MURAL Software
Installation Guide

Version 3.3

Last Updated April 22, 2014
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 INFRINGEMENT OF ANY PATENTS OR OTHER RIGHTS. WITHOUT LIMITING THE FOREGOING, YOU ARE RESPONSIBLE FOR THE SELECTION OF THIS SOFTWARE AND EQUIPMENT AND FOR ITS PERFORMANCE, QUALITY, CAPABILITIES, OR OMISSIONS.

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.

Cisco MURAL Software Installation Guide

Copyright © 2014, Cisco Systems, Inc.All rights reserved.
Table of Contents

Installation Overview .......................................................... 9
Prerequisites ................................................................. 9
System Components ....................................................... 9
Hardware ................................................................. 11
Installation Package ...................................................... 11
Customer Information Questionnaire .................................. 12
Configuring UCS Hardware and Software for MURAL ................. 13
Verifying UCS Hardware Configuration ................................ 14
Verifying Connections to the UCS Networks .......................... 19
Configuring Base UCS Software Settings .............................. 20
Configuring UCS for MURAL ........................................... 23
Configuring Direct Attachments to External SANs ................... 24
Configuring System Profiles for the Cisco UCS Manager .......... 38
Using GMS Lite to Automate Installation of GMS Nodes ................. 43
Before You Begin ...................................................... 43
Configure VM as a GMS Lite Node ..................................... 43
Setting Up the Master GMS Node and Cluster ........................ 44
Installing and Configuring VM for GMS Lite .......................... 47
Setting Up the Master GMS Node ...................................... 55
Setting the Password and IP Addresses ............................... 55
Verifying Zoning and FLOGI on the Fabric Interconnect ........... 56
Allocating Storage for the Master GMS Node ......................... 57
EMC Hardware Installation Prerequisites ............................... 57
Configuring IP Addresses for the EMC System ........................................... 58
Registering the Master GMS Node with EMC ........................................... 58
Creating RAID Groups and LUNs for the GMS Master Node ................. 63
Creating the Storage Group for the Master GMS Node ......................... 68
Adjusting Caching on the EMC ................................................................. 70

**Defining the Deployment Topology Using GMS** ..................................... 74
Accessing the GMS Interface ................................................................. 74
Loading the Base Configuration File ...................................................... 75
Verifying Settings on the Server Details Tab ........................................... 76
Verifying Global Settings ........................................................................ 80
Configuring the Node Clusters ............................................................... 82
Specifying Component Profiles and Application-Specific Settings ........... 83
Validating the Configuration .................................................................. 93

**Manufacturing the Remaining Blades** .................................................. 95

**Installing MURAL on the Blades** ......................................................... 99
Troubleshooting Node Installation .......................................................... 101

**Verify the Processes are Running** ...................................................... 102

**Generate and Push the Information Bases** ........................................... 104
Configuring IBs for EDR ......................................................................... 105
Configuring DCs and Gateways For All IBs .......................................... 107
Synchronize the EDR and BulkStats IBs on the Standby Collector Node ... 114
Fetching BulkStats IBs ........................................................................... 117
Create File for Uncategorized URL, UA, and TAC Reports ................... 118

**Single Certificate Installation** ............................................................... 119
Backing Up and Generating the Keystore Files ........................................... 119
Downloaded the Signed Certificate ......................................................... 121
Downloaded the CA Certificate .............................................................. 121
Installing the Signed Certificate in the Keystore ................................. 122

Processing the Data .................................................................................. 125
Setting Up a New User for the ASR in the Collectors ......................... 125
Ingesting the Data Into the System ....................................................... 126

Validating the System Installations .......................................................... 127
Validating Data on the Collector Nodes .................................................. 127
Validating Data on the Compute Blades (Data Nodes) ......................... 129
Validating Data on the Insta Blades ....................................................... 130
Validating Bulk Stats Data on the Insta Blade .................................... 131
Starting UI Processes and Verifying Data .............................................. 133

Mandatory Parameters for Incoming ASR Files .................................. 136
Mandatory Attributes for Flow EDRs for MURAL ............................... 136
Mandatory HTTP EDR Attributes for MURAL ..................................... 137
ASR-Side Configuration .......................................................................... 137

Manufacturing the Master GMS Blade ..................................................... 141

Glossary .................................................................................................... 151
Installation Overview

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

Prerequisites

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
- Cisco UCS Server Blade administration
- 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
- Locate the Customer Information Questionnaire (CIQ) for the deployment. See "Customer Information Questionnaire" on page 12.
- Verify that each Fabric Interconnect is connected to the storage area network (SAN) controllers through fibre 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, Insta, and so on) are connected to the UCS 6248 Fabric Interconnect. The number of each type of node depends on the deployment, 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 small deployments a blade might host multiple types of nodes. For example the UI and Caching nodes can be separate but are often combined, and in environments that have a lower data flow requirement, the Collector, UI, and Caching nodes might all be combined along with the GMS node.

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 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 node**—Analyzes and aggregates the data, creating *data cubes*. The term 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 deployment, and uses N+1 redundancy.
• **Insta node**—Stores and manages the processed data cubes that are stored in the columnar Insta database. Data cubes are commonly retained for the previous three to six years, depending on the amount of storage. The Insta node cluster has two servers with 1+1 redundancy.

• **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 System (GMS)**—Provides centralized management of the MURAL platform 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.

**Hardware**

The MURAL application is hosted on a redundant pair of UCS 5108 Blade Server Chassis. Each chassis hosts blades on which run the nodes listed above (Collector, Compute, Insta, UI/Caching, and GMS). Data storage is provided by EMC storage devices.

The data flows that feed the MURAL system are generated by a Cisco ASR platform (hereafter referred to 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 `mural.xml` file, which is installed on the GMS node and contains custom configuration settings for your deployment, based on the network topology information in the 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 Customer Information Questionnaire (CIQ) is an Excel spreadsheet of configuration settings based on a site survey that was completed before the installation process. It includes the following worksheets:

- **Contacts**—Identifies site personnel and their responsibilities
- **Space_Power Req**—Specifies space and power requirements
- **IP Survey**—Specifies 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**—Depicts the connections between system components
- **Connectivity**—Specifies details for ports and connections
- **Firewall**—Identifies firewall changes required for connectivity
- **Alarms**—Lists and describes all supported SNMP traps
- **ASR**—Specifies locations for required ASR information bases (IBs)
Configuring UCS Hardware and Software for MURAL

The Cisco Mobility Unified Reporting and Analytics (MURAL) software components (nodes) run on hardware components (blades) installed in Cisco Unified Computing System (UCS) 5108 Blade Servers. Cisco UCS 6248UP 48-Port Fabric Interconnects provide the physical connections between the Blade Servers, the storage area network (SAN) hardware, and the client network (also referred to as the management network).

