Americas Headquarters

Cisco Systems, Inc.

170 West Tasman Drive
San Jose, CA 95134-1706 USA

http://www.cisco.com

Tel: 408 526-4000
     800 553-NETS (6387)

Fax: 408 527-0883
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 COPYRIGHT, TRADEMARK, OR ANY OTHER INTELLECTUAL PROPERTY RIGHTS IN THE DOCUMENTS AND SOFTWARE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS 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. (1005R)

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.

MURAL Software Standard Installation Guide

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

**Installation Overview** ................................................................. 9

Before You Begin ........................................................................... 9

System Components ...................................................................... 10

Hardware ...................................................................................... 11

Installation Package ...................................................................... 11

Customer Information Questionnaire ........................................... 11

Installation Process Steps ........................................................... 12

**Verifying UCS Hardware Configuration for MURAL** .................. 15

Before You Begin ........................................................................... 15

Reviewing Hardware Setup ........................................................... 15

Verifying Slot Assignments for Blades ......................................... 16

Verifying Physical Connections to the Fabric Interconnects ........... 18

Setting the Base Configuration for the UCS System ....................... 23

**Configuring UCS for MURAL** .................................................. 26

Configuring Direct Attachments to External SANs ....................... 27

Configuring System Profiles for the Cisco UCS Manager ............... 41

**Allocating Storage on the EMC** ............................................ 46

EMC Hardware Installation Prerequisites ...................................... 48

Configuring IP Addresses for the EMC System .............................. 49

**Setting Up the Master GMS Node** .......................................... 50

Setting the Password and IP Address(es) ..................................... 50

**Loading and Verifying Initial Configuration Settings** ............... 52

Accessing the GMS User Interface ............................................... 52
Loading the Base Configuration File .................................................. 53
Verifying XML Settings ........................................................................... 54
Validating the XML Configuration .......................................................... 78

**Using GMS Lite to Automate Installation of GMS Nodes** .................. 80
Before You Begin .................................................................................... 80
Configuring GMS Lite Node as PXE Boot Server .................................... 81
Setting Up the Master GMS Node and Cluster ........................................... 82

**Registering MURAL Nodes with EMC** ................................................. 85
Before You Begin .................................................................................... 85
Creating RAID Groups and LUNs ............................................................ 88
Creating Storage Groups ......................................................................... 94
Adjusting Caching on the EMC ............................................................... 97

**Installing MURAL on the UCS Nodes** ............................................... 101
Before You Begin .................................................................................... 101
Applying Patches on MURAL Nodes ....................................................... 101
Installing MURAL on UCS Nodes ............................................................ 101
Configuring Application with Site Specifics ............................................. 103
Troubleshooting Node Installation ......................................................... 105

**Verifying that Processes are Running** .............................................. 106

**Generating and Pushing the Information Bases** ............................... 108
Configuring IBs for EDR ....................................................................... 108
Configuring DCs and Gateways For All IBs ........................................... 109
Copying IBs to the Anomaly Feature ..................................................... 112
Synchronize the IBs on the Standby Collector Node .............................. 112

Copyright © 2015, Cisco Systems, Inc.
Processing the Data ................................................................. 114
    Setting Up a New User for the ASR in the Collectors .......... 114
    Ingesting Data Into the System ....................................... 115

Validating Data on Nodes .................................................. 116
    Validating Data on the Collector Nodes ......................... 116
    Validating Data on the Compute Blades (Data Nodes) ........ 118
    Validating Bulk Stats Data on the Insta Blade ............... 120
    Starting UI Processes and Verifying Data .................... 121
    Updating Whitelists .................................................... 123

Setting Up Offline Reports .............................................. 124
    Uncategorized URL, UA, and TAC Reports .................... 124
    Tethering Reports .................................................... 124
    Rule-Based Reports ................................................... 126

Mandatory Parameters for Incoming ASR Files .................. 128
    Mandatory Attributes for Flow EDRs for MURAL ............ 128
    Mandatory HTTP EDR Attributes for MURAL ................. 129
    ASR-Side Configuration ............................................. 130

APPENDIX I: Installing and Configuring VM for GMS Lite ...... 132
    Before You Begin .................................................... 132
    Installing VM for GMS Lite ...................................... 133

APPENDIX II: Manufacturing the Master GMS Blade .......... 139
    Before You Begin .................................................... 139

Appendix III: Using KVM Software to Boot PXE Blades ...... 148
    Before You Begin .................................................... 148
Rebooting the Blades ................................................................. 148

Appendix IV: Collecting UCS Chassis/Slot and VLAN Information  150

Fetching MAC IDs Feature ......................................................... 151
Finding Chassis/Slot IDs ........................................................... 152
Finding NICs VLAN IDs for Blades ........................................... 153

Glossary .................................................................................... 154
Installation Overview

This document describes how to install the Mobility Unified Reporting and Analytics (MURAL) application. MURAL provides Web-based reporting and analytics for deep packet inspection (DPI) data emerging from your network.

Before You Begin

This document assumes that you have a working knowledge of the following technologies:

- Linux operating system
- Cisco Unified Computing System (UCS) Software, Release 2.1
- EMC storage devices

Before you begin the installation, we recommend that you:

- Review the Release Notes for MURAL 3.3 (or later)
- Complete a training course on MURAL
- Have working knowledge of Cisco UCS Server Blade hardware administration
- Locate the Customer Information Questionnaire (CIQ) for the deployment; see "Customer Information Questionnaire" on page 11
- Verify that each Fabric Interconnect is connected to the storage area network (SAN) controllers through fiber cables.
- Verify all that UCS B200 M2/M3 blade servers are physically installed in the UCS 5108 Blade Server Chassis and that the nodes of all types (Collector, Compute, GMS, Rubix, Insta, and so on) are connected to the UCS 6248 Fabric Interconnect. The number of each type of node depends on your deployment.

Note: Set up hardware as specified in the bill of materials (BOM).
System Components

The following figure shows the components of the MURAL platform, focusing on how the data flows through the system:

The figure depicts each type of node as a separate logical entity. In larger deployments there is often a separate blade for each type of node, whereas in smaller deployments a blade might host multiple types of nodes. For example, the UI and Caching nodes are often hosted on the same blade, and in environments that have a lower data flow requirement, the Collector, UI, and Caching nodes might all be cohosted along with the General Management Server (GMS) node (which does not appear in the figure).

The MURAL platform nodes perform the following functions:

- **Collector node**—Collects data streams pushed to the MURAL platform, interprets the exported flows, enriches them with static data, and assembles data sets. The Collector stores the raw data in the Hadoop Distributed File System (HDFS) and sends it to the Compute node.

- **UI/Caching (Rubix) node**—Hosts the Rubix engine and Rubix data cache. The Rubix engine queries the Insta nodes constantly and when new data is available, it fetches it to store in the data cache, so that it can respond
more quickly to requests from the UI engine. The UI/Caching node is sometimes called the Rubix node. The UI/Caching node uses N+1 redundancy in active-active mode.

- **General Management Server (GMS) node**—Provides centralized management of the other MURAL nodes, such as remote manufacturing of blades (installing the MURAL software), patch management, monitoring of all nodes and operations, and importing and running node configurations. (GMS does not appear in the preceding figure because it does not operate on the flow of network data and processed data cubes.)

**Hardware**

The MURAL nodes are hosted on a redundant pair of UCS 5108 Blade Server Chassis Data storage is provided by EMC storage devices.

The data flows that feed the MURAL system are generated by an ASR 5000 or ASR 5500 platform (referred to in the remainder of this document simply as an ASR).

**Installation Package**

The MURAL software installation package contains the following components:

- An ISO image file. For the image name and associated MD5 checksum, refer to the Release Notes.

- The file, which is used by the master GMS node. This sample configuration file provides configuration settings for your setup based on the network topology information in the Customer Information Questionnaire (CIQ).

- Any software patches that apply to the release. A complete list appears in the Release Notes.

- Management information bases (MIBs)

**Customer Information Questionnaire**

The CIQ is an Excel spreadsheet of configuration settings based on a site survey that was completed before the installation process. Its worksheets include the
indicated kind of information:

- **Contacts**—Site personnel and their responsibilities
- **Space_Power Req**—Space and power requirements
- **IP Survey**—Physical network connections, virtual LANs (VLANs), interfaces, slot assignments, Simple Network Management Protocol (SNMP) and Simple Mail Transfer Protocol (SMTP) settings, and so forth
- **Network Diagrams**—Physical connections between system components
- **Connectivity**—Details for ports and connections
- **Firewall**—Firewall changes required for connectivity
- **Alarms**—All supported SNMP traps
- **ASR**—Locations for required ASR information bases (IBs)

**Installation Process Steps**

The MURAL installation process includes the following steps:

**Warning**: Skipping a task or performing the tasks out of sequence may cause a misconfiguration that results in system failure.

1. Verify that the UCS hardware is correctly set up and configured for the MURAL system. See "Verifying UCS Hardware Configuration for MURAL" on page 15

2. Set basic MURAL settings on the UCS by:
   - Running the ucs-config script to set configuration parameters for the UCS Fabric Interconnect.
   - Configure the Direct-Attach SAN feature.
   See "Configuring UCS for MURAL" on page 26.

3. Set up data storage for the MURAL system:
   - Set up the storage. See "Allocating Storage on the EMC" on page 46.
4. Complete the initial configuration of GMS by:
   a. Set passwords and IP addresses for all nodes. See "Setting Up the Master GMS Node" on page 50
   b. "Loading and Verifying Initial Configuration Settings " on page 52

5. Complete the installation of the MURAL software on the GMS:
   a. Apply available patches on applicable nodes. For information about available patches, see the Release Notes for 3.3 or above.
   b. "Verifying XML Settings " on page 54
   c. "Validating the XML Configuration" on page 78

6. Install MURAL on all other nodes:
   a. Go back and update GMS with the actual WWIDs for LUNs. See steps 1 through 3 of "Verifying Server Details Tab" on page 57
   b. "Generating and Pushing the Information Bases" on page 108

7. Configure environmental parameters specific to your environment:
   a. "Verifying that Processes are Running" on page 106
   b. "Generating and Pushing the Information Bases" on page 108
   c. "Processing the Data " on page 114

8. Verify that the system is working as expected. See "Validating Data on Nodes" on page 116.

9. Prepare the system for data reports:
a. Set up data reporting. See "Setting Up Offline Reports" on page 124.

b. Set parameters for incoming data files. See "Mandatory Parameters for Incoming ASR Files" on page 128
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).

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 Setup

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 18

**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.
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 the 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><strong>Extender 1:Slot 1:</strong></td>
<td><strong>Interconnect A:</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>
</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 1 Fabric</th>
<th>UCS 6248 Fabric Interconnect</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Extender 2:Slot 2:</strong></td>
<td><strong>Interconnect B:</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>

<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:

![Diagram of connections between Fabric Interconnects and UCS networks]

<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:

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

   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:

<table>
<thead>
<tr>
<th>Configuration method: <strong>console</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>This fabric interconnect will be added to the cluster: <strong>Y</strong></td>
</tr>
<tr>
<td>Admin password of interconnect: <strong>admin-password</strong></td>
</tr>
<tr>
<td>Mgmt0 IP address: <strong>Fab-B-management-port-IP-address</strong></td>
</tr>
</tbody>
</table>
Where *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 http://*ip-address-of-cluster*.
**Configuring UCS for MURAL**

To complete the configuration of the UCS for MURAL, run the MURAL configuration scripts for UCS, set up the Cisco UCS Direct-Attached SAN, and set system profile settings for UCS Manager.

A script enables quick configuration for UCS for the MURAL installation. To complete the UCS configuration for MURAL, locate the following files, which can be obtained from either Cisco Advanced Services or Technical Support:

- **ucs-config-version-number.txt** (where *version-number* is the most recent version available)—The configuration parameters in this file are used by the UCS configuration script. You must update this file with your local setup details.

- **ucs-config.exp**—Sets configuration parameters for the UCS Fabric Interconnects, servers, LAN, and SAN.

To run the UCS configuration script, perform the following steps:

1. Edit the **ucs-config-version-number.txt** file, modifying each value that is marked with a Customer Information Questionnaire (CIQ) label to match the value in your CIQ.

2. Save and rename the modified **ucs-config-version-number.txt** file into the same directory as the **ucs-config.exp** script.

3. Verify that you can ping the UCS management IP address:

   ````
   /ucs.exp ucs-mgmt-ip ucs-password
   ```

4. From a Cygwin, Linux, or Mac terminal, run the script and watch for any errors or issues.

   **Tip:** If the script encounters an error, you can recover by resetting the UCS to **defaults.ssh** from the UCS manager. You need to do this for both the A and B sides.
Configuring Direct Attachments to External SANs

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.

To configure the UCS Direct-Attached SAN, complete the tasks described in the following sections:

- "Setting Fabric Interconnects to FC Switching Mode" below
- "Creating VSANs for Zoning" on the next page
- "Designating Storage Ports and Assigning Storage Cloud VSANs" on page 30
- "Confirming the Storage Port WWPN is Logged Into the Fabric Interconnects" on page 32
- "Creating Storage Connection Policies" on page 34
- "Creating SAN Connectivity Policy" on page 36
- "Configuring SAN Cloud Policy" on page 37
- "Creating vHBA Initiator Groups" on page 39
- "Verifying Service Profile Templates" on page 40
- "Configuring System Profiles for the Cisco UCS Manager" on page 41

Setting Fabric Interconnects to FC Switching Mode

To set the Fabric Interconnects to FC Switching mode, perform the following steps:

1. In the UCS Manager, click the Equipment tab at the top of the left-hand navigation pane, then navigate to Fabric Interconnects > Fabric Interconnect identifier, where identifier is a letter like A in the following figure. Open the General tab in the main pane.

2. In the Actions box, select both Set Ethernet Switching Mode and Set FC Switching Mode (in the following figure, the latter does not appear because the list of choices extends beyond the bottom of the box).

3. Click Save Changes.
4. If the value in the **FC Mode** field in the **Status** box is not **Switch**, reboot the system.

5. Repeat steps 1 through 4 for the other Fabric Interconnects.

**Creating VSANs for Zoning**

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

By convention, the name of a VSAN includes the associated ID, in the format **vsan**<i>ID</i>. Note the following restrictions on IDs for VSANs, including storage VSANs, which determine the names you can use:

- ID 4079 (**vsan4079**) is reserved cannot be used in either FC Switching mode or FC End-Host mode.

- If you plan to use FC Switching mode in a Cisco UCS domain, do not assign IDs from the range 3040 through 4078 (**vsan3040** through **vsan4078**), which are not operational in that mode. The Cisco UCS Manager marks them with an error and raises a fault.

To create a VSAN for a Fabric Interconnect, perform the following steps:
1. In the UCS Manager, click the **SAN** tab at the top of the left-hand navigation pane, then navigate to **SAN Cloud > Fabric identifier > VSANs**, where *identifier* is a letter like *A* in the following figure. Click the **General** tab in the main pane.

2. Right-click on **VSANs** in the navigation pane and select **Create VSAN**.

3. In the pop-up window, enter a VSAN name that complies with the restrictions listed above, and the fabric identifier used in Step 1.

4. In the **Properties** box in the main pane, enter the same ID number in both the **VSAN ID** and **FCoE VLAN ID** fields, as shown in the following figure. 

