024</td>
<td>FAB-B</td>
<td>COL-STR-1</td>
<td>COL NODE-2</td>
</tr>
<tr>
<td>5</td>
<td>RAID Group 5</td>
<td>DN-1</td>
<td>6</td>
<td>1024</td>
<td>FAB-A</td>
<td>DN-STR-1</td>
<td>DN-1</td>
</tr>
<tr>
<td>5</td>
<td>RAID Group 5</td>
<td>DN-2</td>
<td>7</td>
<td>1024</td>
<td>FAB-B</td>
<td>DN-STR-2</td>
<td>DN-2</td>
</tr>
<tr>
<td>5</td>
<td>RAID Group 5</td>
<td>DN-3</td>
<td>8</td>
<td>1024</td>
<td>FAB-A</td>
<td>DN-STR-3</td>
<td>DN-3</td>
</tr>
<tr>
<td>5</td>
<td>RAID Group 5</td>
<td>DN-4</td>
<td>9</td>
<td>1024</td>
<td>FAB-B</td>
<td>DN-STR-4</td>
<td>DN-4</td>
</tr>
<tr>
<td>RAID</td>
<td>RAID Group Name</td>
<td>LUN Name</td>
<td>LUN ID</td>
<td>Disk Size (GB)</td>
<td>Controller</td>
<td>Storage Pool</td>
<td>Host - MAP</td>
</tr>
<tr>
<td>------</td>
<td>-----------------</td>
<td>----------</td>
<td>--------</td>
<td>----------------</td>
<td>------------</td>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>5</td>
<td>RAID Group 5</td>
<td>RGE-1</td>
<td>10</td>
<td>1024</td>
<td>FAB-A</td>
<td>UI-STR-1</td>
<td>Rubix NODE-1</td>
</tr>
<tr>
<td>5</td>
<td>RAID Group 5</td>
<td>RGE-2</td>
<td>11</td>
<td>1024</td>
<td>FAB-B</td>
<td>UI-STR-1</td>
<td>Rubix NODE-2</td>
</tr>
<tr>
<td>5</td>
<td>RAID Group 5</td>
<td>UI-1</td>
<td>12</td>
<td>500</td>
<td>FAB-A</td>
<td>UI-STR-1</td>
<td>Rubix NODE-1</td>
</tr>
<tr>
<td>5</td>
<td>RAID Group 5</td>
<td>UI-2</td>
<td>13</td>
<td>500</td>
<td>FAB-B</td>
<td>UI-STR-2</td>
<td>Rubix NODE-2</td>
</tr>
<tr>
<td>5</td>
<td>RAID Group 5</td>
<td>GMS-1</td>
<td>14</td>
<td>200</td>
<td>FAB-A</td>
<td>GMS-STR-1</td>
<td>GMS NODE-1</td>
</tr>
<tr>
<td>5</td>
<td>RAID Group 5</td>
<td>GMS-2</td>
<td>15</td>
<td>200</td>
<td>FAB-B</td>
<td>GMS-STR-2</td>
<td>GMS NODE-2</td>
</tr>
</tbody>
</table>

**Note:** Prior to setting up the RAID groups, it might be useful to prepare a table in order to ensure all disks required have been allocated.

After creating the RAID groups, create the LUNs. The above table shows example disk sizes, but you must contact Technical Support to confirm the sizing for your site-specific environment.

To create RAID groups and create and assign the LUN for the master GMS node, perform the following steps:

1. In the EMC Unisphere interface, mouse over the Storage icon in the title bar and select Storage Pools. Open the RAID Groups tab and click Create as shown in the figure.
2. In the **Create Storage Pool** window that pops up, create RAID groups 5, 10, and 100 with the parameters specified in the **Storage Pool ID** and **RAID Configuration** columns of the following table (which is the same as in the introduction, reproduced here for your convenience). As mentioned, the values in the Disks column are examples only; consult with Technical Support about the RAID groups to assign to the disks in your deployment.

<table>
<thead>
<tr>
<th>RAID Group</th>
<th>Storage Pool ID</th>
<th>RAID Configuration</th>
<th>Disks</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4, 5, 6, 7, 8, 9</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10, 11, 12, 13</td>
</tr>
<tr>
<td>100 (not used)</td>
<td>100</td>
<td>Unbound</td>
<td>0, 1, 2, 3</td>
</tr>
</tbody>
</table>

Repeat the following steps for each of the three RAID groups:

a. In the **Storage Pool Type** field, click the **RAID Group** radio button if it is not already selected.

b. In the **Storage Pool ID** field, type the value in that column of the preceding table.

c. In the **RAID Configuration** field, select from the drop-down menu the value from that column of the preceding table.

d. Click the **Manual** radio button if it is not already selected, then click the **Select...** button.

e. In the **Disk Selection** window that pops up, move the disks specified in the **Disks** column of the preceding table from the **Available Disks** box to the **Selected Disks** box.

f. Click the **OK** button in the **Disk Selection** window.
3. After creating all three RAID groups, click the **OK** button in the **Create Storage Pool** window.