The standard MURAL deployment has been tested and validated for the topology shown in the following figure.

Perform the tasks described in the following sections:

- "Verifying UCS Hardware Configuration" on the next page
- "Configuring Base UCS Software Settings" on page 20
Verifying UCS Hardware Configuration

Verify UCS hardware configuration, including slot assignments for blades, connections between Fabric Interconnects, SAN uplinks, and network uplinks.

Verifying Slot Assignments for Blades

The IP Survey worksheet in the Customer Information Questionnaire (CIQ) specifies for your deployment which nodes run the blades installed in Blade Server slots. 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 following sample slot assignments provide for high availability by placing redundant nodes of each type on different chassis (for example, the Compute 1 node is on Chassis 1 and the Compute 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.

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>UI/Caching 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.
Verifying Physical Connections to the Fabric Interconnects

Verify the physical connections between the Fabric Interconnects and other hardware components.

Verifying Connections to the Management Network

Verify that the physical connections between the Fabric Interconnects and the management network match the following figure and table. In particular, verify the following:

- 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
Cisco MURAL Software Installation Guide

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Beaconing LED and Reset button</td>
</tr>
<tr>
<td>2</td>
<td>System status LED</td>
</tr>
<tr>
<td>3</td>
<td>UCS cross-connect port L1</td>
</tr>
<tr>
<td>4</td>
<td>UCS cross-connect port L2</td>
</tr>
<tr>
<td>5</td>
<td>Network management port</td>
</tr>
<tr>
<td>6</td>
<td>Console port</td>
</tr>
<tr>
<td>7</td>
<td>USB port</td>
</tr>
</tbody>
</table>

**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:
The following table indicates how to connect the ports in UCS 2014XP Fabric Extenders on Chassis 1 to the ports on Fabric Interconnects A and B.

<table>
<thead>
<tr>
<th>Chassis 1 Fabric Extender and Port</th>
<th>Fabric Interconnect and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Extender 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>
<tr>
<td><strong>Extender 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>
The following table indicates how to connect the ports in UCS 2014XP Fabric Extenders on Chassis 2 to the ports on Fabric Interconnects A and B.

<table>
<thead>
<tr>
<th>Chassis 2 Fabric Extender and Port</th>
<th>Fabric Interconnect and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Extender 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</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 SAN match the following figure and table:
Verifying Connections to the UCS Networks

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>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>
Configuring Base UCS Software Settings

To set the admin password and management port IP address, set up a cluster for the Fabric Interconnects, and specify the default gateway, perform the following steps:
1. Set the console port parameters on the computer terminal (or console server) to the following values:
   - 9600 baud
   - 8 data bits
   - No parity
   - 1 stop bit

2. Connect to the console port of Fabric Interconnect A.

3. At the prompts, set the indicated parameters:

   Configuration method: **console**
   Setup mode: **setup**
   New fabric interconnect: **Y**
   Enforce strong password: **Y**
   Admin password: **admin-password**
   Is this Fabric Interconnect part of a cluster: **Y**
   Switch fabric: **A**
   System Name: UCS-name /* do not include final -A or -B */
   Mgmt0 IP address: Fabric-A-mgmt-port-IP-address
   Mgmt0 Netmask: mgmt-port-IP-netmask
   IPv4 default gateway: gateway-address-in-mgmt-subnet
   Cluster IPv4 address: Virtual-IP-address-for-FI-cluster /* usually belonging to management subnet */

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

2. Connect to the console port of Fabric Interconnect B, and verify the redundancy cables to Fabric Interconnect A are connected. At the prompts, set the following parameters:

   Configuration method: **console**
   This fabric interconnect will be added to the cluster: **Y**
   Admin password of interconnect: **admin-password** <same as for Fabric A>
   Mgmt0 IP address: Fab-B-management-port-IP-address
You can now log in to the management UI from a web browser at http://Virtual-IP-address-for-FI-cluster.
Configuring UCS for MURAL

To complete the configuration of the Cisco Unified Computing System (UCS) for Cisco Mobility Unified Reporting and Analytics (MURAL), run the MURAL configuration scripts for UCS, configure Direct Attached Storage (DAS) in UCS, and set system profile settings for UCS Manager.

A script enables quick configuration for UCS for the MURAL installation. 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)—Specifies parameters used by the UCS configuration script. You must update the file with information specific to your deployment.

- **ucs-config.exp**—Sets configuration parameters for the UCS Fabric Interconnects, servers, LAN, and storage area network (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 the modified **ucs-config-version-number.txt** file in the same directory, renaming it to **ucs-config.exp** (the .exp extension indicates that it is a script).

3. Run the following command to verify that you can ping the UCS management IP address:

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

4. From a Cygwin, Linux, or Mac terminal, run the script and note 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 configure Direct Attached Storage (DAS) in UCS, which enables you to directly attach a fiber-channel SAN to the Fabric Interconnects. Complete the tasks described in the following sections:

- "Setting Fabric Interconnects to FC Switching Mode" below
- "Creating VSANs for Zoning" on the facing page
- "Designating Storage Ports and Assigning Storage Cloud VSANs" on page 28
- "Confirming the Storage Port WWPN is Logged Into the Fabric Interconnects" on page 30
- "Creating Storage Connection Policies" on page 32
- "Creating SAN Connectivity Policy" on page 33
- "Configuring SAN Cloud Policy" on page 34
- "Creating vHBA Initiator Groups" on page 36
- "Verifying Service Profile Templates" on page 37
- "Configuring System Profiles for the Cisco UCS Manager" on page 38

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 SAN (VSAN) for each Fabric Interconnect.