   **Note:** You can use the values 3010 and 3020 for the VSANs. Ensure that these values are not used in the network.

5. In the **FC Zoning Settings** box in the main pane, click the **Enabled** radio button if it is not already selected.

6. Click the **Save Changes** button.

7. Repeat Steps 1 through 6 for the other **Fabric identifier** items under **SAN Cloud** where *identifier* is a letter like *B*.

8. Navigate to **Storage Cloud > Fabric identifier > VSANs**, and repeat Steps 1 through 6 for all **Fabric identifier** items under it.
The following sample figure shows the navigation pane after VSANs are created for Fabric Interconnects Fabric A and Fabric B under SAN Cloud and Storage Cloud. As indicated, you can use the same VSAN ID in both clouds.

**Designating Storage Ports and Assigning Storage Cloud VSANs**

For each Fabric Interconnect, configure the ports connecting to the storage array as type FC, reboot, and then designate the FC Ports as FC Storage Ports.
To designate storage ports, perform the following steps:

1. In the UCS Manager, click the **Equipment** tab at the top of the left-hand navigation bar, then navigate to **Fabric Interconnects > Fabric Interconnect identifier**, where *identifier* is a letter like *A*. Right-click **Fabric Interconnect identifier** and select **Configure Unified Ports** to open the pop-up window shown in the following figure.

![Configure Unified Ports](image)

2. Use the slider to configure the ports connecting to the storage array as type **FC**.

3. Repeat steps 1 and 2 for the other Fabric Interconnects.

4. Wait until all Fabric Interconnects have rebooted.

5. Navigate back to the first **Fiber Interconnect identifier**, then to **Fixed Module > FC Ports > FC Port 31**.

6. In the main pane, make the following settings:
   a. In the **Actions** box, select **Configure as FC Storage Port**.
   b. In the **Properties** box, select the appropriate VSAN from the **VSAN** drop-down menu. In the following figure, **vsan3010** is selected for Fabric Interconnect A.
7. Repeat Step 6 for **FC Port 32**.

8. Click **Save Changes**.

9. Repeat Steps 5 through 8 for the other Fabric Interconnects, ensuring the correct VSANs are selected.

**Confirming the Storage Port WWPN is Logged Into the Fabric Interconnects**

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 Fabric Interconnects, perform the following steps:

1. Use SSH to log in as **admin** to the virtual IP address of the Fabric Interconnect.

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

```
hostname# 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.
```
...  

hostname (nxos)#

**Note:** You can run `?` in the prompt to get help.

3. Run the `show zoneset active` command to display the active zonesets.

    hostname (nxos) # show zoneset active

The resulting output may resemble:

<table>
<thead>
<tr>
<th>zoneset name</th>
<th>zone name</th>
<th>vsan ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname-­­-­­vsan-­­3010-zoneset vsan 3010</td>
<td>hostname_A_8_UI1_vHBA-A vsan 3010</td>
<td>3010</td>
</tr>
<tr>
<td></td>
<td>* fcid 0x6c0000 [pwn 20:00:00:05:ad:1e:11:2f]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* fcid 0x6c000f [pwn 50:06:01:68:3e:e0:0a:6b]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* fcid 0x6c01ef [pwn 50:06:01:60:3e:e0:0a:6b]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>hostname_A_7_GMS1_vHBA-A vsan 3010</td>
<td>3010</td>
</tr>
<tr>
<td></td>
<td>* fcid 0x6c0003 pwn 20:00:00:05:ad:1e:11:4f</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* fcid 0x6c000f [pwn 50:06:01:68:3e:e0:0a:6b]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* fcid 0x6c01ef [pwn 50:06:01:60:3e:e0:0a:6b]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>hostname_A_6_INSTA1_vHBA-A vsan 3010</td>
<td>3010</td>
</tr>
<tr>
<td></td>
<td>* fcid 0x6c0004 [pwn 20:00:00:05:ad:1e:11:7f]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* fcid 0x6c000f [pwn 50:06:01:68:3e:e0:0a:6b]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* fcid 0x6c01ef [pwn 50:06:01:60:3e:e0:0a:6b]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>hostname_A_5_INSTA2_vHBA-A vsan 3010</td>
<td>3010</td>
</tr>
<tr>
<td></td>
<td>* fcid 0x6c0005 [pwn 20:00:00:05:ad:1e:11:5f]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* fcid 0x6c000f [pwn 50:06:01:68:3e:e0:0a:6b]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* fcid 0x6c01ef [pwn 50:06:01:60:3e:e0:0a:6b]</td>
<td></td>
</tr>
</tbody>
</table>

4. Run the `show flogi database vsan vsan-ID` command, where `vsan-ID` is the identifier for the VSAN. In the following example, the VSAN ID for Fabric Interconnect A is 3010.

5. Make a note of the world wide port numbers in the **PORT NAME** column,
which are used in "Creating Storage Connection Policies" below.

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>VSAN</th>
<th>FCID</th>
<th>PORT NAME</th>
<th>NODE NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>fc1/31</td>
<td>3010</td>
<td>0x1000ef</td>
<td>50:06:01:60:3e:a0:28:d2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>50:06:01:60:be:a0:28:d2</td>
<td></td>
</tr>
<tr>
<td>fc1/32</td>
<td>3010</td>
<td>0x1001ef</td>
<td>50:06:01:69:3e:a0:28:d2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>50:06:01:60:be:a0:28:d2</td>
<td></td>
</tr>
</tbody>
</table>

6. Run the `exit` command.

7. Repeat Steps 1 through 5 on the other Fabric Interconnects.

   **Note:** For instance, connect to `nxos B` where B is for Fabric Interconnect B.

The following sample, the `show flogi database vsan vsan-ID` command uses the VSAN ID for Fabric Interconnect B, 3020.

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>VSAN</th>
<th>FCID</th>
<th>PORT NAME</th>
<th>NODE NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>fc1/31</td>
<td>3020</td>
<td>0x4200ef</td>
<td>50:06:01:61:3e:a0:28:d2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>50:06:01:60:be:a0:28:d2</td>
<td></td>
</tr>
<tr>
<td>fc1/32</td>
<td>3020</td>
<td>0x4201ef</td>
<td>50:06:01:68:3e:a0:28:d2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>50:06:01:60:be:a0:28:d2</td>
<td></td>
</tr>
</tbody>
</table>

**Creating Storage Connection Policies**

Create a storage connection policy for each Fabric Interconnect.

To create storage connection policies, perform the following steps:

1. In the UCS Manager, click the **SAN** tab at the top of the left-hand navigation bar, then navigate to **Policies > root**. Right-click **Storage Connection Policies** and select **Create Storage Connection Policies**.

2. In the pop-up window, apply the following settings. The `FI-ID` variable is the Fabric Interconnect identifier, such as **A**.
Name—2. Enter a name that complies with local naming conventions, such as `storage-conn-polFI-ID`.

Zoning Type field in the Properties box in the main pane, click the Single Initiator Multiple Targets radio button.

Add FC Target Endpoints—The WWPN displayed for port 31 in the output from the `show flogi database vsan vsan-ID` command in "Confirming the Storage Port WWPN is Logged Into the Fabric Interconnects" on page 32.

Path—FI-ID

VSAN—The VSAN created for the Fabric Interconnect in "Creating VSANs for Zoning" on page 28, such as `vsan3010` for Fabric Interconnect A

For example,

| Name: storage-conn-polA Zoning = Single Initiator Multiple Target |
|--------------------------|--------------------------|
| Add FC Target Endpoints  |
| In FC Target Endpoints, enter WWPN printed in the last section for the related VSAN. |
| Path (select FI A or B)  |
| VSAN (created earlier for respective FI) |

3. Repeat Step 2 for port 32.

4. Repeat Steps 1 through 3 to create storage connection policies for the other Fabric Interconnects.

The following example figure shows the result for Fabric Interconnect A. The settings from Step 2 are recorded in the Fc Target Endpoints box.
Creating 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, perform the following steps:

1. In the UCS Manager, click the SAN tab at the top of the left-hand navigation bar, then navigate to Policies > root. Right-click Storage Connection Policies and select Create SAN Connectivity Policy.

2. Click Add. Enter the values shown in the following example, ensuring that
the name complies with local naming conventions.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>vHBA-A</td>
</tr>
<tr>
<td>WWNN Assignment</td>
<td>wwnn-pool1(768/784)</td>
</tr>
<tr>
<td>Fabric ID</td>
<td>A</td>
</tr>
<tr>
<td>Select VSAN</td>
<td>vsan3010 (Storage Connection Policy (created earlier))</td>
</tr>
<tr>
<td>Adaptor Policy</td>
<td>VMWare</td>
</tr>
</tbody>
</table>

3. Repeat Steps 1 and 2 for the other vHBA.

**Configuring SAN Cloud Policy**

The SAN cloud policy **San Con Pol A** shows two vHBAs: **vHBA-A** and **vHBA-b**.

![SAN Cloud Policy](image)

The following figure shows 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.
The following screen shows 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.

![Image of Cisco UCS Manager SAN tab]

**Creating vHBA Initiator Groups**

To create a vHBA initiator group for the storage connectivity policy, perform the following steps:

1. In the UCS Manager, click the **SAN** tab at the top of the left-hand navigation bar, then navigate to **Policies > root > SAN Connectivity Policies**.
2. Add SAN Connectivity Policies for FI A/B (the preceding example shows **SAN-con-pol-A**).
3. Select **SAN Connectivity Policies**, for example: SAN-con-pol-A.
4. Add values like the following:
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 the above steps for the other Fabric Interconnects.

Verifying Service Profile Templates

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

To verify service profile templates, perform the following steps:

1. In the UCS Manager, click the Servers tab at the top of the left-hand navigation bar, then navigate to Service Profile Templates > root >> Service Template template-name > vHBAs.

2. Select SAN Connectivity Policy. Verify that vHBAs have been applied to the service profile template, and that all details are correct.

3. Click Save Changes.

4. Repeat steps 1 through 3 for the other vHBAs.
The following figure shows a vHBA configuration within a service template.

![vHBA configuration](image)

This completes the configuration of Cisco UCS Direct-Attached SAN.

**Configuring System Profiles for the Cisco UCS Manager**

Configure profiles in the Cisco UCS Manager that modify the default settings of hardware systems in accordance with the following recommended settings.

**Ethernet Adapter Policy**

Configure the Ethernet adapter policy for all Ethernet interfaces.

To configure Ethernet adapter policy on the UCS, perform the following steps:

1. In the UCS Manager, click the **Servers** tab at the top of the left-hand navigation bar, then navigate to **Policies > root > Eth Adapter Policy Default > General**.

2. Enter the field values as shown in the following table. Fields that are not mentioned, or whose values are specified as **Default**, do not need to be changed.

**Note:** Ensure that the Resources and Options values are set correctly, as recommended in the table.
### Field Name | Field Value
--- | ---
Transmit Queues | 1
**Ring Size** | Default
Receive Queues | 8
**Ring Size** | Default
Completion Queues | 9
Interrupts | 16
Transmit Checksum Offload | Enabled
Receive Checksum Offload | Enabled
TCP Segmentation Offload | Enabled
TCP Large Receive Offload | Enabled
Receive Side Scaling | Enabled
**Fallback Timeout** | Default
Interrupt Mode | MSI X
Interrupt Coalescing type | Min
Interrupt Timer | 350

#### Bios Policy (Processor Page)

Configure values on the **Processor** page under **Bios Policy**.

1. In the UCS Manager, click the **Servers** tab at the top of the left-hand navigation bar, then navigate to **Policies > root > BIOS Policies > mural-bios > Advanced > Processor**.

2. Enter the field values as shown in the following table. Fields that are not mentioned, or whose values are specified as **Default**, do not need to be changed.

### Field Name | Field Value
--- | ---
Turbo Boost | Disabled
Enhanced Intel SpeedStep | Enabled
Hyper Threading | Default
Core Multiprocessing | all
Execute Disable Bit | Default
Virtualization Technology | Disabled (Enabled if VMs are expected to be run on the systems)
### Specifying Boot Order of Devices

To specify the boot order for devices, perform the following steps:

1. In the UCS Manager, click the **Servers** tab at the top of the left-hand navigation bar, then navigate to **Policies > root > Boot Policies > Boot Policy Default (or configured for service profiles) > General**.

2. Set the order of preference for boot devices as shown in the following figure.
   - **a.** Local Disk
   - **b.** LAN Boot (in the case of PXE boot, ensure that both interfaces are added--for example, `vnic0` and `vnic1`)
   - **c.** Other Devices
Setting the RAID Policy

We recommend that you run a RAID 1 setup. Cisco systems allow configuration of RAID setup using the LSI MegaRaid Configuration tool in BIOS.

**Note:** Set up hardware RAID 1 on the local disk.

**Caution:** Do not use the Any configuration mode on servers with MegaRAID storage controllers.

To set the RAID policy, perform the following steps:

1. In the UCS Manager, click the **Servers** tab at the top of the left-hand navigation bar, then navigate to **Policies > root > Local Disk Configuration Policies > Local Disk**.

2. Select **Configuration Policy Default > General**.

3. In the Properties box, select **RAID 1 Mirrored** from the **Mode** drop-down
menu, as shown in the figure:

For more information, see the *Cisco UCS Manager GUI Configuration Guide, Release 2.1*. 
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.

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 **pwnn** in the output refers to WWPNs.

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

The resulting output may resemble:

```
zoneset name hostname-vsan-3010-zoneset vsan 3010
zone name hostname_A_12_UI1_vHBA-A vsan 3010
  * fcid 0x100003 [pwnn 20:00:00:05:ad:1e:11:df]
  * fcid 0x1000ef [pwnn 50:06:01:60:3e:a0:28:d2]
  * fcid 0x1001ef [pwnn 50:06:01:69:3e:a0:28:d2]

zoneset name hostname-vsan-3010-zoneset vsan 3010
zone name hostname_A_11_UI2_vHBA-A vsan 3010
  * fcid 0x100006 [pwnn 20:00:00:05:ad:1e:11:ff]
  * fcid 0x1000ef [pwnn 50:06:01:60:3e:a0:28:d2]
  * fcid 0x1001ef [pwnn 50:06:01:69:3e:a0:28:d2]
```
Run the `show zoneset active` command again for the other Fabric Interconnect:

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

The resulting output may resemble:

```
zoneset name hostname-vsan-3020-zoneset vsan 3020
  zone name hostname_B_24_UI1_vHBA-B vsan 3020
  * fcid 0x420007 [pwn 20:00:00:05:ad:1e:11:2e]
  * fcid 0x4200ef [pwn 50:06:01:61:3e:a0:28:d2]
  * fcid 0x4201ef [pwn 50:06:01:68:3e:a0:28:d2]

zoneset name hostname_B_23_UI2_vHBA-B vsan 3020
  * fcid 0x420009 [pwn 20:00:00:05:ad:1e:11:5e]
  * fcid 0x4200ef [pwn 50:06:01:61:3e:a0:28:d2]
  * fcid 0x4201ef [pwn 50:06:01:68:3e:a0:28:d2]
```

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).

**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.
  - From SPS A and SPS B to SP A and SP B
  - 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>Item</td>
<td>Value</td>
</tr>
<tr>
<td>-----------------------------</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**.

**Configuring IP Addresses for 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.

Proceed to next section once UCS and EMC hardware configurations are completed.
Setting Up the Master GMS Node

After the master GMS blade is manufactured (the MURAL software is loaded on it), set the administrator password for the node, assign IP address(es), and verify correct zoning on the fabric interconnect.