4. Navigate to **Storage > LUNs > LUNs** and click **Create**. The **Create LUN** window pops up.
5. Referring to the values for GMS-1 in the preceding table of LUN parameters, perform the following steps:

   a. In the **Storage Pool Type** field, click the **RAID Group** radio button if it is not already selected.

   b. Select to match the RAID level. Note that the Insta nodes should be RAID type 10, while the other nodes should be RAID type 5.

   c. In the **User Capacity** field, select from the drop-down menu the value (in GB) closest to that provided by Technical Support for the **Disk Size** field.

   d. Select the **LUN ID** from the drop-down menu. LUN IDs auto-increment. Disks that are already assigned are not available.

   e. Enter the **LUN Name**.

6. Click **Apply**.

7. Repeat Steps 4 through 6 for each of the nodes listed in the table above.

    Note that for the Insta nodes, you must create a total of four LUNs, each in RAID Group 10 (while the other types of nodes are in RAID Group 5):

    * INSTA-1 (to be associated with dboot1 on both Insta nodes)
    * INSTA-2 (to be associated with dboot2 on both Insta nodes)

8. Navigate to the **Storage > LUNs** tab, verify that the parameters match the values specified in the previous step, as shown in the following figure.
Create Storage Groups

For Collector, Compute, Rubix, and GMS nodes, assigning the nodes to storage groups is a straightforward one-to-one relationship—the LUN assigned to each node has its own storage group.

However, the Insta nodes require two storage groups, each of which contains two LUNs:

- INSTA1-DB
  - INSTA-1
  - INSTA-2
- INSTA2-DB
  - INSTA-1
  - INSTA-2

To create the storage group for the master GMS node and associate it with the appropriate LUN, perform the following steps:

1. In the EMC Unisphere interface, mouse over (do not click) the Hosts icon in the title bar, and select Storage Groups. Click Create. A Create Storage Group window similar to the following pops up.
The value in the **Storage Group Name** field auto-increments.

**Note:** We recommend inserting the node name in front of the autogenerated value to make the storage group easier to identify in future. In the example, the recommended value is **GMS-1 Storage Group 8**.

2. Click the **OK** button.

3. In the **Storage Group Properties** window opens. Go to the **Hosts** tab and move the appropriate node from the **Available Hosts** column to the **Hosts to be Connected** column.

4. Click the **OK** button, then **Apply**.
5. Repeat Steps 1 through 4 to create storage groups and assign the associated host name for each of the following nodes:

- GMS nodes
- Collector nodes
- Rubix nodes
- Compute (also called DN for Data Node) 1
- Compute 2, and so on

6. Repeat Steps 4-6 to create an Insta1-DB storage group and from the Hosts tab, move host INSTA-1 to the Hosts to be connected column.

7. Go to the LUNs tab in the properties window for the Insta1-DB storage group and select LUN INSTA-1. Click Add.

Also select and click Add for LUN INSTA-2 and LUN INSTA-2-DB

8. Click Apply and Yes to confirm your changes.

9. Repeat steps 6 through 8 to create an Insta2-DB storage group containing the LUNs INSTA-1 and INSTA-2.

10. Verify that all storage groups are similar to the following example.
Adjust Caching on the EMC

You must adjust the caching settings on the EMC for your MURAL setup to keep data in memory for the correct amount of time.

To adjust caching, perform the following steps:

1. In the EMC Unisphere interface, navigate to System Management > Manage Cache.

2. Disable all caching under SP Cache.

   On the Storage System Properties window that pops up, open the SP Cache tab. Click the SP A Read Cache, SP B Read Cache, and SP Write Cache check boxes to remove the checks and disable caching. Click the OK button.

3. Adjust the SP memory.
Open the **SP Memory** tab, and use the sliders in the **User Customizable Partitions** region to set all three values to 1152. Click the **OK** button.

4. After completing the changes, re-enable all cache check boxes under the SP Cache tab.

   Return to the **SP Cache** tab and re-enable caching by clicking the **SP A Read Cache**, **SP B Read Cache**, and **SP Write Cache** check boxes to replace the checks. Click the **OK** button.
EMC is now configured for MURAL. Now reboot the blades on which LUNs are attached, using the `reload` command:

```
> en
# conf t
# reload
```

Wait until blade comes up after reboot, login to each MURAL node and verify LUN WWID numbers.

```
> en
# conf t
(config)# username admin password admin@123
(config)# license install LK2-RESTRICTED_CMDS-88A4-FNLF-XCAU-U
(config)# tps multipath show
(config)# write memory
```