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

- ID 4079 (VSAN name 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 (VSAN names 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 window that pops up, 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 **ID** and **FCoE VLAN ID** fields, as shown in the following figure.

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**.
8. Navigate to **Storage Cloud > Fabric identifier > VSANs**, and repeat Steps 1 through 7.

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. If you choose to assign VSAN IDs 3010 and 3020 as in the figure, verify that they are not already used elsewhere in your network.
Designating Storage Ports and Assigning Storage Cloud VSANs

For each Fabric Interconnect, configure the ports connecting to the storage array as type FC, then designate them as FC Storage Ports and assign a Storage Cloud VSAN to them.

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.

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.

**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.

```bash
hostname# connect nxos
```

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

```bash
hostname (nxos)# show zoneset active
zoneset name hostname-vsan-3010-zoneset vsan 3010
  zone name hostname_A_8_UI1_vHBA-A vsan 3010
  * fcid 0x6c0000 [pwwn 20:00:00:05:ad:1e:11:2f]
  * fcid 0x6c00ef [pwwn 50:06:01:68:3e:e0:0a:6b]
  * fcid 0x6c01ef [pwwn 50:06:01:60:3e:e0:0a:6b]

zoneset name hostname_A_7_GMS1_vHBA-A vsan 3010
  * fcid 0x6c0003 pwwn 20:00:00:05:ad:1e:11:4f
  * fcid 0x6c00ef [pwwn 50:06:01:68:3e:e0:0a:6b]
```
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. Make a note of the world wide port numbers in the **PORT NAME** column, which are used in "Creating Storage Connection Policies" on the next page.

```
hostname (nxos)# show flogi database vsan 3010

INTERFACE VSAN FCID PORT NAME NODE NAME
--------- ---- ----- ------------ ----
fc1/31 3010 0x1000ef 50:06:01:60:3e:a0:28:d2
50:06:01:60:be:a0:28:d2
fc1/32 3010 0x1001ef 50:06:01:69:3e:a0:28:d2
50:06:01:60:be:a0:28:d2
```

5. Run the `exit` command.

```
hostname (nxos)# exit
```

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

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

```
hostname (nxos)# show flogi database vsan 3020

INTERFACE VSAN FCID PORT NAME NODE NAME
--------- ---- ----- ------------ ----
fc1/31 3020 0x4200ef 50:06:01:61:3e:a0:28:d2
```
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 window that pops up, make the following settings. The FI-ID variable is the Fabric Interconnect identifier, such as A.
   - For **Name**—**storage-conn-polFI-ID**
   - For **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 30
   - For **Path**—**FI-ID**
   - For **VSAN**—The VSAN created for the Fabric Interconnect in "Creating VSANs for Zoning" on page 25, such as vsan3010 for Fabric Interconnect A

3. Repeat Step 2 for port 32.

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

5. Repeat Steps 1 through 4 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>Name</th>
<th>vhBA-A</th>
</tr>
</thead>
<tbody>
<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.

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.
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.

This completes the configuration of DAS.

**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.

**Configuring Ethernet Adapter Policy**

To configure Ethernet adapter policy for all Ethernet interfaces, 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

### Configuring BIOS Policy (Processor Page)

To configure BIOS 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 > 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
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhanced Intel SpeedStep</td>
<td>Enabled</td>
</tr>
<tr>
<td>Hyper Threading</td>
<td>Default</td>
</tr>
<tr>
<td>Core Multiprocessing</td>
<td>all</td>
</tr>
<tr>
<td>Execute Disable Bit</td>
<td>Default</td>
</tr>
<tr>
<td>Virtualization Technology</td>
<td>Disabled (Enabled if VMs are expected to be run on the systems)</td>
</tr>
<tr>
<td>Direct Cache Access</td>
<td>Enabled</td>
</tr>
<tr>
<td>Processor C State</td>
<td>Disabled</td>
</tr>
<tr>
<td>Processor C1E</td>
<td>Enabled</td>
</tr>
<tr>
<td>Processor C3 Report</td>
<td>Default</td>
</tr>
<tr>
<td>Processor C6 Report</td>
<td>Default</td>
</tr>
<tr>
<td>Processor C7 Report</td>
<td>Default</td>
</tr>
<tr>
<td>CPU Performance</td>
<td>hpc</td>
</tr>
<tr>
<td>Max variable MTRR Setting</td>
<td>Default</td>
</tr>
</tbody>
</table>

**Setting the Boot Order of Devices**

To set 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)**. Open the **General** tab in the main pane.

2. Set the order of preference for boot devices as shown in the following figure.
   a. Local Disk
   b. LAN (in the case of PXE boot, ensure that both interfaces are added--
for example, \texttt{vnic0} and \texttt{vnic1})

\subsection*{C. Other Devices}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{example.png}
\caption{Example figure showing UCS Manager interface for setting RAID policy.}
\end{figure}

\section*{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.

\textbf{Note:} Set up hardware RAID 1 on the local disk.

\textbf{Caution:} Do not use the \texttt{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 \texttt{Servers} tab at the top of the left-hand navigation bar, then navigate to \texttt{Policies} \texttt{root} > \texttt{Local Disk Configuration Policies} > \texttt{Local Disk}.

2. Select \texttt{Configuration Policy Default} > \texttt{General}.
3. In the Properties box, select **RAID 1 Mirrored** from the **Mode** drop-down menu, as shown in the figure.

![Properties Box](image)

For more information, see the *Cisco UCS Manager GUI Configuration Guide, Release 2.1*. 
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 "Manufacturing the Master GMS Blade" on page 141.

**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 previous section, "Installing and Configuring VM for GMS Lite" on page 47 provides instructions on installing and configuring VirtualBox.

The VM software needs to be configured to the following specifications:

- OS type: linux 64 bit
- RAM: Minimum 2 GB
- HDD: IDE: Minimum 50 GB (dynamically allocated)
- CPU Cores: Minimum 1

**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.

**Configure VM as a GMS Lite Node**

When you launch the VM software, it opens a command prompt.

1. Go to the configure terminal:

   ```
   > en
   # conf t
   ```

2. Start the GMS server:

   ```
   (config)# pm process gms_server restart
   ```

3. Verify that GMS Lite is running:
Configure the XML file for System Configuration

1. Open the GMS Lite user interface by going to the URL: https://VM-IP/configure
   Where VM-IP is the IP address of your laptop.