GMS Lite can be used to prepare the GMS XML configuration file and PXE boot server to manufacture the master GMS node.

1. Install VirtualBox software on the laptop used to install the MURAL system. Ensure the laptop is connected to network using the Ethernet port and the bridged adapter from the VM host machine (laptop).

2. Create VM using pre-configured Vdisk image, shipped with this release, as described in the section "APPENDIX I: Installing and Configuring VM for GMS Lite" on page 132

3. If it is not possible to use GMS Lite, go to the section "APPENDIX II: Manufacturing the Master GMS Blade" on page 139 to prepare the master GMS node. This section will install the master GMSnode, then use that node to manufacture and install all other nodes.

Setting the Password and IP Address(es)

To set the administrator password and IP address(es) on the master GMSnode, perform the following steps:

Note: Multiple IP addresses are only required if there are multiple interfaces.

1. Log in to the master GMS node using the VM console as admin.

2. Enter config mode and set the password for the admin user. We recommend setting the password to admin@123, which is the standard value that Technical Support expects to use when they log in to a blade to help you with a problem.

```bash
> en
# conf t
```
MURAL Software Standard Installation Guide

3. Enter config mode again and define the IP address(es) for the management interface and default gateway.

   > en
   # conf t
   (config)# interface mgmt-interface ip-address mgmt-IP-of-GMS-server subnetmask-of-mgmt-net
   (config)# ip-default-gateway mgmt-network-default-gateway-IP
   (config)# write memory

   For example,

   (config)# interface eth0 ip address 192.168.103.78 /24
   (config)# ip default-gateway 192.168.103.1

4. Install the license.

   > en
   # conf t
   (config)# license install LK2-RESTRICTED_CMDS-88A4-FNLG-XCAU-U
   (config)# write memory

5. Start the GMS Server:

   > en
   # conf t
   (config)# pm process gms_server launch auto
   (config)# pmx register pgsql
   (config)# write memory
   (config)# pm process tps restart
   (config)# pm process gms_server restart


The next section guides you through creating the XML that will be used to manufacture and configure the MURAL system on all the blades.
**Loading and Verifying Initial Configuration Settings**

This topic explains how to define the deployment topology using the General Management System (GMS) instead of having to install and configure software manually on each blade. GMS is a node that enables installation and monitoring of the software.

In this section, you must specify the world wide identifier (WWID) associated with logical unit number (LUN) of each node. When you first configure the GMS, WWIDs for the LUNs are not yet configured (because you have not yet configured EMC) and you must use "dummy" values as placeholders. You will configure the LUNs in "Allocating Storage on the EMC" on page 46, and then revisit this section to specify the actual WWIDs.

- During the first time through these procedures, the actual WWID is only available for the master GMS node so you must use temporary placeholder values for all other nodes.

- During the second time through these procedures, you specify the real WWIDs that you associated with the LUNs when you configured them in "Allocating Storage for the Remaining Nodes" on page 1.

**Notes:**

- The GMS user interface requires Java Plug-in 10.40.2.43 or above, and JRE version 1.7.0_40-b43 or above.

Before you begin, locate your Customer Information Questionnaire (CIQ)—for some of the steps in this procedure, you will need to refer to the information on the **IP Survey** tab.

**Accessing the GMS User Interface**

To access the GMS user interface (UI), perform the following steps:

1. In a browser, access the following URL:

   `http:// IP-Address-GMS-Lite/configure`
Note: The preferred browser for opening the GMS Applet is Mozilla Firefox v28.0 (or above) with Java Applet plugin v7 update 51.

2. Log in as admin using the password you defined in "Setting Up the Master GMS Node" on page 50 (the recommended password is admin@123).

3. In the Java applet pop-up window, enter user name and password:

![Authentication Required](image)

4. Once you have logged in, the GMS UI displays a series of screens, where you enter configuration information. Proceed as outlined in the following sections.

### Loading the Base Configuration File

A sample configuration file is provided with the installation package. This file, `mural.xml`, is configured specifically for the software version and can be changed for the local set up according to the bill of materials (BoM). In this case, it includes a logical grouping of the nodes into two chassis (blade enclosure) and configuration settings for all of the system components.

In most cases, you only need to verify settings in the XML file, but there may be instances where you need to modify them. For example, it would be necessary if the slot numbers for the blades were changed or if some values were not known when you filled out the CIQ. Profiles are provided for system components, and in some cases you might select from among different profiles to choose the one that provides optimal settings for your environment.
**Warning:** Do not modify the file directly in a text editor. Use the GMS UI to make any modifications to the *mural.xml* file.

To upload the configuration file in the GMS UI:

1. Click the file navigation button (…) to the right of the first text field.
2. Navigate to and select the configuration file.
3. Select the **Load Config File** button.

4. When the configuration file is loaded, the GMS UI appears.
5. Configuration information is loaded from the *mural.xml* file, populating fields on each tab with values that are specific to your deployment.

**Note:** In many cases, all you need to do is verify the settings are correct. If you find incorrect values, you can

6. The file prescribes a logical grouping of the nodes into two chassis (blade enclosure).

Proceed with the initial configuration as outlined in "Verifying XML Settings " below. You need to check the XML against values specified as necessary for your deployment.

**Verifying XML Settings**

Click on the name of a chassis to see more details and verify settings, as shown in the following image:
The hardware type, chassis number and chassis logical name are displayed, as well as the list of nodes (blades) in each slot.

**Note:** In most cases you only need to verify settings in the subsequent sections. You might need to modify settings if, for example, the slot numbers for blades have changed or some information was not yet known when the CIQ was completed for your deployment.

Proceed with verifying settings applied by the configuration file as outlined below.

**Before You Begin**

Before verifying anything in the XML file, you need to look up the following under the Interface Members section:

1. MAC addresses of the GMS node and interface bindings, see "Updating MAC IDs for Nodes " on the next page.

2. WWIDs for the storage allocated to each node, see "Finding WWIDs of
LUNs" on page 1:

- master and standby GMS nodes
- all Collector nodes
- all Compute nodes
- all Rubix nodes
- both Insta nodes

During the initial configuration process, you must do this for each node in each of the two logical chassis.

Locate this information before "Verifying XML Settings " on page 54

**Understanding MAC Addresses and LUN WWIDs**

The number of LUNs, and therefore the number of WWIDs, assigned to each node depends on the type of node:

- Compute nodes—Each node has one WWID assigned
- Insta nodes—Each Insta node (being clustered) has two assigned WWIDs—
  one assigned to `dbroot1` of both Insta 1 and Insta 2, one assigned to
  `dbroot2` of both Insta 1 and Insta 2.

**Updating MAC IDs for Nodes**

From the **Server Details** tab, select **Chassis > Node**. Once there, update MAC addresses using values recorded on the CIQ sheet for both the NIC ports of that node. MAC addresses need to be updated for each node, added in the GMS.

GMS also has a **Fetch MAC IDs** feature to quickly update MAC addresses for all the nodes, together by fetching the information from Cisco UCS Manager (Version 2.2(1b)). Go to Appendix IV, section "Fetching MAC IDs Feature" on page 151 to fetch MAC Addresses for all the nodes in GMS.

**Finding WWIDs of LUNs**

If you are at a stage where UCS configuration is not yet fully set up, then you can use a dummy WWID for each blade. However, if you have configured both UCS and EMC, you must enter the actual WWID, which you can find as described below.
To find the WWID of LUNs, perform the following steps:


2. From the Storage tab, select LUNs. Highlight the destination LUN and click Properties.

3. The unique ID is displayed. To derive the WWID, remove the separator ': ' from the unique ID and add a prefix 3. For example 360060160c7102f004887f4015d49e211.

**Setting Storage WWIDs**

On the initial configuration, EMC is not yet configured and you must enter dummy values. After EMC is configured, you will return to this procedure and enter the actual values for the WWIDs of the LUNs.

*Note:* Only update the WWIDs under the Storage section after manufacturing is completed in later sections.

Ensure that the same WWID is assigned to dbroot1 for both the Insta 1 and Insta 2 nodes. Likewise, ensure that the same WWID is assigned to dbroot2 for both Insta nodes.

**Verifying Server Details Tab**

The figures in the following sections show a sample configuration. Your configuration may be different. Verify in the GMS user interface (UI) that all the nodes in your deployments have been configured.

To verify the MAC addresses of interface bindings and storage partitions for each node, perform the following steps:

*Note:* Throughout this section, if the value is incorrect, click on Add to create a new entry and set the correct value. Then select the incorrect entry and click Delete to remove it.

1. Open the Server Details tab in the GMS UI.

2. In the Chassis box, select the chassis.
3. The **Slot** section lists the nodes (blades) in each slot. Select a node to verify or modify its WWID values.

   **Note:** Even if entering dummy values for the WWIDs, you must ensure that they are unique among all the nodes (with the exception of the WWIDs that are shared between Insta1 and Insta2). If the WWIDs are not unique, the final validation step fails with an error message and you cannot save the file until it is corrected.
4. Repeat steps 1 through 3 for each of the following nodes in Chassis 1:

- First GMS node
- First Collector node
- First Compute node
- First Insta node
- First Rubix node

**Note:** Ensure that the same WWID is assigned to dbroot1 and dbroot2 for both Insta 1 and Insta 2 in the GMS configuration.
5. If using a dual chassis, repeat steps 1 through 4 for each of the following nodes in Chassis 2:

- Second GMS node
- Second Collector node
- Second Compute node
- Second Insta node
- Second Rubix node

6. In the **Interface Members** box, verify that the MAC address of the interface binding for the node matches the value written in your CIQ.

![Interface Members](image)

**Verifying Networks Tab**

To define the networks of the blades, perform the following steps:

1. Under the **Networks** tab, verify the following fields for the internal (management) network:

   - Network Name
   - Network IP Address: prefix and subnet
   - Interface Type
   - Network Interface
   - Network Range
2. Repeat the previous step for external (control) networks.

**Verifying Global Settings Tab**

Verify the global settings for the system and IP addresses configured for each node cluster.

To verify the network IP address, global settings, and IP addresses of the nodes:

Under the **Global Settings** tab, verify the following information for the MURAL system:

1. DNS server
2. Default gateway
3. NTP server IP address
4. NTP version

5. SNMP Details
Set the Collector IP address as the SNMP Server IP.

6. Pre-Defined Users

Set Passwords for Pre-defined users and add other users required to send EDR data into MURAL system or collect MURAL reports.

Verifying Nodes Tab

Define the management and data IP address and subnet mask of each node.

Verifying Clusters Tab

The mural.xml configuration file included with your installation package includes configurations of the node clusters. The figures below show an example—the
actual configurations for your setup might be different depending on how much traffic is being sent to the MURAL system.

During initial configuration, you must create clusters for each type of node and add the member nodes to each cluster.

To configure a cluster, perform the following steps:

1. Go to the **Clusters** tab.

2. From the **Cluster Type** list, select the cluster you want to configure or verify.

3. Select **Cluster Type** from the drop-down list, enter the **Cluster Name**, and **Cluster Interface**, and click **Add**. For example, the following figure shows a Collector cluster called COL-CLUS:

4. Select the newly created cluster, and under **Cluster VIPs**, click **Add** and enter the virtual IP address of the new cluster.

5. Repeat steps 2 through 4 for the rest of the nodes.

- GMS
- Collector
- Rubix
6. Define the GMS, Collector, Rubix, and Insta clusters.
   a. Set the GMS, Collector, Rubix, and Insta cluster type to **1+1 HA**.
   b. Set the Compute Cluster as **N Node**.

**Verifying Applications Tab and Specifying Component Profiles**

This section describes how to load profiles for each component. These profiles set the configurations for the components. You can then change individual settings to adjust the configuration for your environment.

Profiles are provided for system components, and in some cases you might select from among different profiles the one that provides optimal settings for your deployment.

Templates for GMS, Postgres, HDFS, Solution, Collector and Rubix need to be properly defined for GMS cluster.

Configuration requirements for this deployment are provided here. For guidance on how to apply these settings, skip to "Applying Profile Settings" on page 77.

- Collector GMS Cluster with the following values.

Ensure that Rubix Atlas and Launcher profiles are added to the application instance 1 and the remaining profiles are added to the application instance 2.

<table>
<thead>
<tr>
<th>App Name</th>
<th>App Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMS</td>
<td>gms_default_without_nbi_template</td>
</tr>
<tr>
<td></td>
<td><strong>Clusters</strong>—GMS Cluster</td>
</tr>
<tr>
<td></td>
<td><strong>Application Instance</strong> = 1</td>
</tr>
<tr>
<td>App Name</td>
<td>App Profile</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| PostgreSQL | postgresql_custom_mural | Clusters—GMS Cluster  
Application Instance = 1 |

- Collector Cluster with the following values:

<table>
<thead>
<tr>
<th>App Name</th>
<th>App Profile</th>
<th>Settings</th>
</tr>
</thead>
</table>
| Collector | collector_custom_adaptor_bulkstats_template | Clusters = COL-CLUS  
Application Instance = 1 |

Change the format of the following values to `/data/collector/bulkstats_files/gateway_name`:

- BulkStats file input directory, specified by
  
adaptor.bulkStats.input.fileConfig.
bulkStatsFile1.inputDirectory

Change the format of the following values to `/data/collector/bulkstats_files_backup/gateway_name`:

- BulkStats filebackup directory, specified by
  
adaptor.bulkStats.input.fileConfig.
bulkStatsFile1.backupDirectory

Refer to the table to set the gateway names, filename formats, and transfer filename format.
<table>
<thead>
<tr>
<th>App Name</th>
<th>App Profile</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collector</td>
<td>collector_custom_adaptor_edrhttp_edrflow_template</td>
<td></td>
</tr>
<tr>
<td>App Name</td>
<td>App Profile</td>
<td>Settings</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Clusters = COL-CLUS</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Application Instance = 1</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>adaptor.edrflow.numThreads</strong> = 8 for 24 CPU, 11 for 32 CPU</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>adaptor.edrhttp.numThreads</strong>s = 8 for 24 CPU, 11 for 32 CPU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Output directory for EDR flow, specified by the parameter adaptor.edrflow.output.directory. The format of the value is /data/collector/1/output/edrflow/%y/%m/%d/%h/%mi/gateway-name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Output directory for EDR HTTP, specified by the parameter adaptor.edrhttp.output.directory. The format of the value is /data/collector/1/output/edrhttp/%y/%m/%d/%h/%mi/gateway-name (where %y/%m/%d/%h/%mi/ indicates the format of the time value).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• File name and transfer file name for EDR flow, specified by the parameter adaptor.edrflow.input.fileConfig.flowfile.FileNameFormat adaptor.edrflow.input.fileConfig.flowfile.TransferFileNameFormat</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• File name and transfer file name for EDR HTTP, specified by the parameters adaptor.edrhttp.input.fileConfig.httpfile.FileNameFormat</td>
</tr>
<tr>
<td>App Name</td>
<td>App Profile</td>
<td>Settings</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mat</td>
<td>adaptor.edrhttp.input.fileConfig.httpfile.TransferFile-NameFormat</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Refer to the <a href="#">table</a> to set the gateway names, filename formats, and transfer filename format.</td>
<td></td>
</tr>
<tr>
<td>solution</td>
<td>solution_custom_mural</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Clusters = COL-CLUS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application Instance = 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Client name = cisco</td>
<td></td>
</tr>
<tr>
<td></td>
<td>isStarterPack = false</td>
<td></td>
</tr>
<tr>
<td></td>
<td>timezone = Refer to the <a href="#">table</a> for valid values.</td>
<td></td>
</tr>
<tr>
<td>DFS</td>
<td>dfs_custom_template</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Clusters = COL-CLUS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application Instance = 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>hadoop.mapred.min.split.size = 134217728</td>
<td></td>
</tr>
<tr>
<td>Hive</td>
<td>hive_custom_mural</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Clusters = COL-CLUS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application Instance = 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Use this profile only if Anomaly is enabled.</td>
<td></td>
</tr>
</tbody>
</table>
When you set the value for `timeZone`, ensure that the value is the same as what was used in the UI templates. The following table lists the different `timeZone` values that can be used.