2. Configure and modify the XML file by following steps 2-40 of section "Defining the Deployment Topology Using GMS" on page 74.

3. Activate the xml file on this VM by running:
   
   (config)# gms config mural.xml activate

Setting Up the Master GMS Node and Cluster

1. Mount the image on the GMS Lite virtual machine:
   
   (config)# image mount mfgcd-guavus-x86_64-20140315-133212.iso
   
   The resulting output may resemble:
   
   Copying linux...
   Copying rootflop.img...
   Copying image.img...

2. Verify the image on the GMS node:
   
   (config)# ls /var/opt/tms/images/ mfgcd-guavus-x86_64-20140315-133212.iso

3. Complete the following steps to reboot the master GMS blade from the KVM console:
a. Open the blade’s KVM console.

b. Press **CTRL-ALT-DEL** as explained earlier in this installation guide to reboot the blade. An alternative is to click **Reset** from the top of the KVM console.

c. Once prompted, press **F12** to boot from the network.

Once the blades start booting from the network, GMS begins the manufacture process in parallel across all GMS blades by using PXE boot to push the image.

**Note:** A blade takes approximately 45 minutes to manufacture with the new image.
Wait until the last blade for the PXE boot has been manufactured and a log in prompt displays.

4. Download the patches from the FTP server to the master GMS server in the /data directory. Apply all patches applicable for GMS node.

   **Note:** In the *CISCO MURAL Release Notes* for software version 3.3 (and later) see "Download and Apply Patches to the GMS Server" for a complete list of patches and installation instructions.

5. On GMS Lite VM, shut down the GMS server:

   ```
   > en
   # conf t
   (config)# no pm process gms_server launch auto
   (config)# pm process gms_server terminate
   ```

   **Note:** This is required as this VM will not be used further for system installation. GMS HA cluster will be responsible for manufacturing/Installing the system.

6. SSH into the GMS blade manufactured above with the user name and password specified during the GMS configuration. A successful log on indicates that manufacturing the blade is successful.

7. Configure the GMS server on this node as mentioned in "Setting Up the Master GMS Node" on page 55. After configuration, verify that GMS server is running:

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

8. Copy the configuration xml from VM server to the new master GMS node:
9. Install the master GMS node.

10. Manufacture the standby GMS node according to the section "Manufacturing the Remaining Blades" on page 95.

11. Install and configure the standby GMS node according to "Configuring the Standby GMS Node" on page 1.

   **Note:** At this point, the GMS HA cluster is up and can be used to manufacture and configure all other nodes.

### Manufacturing All Other Blades

To manufacture all other nodes except GMS nodes, see the "Manufacturing the Remaining Blades" on page 95.

### 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-step details to create a VM using VirtualBox and to import a pre-configured Vdisk image onto the laptop.

**Note:** 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 43.

**Note:** If you have chosen to manually install the GMS nodes and not use GMS Lite, you can skip to "Manufacturing the Master GMS Blade" on page 141.
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

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. Select VM Name, Type and Version:

   ![Create Virtual Machine](image)

   Name: VM3.1.1
   Type: Linux
   Version: Other Linux (64-bit)

5. Choose RAM size (min 2 GB) and press **Next:**
6. Select **Use an existing virtual hard drive file**.

7. Select the vdisk image file from directory path and click **Open**:

8. Click **Create**.
9. VM creation is complete.

Configuring the VM for GMS Lite

1. Select VM from left pane and check configuration from right pane:

2. To view the VM configuration, select **VM > Settings > Storage**:
3. In the Storage Tree viewing window:
   a. Remove vdisk from the IDE controller.
   b. Add the SCSI Controller attach a vdisk to it.
   c. Enable “Host I/O cache” for SCSI controller.

4. Navigate to VM > Settings > Network.
5. Under Adapter 1, select:
   a. Attached to: **Bridge Adapter**
   b. Name: **NIC Ethernet LAN port**
   c. Promiscuous Mode: **Allow VMs**

6. Navigate to **VM > Settings > Serial Ports**.

7. Under Port 1 check the box for **Enable Serial Port**:

8. Click **OK**.
9. VM configuration completed, see VM info:

10. Select VM then **Start** to power on.

11. Log in from the VM console as an admin user and go to the configure terminal:

   ```
   > en
   # conf t
   ```

12. Assign appropriate IP addresses for the management interface and default gateway:

   ```
   (config)# interface eth0 ip address gms-lite-ip-address subnet-mask
   ```

   For example:

   ```
   (config)# interface eth0 ip address 192.168.103.78 /24
   ```

   ```
   (config)# ip default-gateway mgmt-network-default-gateway-IP
   ```

   For another example:
13. Re-create and enable swap.

14. Identify swap device (disk volume for swap):

```
# fdisk -l | grep -i swap
/dev/sda7  1098  1620  4200997  82 Linux swap /
```

Solaris

```
# free -m
# mkswap /dev/sda7
# swapon -a
# free -m
```

The VM is now ready to use as GMS lite server; refer to "Using GMS Lite to Automate Installation of GMS Nodes" on page 43 for installing GMS patches and performing other configurations.
Setting Up the Master GMS Node

After the master GMS blade is manufactured (the MURAL software is loaded on it) as described in "Manufacturing the Master GMS Blade" on page 141, you set the administrator password for the node, assign IP addresses, and verify correct zoning on the fabric interconnect.

Setting the Password and IP Addresses

To set the administrator password and IP addresses on the master GMS node, perform the following steps:

1. Log in to the master GMS node via the console as **admin**, if you have not already.

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.