<table>
<thead>
<tr>
<th>TimeZone String</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>US/Central</td>
<td>United States Central Standard Time</td>
</tr>
<tr>
<td>US/Eastern</td>
<td>United States Eastern Standard Time</td>
</tr>
<tr>
<td>Time Zone String</td>
<td>Country</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>US/Pacific</td>
<td>United States Pacific Standard Time</td>
</tr>
<tr>
<td>America/Lima</td>
<td>Peru</td>
</tr>
<tr>
<td>Chile/EasterIsland</td>
<td>Chile</td>
</tr>
<tr>
<td>Africa/Johannesburg</td>
<td>South Africa</td>
</tr>
<tr>
<td>Asia/Manila</td>
<td>Philippines</td>
</tr>
<tr>
<td>Egypt</td>
<td>Egypt</td>
</tr>
<tr>
<td>Europe/Amsterdam</td>
<td>Netherlands</td>
</tr>
<tr>
<td>Europe/Dublin</td>
<td>Ireland</td>
</tr>
<tr>
<td>UTC</td>
<td>Universal Co-ordinated Time</td>
</tr>
</tbody>
</table>

**Note:** The workflow profile contains configuration settings for the MapReduce jobs.

When you set up Gateway names for the Collector, refer to the following table that lists certain guidelines and samples:

<table>
<thead>
<tr>
<th>Filename Pattern</th>
<th>Regex in Wrapper CLI</th>
<th>Regex in Collector Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gatewayname_(multiple strings separated by underscore or hyphen or both)_flow_timestamp_str4.gz</td>
<td>* * <em>-%MM%DD%YYY%hh%mm%ss</em>.gz</td>
<td>%DC_<em>_</em>.%MM%DD%YYYY%hh%mm%ss*.gz</td>
</tr>
</tbody>
</table>

**Example:** Gatewayname_str1_str2_str3_flow_timestamp_str4.gz

**Timestamp:** MMDDYYYYhhmmss
<table>
<thead>
<tr>
<th>Filename Pattern</th>
<th>Regex in Wrapper CLI</th>
<th>Regex in Collector Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gatewayname_ (multiple strings separated by underscore or hyphen or both) _flow_timestamp_str4_str5.gz</td>
<td>* _ * _ %MM% DD%YYYY% hh%mm%ss *_.gz</td>
<td>%DC_* _ <em>_.%MM%DD% YYYY%hh% mm%ss</em>.gz</td>
</tr>
<tr>
<td><strong>Example:</strong> Gatewayname_str1_str2_str3_flow_timestamp_str4_str5.gz</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Timestamp:</strong> MMDD YYYhhmmss</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gatewayname_ (multiple strings separated by underscore or hyphen or both) _flow_string_timestamp_string.gz</td>
<td>* _ * _ %MM% DD% YYYY%hh%mm %ss_*_.gz</td>
<td>%DC_* _ <em>_.%MM%DD% YYYY%hh% mm%ss</em>.gz</td>
</tr>
<tr>
<td><strong>Example:</strong> Gatewayname_str1_str2_str3_flow_str4_timestamp_str5.gz</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Timestamp:</strong> MMDDYYYY hhmmss</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gatewayname_ (multiple strings separated by underscore or hyphen or both) _flow_string_timestamp_string_string.gz</td>
<td>* _ * _ %MM% DD %YYYY%hh %mm%ss_ *_.gz</td>
<td>%DC_* _ <em>_.%MM%DD %YYYY%hh% mm%ss</em>.gz</td>
</tr>
<tr>
<td><strong>Example:</strong> Gatewayname_str1_str2_str3_flow_str4_timestamp_str5_str6.gz</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Timestamp:</strong> MMDDYYYY hhmmss</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Filename Pattern</td>
<td>Regex in Wrapper CLI</td>
<td>Regex in Collector Configuration</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Gatewayname_(multiple strings separated by underscore or hyphen or both)_flow_string_timestamp_string_string.gz</td>
<td><em>.</em>.<em>.</em>%YYYY%MM%DD%hh%mm%ss_*.gz</td>
<td>%DC_<em>.</em>.<em>.</em>%YYYY%MM%DD%hh%mm%ss*.gz</td>
</tr>
<tr>
<td>Example: Gatewayname_str1_str2_str3_flow_str4_timestamp_str5_str6.gz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gatewayname_(multiple strings separated by underscore or hyphen or both)_flow-string_timestamp_string_string.gz</td>
<td><em>.</em>.<em>-</em><em>%MM%DD%YY%YY%hh%mm%ss</em>*.gz</td>
<td>%DC_<em>.</em>.<em>.</em>%MM%DD%YY%YY%hh%mm%ss*.gz</td>
</tr>
<tr>
<td>Example: Gatewayname_str1_str2_str3_flow-str4_timestamp_str5_str6.gz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timestamp: YYYYMMDDhhmmss</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gatewayname_(multiple strings separated by underscore or hyphen or both)_flow-string_timestamp_string_string.gz</td>
<td><em>.</em>.<em>-</em><em>%MM%DD%YY%YY%hh%mm%ss</em>*.gz</td>
<td>%DC_<em>.</em>.<em>.</em>%MM%DD%YY%YY%hh%mm%ss*.gz</td>
</tr>
<tr>
<td>Example: Gatewayname_str1_str2_str3_flow-str4_timestamp_str5_str6.gz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gatewayname_(multiple strings separated by underscore or hyphen or both)_flow-string_timestamp_string_string.gz</td>
<td><em>.</em>.<em>-</em><em>%MM%DD%YY%YY%hh%mm%ss</em>*.gz</td>
<td>%DC_<em>.</em>.<em>.</em>%MM%DD%YY%YY%hh%mm%ss*.gz</td>
</tr>
<tr>
<td>Example: Gatewayname_str1_str2_str3_flow-str4_timestamp_str5_str6.gz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timestamp: MMDDYYYYhhmmss</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Notes:

- It is mandatory to send gateway name as the first substring followed by an underscore.

- You can replace 'http' with 'flow'.

- If the timestamp is in the MMDDYYYYhhmmss format, set the %MM%DD%YYYY%hh%mm%ss parameter in the Regex pattern.

- If the timestamp is in the YYYYMMDDhhmmss format, set the %YYYY%MM%DD%hh%mm%ss parameter in the Regex pattern.

Later in this installation procedure you will change the Oozie start time and start all of the jobs.
Rubix with the following values:

Ensure that Rubix Atlas and Launcher profiles are added in 1st application instance and remaining profiles to 2nd.

<table>
<thead>
<tr>
<th>App Name</th>
<th>App Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Settings</td>
</tr>
<tr>
<td>Solution</td>
<td>solution_custom_mural</td>
</tr>
<tr>
<td></td>
<td>Application Instance = 2</td>
</tr>
<tr>
<td></td>
<td>Clusters = RUBIX-CLUS</td>
</tr>
<tr>
<td></td>
<td>Client name = cisco</td>
</tr>
<tr>
<td></td>
<td>isStarterPack = false</td>
</tr>
<tr>
<td></td>
<td>timezone = Refer to the table for valid values. The selected timezone is applied to all the UI applications.</td>
</tr>
<tr>
<td>Rubix</td>
<td>rubix_custom_launcher_mural*</td>
</tr>
<tr>
<td></td>
<td>Use this only if HET is enabled.</td>
</tr>
<tr>
<td></td>
<td>Application Instance = 1</td>
</tr>
<tr>
<td></td>
<td>Clusters = RUBIX-CLUS</td>
</tr>
<tr>
<td>Rubix</td>
<td>rubix_custom_atlas_distributed_mural</td>
</tr>
<tr>
<td></td>
<td>Application Instance = 1</td>
</tr>
<tr>
<td></td>
<td>Clusters = RUBIX-CLUS</td>
</tr>
<tr>
<td>Rubix</td>
<td>rubix_custom_rge_mural</td>
</tr>
<tr>
<td></td>
<td>rubix_custom_bulkstats_mural</td>
</tr>
<tr>
<td></td>
<td>rubix_custom_cacheless_mural</td>
</tr>
<tr>
<td></td>
<td>Application Instance = 2</td>
</tr>
<tr>
<td></td>
<td>Clusters = RUBIX-CLUS</td>
</tr>
</tbody>
</table>
### Application Configuration

<table>
<thead>
<tr>
<th>App Name</th>
<th>App Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rubix</td>
<td>rubix_custom_httperror_mural*</td>
</tr>
<tr>
<td></td>
<td>rubix_custom_anomaly_mural**</td>
</tr>
<tr>
<td></td>
<td>* Use this only if HET is enabled.</td>
</tr>
<tr>
<td></td>
<td>** Use this only if Anomaly is enabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Application Instance = 2</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Clusters = RUBIX-CLUS</strong></td>
</tr>
</tbody>
</table>

Set the following property values:

- For profile `rubix_custom_anomaly_mural`, set:
  
  ```
  application.anomaly.sessionCookieDomain = Default as per the requirement
  application.anomaly.mailHost = e.g. - mx1.cisco.com
  application.anomaly.mailSender = e.g. support@cisco.com
  application.anomaly.mailPort = 25
  ```

- For profile `rubix_custom_atlas_distributed_mural`, set:
  
  ```
  application.atlas.rubixFQDN = Default or per requirement
  application.atlas.rgeSolutionURL = Default or per requirement
  application.atlas.anomalySolutionURL = Default or per requirement
  application.atlas.bulkStatsURL = Default or per requirement
  application.atlas.sessionCookieDomain = Default or per requirement
  application.atlas.cachePresistToDisk = false (if no extra lun for disk caching)
  ```
application.atlas.numOwners = 2

- For profile rubix_custom_bulkstats_mural, set:
  application.bulkstats.sessionCookieDomain = Default or per requirement
  application.bulkstats.cachePresistToDisk = false (if no extra lun for Disk caching)
  application.bulkstats.numOwners = 2

- For profile rubix_custom_cacheless_mural, set:
  application.reportAtlas.sessionCookieDomain = Default or per requirement

- For profile rubix_custom_httperror_mural, set:
  application.httperror.sessionCookieDomain = Default or per requirement

- For profile rubix_custom_launcher_mural, set:
  application.launcher.dpiURL = Default or per requirement
  application.launcher.httpURL = Default or per requirement
  application.launcher.sessionCookieDomain = Default or per requirement

- For profile rubix_custom_rge_mural, set:
  application.rge.sessionCookieDomain = Default or per requirement
  application.rge.mailHost = e.g. - mx1.cisco.com
  application.rge.mailSender = e.g. support@cisco.com
  application.rge.mailPort = 25
Insta Cluster with the following values:

<table>
<thead>
<tr>
<th>App Name</th>
<th>App Profile</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insta</td>
<td>insta_custom_httperror_flattest</td>
<td>Application Instance = 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Clusters = INSTA-CLUS</td>
</tr>
<tr>
<td>Insta</td>
<td>insta_custom_mural_bulkstats_flattest</td>
<td>Application Instance = 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Clusters = INSTA-CLUS</td>
</tr>
<tr>
<td>Insta</td>
<td>insta_custom_mural_dpi_flattest</td>
<td>Application Instance = 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Clusters = INSTA-CLUS</td>
</tr>
</tbody>
</table>

Compute Cluster with the following values:

Attach the compute-based profile to the Compute cluster and verify that the name is correct for your setup.
App Name | App Profile | Settings
---|---|---
Compute | compute_default_template | Application Instance = 1
| | Clusters = DN-CLUS

**Applying Profile Settings**

Apply the above profile settings by following these steps:

1. Select the **Applications** tab:

2. Start with the **Available Profiles** section:
   
   a. For **Application Name**, select the name of the system component from the drop-down menu.

   b. For **Application Profile**, select the profile you want to attach to the
3. Scroll through the table in the Application section to find and select the Application Profile you just added. When you click on it, the UI opens two new sections below it: Clusters and Profiles.

4. In the Cluster section, click the Add button to add a new row to the empty table.

5. Attach the profiles as required.

After completing all configurations on the Server Details, Networks, Global Settings, Nodes, Clusters, and Applications tabs as described in the previous sections, validate the configuration settings as described in the section "Validating the XML Configuration" below.

**Validating the XML Configuration**

To validate the GMS configuration, perform the following steps:

1. Click **Validate** on the bottom bar of the GMS interface.

   If any field or value entered is incorrect, a list of errors is displayed.

2. For each error, click the error and then the **Go** button to display the entry in the GMS configuration that is causing the error.
3. Correct any errors by following the steps in "Verifying XML Settings " on page 54

4. Click **Validate** again. When all errors have been resolved, the message **Validation successful** displays on the screen.

5. Click **Save Server File** to save the configuration to the GMS server.

   **Note:** The **Save Server File** is not operational until all validation errors are corrected. To save the file without correcting all errors and completing the validation, click **Save Local File**.

6. To activate the configuration after you have made changes, you must run the **gms config mural.xml activate** command. Until you activate the new configuration file, the system runs the previously saved configuration.
Using GMS Lite to Automate Installation of GMS Nodes

This section explains how to use GMS Lite to manufacture your GMS nodes, instead of manually manufacturing them individually. To manufacture the nodes individually using the manual method, see "APPENDIX II: Manufacturing the Master GMS Blade" on page 139.

Note: The laptop you use for installation must be in the same IP subnet as the MURAL system.

Before You Begin

Ensure that the laptop has a VM management software such as VirtualBox already installed. The section "APPENDIX I: Installing and Configuring VM for GMS Lite" on page 132 provides instructions on installing and configuring VirtualBox.

Warning: Ensure that your laptop and VM are in the same subnet as all other nodes of setup. This is essential for PXE booting the GMS server to be successful.

1. > en
   # _shell
   # cli -t "en" "config t" "show pm process gms_server" | grep
   "Current status"
   
   Current status: running

Activate the XML File

1. Login into GMS Lite (using SSH) as admin user.

   > en
   # _shell

2. Activate the xml file on this VM

   (config)# gms config mural.xml activate
Configuring GMS Lite Node as PXE Boot Server

1. Download the ISO image that was included with the MURAL software package to the machine from which you will access the Cisco UCS blades:

   mfgcd-x86_64-20140731-005012.iso

   **Note:** The MD5 checksum for the iso file is

   7c0e95cc2ff98edc1366792b01934 /data/mfgcd-x86_64-20140731-005012.iso

2. Download the ISO image that was included with the MURAL software package to the machine from which you will access the Cisco UCS blades:

   mfgcd-x86_64-20140731-005012.iso

   **Note:** The MD5 checksum for the iso file is

   7c0e95cc2ff98edc1366792b01934 /data/mfgcd-x86_64-20140731-005012.iso

3. Login into GMS Lite node (using SSH), as an admin user and load the image onto the machine you are going to build.

   > en
   # conf t
   (config)# image fetch scp://admin@IP-local-remote-machine/ directory-path-on-localmachine/iso-image-name

   Where:

   - *IP-local-remote-machine* is the IP address of the machine where the ISO image for the build has been downloaded.
   - *iso-image-name* is the iso image you downloaded in step 1.

   For example:

   (config)# image fetch
   scp://debug@50.204.88.45/data/ftp/software/images/cisco_mural/mural_3_4/mfgcd-x86_64-20140731-005012.iso
Setting Up the Master GMS Node and Cluster

1. Mount the image on the GMS Lite virtual machine:

```
(config)# image mount mfgcd-x86_64-20140731-005012.iso
```

The resulting output may resemble:

```
Copying linux...
Copying rootflop.img...
Copying image.img...
```

2. Verify the image on the GMS Lite node:

```
(config)# ls /var/opt/tms/images/ mfgcd-x86_64-20140731-005012
```

3. Launch PXE boot for all the MURAL nodes, one by one to manufacture the nodes with the ISO image.

```
[admin@gmsLiteVM ~]# cli -m config
(config)# _shell
gmsLiteVM (config)# gms pxeBoot cluster cluster-name node
node-name ucsManagerIP IP-UCS-Manager loginName UserName
loginPassword UserPassword
```

Where:

- `cluster-name` is the cluster name, such as **DN-CLUS**. Use **all** instead of a name to launch PXE boot on all nodes at once.
- `node-name` is a specific node assigned to the named cluster. Use **all** instead of a name to launch PXE boot on all nodes at once.

**Note:** Launching PXE boot on all nodes simultaneously triggers blade reboot from the network. Once the blade start booting from the network, GMS Lite pushes the image on the blade using PXE boot. Then the manufacture process can be started on each blade in parallel.

- **IP-UCS-Manager** is the IP address of the UCS.
- *UserName* is an account with UCS Manager admin privileges on all the MURAL nodes.
- *UserPassword* is the correct password for the *UserName*.

For example, when starting PXE boot on a single node, the code may look like this,

```plaintext
gmsLiteVM(config)# gms pxeBoot cluster DN-CLUS node UCS-DN-1
ucsManagerIP 192.168.125.4 loginName Domain1\user1
loginPassword *
```

The resulting output may resemble:

```
Total number of nodes to be processed: 1
Total number of nodes processed: 1 ......
All nodes processed
Cluster: DN-CLUS
Node: UCS-DN-1 Successfully Pxebooted
```

**Note:** A blade takes approximately 20 minutes to manufacture with the new image. Run below command to check the blade manufacture status.

4. To see PXE boot status, check the blade manufacture status.

```plaintext
gmsLiteVM (config)# gms show manufacturing-status cluster
ClusterName
```

Where *ClusterName* is the cluster of nodes you want to see the PXE boot status for, such as *DN-CLUS*. Use **all** instead of a name to launch PXE boot on all nodes at once.

The resulting output may resemble:

```
UCS-DN-1: OK : Product release: 3.6.2
UCS-DN-2: OK : Product release: 3.6.2
```

In case command based PXE boot from GMS is not possible as mentioned in above section, use "Appendix III: Using KVM Software to Boot PXE Blades " on page 148.
After successful manufacturing of the blades, proceed with next section to attach the SAN storage with respective nodes.
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.

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.

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).

![Register Initiator Record](image1)

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:

![Host List](image2)

### Creating 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>
<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-2</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>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>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):
MURAL Software Standard Installation Guide

- INSTA-1 (to be associated with dbroot1 on both Insta nodes)
- INSTA-2 (to be associated with dbroot2 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.

![Storage LUNs Tab](image)

**Creating 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.

![Create Storage Group window](image)

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.

![Image of Storage Group Properties window]

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.

---

**Adjusting 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:

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

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

```bash
> en
# conf t
(config)# username admin password admin@123
(config)# license install LK2-RESTRICTED_CMDS-88A4-FNLG-XCAU-U
(config)# tps multipath show
(config)# write memory
```
Installing MURAL on the UCS Nodes

In previous steps, you set the configuration parameters for your environment in the mural.xml file. Now you need to load this file onto each blade.

Before You Begin

Complete these tasks before you install MURAL on the UCS nodes.

Updating the WWIDs in GMS

EMC is now configured for all the MURAL nodes. Now that you have configured both UCS and EMC, return to the GMS to configure the actual WWIDs for the LUNs used in the MURAL system. During the initial configuration you used dummy values as placeholders, and now that the actual WWIDs are available, you must specify them in the GMS.

In GMS, go to Server Details tab and update WWIDs in Storage section for each MURAL nodes. Save the updated XML file on GMS Server. Reference Steps 1 through 3 of "Verifying Server Details Tab" on page 57

Applying Patches on MURAL Nodes

Download the patches from the FTP server to the /data directory of the GMS Lite server. Apply all patches that apply to the respective MURAL nodes.

For a complete list of patches and instructions for applying them, see the release notes for the current software version (3.4.2 or later).

Installing MURAL on UCS Nodes

This installation process can either be done individually or all at once. Both methods are described in this section.

Installing Appliance on Individual Nodes

To install the appliance on the various MURAL nodes, use the following steps:
1. SSH to the GMS Lite server as an admin user, using the management IP address.

2. Go to \_shell.

   > en
   # \_shell

3. Run the activation command.

   (config)# gms config mural.xml activate

4. Install the appliance on the standby GMS node:

   (config)# install appliance cluster cluster-name GMS node GMS-2 force-format

   The resulting output may resemble:

   Installation in progress, check /data/gms/logs/GMS-2\_cmc.log file for more details

   Periodically check the installation status until a successful message returns, as shown below:

   gmsLiteVM (config)# install appliance show installation-status
   cluster GMS
   gms-1 : Node successfully installed.
   gms-2 : Node successfully installed.

   **Note:** The status may not show any output for 30 minutes. Wait and try again till the "Node successfully installed" message is displayed.

5. Repeat step 4 for the other clusters. Run,

   (config)# install appliance cluster cluster-name ClusterName
   force-format

   Where ClusterName is replaced by:

   - DN-CLUS (approximately 20-30 minutes)
   - COL-CLUS (approximately 45-60 minutes)
- INSTA-CLUS (approximately 45-60 minutes)
- RUBIX-CLUS (approximately 30 minutes)

**Installing Appliance on All Nodes**

1. SSH to the GMS server using the management IP address and start the installation on all UCS nodes (fetches the software and puts it on the blade):

```
  > en
  # conf t
  (config)# install appliance all force-format
```

2. Monitor the installation status on all UCS blades:

```
  (config)# install appliance show installation-status all
```

**Note:** The installation process takes approximately one hour to complete, although it may vary by installation site.

The above command shows the percentage of the installation status per blade server. When the installation on all nodes is complete, the following message is displayed for every node:

```
Node successfully installed
```

**Configuring Application with Site Specifics**

Execute below commands in both the Collector nodes to copy solution configuration file that is dependent on apps enabled for deployment. Content Analytics is default solution for Cisco MURAL sites. Following applications can also be enabled/disabled using this script.

- Tethering
- HTTP Error Tracking
- Anomaly

**Note:** Hardware at each deployment is sized to run a set of apps. Apps beyond this set will not be able to run on same hardware.
1. Log into the master Insta node and reload the server for the zram changes to take effect:

```
> en
# conf t
(config) # wri mem
(config) # reload
```

Wait for this server to come up as the standby node. Repeat the steps on the other Insta node (the new master Insta node).

2. Log into the master Collector node as an administrator.

```
collector-1 [COL-CLUS: master] > en
collector-1 [COL-CLUS: master] # _shell
```

3. Change directory to the folder with scripts.

```
[admin@collector-1 ~]# cd /opt/etc/scripts/
```

4. Run the following installation script and respond to the prompts with a Y.

```
[admin@collector-1 scripts]# ./install_solution_config.sh
is tethering app enabled, enter (Y/N) : Y
is httperror app enabled, enter (Y/N) : Y
is anomalyDetection app enabled, enter (Y/N) : Y
```

The resulting output may resemble:

```
 atlas:tethering
 solutionConfig.json generated successfully at path/data/CoreJob/config
[admin@collector-1 scripts]#
```

**Configuring the Rule-Based Reporting Feature**

If the Rule-based report feature is enabled, edit the following file in both of the NameNodes: /opt/etc/oozie/EDR/Feed/EDRFlowFeed.json

1. Change the property value to **true** for:

   com.guavus.mapred.atlas.app.dpiapp.feature.rulebase.RulebaseMapper
2. After the change is made, run this command to verify the change has been applied:

```bash
# grep "com.guavus.mapred.atlas.app.dpiapp.feature.rulebase.RulebaseMapper" /opt/etc/oozie/EDR/Feed/EDRFlowFeed.json
```

The resulting output may resemble:

```
"com.guavus.mapred.atlas.app.dpiapp.feature.rulebase.RulebaseMapper" : "true",
```

**Troubleshooting Node Installation**

If the installation fails at any point, please contact Technical Support.

Logs can be collected on the GMS server from the location `/data/gms/logs`. 
Verifying that Processes are Running

After making any performance-related modifications, verify that the processes are running.

**Note:** After you make any modifications, wait at least 15 minutes to ensure processes have had a chance to restart before running the following commands.

1. Log in to the master NameNode and verify that all Compute nodes have joined the HDFS cluster. The output shown in the following sample command sequence indicates correct configuration.

```
> en
(config)# _shell
# ps -ef | grep hadoop | awk '{print $NF'}
  org.apache.hadoop.hdfs.server.datanode.DataNode
  org.apache.hadoop.hdfs.server.namenode.NameNode
  hadoop
  org.apache.hadoop.hdfs.server.namenode.NameNode
  org.apache.hadoop.hdfs.server.namenode.SecondaryNameNode
  org.apache.hadoop.mapred.JobTracker
# hadoop dfsadmin -report 2>/dev/null | egrep "available|Name|Status"
  Datanodes available: 3 (3 total, 0 dead)
  Name: 10.10.2.13:50010
  Decommission Status : Normal
  Name: 10.10.2.14:50010
  Decommission Status : Normal
  Name: 10.10.2.17:50010
  Decommission Status : Normal
```

**Note:** These are internal IP addresses.

```
> en
# conf t
(config)# show pm process collector | grep status
  Current status: running
```

2. Log into the standby NameNode and repeat the previous step.
3. Log in to the master Insta node, and run the following commands to check on the processes.

```
> en
# conf t
(config)# show pm process insta
Current status: running
(config)# insta infinidb get-status-info
```

**Note:** Processes are running correctly if the output reports *ACTIVE* state for all modules, and *RUNNING* status for all instances and Adapter.

4. Log in to the standby Insta node, and repeat the previous step.

5. Run the following command to verify that Postgres is running on the master GMSnode.

```
> en
# _shell
# ps -ef |grep pgsql
```

The resulting output may resemble:

```
postgres 2990  1  0 timestamp /usr/pgsql-9.2/bin/postmaster -p 5432 -D /data/pgsql/9.2/data
```

6. Log into the standby NameNode and repeat the two previous steps.
Generating and Pushing the Information Bases

To configure your system for the data specific for your environment, you must update the information bases (IBs) and fetch them. In some cases, you might need to also manually modify the IBs to add or reclassify entries.

Configuring IBs for EDR

The following table shows a sample data set for setting up the IBs.

<table>
<thead>
<tr>
<th>DC</th>
<th>Kansas</th>
<th>GGSNIP</th>
<th>27.23.157.1</th>
<th>SSNIP</th>
<th>2.2.2</th>
<th>UBCITY</th>
<th>APN</th>
<th>broadband</th>
<th>GROUP</th>
<th>broadband</th>
<th>RADIUS 1</th>
<th>RADIUS 2</th>
<th>RADIUS 3</th>
<th>RADIUS 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region</td>
<td>Area</td>
<td></td>
<td></td>
<td>Region</td>
<td>Area</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MW</td>
<td>USA</td>
<td></td>
<td></td>
<td>SGSN</td>
<td>USA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Kansas-GGSN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Use the above table for example purposes only. You should use the data that matches your environment. For example, for GGSN, you might use GGSN, PGW, or HA. In this case, GGSMIP is the management IP address. For SGSN, you might use SGSN, SGW, HSGW, or PDSN. In this case, SSSNIP is the service IP address.

To configure the IBs for EDR:

1. Log in to the master Collector node, and update IBs from the image.

```
> en
# conf t
[admin@collector-1 ~] (config)# pmx
pm extension> subshell aggregation_center
pm extension (aggregation center)> update all ibs from image
```

2. Now we need to add GGSN, SGSN, and APN information bases by running:

```
pm extension (aggregation center)> edit ib ib-file-name.map
add
IB IP: ib-IP-address
IB: ib-name
APN Group: group-name
```
Where the italicized words are replaced with the corresponding values from the table below for GGSN, SGSN, and APN information bases:

<table>
<thead>
<tr>
<th>IB</th>
<th>ib-file-name</th>
<th>ib-IP-address</th>
<th>ib-name</th>
<th>group-name</th>
</tr>
</thead>
<tbody>
<tr>
<td>GGSN</td>
<td>ipGgsn</td>
<td>27.23.157.1</td>
<td>GGSN1</td>
<td>(not applicable)</td>
</tr>
<tr>
<td>SGSN</td>
<td>ipSgsn</td>
<td>2.2.2.1</td>
<td>SGSN1</td>
<td>(not applicable)</td>
</tr>
<tr>
<td>APN</td>
<td>apnGroup</td>
<td>(not applicable)</td>
<td>Sushfone-1</td>
<td>Sushfone-1</td>
</tr>
</tbody>
</table>

3. Verify the IP addresses and names were successfully added by running:

```
pm extension (aggregation center)> show ib ib-file-name.map
```

Where `ib-file-name` is:

- `ipGgsn`
- `ipSgsn`
- `apnGroup`

The resulting output may resemble:

```
1    [27.23.157.1] [GGSN1]
1    [2.2.2.1] [SGSN1]
1    [Sushfone-1] [Sushfone-1]
2    [Sushfone-2] [Sushfone-2]
3    [Sushfone-3] [Sushfone-3]
```

4. Exit the aggregation subshell by running `quit`.

5. To configure the IBs for BulkStats:

```
pm extension> subshell bulkstats
pm extension (bulk stats)> update all ibs from image
pm extension (bulk stats)> quit
```

### Configuring DCs and Gateways For All IBs

Add all new DC/gateways to the configuration for the system. DC, ASR, and Gateway are synonymous terms and hold same meaning for the system. Gateway/DC name is a unique key for a gateway configuration. In theBulkStat hierarchy, the gateway name and DC name are the same.
Guidelines for adding gateways:

- All input directories are created under the `/data/collector` path. Hence, in the example below, the ASR should send EDR files to `/data/collector/California/edr111` and send the Bulkstats file to `/data/collector/California/bs111`.

  **Important:** Confirm the actual input directories with the Cisco Technical Support team for your ASR platform.

- Ensure that you provide different input paths for each new gateway being added.

- The `/edr-file-path` and `/bulkstat-file-path` should always start with a forward slash (/).

- The filename pattern provided here should be in sync with the Collector configurations. For guidelines on the regex value to be used for the filename format, see the "Verifying Applications Tab and Specifying Component Profiles" section in "Verifying XML Settings" on page 54. Refer to the values in the Wrapper CLI column for sample filename formats.