   ```
   > en
   # conf t
   (config)# username admin password admin@123
   (config)# write mem
   (config)# _shell
   ```

3. Enter config mode again and define the IP addresses 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)# license install LK2-RESTRICTED_CMDS-88A4-FNLG-XCAU-U
   (config)# write memory
   (config)# _shell
   ```
Verifying Zoning and 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 example.

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

```
hostname-A(nxos)# show zoneset active
zone name ucs_hostname_A_10_GMS1_vHBA-A vsan 3010  
  * fcid 0x100005 [pwwn 20:00:00:05:ad:1e:11:1f]  
  * fcid 0x1000ef [pwwn 50:06:01:60:3e:a0:28:d2]  
  * fcid 0x1001ef [pwwn 50:06:01:69:3e:a0:28:d2]

hostname-B(nxos)# show zoneset active
zone name ucs_hostname_B_22_GMS1_vHBA-B vsan 3020  
  * fcid 0x420001 [pwwn 20:00:00:05:ad:1e:11:4e]  
  * fcid 0x4200ef [pwwn 50:06:01:61:3e:a0:28:d2]  
  * fcid 0x4201ef [pwwn 50:06:01:68:3e:a0:28:d2]
```

Proceed to "Allocating Storage for the Master GMS Node" on the facing page.
Allocating Storage for the Master GMS Node

This topic describes how to allocate storage on EMC hardware for the master General Management Server (GMS) node. The storage arrays host the Hadoop distributed file system (HDFS) connected to the Collector and Compute nodes and the columnar database used by the Insta nodes.

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, record 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>
</tbody>
</table>
### Item | Value
--- | ---
Subnet mask and gateway for above |  
Admin name/password |  
Storage system serial number |  
Scope |  
DNS server address (optional) |  
Time server address |  
Inbound email address |  

**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.

**Registering the Master GMS Node with EMC**

Next you associate the master GMS node 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 memory to the master GMS node, ensuring that its definition in the EMC Unisphere interface matches its definition in the Unified Computing System (UCS). If EMC has been previously configured with MURAL, you still need to verify that the existing definition in EMC exactly matches the definition in the UCS.

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

**Before You Begin**

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

<table>
<thead>
<tr>
<th>Node - WWNN</th>
<th>WWPN - 1</th>
<th>WWPN - 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMS-1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To register the master GMS node with EMC:

1. In the EMC Unisphere interface, mouse over the **Hosts** icon in the title bar and 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.

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 and is hard-coded into every FC host bus adapter (HBA). For a device to operate correctly in a storage area network (SAN), its WWN needs to be registered with the SAN.
The two halves of the identifier in the WWN/IQN field must match the WWNN and WWPN values reported in the UCS Manager, which are each 8-digit hexadecimal numbers. To display them, click the SAN tab at the top of the left-hand navigation bar, then navigate to Pools > root. Click the Initiators tab in the main region of the window.

To display the WWNN, navigate to WWNN Pools > WWNN Pool wwnn-pool1, which is the pool name assigned by the UCS configuration script that ran in "Configuring UCS for MURAL" on page 23. In the Assigned To column of the table in the main pane, locate the rows for GMS-1. The WWNNs appear in the Name column of those rows.

To display the WWPN, navigate to WWPN Pools > WWPN Pool wwpn-pool1. Locate the rows for GMS-1 as described in the previous paragraph.

3. On the Register Initiator Record screen, perform the following steps:
a. Verify that the value in the **Initiator Type** field is **SGI**, selecting it on the drop-down menu if necessary.

b. Verify that the value in the **Failover Mode** field is **ALUA–mode 4** (the default as shown in the figure), selecting it on the drop-down menu if necessary.

c. Click the **New Host** radio button if it not already selected.

d. Enter the master GMS node's hostname and IP address in the **Host Name** and **IP Address** fields.

4. Navigate to **Dashboard > Hosts > Host List** in the EMC Unisphere interface and verify that the master GMS node is correctly configured.
Creating RAID Groups and LUNs for the GMS Master Node

Next create RAID groups, then create the logical unit number (LUN) for the master GMS node and assign it to the associated RAID group.

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

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 Group</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-1-PGSQL</td>
<td>1</td>
<td>50</td>
<td>FAB-A</td>
<td>INSTA-STR-2</td>
<td>INSTA NODE-1</td>
</tr>
</tbody>
</table>
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></td>
<td>5</td>
<td>5</td>
<td>4, 5, 6, 7, 8, 9</td>
</tr>
<tr>
<td></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. In the **RAID Type** field, select **RAID5: Distributed Parity (High Throughput)** from the drop-down menu.

   c. In the **Storage Pool for new LUN** field, select **5** from the drop-down menu.

   d. 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.

   e. In the **LUN ID** field, select **12** from the drop-down menu.

   f. In the **LUN Name** region, click the **Name** radio button if it is not already selected, and type **GMS-1** in the box.

6. Click **Apply**.

7. On the **LUNs** tab, verify that the parameters for **GMS-1** match the values
Creating the Storage Group for the Master GMS Node

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 the Hosts icon in the title bar, and select Storage Groups. Click Create. A Create Storage Group window similar to the following pops up.

The value in the Storage Group Name field is generated automatically, the final number being the next one available in the sequence of assigned numbers. 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 that pops up, open the **Hosts** tab and move **GMS-1** from the **Available Hosts** column to the **Hosts to be Connected** column.

4. Click the **OK** button, then the **Apply** button.

5. Verify that the list of storage groups for the master GMS node is similar to the following example.
Cisco MURAL Software Installation Guide

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. 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. 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. 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 the master GMS node. Proceed to "Starting the GMS Server Process".
Defining the Deployment Topology Using GMS

This topic explains how to use the General Management Server (GMS) to define the deployment topology from a single node instead of having to install and configure software manually on each blade.

Notes:

- You perform the procedures in this topic twice, the first time after starting the GMS server process as described in "Starting the GMS Server Process" and the second after allocating storage for the remaining nodes as described in "Allocating Storage for the Remaining Nodes". Both times you must specify the world wide identifier (WWID) associated with logical unit number (LUN) of each node. During the first pass, however, the actual WWID is available only for the master GMS node, so you must specify dummy placeholder values for all other nodes. During the second pass, 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.

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

- The VLANs and Bonds tabs in the GMS interface are not used in this version of MURAL.

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 Interface

To access the GMS interface, perform the following steps:

1. In a browser, access the following URL:

   http://Master-GMS-Node-IP-Address/configure

2. Log in as admin, providing the password you defined in "Setting Up the Master GMS Node" on page 55 (the recommended password is

Copyright © 2014, Cisco Systems, Inc.
admin@123).

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

![Java applet pop-up window]

4. Proceed as outlined in the following sections.

**Loading the Base Configuration File**

The MURAL installation package includes a sample configuration file, `mural.xml`, that is specific to the software version. The file prescribes a logical grouping of the nodes into two chassis (blade enclosures) and configuration settings for all of the system components based on the information in the CIQ.

**Note:** We strongly recommend that you use the GMS interface to make any modifications to the `mural.xml` file; do not modify the file directly in a text editor.
Cisco MURAL Software Installation Guide

The settings for the MURAL system are preconfigured based on the *mural.xml* file, and in most cases you only need to verify these settings. 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. Use the GMS interface to modify the settings as needed.

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.

To upload the configuration file from the local machine to the GMS, perform the following steps:

1. In the GMS interface, click the file navigation button (…) to the right of the top field, navigate to the configuration file, then click the **Load Config File** button.

   ![GMS file navigation and load button](image)