- The ASR should send the gateway name in place of `%DC`, as specified in the file name pattern in the Collector configurations.

- If the filenames will have file extensions of `.gz` or `.txt`, then you must provide `"."` in the file name format configuration when adding the gateway.

- All incoming files should contain the string as per their type in the file name; that is, flow EDR files should contain the string "flow," delimited by an underscore (_) or hyphen (-) and similarly HTTP EDR files must contain string "http," delimited by an underscore (_) or hyphen (-) (thus, combinations can also be used, such as "_flow-") or "-http_ ").

To configure gateways:

1. Add gateway information for each gateway (refer to guidelines above for clarification about input parameters):
pm extension (aggregation_center)> add gateway name gateway-name
    region gateway-region
    location gateway-area
    schema_version bulkstat-schema-version
    ip gateway-IP
    timezone gateway-timezone
    edr-filename-pattern incoming-EDR-fileName-pattern
    bulkstat-filename-pattern incoming-BS-fileName-pattern
    type gateway-type
    edr-file-path gateway-edr-file-path
    bulkstat-file-path incoming-BS-files-path-on-collector

**Note:** See "Modifying Gateway Attributes" on page 1 for more information on gateway attributes and a sample of the output generated by this command.

2. Verify the new gateway has been added:

    pm extension (aggregation_center)> show gateways

3. Add IPs for all Collectors to push this information to all Collectors:

    pm extension (aggregation_center)> set collector IPs comma-separated-ip-list

**Example:**

    pm extension (aggregation_center)> set collector IPs 192.168.1.1,192.168.2.2

**Note:** These are internal IP addresses.

4. Set and verify the IP addresses for all Collectors:

    pm extension (aggregation_center)> set collector IPs 192.168.103.110,192.168.103.113
    pm extension (aggregation_center)> show collector IPs

5. Set the BulkStats timezone to **UTC** in **gateway.conf** for every gateway.
The reason for this is that the ASR internally changes the time zone to GMT for the BulkStats file. Edit `gateway.conf` for every BulkStats source at the path:

```
/data/configs/gateway/gateway.conf "timezone": "UTC"
```

6. Push the gateway configuration to all the Collectors:

```
pm extension (aggregation center)> push gateway configuration
```

7. Generate and push all IBs:

```
pm extension (aggregation center)> generate all ibs
pm extension (aggregation center)> push all ibs
pm extension (aggregation center)> quit
```

8. Generate and push IBs on Bulkstats:

```
pm extension> subshell bulkstats
pm extension (bulk stats)> generate all ibs
pm extension (bulk stats)> push all ibs
```

9. Write changes to memory:

```
(config)# write memory
```

**Copying IBs to the Anomaly Feature**

After the above `push` command completes, update all IBs if the Anomaly Detection feature is enabled.

```
[admin@collector-1 ~]# pmx
Welcome to pmx configuration environment
pm extension> subshell anomaly
pm extension (anomaly)> update all ibs
```

**Synchronize the IBs on the Standby Collector Node**

After the above `push` command completes, run the following command on the standby Collector node from the CLI configure terminal.
1. Go to the `bulkstats` subshell.

```bash
host [cluster : master|standby](config)# pmx subshell
bulkstats
```

2. Fetch all IBs.

```bash
pm extension (bulk stats)> fetch all ibs from inbox
```

3. Go to the `aggregation_center` subshell.

```bash
host [cluster : master|standby](config)# pmx subshell
aggregation_center
```

4. Fetch all IBs.

```bash
pm extension (aggregation_center)> fetch all ibs from inbox
```

5. If Anomaly Detection is enabled, go to the `anomaly` subshell.

```bash
host [cluster : master|standby](config)# pmx subshell anomaly
```

6. Fetch all IBs.

```bash
pm extension (anomaly)> fetch all ibs from inbox
```

7. Run the `quit` command twice to exit and run the following command to write changes to memory.

```bash
(config)# wr mem
```
Processing the Data

This section includes information for setting up an ASR user in the Collector nodes and sending the EDR and BulkStats data feeds to the MURAL platform, setting the data start time, and running the data processing commands.

Use one of the ASR data feed methods to send data to the MURAL platform.

Setting Up a New User for the ASR in the Collectors

To set up a new user for the ASR in the Collectors:

1. Log on to the master Collector node and create the user:

```
# en
> conf t
(config)> username userid password password
(config)> write memory
(config)> _shell
```

**Note:** The username and password should be the same ones configured on the ASR for EDR and BulkStats file transfers.

2. Edit `/etc/ssh/sshd_config` to set the following parameters, in case a PAM related authentication error is reported in the master Collector node `/var/log/messages` for the ASR:

```
# mount -o remount,rw /
# vi /etc/ssh/sshd_config
UsePAM no
PasswordAuthentication yes
```

3. Set the sshd_config file attribute as immutable.

```
# chattr +i /var/opt/tms/output/sshd_config
```

Verify the sshd_config file attribute as below.

```
# lsattr /var/opt/tms/output/sshd_config
-i---------- /var/opt/tms/output/sshd_config
```
4. Run the `sshd restart` command:

```
# en
> conf t
(config) pm process sshd restart
```

5. Repeat steps 1 through 3 on the standby Collector node.

**Ingesting Data Into the System**

Start sending the EDR and BulkStats data feeds to the MURAL platform. If the ASR is used as an input node, the start time from the filename is created in the incoming EDR flow directory.

**Note:** The path is mentioned in the IOG while you are adding gateway. The path where ASR will dump the EDR’s would be `/data/collector/GW_Name/edr`. **GW_Name** would be the gateway you added up while configuring the GCU.

The file name has the timestamp, which can be used for job scheduling in the following process.

**Note:** It is assumed that the timestamp on the data that is pushed to the platform is greater than or equal to the current time, and not an old timestamp.
Validating Data on Nodes

This section includes instructions for validating data after completing the system installations.

Validating Data on the Collector Nodes

1. Log in to the master Namenode and go to _shell.

   > en
   # _shell

2. Run the indicated hadoop commands for the mm variable (minutes) in the timestamp), specify a multiple of 5 (05, 10, 15, and so on) up to 55.

   Note: Specify the year, month day, hour, and minute for which data is being sent to the PROD-NAME-SHORT system.

   # hadoop dfs -ls /data/collector/1/output/edrflow/YYYY/MM/DD/HH/mm/*
   2>/dev/null
   # hadoop dfs -ls /data/collector/1/output/edrhttp/YYYY/MM/DD/HH/mm/*
   2>/dev/null
   # hadoop dfs -ls /data/collector/1/output/bulkStats/YYYY/MM/DD/HH/mm/*
   2>/dev/null

   If the Collector node is receiving data in the expected format, it retains the data in HDFS. These directories and files are updated continuously as the data keeps coming in.

Setting the Data Start Time

To set the data start time in the configuration, perform the following steps:

1. Log in to the master Namenode and make the / file system writable.

   > en
   # _shell
   # mount -o remount,rw /
   # cd /opt/deployment/Mural_setStartTime/
   # ./setOozieTime --dataStartTime data-start-time --node collector-mgmt-IP --password admin-password
2. Execute the `setOozieTime` script to set the time at which EDR and BulkStats data starts coming into the Hadoop directories listed in "Validating Data on the Collector Nodes" on the previous page.

For example, if EDR and Bulkstats data starts coming into the Hadoop system from April 1, 2013, 06:00 onwards, run the following scripts with the `start_time` value as "2013-04-01T06:00Z":

```
# ./setOozieTime --dataStartTime 2013-04-01T06:00Z --node
192.168.147.11 --password admin@123
```

**Note:** Enter minutes as a multiple of 5. For example, "2013-04-01T06:00Z." Ensure that there is a continuous flow of data into the Hadoop without any gaps since the specified time.

3. Execute the Set Job Time Script for both the master and standby Namenodes.

**Note:** This script may take up to 30 minutes to complete for one node. Therefore, please wait it completes and returns to the prompt.

**Starting the Data Processing**

Log into the master Collector node and run the data processing commands from the Oozie subshell:

```
> en
# conf t
(config)# pmx
Welcome to pmx configuration environment.
pm extension> subshell oozie
pm extension (oozie)> run job all
```

The command output shows all the jobs that were initiated and if the jobs started successfully or not.

**Note:** It may take approximately 20 minutes to start all the jobs, depending upon what all applications are enabled.
Validating Data on the Compute Blades (Data Nodes)

This section includes the steps required to validate data on the Compute blades (Data nodes) following the installation process.

**Caution:** Wait two hours after completing the steps in "Starting the Data Processing" on the previous page. This allows sufficient time for the jobs that process the collector data to start, and the done.txt files to be updated. Not waiting could result in the checks failing.

### Validating EDR Data

1. Log in to the master Collector node and go to the `_shell`.

   ```
   > en
   # _shell
   ```

2. Check the last timestamp for the Core job.

   ```
   > en
   # _shell
   # hadoop dfs -text /data/CoreJob/done.txt 2>/dev/null
   ```

3. Check the last timestamp for EDR data cubes being generated by the EDR job.

   ```
   # hadoop dfs -text /data/EDR/done.txt 2>/dev/null
   ```

4. Check the last timestamp for CubeExporter data cubes.

   ```
   # hadoop dfs -text /data/CubeExporter/done.txt 2>/dev/null
   ```

5. Check the last timestamp for generated and exported Bulkstats data cubes.

   ```
   # hadoop dfs -text /data/BulkStat/done.txt 2>/dev/null
   # hadoop dfs -text /data/BSAgg15min/done.txt 2>/dev/null
   # hadoop dfs -text /data/BulkStatExporter_15min/done.txt 2>/dev/null
   ```

### Validating Insta Data

1. Log in to the master Insta node and check the name of the database configured for EDR:
> en
# _shell
# cli -t "en" "conf t" "show runn full" |
grep "insta instance 0 cubes-database" | awk -F ' ' '{print $5}'
database_mural

2. Open the **idbmysql** user interface and select the database.

```bash
idbmysql
Welcome to the MySQL monitor. Commands end with ; or \g.
...
mysql> use database_mural;
Database changed
```

3. Display the values in the **mints** and **maxts** columns for the 60-minute bin class and -1 aggregation level (shown in the first row of the following example).

```bash
mysql> select * from bin_metatable;
+-----------------+-----------------+-------+-------+---------------+
| binclass | aggregationinterval | mints | maxts | bintype |
|-----------------+-----------------+-------+-------+---------------+
| 60min | -1 | 1406710800 | 1409295600 | NULL |                      |
| 60min | 86400 | 0 | 0 | NULL |                      |
| 60min | 604800 | 0 | 0 | NULL |                      |
| 60min | 2419200 | 0 | 0 | NULL |                      |
+-----------------+-----------------+-------+-------+---------------+
4 rows in set (1.14 sec)
Press Ctrl+D to exit
mysql> Bye
```

4. Run the **date** command to convert the values from the **mints** and **maxts** columns to human-readable format.

The following example indicates that data was processed between 09:00 on July 30 and 07:00 on August 29.

```bash
# date -d @1406710800
Wed Jul 30 09:00:00 UTC 2014
# date -d @1409295600
Fri Aug 29 07:00:00 UTC 2014
```
Validating Bulk Stats Data on the Insta Blade

1. Use SSH to log in to the master Insta node and check the name of the database configured for EDR:

   ```
   > en
   # _shell
   # cli -t "en" "conf t" "show runn full" |
   grep "insta instance 1 cubes-database" | awk -F ' ' '{print $5}
   'bulkstats
   ```

2. Open the `idbmysql` user interface and select `bulkStats` as the database.

   ```
   # idbmysql
   Welcome to the MySQL monitor. Commands end with ; or \g.
   ...
   mysql> use bulkStats;
   Database changed
   ```

3. Display the values in the `mints` and `maxts` columns for the 900 aggregation interval (shown in the second row in the example).

   ```
   mysql> select * from bin_metatable;
   +-------------+-----------------+-------+-------+--------------+
   | binclass    | aggregationinterval | mints | maxts  | binType      |
   +-------------+-----------------+-------+-------+--------------+
   | 5min        | -1              | 0     | 0     | NULL        |
   | 5min        | 900             | 1406713500 | 1409301900 | NULL        |
   | 5min        | 3600            | 0     | 0     | NULL        |
   | 5min        | 86400           | 0     | 0     | NULL        |
   | 5min        | 604800          | 0     | 0     | NULL        |
   | 5min        | 2419200         | 0     | 0     | NULL        |
   +-------------+-----------------+-------+-------+--------------+
   6 rows in set (12.18 sec)
   mysql> quit
   ```

4. Convert the date format. Run the `date` command with the value of `maxts` (captured from the step above) for the row which shows `aggregationinterval` as 900.

   ```
   120
   ```
The following example indicates that data was processed between 09:45 on July 30 and 08:45 on August 29.

```
# date -d @1406713500
Wed Jul 30 09:45:00 UTC 2014
# date -d @1409301900
Fri Aug 29 08:45:00 UTC 2014
```

**Starting UI Processes and Verifying Data**

Starting the UI processes and verify UI data. Ensure that the URL is set up in the DNS for the production system.

**Starting the Rubix Tomcat Instance on Both UI Nodes**

**Note:** You should only start UI Tomcat instances after at least two hours of data has been pushed into the Insta node.

1. Log in to the master UI node.

   ![Login Command](image)

2. Run the following commands to start the EDR process.

   ![EDR Process Commands](image)

   Check the tomcat process status using command:

   ![Tomcat Status Command](image)

   **Note:** Ensure the running status of above service as Current Status: running before proceeding to start next process.

3. Run the following commands to start the other processes.

   ![Other Process Commands](image)
Where *ApplicationName* is replaced by the following applications in the same order:

- bulkstats
- reportAtlas
- rge
- anomaly (if Anomaly is enabled)
- httperror
- launcher

Check the tomcat process status using command:

```
(config)# rubix status ApplicationName atlas
```

**Note:** Ensure the running status of above service as **Current Status:** running before proceeding to start next process. Check the corresponding rubix.log file to ensure that Atlas and HET applications are started properly without any exception.

4. Log in to the standby UI node and repeat Steps 2 and 3.

5. Access the UIs by going to the URL **https://domain-name:21443/**

The domain name to be used is the one which was provided at the time of initial configuration via GMS for the UI nodes configuration details. For example:

```
https://demo.cisco.com:21443/
Username: admin
Password: admin123
```

**Note:** Since the common certificate installation procedure is not finalized, you must click the same URL for the BulkStats and RGE ports once before opening the actual URL.

Visit the following ports once and accept the certificates:

```
https://domainName:20443/
https://domainName:30443/
```
For example:

https://demo.cisco.com:20443/
https://demo.cisco.com:30443/

If the Anomaly feature is enabled, also run the command on port 50443. For example,

https://demo.sanmateo.com:50443/

**Note:** Once the installation is completed, be sure to back up the configurations. Refer to the *Operations and Troubleshooting Guide* for more information.

**Updating Whitelists**

After running MURAL system for 2-3 hours, run the following command from master Namenode to generate updated whitelists:

```bash
# pmx subshell aggregation_center
pm extension (aggregation center)> generate whitelist
pm extension (aggregation center)> setting attribute (jobStart)
setting attribute (jobEnd)
INFO: GenericJobScheduler: starting job
job: 0000000-140809225350409-oozie-admi-C
INFO: GenericJobScheduler: job started successfully
Running Whitelist Creation Job
pm extension (aggregation center)> quit
pm extension> quit
```

Observe the categorization in UI after 2 hours to see the effects of whitelists update.
Setting Up Offline Reports

Uncategorized URL, UA, and TAC Reports

Create a file named `serverFile_uncatReports` on the master Namenode containing the destination information, to which the uncategorized URL, UA, and TAC reports would be copied.

1. The `serverFile_uncatReports` file contains the entries for the data transfer destination location. This file has the following format:
   
   | IP, username, password, location-to-copy-reports |
   
   For example,
   
   192.168.156.96, admin, admin@123, /data/offline_uncat_reports
   
   **Note:** The delimiter in this file must be ", " (comma followed by a space).

2. Log into the master Namenode and navigate to the `/data/work` subdirectory:

   ```shell
   > en
   # _shell
   # cd /data
   # cd work
   ```

3. Create the `serverFile_uncatReports` file:

   ```shell
   # vi /data/work/serverFile_uncatReports
   192.168.156.96, admin, admin@123, /data/offline_uncat_reports
   ```

   **Note:** For the SCP protocol, the destination path should be the destination server. The destination path is not required for SFTP.

4. Create the same file on the standby Namenode.

Tethering Reports

Create a file called `serverFile_tethering` with details of the ASR 5000 gateways, where the TAC, OS or UA databases, created as a result of tethering
processing, need to be pushed.

1. The `serverFile_tethering` file contains the entries for the data transfer destination location. This file has the following format:

```
Gateway-IP, gateway-username, gateway-password, location-to-copy-reports
```

Where:

- `Gateway-IP` is the ASR5K gateway IP address
- `gateway-username` is the username for logging into ASR5K Gateway
- `gateway-password` is the corresponding password to the username
- `location-to-copy-reports` is the location on the ASR5K Gateway machine where databases need to be copied

2. Log in to the master Namenode:

```
> en
# _shell
```

3. Go to the data directory and create a sub-directory named work:

```
# cd /data
# mkdir work
```

4. Go to the work subdirectory and create the `serverFile_tethering` file:

```
# cd work
# vi /data/work/serverFile_tethering
192.168.156.96, admin, admin@123, /data/tethering_ibs
```

**Note:** The delimiter in this file must be ", " (comma followed by a space).

5. Create the same file on the standby Namenode as well.

For the SCP protocol, the destination path should be present at the destination server. This is not required for SFTP.

This file can have multiple rows of this kind.
Rule-Based Reports

Create a file named serverfile_Rulebase with details of ASR IPs, access details and report destination paths.

1. The serverFile_Rulebase file contains the entries for the data transfer destination location. This file has the following format:

| Gateway-IP, gateway-username, gateway-password, location-to-copy-reports |

Where:

- Gateway-IP is the ASR5K gateway IP address
- gateway-username is the username for logging into ASR5K Gateway
- gateway-password is the corresponding password to the username
- location-to-copy-reports is the location on the ASR5K Gateway machine where databases need to be copied

2. Log in to the master Namenode:

```
> en
# _shell
```

3. Go to the data directory and create a sub-directory named work:

```
# cd /data
# mkdir work
```

4. Go to the work subdirectory and create the serverFile_tethering file:

```
# cd work
# vi /data/work/serverfile_Rulebase
192.168.156.96, admin, admin@123, /data/ruleBase_reports
```

**Note:** The delimiter in this file must be ", " (comma followed by a space).

5. Create the same file on the standby Namenode as well.

   For the SCP protocol, the destination path should be present at the
destination server. This is not required for SFTP.

This file can have multiple rows of this kind.
Mandatory Parameters for Incoming ASR Files

The following is the list of mandatory headers that need to be present in files coming from the ASR so that the MURAL system can deduce meaningful information.

Mandatory Attributes for Flow EDRs for MURAL

Flow EDR data sent by the ASR platform to the MURAL system must contain the following attributes:

- sn-start-time
- sn-end-time
- radius-calling-station-id
- sn-app-protocol
- sn-rulebase
- p2p-protocol
- sn-server-port
- sn-volume-amt-ip-bytes-downlink
- sn-volume-amt-ip-pkts-uplink
- sn-volume-amt-ip-pkts-downlink
- sn-volume-amt-ip-bytes-uplink

Sample:

```
```
Mandatory HTTP EDR Attributes for MURAL

HTTP EDR data sent to the MURAL system must contain the following attributes:

- sn-start-time
- sn-end-time
- transaction-downlink-packets
- transaction-uplink-packets
- transaction-downlink-bytes
- transaction-uplink-bytes
- http-content type
- radius-calling-station-id
- http-host
- http-url
- http-user-agent
- bearer-3gpp rat-type
- bearer-3gpp imei
- http reply code

Sample:

```
1381518310,1381518338,1000000019,15000,15000,1.1.1.1,27.2.248.155,images.craigslist.org,image/png,images.craigslist.org,11,,60,1,1,Sushfone-1,,,GET,506 Variant Also Negotiates,"Dalvik/1.6.0 (Linux; U; Android 4.0.3; Galaxy Nexus Build/ICL53F)"
```
**ASR-Side Configuration**

The corresponding configuration on the side of the ASR platform is as follows:

```
<table>
<thead>
<tr>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>edr-format edr-flow-format</td>
</tr>
<tr>
<td>attribute  sn-start-time format</td>
</tr>
<tr>
<td>attribute  sn-subscriber-ip-address</td>
</tr>
<tr>
<td>attribute  sn-subscriber-port</td>
</tr>
<tr>
<td>attribute  sn-start-time format</td>
</tr>
<tr>
<td>attribute  sn-charge-volume ip</td>
</tr>
<tr>
<td>attribute  sn-charge-volume ip</td>
</tr>
<tr>
<td>attribute  sn-charge-volume ip</td>
</tr>
<tr>
<td>attribute  sn-charge-volume ip</td>
</tr>
<tr>
<td>attribute  sn-charge-volume ip</td>
</tr>
<tr>
<td>attribute  sn-direction</td>
</tr>
<tr>
<td>rule-variable bearer ggsn-address</td>
</tr>
<tr>
<td>rule-variable bearer 3gpp2 bsid</td>
</tr>
<tr>
<td>attribute  sn-flow-start-time</td>
</tr>
<tr>
<td>attribute  sn-flow-end-time</td>
</tr>
<tr>
<td>attribute  sn-flow-id</td>
</tr>
<tr>
<td>attribute  sn-closure-reason</td>
</tr>
<tr>
<td>attribute  radius-calling-station-id</td>
</tr>
<tr>
<td>rule-variable p2p protocol</td>
</tr>
<tr>
<td>rule-variable bearer 3gpp imsi</td>
</tr>
<tr>
<td>attribute  radius-called-station-id</td>
</tr>
<tr>
<td>rule-variable ip server-ip-address</td>
</tr>
<tr>
<td>attribute  sn-server-port</td>
</tr>
<tr>
<td>attribute  sn-app-protocol</td>
</tr>
<tr>
<td>attribute  sn-parent-protocol</td>
</tr>
<tr>
<td>rule-variable ip protocol</td>
</tr>
<tr>
<td>attribute  sn-volume-amt ip</td>
</tr>
<tr>
<td>attribute  sn-volume-amt ip</td>
</tr>
<tr>
<td>attribute  sn-volume-amt ip</td>
</tr>
<tr>
<td>attribute  sn-volume-amt ip</td>
</tr>
<tr>
<td>rule-variable bearer 3gpp charging-id</td>
</tr>
<tr>
<td>rule-variable bearer 3gpp imei</td>
</tr>
<tr>
<td>rule-variable bearer 3gpp rat-type</td>
</tr>
<tr>
<td>rule-variable bearer 3gpp user-location-information</td>
</tr>
<tr>
<td>rule-variable bearer 3gpp sgsn-address</td>
</tr>
<tr>
<td>rule-variable traffic-type</td>
</tr>
<tr>
<td>rule-variable voip-duration</td>
</tr>
</tbody>
</table>
```
attribute sn-end-time format seconds priority 180

#exit
edr-format edr-http-format
  rule-variable ip subscriber-ip-address priority 4
attribute sn-charge-volume ip pkts uplink priority 8
attribute sn-charge-volume ip pkts downlink priority 9
attribute sn-start-time format seconds priority 10
attribute sn-charge-volume ip bytes downlink priority 11
attribute sn-charge-volume ip bytes uplink priority 12
attribute sn-end-time format seconds priority 20
attribute radius-calling-station-id priority 30
attribute radius-called-station-id priority 40
rule-variable ip server-ip-address priority 50
rule-variable http user-agent priority 55
rule-variable http host priority 70
rule-variable http content type priority 80
attribute transaction-downlink-bytes priority 90
attribute transaction-uplink-bytes priority 100
attribute transaction-downlink-packets priority 110
attribute transaction-uplink-packets priority 120
rule-variable bearer 3gpp charging-id priority 160
# exit
APPENDIX I: Installing and Configuring VM for GMS Lite

A Virtual Machine (VM) is used to configure the GMS Lite application for atlas releases. When used with GMS Lite in this way, the VM software uses laptops on-site to quickly configure other GMS nodes, including a GMS HA (High Availability) cluster or stand-alone server.

This section presumes you are choosing to use VirtualBox as the tool and provides step-by-steps details to create a VM using VirtualBox and to import a pre-configured Vdisk image onto the laptop.

If you already have a VM you may skip this section and proceed to "Using GMS Lite to Automate Installation of GMS Nodes" on page 80.

If you have chosen to manually install the GMS nodes and not use GMS Lite, you can skip to "APPENDIX II: Manufacturing the Master GMS Blade" on page 139.

Before You Begin

1. Download the latest stable release of VirtualBox software.

2. Download the Vdisk image copy (vm35rc1Copy.qcow.gz)

3. Ensure you have these tools installed:
   - File decompression tool (like rar or unzip) installed
   - Bridge Connectivity Support from LAN over Ethernet (en0/LAN) port

4. Configure the VM with following specifications:
   - OS type: linux 64 bit
   - RAM: Minimum 2 GB
   - HDD: IDE: Minimum 50 GB (dynamically allocated)
   - CPU Cores: Minimum 1
   - Network Port Speed (eth0) – 100 mbps full duplex

   **Note:** Ensure that your laptop and VM are in the same subnet as all other nodes of setup. This is essential for PXE booting the GMS server to be successful.
Installing VM for GMS Lite

1. Install VirtualBox software into laptop and launch the application.

2. Decompress vdisk file under a location designated on the target machine, the laptop.

3. Launch VirtualBox software and select **New** to create VM.

4. Click **Hide Description**.

5. In the Create Virtual Machine window that pops up, make the following settings on the Name and operating system screen, then click the Next button:
   - **Name**—The virtual machine name (**GMS-Lite** in the figure)
   - **Type**—Linux
   - **Version**—Other Linux (64-bit)
   - **Memory Size**—2 GB (Minimum)
   - **Hard Drive**—Select **Do not add a virtual hard drive**
6. Click **Create**.

7. VM creation is completed, select VM from left pane and check configuration from right pane.
8. VM Configuration: **Select VM > Settings > Storage**

9. Make the following changes in the Storage Tree box:
MURAL Software Standard Installation Guide

a. Create an **SCSI Controller** and place the Vdisk under it.

b. For the SCSI controller, click the **Use Host I/O Cache** check box to add the check (see the preceding figure).

10. When you click the **Vdisk** to select it, a detailed list of attributes appears in the main pane, as shown in the following figure.

![Diagram showing Vdisk attributes](image)

11. Press **OK** to save changes.

12. Go to **VM > Settings > Network**.

13. Select **Bridged Adapter, NIC** for Ethernet LAN port, and **Allow VMs**.
14. Navigate to **VM > Settings > Serial Ports**.

15. Select **Port 1 > Enable Serial Port**, and press **OK**.

16. VM configuration completed, see VM info.
17. Select the VM. Press Start to power on.

18. Login from the VM console as an admin user using the password admin@123.

19. Re-create and enable swap. Identify swap device (disk volume for swap).

```bash
# fdisk -l | grep -i swap
/dev/sda7   1098  1620   4200997  82 Linux
swap / Solaris
#
# free -m
# mkswap /dev/sda7
# swapon -a
# free -m
```

VM is now ready to use as GMS lite server. Go back to "Setting Up the Master GMS Node" on page 50 to continue the MURAL system installation.
APPENDIX II: Manufacturing the Master GMS Blade

**Note:** Only use this topic as an alternative to manufacturing the GMS blade with GMS Lite as described in "Using GMS Lite to Automate Installation of GMS Nodes" on page 80.

The master GMS blade hosts the master GMS node, a MURAL platform component that enables centralized installation and monitoring of all the blades on the MURAL system.

Follow these steps to manufacture (install the operating system software on) the master GMS blade.

**Before You Begin**

- Configure Serial over LAN (SOL) on all the blades during EMCsetup.
- Locate your CIQ, and refer to it for such details as UCS access credentials and KVM SOL IP address.

To manufacture the GMS blade, perform the following steps:

1. Download the ISO image included with the MURAL software package to the machine from which you will access the Cisco UCS blades.

   The ISO image filename is `mfgcd-x86_64-20140731-005012.iso`

   To verify the MD5 checksum of the image, run the `md5sum filename` command.

   ```
   # md5sum mfgcd-x86_64-20140731-005012.iso
   7c0e95cc2ff98ed139c366792b01934 mfgcd-x86_64-20140731-005012.iso
   ```

2. Open the Cisco UCS - KVM Launch Manager in a browser and enter your login credentials.

   **Note:** For best performance, access the KVM Launch Manager in Firefox with Java version 6 or greater.

   The UCS - KVM Launch Manager application opens and displays all blades available on the chassis.
3. Click the **Launch** button for the first node (**Server1** in the following figure).

Click **OK** to download and open the **kvm.jnlp** file.

4. The console for the port opens. Navigate to

   **KVM Console > Virtual Media**, click **Add Image**, and specify the path of the ISO image that you downloaded in Step 1.

5. Click the check box in the **Mapped** column for the added ISO image, which is then mounted.
6. Reboot the blade to use the newly mounted image. Go to the KVM tab and select **Ctrl-Alt-Del** from the **Macros > Static Macros** drop-down menu.

7. When the boot screen appears, press **F6** to select the boot menu.
8. Select Virtual CD/DVD so the blade boots with the mounted ISO image.

9. Select **Enter Setup** to open the setup utility.
10. On the **Boot Options** tab, verify that the value in the **Boot Option #1** field is *CD/DVD* as shown in the following figure. If you change the value, press the **F10** key to save and exit; if the value is already correct, press the **Esc** key to exit.

![Boot Options Tab](image1.png)

11. At the **#** prompt, run the **manufacture** command to manufacture the master GMS blade.
The following command is appropriate for a single disk configured as RAID 1, as indicated by the `-L 1D` argument. The master GMS blade has a second disk that functions as the mirrored disk in the RAID configuration.

```
# manufacture.sh -v -t -f /mnt/cdrom/image.img -m 1D -L 1D --cc no --cs no --cl no -a
```

12. Follow the manufacture process:

```
Running startup scripts.
Running /etc/init.d/rcS.d/S10tms_dhcp
Starting DHCP client on interfaces: eth0 eth1
DHCP client started on eth0
DHCP client started on eth1
Sending discover...
...
dhcp eth0: failed to get lease
...
No lease, failing
...
Running /etc/init.d/rcS.d/S30tms_autostart
Automatically mounted cdrom /dev/scd to /mnt/cdrom
Running /etc/init.d/rcS.d/S34automfg
- Automatic manufacture is not enabled. Type 'automfg' to start it.
Processing /etc/profile... Done
#
# manufacture.sh -t -v -f /mnt/cdrom/image.img -m 1D -L 1D --cc no --cs no --cl no -a
-- Extracting files for VAR_1
-- Post-extractIon work for: VAR_1
-- Nothing to do for location HA_1.
== Extracting for location DATA_1 onto /dev/sdall
-- Mounting /dev/sdall on /tmp/mnt_image_wi/DISK1/DATA//data
-- Extracting files for DATA_1
```
== Updating bootmgr settings
== Cleanup
====== Ending image install at 20131227-085046
== System successfully imaged
-- Writing Host ID: 09fc39658d3d
== Zeroing the destination partition disk /dev/sda9 with dd
== Calling imgverify to verify manufactured system
== Using layout: ID
== Using dev list: /dev/sda
== Verifying image location 1
=== Mounting partitions
=== Checking manifest
=== Unmounting partitions
=== Image location 1 verified successfully.
== VerifyIng image location 2
=== Mounting partitions
=== Checking manifest
=== Unmounting partitions
=== Image location 2 verified successfully.
== Done
====== Ending manufacture at 20131227-085738
-- Manufacture done.
#

reboot

13. The system will show a message Manufacture done and return to a # prompt once the manufacturing of a blade has been completed.

14. Deselect the ISO image selected in Step 5 of this procedure. Type reboot to reboot the node with the new ISO image.

15. Run the **reboot** command to reboot the node with the new ISO image.

    # reboot

16. Use SSH to log in to the master GMS blade as user **admin**. Continue to
"Setting Up the Master GMS Node" on page 50.

17. Create soft links to copy all the required profiles:

```bash
# cd /config/gms/Profiles/Custom/
# pwd
/config/gms/Profiles/Custom
# ln -s /opt/deployment/GMS_Templates/collector/Feed/bulkstats/collector_adaptor_bulkstats_template.xml.
# ln -s /opt/deployment/GMS_Templates/collector/Feed/edrhttp_edrflow/collector_adaptor_edrhttp_edrflow_template.xml.
# ln -s /opt/deployment/GMS_Templates/hadoop/dfs_template.xml.
# ln -s /opt/deployment/GMS_Templates/hive/hive_mural.xml.
# ln -s /opt/deployment/GMS_Templates/insta/App/bulkstats/insta_mural_bulkstats_flat.xml.
# ln -s /opt/deployment/GMS_Templates/insta/App/dpi/insta_mural_dpi_flat.xml.
# ln -s /opt/deployment/GMS_Templates/insta/App/httperror/insta_httperror_flat.xml.
# ln -s /opt/deployment/GMS_Templates/oozie/App/anomalyDetection/workflow_anomaly_with_timeout_jobs.xml.
# ln -s /opt/deployment/GMS_Templates/oozie/App/bulkstats/workflow_bulkstat_mural_with_timeout.xml.
# ln -s /opt/deployment/GMS_Templates/oozie/App/dpi/workflow_dpi_with_timeout_jobs.xml.
# ln -s /opt/deployment/GMS_Templates/oozie/App/dynamicWhitelisting/workflow_dynamic_whitelisting_with_timeout.xml.
# ln -s /opt/deployment/GMS_Templates/oozie/App/httperror/workflow_httperror_with_timeout.xml.
```
```
# ln -s /opt/deployment/GMS_Templates/oozie/App/rulebase/workflow_rulebase_apn_with_timeout.xml.
# ln -s /opt/deployment/GMS_Templates/oozie/App/tethering/workflow_tethering_with_timeout.xml.
# ln -s /opt/deployment/GMS_Templates/oozie/Feed/edrhttp_edrflow/workflow_edrhttp_edrflow.xml.
# ln -s /opt/deployment/GMS_Templates/oozie/Feed/edrhttp_edrflow/workflow_hive_edrhttp_edrflow_with_timeout.xml.
# ln -s /opt/deployment/GMS_Templates/postgres/postgresql_mural.xml.
# ln -s /opt/deployment/GMS_Templates/rubix/anomaly/rubix_anomaly_mural.xml.
# ln -s /opt/deployment/GMS_Templates/rubix/bulkstats/rubix_bulkstats_mural.xml.
# ln -s /opt/deployment/GMS_Templates/rubix/dpi/rubix_atlas_distributed_mural.xml.
# ln -s /opt/deployment/GMS_Templates/rubix/httperror/rubix_httperror_mural.xml.
# ln -s /opt/deployment/GMS_Templates/rubix/launcher/rubix_launcher_mural.xml.
# ln -s /opt/deployment/GMS_Templates/rubix/reportAtlas/rubix_cacheless_mural.xml.
# ln -s /opt/deployment/GMS_Templates/rubix/rge/rubix_rge_mural.xml.
# ln -s /opt/deployment/GMS_Templates/solution/solution_mural.xml.
16.18. #
```
Appendix III: Using KVM Software to Boot PXE Blades

Before You Begin

- Configure Serial over LAN (SOL) on all the blades during EMC setup.
- Locate your CIQ, and refer to it for such details as UCS access credentials and KVM SOL IP address.

Rebooting the Blades

1. Open the Cisco UCS - KVM Launch Manager in a browser and enter your login credentials.

   **Note:** Firefox with Java version 6, or above, is the most suitable browser to access the UCS.

   You will see all the blades available on the chassis.

2. Click the **Launch** button for the first node (**Server1**).

   Click **OK** to download and open a **kvm.jnlp** file.

   A keyboard access warning message appears—click **OK**.

3. The console for the port opens. Complete the following steps to reboot Master GCR blade from the KVM Console:
   a. Open the KVM Console of the blade.
   b. Press **CTRL-ALT-DEL**, as explained in "Manufacturing the GCR Blade" to reboot the blade. You can also click Reset from the top of the KVM console.
   c. After the prompt, press **F12** as soon as possible to boot from the network.

   The following figure shows the results of clicking **F12**.

Once the blades start booting from the network, GMS pushes the image on all the blades using PXE boot for the manufacture process to start on each blade in parallel.
A blade takes approximately 20 minutes to manufacture with the new image. Wait until blade for which PXE boot was issued has been manufactured. A login prompt is displayed once the image has been manufactured on a blade.

Go back to Registering MURAL Nodes on the EMC section to continue MURAL system installation.
Appendix IV: Collecting UCS Chassis/Slot and VLAN Information

We need to collect following details from CISCO UCS Manager to update the GMS Configuration for Server details.

- Chassis IDs
- Chassis Serial Numbers
- Blade slot IDs
- vNIC IDs (like eth0, eth1) and corresponding VLAN IDs for all the blades

1. Open web browser from laptop and enter the UCS Manager URL, as https://UCS-MANAGER-IP/

2. Press Launch UCS Manager and login into UCS manager using valid user access details. UCS Manager interface will appear on screen after
successful login, as shown below:

![Image of a computer interface with a list of interfaces and a fetch MAC IDs feature.

**Fetching MAC IDs Feature**

GMS can collect and populate MAC Addresses from the UCS Manager for all the MURAL blades. Navigate to **GMS UI > Server Tab > Chassis Pane** to find the **Fetch MAC IDs** feature. Provide the **vNIC port** and **VLAN_ID** details for all the node interfaces as documented in the CIQ sheet.

1. Under the **Interface Members** section,
   b. Enter an **IFC_Number** (such as eth0 or eth1) and their respective VLAN-IDs, as per CIQ sheet.
   c. Leave the **Mac Address** field empty.

2. Press **Fetch MAC IDs** button and provide UCS Manager IP and valid login.
credentials when prompted. Press OK to fetch the MAC addresses of all the blades.

3. After successful execution of **Fetch MAC IDs** command, MAC addresses will be updated in the Interface Members inventory for all the MURAL blades.

**Finding Chassis/Slot IDs**

1. From left pane, select **Equipment > Chassis > Chassis N** (for which details need to be collected, like Chassis 2)

2. Make a note of the Chassis ID (like ID: 2) and serial number. Do the same for all the installed chassis and update the CIQ sheet.
Finding NICs VLAN IDs for Blades

1. From left pane, select **Equipment > Chassis > Chassis-1 > Server > Server-name > Adapter 1 > NICs**. From right pane, expand **NIC 1**, select **vNIC eth0** and double click to open its properties as shown below:

![NIC Properties](image)

**Note:** VLAN ID is 103 for eth0 NIC port; Use it as vlan-103 in GMS.

![NIC Properties](image)

**Note:** VLAN ID is 180 for eth1 NIC port; Use it as vlan-180 in GMS.

2. Make a note of the **VLAN ID** for this **NIC Port(eth0)**. Repeat the same steps to collect the VLAN ID for **eth1 port** and update the CIQ sheet.

**Caution:** Please ensure to collect the correct values for Chassis and blade inventory values, like Chassis Number (same as Chassis ID), Logical Name (same as Chassis S/N), node slot ID and node interface VLAN_ID, etc. GMS server uses these details to initiates PXE boot on all the blades, installed in these chassis.

**Note:** Incorrect chassis-slot IDs details in GMS may severely impact unexpected node(s) installed in these chassis under UCS manager.
# Glossary

## A

**ASR**
Cisco ASR 5000 or ASR 5500 Series platforms. The routing platform that pushes the data flows to the MURAL system.

## B

**Big data**
A collection of data that is too large to manage, store, or analyze by traditional methods.

## C

**Caching node**
Hosts the Rubix engine and data cache. The Rubix engine queries the Insta nodes constantly and when new data is available, it fetches it to store in the data cache, so that it can respond more quickly to requests from the UI engine. The Caching node is sometimes called the Rubix node. The Caching node uses N+1 redundancy in active-active mode.

**CIQ**
An Excel spreadsheet containing a site survey that you completed before beginning the installation process.

**Collector Cluster**
The cluster of nodes consisting of the Collector nodes in active/standby High Availability clustering.

**Collector node**
Collects data streams pushed to the MURAL platform, interprets the exported flows, enriches them with static data, and assembles data sets. The Collector stores the raw data in the Hadoop file system (HDFS) and sends it to the Compute node. The Collector node cluster can have any number of servers, in pairs for master and standby and uses 1+1 redundancy (transparent failover between pairs of active-active nodes).

**Compute cluster**
The cluster consisting of the master and standby Compute nodes.
Compute node  Analyzes and aggregates the data, creating *data cubes*. Data cube is a convenient shorthand for the data structure, which is actually multi-dimensional and not limited to the three dimensions of a cube. The Compute node cluster can have any number of servers, depending on the implementation, and uses N+1 redundancy.

Cube engine  A process that is hosted on the UI/Caching node. The Cube engine forwards requests from the UI engine to the Insta node. It also prefetches data and locally caches it so that if the requested data is in the local cache, it can return the response directly without querying the Insta node.

**D**

Direct-Attached SAN  A feature on Cisco UCS that enables you to attach a fiber-channel SAN directly to the Fabric Interconnects.

Downlink Rate  The average bytes received by the mobile device from the Internet during a selected interval.

Downlink Tonnage  The total amount of data received by the mobile device from the Internet.

DPI  Deep packet inspection—an advanced form of packet filtering that makes it possible to examine more than just the packet header.

**F**

Fabric Interconnect  Part of the Cisco UCS platform that provides both network connectivity and management capabilities to all attached blades and chassis.

FC Switch Mode  Fibre channel switch mode, a mode on the Fabric Interconnects.

FCID  A 24-bit field used to route frames through a FC network.

flogi database  Fabric login database.

G
GMS node  General Guavus Management System node. This node provides centralized management of the MURAL platform nodes, such as remote manufacturing of blades, patch management, monitoring of all nodes and operations, and importing and running node configurations.

Hadoop  Open-source software that supports running applications on large clusters of hardware. See http://hadoop.apache.org/

Image  Comprised of the operating system plus the application bundle.

Insta node  Stores and manages the processed data in a columnar database, the Insta database, a columnar database that stores the processed data cubes, commonly three to six years' worth. The Insta node cluster has two servers with 1+1 redundancy.

Manufacture  Manufacturing a blade is the installing the MURAL operating system on the blade.

MIBs  A database used for managing the entities in a communications network; associated with the Simple Network Management Protocol (SNMP).

MURAL  Cisco Mobility Unified Reporting and Analytics (MURAL) application, which provides Web-based reporting and analytics abilities for deep packet inspection (DPI) data emerging from the network.

mural.xml file  Contains sample configuration settings for your setup, including a logical grouping of the nodes into two chassis and configuration settings for all of the system components. These settings are based on the details of your network that were supplied in the Customer Information Questionaire (CIQ).

N
**NX-OS**  Cisco Nexus Operating System

**O**

**Oozie**  A workflow scheduler designed by Apache to manage Hadoop jobs. Oozie is bundled on the system and hosted on the Collector nodes.

**P**

**PGSQL disks**  On a MURAL installation, these are storage partitions for the Postgres database and will store Rubix-related data.

**R**

**Rate (bps)**  Amount of data sent and received per second between the device and the Internet. (Bytes per Second – bps)

**RG engine**  Report Generation engine, which serves as the HTTP request server. In Cisco MURAL, it is hosted on the same blade as the UI engine.

**Rubix engine**  See Cube engine.

**Rubix node**  See Caching node.

**S**

**SAN**  Storage area network. A high-speed network of storage devices that also connects those storage devices with servers. It provides block-level storage that can be accessed by the applications running on any networked servers.

**T**

**TAC**  Type Allocation Code – The initial 8 digit portion of the 15 digit IMEI code used to uniquely identify wireless devices.

**Tonnage (MB)**  Total volume amount of data sent and received (Megabytes – MB)

**U**

**UCS**  UCS 5108 Blade Server, connected to UCS 6248 Fabric Interconnects, hosts the MURAL application.

**UI node**  See Caching node.
Uplink Rate  The average bytes sent from the mobile device out to the Internet during a selected interval.

Uplink Tonnage  The total amount of data sent from the mobile device out to the Internet.

V  

vHBA Initiator Group  vHBA initiator groups determine the fiber channel zoning configuration for all vHBAs in a service profile. Cisco UCS Manager does not include any default vHBA initiator groups. You must create vHBA initiator groups in any service profile that is to be assigned to servers included in a zone.

VSAN  Virtual storage area network (SAN). A collection of ports from a set of connected Fiber Channel switches that form a virtual fabric that interconnects hosts and storage devices. A VSAN allows you to have logically separate fabrics without having to have different physical fabrics.

W  

WWN  World Wide Name. A unique identifier that is assigned to a manufacturer that is hard-coded into a Fiber Channel (FC) device. A unique 16-digit hexadecimal number, such as 21-00-00-30-D9-00-12-34. This identifier is hard-coded into every FC host bus adapter (HBA).

WWNN  World Wide Name Node. A world wide name assigned to a port in a Fibre Channel fabric, in this context, a port on a MURAL node.

WWPN  World Wide Name assigned to a port in a Fiber Channel fabric to uniquely identify it in the network.

Z  

Zoneset  A container for one or more zones in the fabric. Zones need to be a member of a zoneset in order to be used. Only one zoneset can be active at one time in any given VSAN.