   When the configuration file is loaded, the GMS interface appears. Fields on each tab are populated with values from the *mural.xml* configuration file that are specific to your deployment, so in many cases all you need to do is verify that the setting is correct.

2. Proceed as outlined in the following sections.

**Verifying Settings on the Server Details Tab**

Verify the MAC addresses of interface bindings and WWIDs for the storage allocated to each node—master and backup Collector nodes, all Compute nodes, both UI/Caching (Rubix) nodes, both Insta nodes, and both UI nodes. Repeat the process for each node in both of the two logical chassis.
The first two sections explain how to locate the information you need to verify in the third section:

- "Finding MAC Addresses for Nodes" below
- "Finding WWIDs of LUNs" below
- "Defining the Deployment Topology Using GMS" on page 74

**Finding MAC Addresses for Nodes**

To find the MAC address for each node (blade), login to the UCS Manager and navigate to **Server > root**, then select and expand the blade. For example, click on **COLLECTOR1/Expand Vnicos/Vnic0** or **Vnic1** to find the MAC addresses for interfaces **eth0** and **eth1**, respectively.

**Finding WWIDs of LUNs**

If you are performing the procedures in this topic for the first time (after starting the master GMS server process as described in "Starting the GMS Server Process"), you specify dummy placeholder values for the WWIDs of all nodes other than the master GMS node. You can skip this section and proceed to "Setting the MAC Address and LUN WWIDs" below. "Setting the MAC Address and LUN WWIDs" below"Allocating Storage for the Remaining Nodes" on page 1, perform the steps in this section to learn the actual WWID for all nodes.

To find the WWID of LUNs, perform the following steps:

1. Log in to the EMC Unisphere interface at **http://IP-Address-EMC**.
2. Mouse over the **Storage** icon in the title bar and 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 prefix the ID with **3**, for example **360060160c7102f004887f4015d49e211**.

**Setting the MAC Address and LUN WWIDs**

For the master GMS node (on the first pass through this topic) or all nodes (on the second pass), set the MAC address and the WWID of the associated LUNs. The
number of LUNs, and therefore the number of WWIDs, assigned to each node depends on the type of node:

- Collector nodes, Compute nodes, and UI nodes each have one WWID.

- Each Insta node (being clustered) has three assigned WWIDs—one assigned to `dbroot1` of both Insta 1 and Insta 2, one assigned to `dbroot2` of both Insta 1 and Insta 2, and one assigned to `pgsql`. The `pgsql` storage partitions are for the Postgres database and store Rubix-related data; there is one `pgsql` storage partition for each Insta node.

**Note:** 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.

The figures in this section show a sample configuration. Your configuration is different. It is important to verify in the GMS interface that the configuration for all 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:

1. Open the **Server Details** tab in the GMS interface.

2. In the **Chassis** box, select the chassis. The **Slot** box lists the nodes (blades) in each slot.
3. In the **Slot** box, select the node.

4. In the **Interface Members** box, verify that the MAC address of the interface binding for the node matches the value in your CIQ. If it does not, click the **Add** button to create a new entry and set the correct MAC address. Then select the incorrect entry and click the **Delete** button.

5. In the **Storage** box (see the preceding figure), verify that the value in the **Storage_WWID** column matches the value you learned in "Finding WWIDs of LUNs" on page 77. If it does not, click the **Add** button to create a new entry and set the correct WWID. Select the incorrect entry and click the **Delete** button.

On the first pass through this topic, you can verify the WWID only for the master GMS node. For all other nodes, you must specify a dummy placeholder WWID that nevertheless is unique and in the correct format. We recommend deriving the dummy WWIDs from the master GMS node's WWID by changing the last three digits. For example, if the master GMS node's WWID is **360060160c7102f004887f4015d49e211**, change **211** to **212** in the first dummy WWID.
(360060160c7102f004887f4015d49e212), to 213 in the second dummy WWID (360060160c7102f004887f4015d49e213), and so on.

On the second pass through this topic, you must verify that the actual WWIDs match.

6. Repeat Steps 3 through 5 for each of the following nodes in Chassis 1:
   - First Collector node
   - Second Collector node
   - First Compute node
   - Second Compute node
   - Third Compute node
   - Fourth Compute node
   - First UI/Caching (Rubix) node
   - Second UI/Caching (Rubix) node
   - First Insta node
   - Second Insta node

   **Tip:** Ensure that the same WWID is assigned to `dbroot1` for both Insta 1 and Insta 2 in the GMS configuration, and that the WWID for the `pgsql` storage partition is unique for each Insta node.

7. Repeat steps 2 through 6 for Chassis 2.

### Verifying Global Settings

Verify the global settings for the system (DNS, default gateway, and NTP), and IP addresses configured for each node cluster and for the standalone GMS node.

The Collector nodes have three IP addresses and all other nodes have two IP addresses:

- **Internal** or Control Network—The network that the nodes will use to communicate among themselves. For the `eth0` interface, we recommend
you use a control IP address of the format 192.x.x.x.

- **External** or Management Network—The management network that will be used to SSH to the blades. For the eth1 interface, we recommend you use a physical or management IP address of the format 10.x.x.x. In the example below, eth3 is used for this interface. The management IP address can be used for the eth0 interface when an internal network is not available.

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

1. Under the **Networks** tab, verify the following fields for the internal (Management Network) and external (Control Network) networks:
   - Network name
   - Network prefix
   - Network subnet
   - Interface type
   - Management type
   - Network member

2. Under the **Global Settings** tab, enter the following information for the MURAL system:
   - DNS server
   - Default gateway
Cisco MURAL Software Installation Guide

- NTP server IP address
- NTP version

3. Under the **Nodes** tab, define the internal and external IP addresses and subnet masks of each node.

---

### Configuring the Node Clusters

The **mural.xml** 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. In the GMS interface, select the **Clusters** tab.
2. In the upper **Cluster** box, select the cluster to be configured or verified.
3. Fill in the fields in the lower **Cluster** area by selecting a cluster type from drop-down menu in the **Cluster Type** field, and typing the cluster name and interface in the **Cluster Name** and **Cluster Interface** fields. Click the **Add** button. The following figure shows a Collector cluster called COL-CLUS:

![Cluster Configuration](image)

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 following nodes:
   - GMS
   - Collector
   - Compute
   - Insta
   - UI/Caching (Rubix)

**Specifying Component Profiles and Application-Specific Settings**

This section describes how to load profiles that set the configuration for each component. You can then change individual settings as appropriate for your
deployment.

What is meant by a "component"?

To load the profiles that you want to associate with each component, perform the following steps:

1. Select the **Applications** tab.

2. Under **Application Name**, select the name of the system component from the drop-down menu.

3. Under **Application**, the GMS interface displays the list of profiles. Select the profile that you want to attach to the system component.

4. Attach the DFS template to the Collector cluster. This template configures HDFS on the cluster.
   a. Under **Available Profiles > Application Name**, select **Collector**.
   b. Under **Application**, select **DFS**.
   c. Under **Application > Clusters**, select the Collector cluster and verify that the name is correct for your setup (in this example, **COL**-
d. In the DFS template, update Hadoop Oozie server to be control VIP of the Collector blade, as shown below:

5. Attach the solution-based profile to the Collector cluster. Verify that the cluster name and the expected start date (DataStartTime) are correct for your setup.

**Note:** It is safe to set the time here as GMS does not run all of the jobs. Later in this installation procedure you will change the Oozie start time and start all of the jobs (see "Setting the Data Start Time" on page 128).

2. Attach the workflow-related profile to the Collector cluster. The workflow profile contains configuration settings for the MapReduce jobs.

6. Attach the compute-based profile to the Compute cluster and verify that the name is correct for your setup.

7. Attach the Insta-related profile to the Insta cluster, and verify that the name of the cluster is correct for your setup. The following screen shows an example Insta profile.
8. Attach the Postgres-related profile for the Postgres application and assign it to the Insta cluster, as shown in the following screen:

9. Attach the GMS-related profile for the GMS application and assign it to the GMS cluster:
10. Attach the Postgres-related profile for the Postgres application and assign it to GMS cluster:

```
```

11. Attach the Collector-based templates (collector_custom_adaptor_edrhttp_edrflow_template and collector_custom_adaptor_bulkstats_template) to the Collector cluster, specifying Collector as the Application Name:

```
```
Verify that the following parameters are correct for your setup:

- Cluster name, specified by the parameter `Cluster_Name`.

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

The format of the value is `/data/collector/bulkstats_files/gateway_name`.

An example value is `/data/collector/bulkstats_files/GMPLAB1/`,
where the ASR is located in the DC called GMPLAB1.

- **BulkStats file backup directory**, specified by the parameter `adaptor.bulkStats.input.fileConfig.bulkStatsFile1.backupDirectory`.
  
  *The format of the value is* `/data/collector/bulkstats_files/gateway-name`.

- **BulkStats file name format**, specified by the parameter `adaptor.bulkStats.input.fileConfig.bulkStatsFile1.fileNameFormat`.
  
  *The format of the value is* `*_%YYYY%MM%DD%hh%mm%ss`.

- **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`.

- **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)*.

12. Attach the appropriate profile to the Rubix cluster and verify the values of the following parameters:

- `application.atlas.sessionCookieDomain`

  *For example, if the URL to be used is* [https://today.mural.com](https://today.mural.com)*, then the correct value is* `mural.com`.

- `application.atlas.timeZone`

  *The time zone of location of the ASR, for example,* `America/Argentina/Buenos_Aires`.
Cisco MURAL Software Installation Guide

- application.bulkstats.sessionCookieDomain
- application.reportAtlas.sessionCookieDomain
- application.reportAtlas.rgeUrl

URL to be used, for example, https://today.mural.com:30443. Note that the port number must be 30443.

- application.reportAtlas.bulkStatsURL
- application.rge.mailNotificationHost

Customer mail host, for example, mx1.cisco.com.

- application.rge.mailNotificationSender

Destination email address, for example, support@cisco.com.

- application.rge.rgekeyStoreAlias

**Caution:** Do not change this value from app2.guavus.com.

- application.bulkstats.timeZone

Time zone of the location of the ASR.

- application.reportAtlas.timeZone

Time zone of the location of the ASR.

The following screens show an example:
Note: Set the application.timeZone property to the same TimeZone value for all applications (such as Atlas, RGE, and Bulkstats).

For TimeZones, refer the table below. TimeZone string has to be used for application.timeZone property and it should be same for all apps i.e. Atlas, RGE, Bulkstats. numOwners also needs to be changed as number of tomcats that will be running.

<table>
<thead>
<tr>
<th>TimeZone String</th>
<th>Actual Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CST6CDT</td>
<td>United States central standard time</td>
</tr>
<tr>
<td>EST5EDT</td>
<td>United States eastern standard time</td>
</tr>
<tr>
<td>Chile/Continental</td>
<td>Chile time</td>
</tr>
<tr>
<td>America/Argentina/Buenos_Aires</td>
<td>Argentina time</td>
</tr>
<tr>
<td>CET</td>
<td>Central European time</td>
</tr>
<tr>
<td>GMT</td>
<td>Greenwich mean time</td>
</tr>
</tbody>
</table>

13. Specify the solution-based template to the Solution application and attach it to the Rubix Cluster as Instance 2:
14. Ensure that Application Profiles are attached to the Rubix cluster as in the following sample screen shots:
Validating the Configuration

After completing all configurations on the Server Details, Networks, Global Settings, Nodes, Clusters, and Applications tabs as described in the previous sections, you must validate the configuration settings.

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 in turn, 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.

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**.

To activate the configuration after you have made changes, you must run the `gms config config-file.xml activate` command. Until you activate the new script, the system runs the previously saved configuration.

If you are completing the procedures in this topic for the first time (only the master GMS node has an actual WWID), proceed to "Setting Up the Master GMS Node" on page 55.

If you are completing the procedures in this topic for the second time (all nodes have actual WWIDs), proceed to "Configuring the Standby GMS Node" on page 1.
Manufacturing the Remaining Blades

To manufacture the blades for all nodes other than the master GMS node, perform the following steps:

1. Manufacture all the blades using PXE boot via GMS. The IP-local-remote-machine variable is the IP address of the machine onto which the ISO image for the build was downloaded.

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

For example:

```
(config)# image fetch scp://admin@45sds.guavus.com/software/images/cisco_mural/mural3_3mr1/mfgcd-guavus-x86_64-20140315-133212.iso
(config)# image mount mfgcd-guavus-x86_64-20140315-133212.iso
Copying linux...
Copying rootflop.img...
Copying image.img...
```

2. Verify the image on the GMS node:

```
# ls /var/opt/tms/images/
mfgcd-guavus-x86_64-20140315-133212.iso
```

3. Complete the following steps to reboot each blade from the KVM console:

   a. Open the KVM console of the blade.

   b. Press **CTRL-ALT-DEL**, as explained in "Manufacturing the Master GMS Blade" on page 141 to reboot the blade. You can also click **Reset** from the top of the console window.

   c. After the prompt, press the **F12** key as soon as possible to boot from the network.

   d. Repeat steps a through c for all blades, except those designated for
GMS.

The following figure shows the results of pressing the **F12** key.

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 the last blade for which PXE boot was issued has been manufactured. A login prompt is displayed once the image has been manufactured on a blade.

**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

---

**Copyright © 2014, Cisco Systems, Inc.**
hosts, as shown for **FI A** and **FI B** in the following example.

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

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

 zone name hostname_A_11_UI2_vHBA-A vsan 3010
   * fcid 0x100006 [pwwn 20:00:00:05:ad:1e:11:ff]
   * fcid 0x1000ef [pwwn 50:06:01:60:3e:a0:28:d2]
   * fcid 0x1001ef [pwwn 50:06:01:69:3e:a0:28:d2]

hostname-B(nxos)# show zoneset active
zoneset name hostname-vsan-3020-zoneset vsan 3020
 zone name hostname_B_24_UI1_vHBA-B vsan 3020
   * fcid 0x420007 [pwwn 20:00:00:05:ad:1e:11:2e]
   * fcid 0x4200ef [pwwn 50:06:01:61:3e:a0:28:d2]
   * fcid 0x4201ef [pwwn 50:06:01:68:3e:a0:28:d2]

 zone name hostname_B_23_UI2_vHBA-B vsan 3020
   * fcid 0x420009 [pwwn 20:00:00:05:ad:1e:11:5e]
   * fcid 0x4200ef [pwwn 50:06:01:61:3e:a0:28:d2]
   * fcid 0x4201ef [pwwn 50:06:01:68:3e:a0:28:d2]
```
4. Log in to the UCS Manager on the FI and navigate to Servers > Service Profiles > root > Service Profile profile-name (in the following figure, the profile name is HS-ESX01). Access the FC Zones tab and in each FC Target row, verify that the WWPNs in the Name and Target WWPN fields are the same.

Proceed to "Allocating Storage for the Remaining Nodes" on page 1.
Installing MURAL on the Blades

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 Reflex platform blades.

- Update WWIDs on GMS configuration
  
  Before proceeding to the next section of this guide, ensure that the GMS configuration has been updated with WWID of all LUNs. See "Defining the Deployment Topology Using GMS" on page 74.

- Apply all available patches on the appropriate nodes.
  
  Before beginning the next section of this installation guide, patches and configuration changes must be applied on the nodes. To apply patches, follow the instructions in the Release Notes for your software version.

To install software on the blades:

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 cluster cluster-name cluster-name
   ```

2. To install all the nodes together:
   
   ```
   > en
   # conf t
   (config) # install appliance all force-format
   ```

3. Monitor the installation process on all 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 messages are displayed:

<table>
<thead>
<tr>
<th>Node Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collector-GMS-1</td>
<td>Node successfully installed</td>
</tr>
<tr>
<td>Collector-GMS-2</td>
<td>Node successfully installed</td>
</tr>
<tr>
<td>Compute-GMS-1</td>
<td>Node successfully installed</td>
</tr>
<tr>
<td>CachingCompute-GMS-2</td>
<td>Node successfully installed</td>
</tr>
<tr>
<td>Rubix-GMS-1</td>
<td>Node successfully installed</td>
</tr>
<tr>
<td>Rubix-GMS-2</td>
<td>Node successfully installed</td>
</tr>
</tbody>
</table>

4. After the installation completes for all the nodes, modify the files as detailed below, and run the script `finalize.pl` from `/opt/gms/config-mgmt/scripts` directory of the GMS node.

   a. Parameters file: edit as per the requirement of the setup.

   b. `br_cert.pem`: Certificate for the RGE nodes. Refer to the section 'Certificate Installation' below for instructions to generate a new certificate.

      **Note:** If certificate is generated using third party tool, contact the concerned authority for porting it to Guavus solutions.

   c. `certificate_installation`: This file contains the cli commands for installing the certificate

   d. `mop_collector`: If additional configurations are to be applied to the Collector nodes, enter the cli commands in this file

   e. `mop_dn`: If additional configurations are to be applied to the Data nodes, enter the cli commands in this file

   f. `mop_insta`: If additional configurations are to be applied to the Insta nodes, enter the cli commands in this file

   g. `mop_rubix`: If additional configurations are to be applied to the Rubix
nodes, enter the cli commands in this file

h. mop_rge: If additional configurations are to be applied to the RGE
nodes, enter the cli commands in this file

i. Run the script:

   (GMS-Server) # cd /opt/gms/config-mgmt/scripts
   (GMS-Server) # perl finalize.pl

**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`. 
Verify the 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 Collector node 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

```
# cli -t "en" "conf t" "show pm process collector" | grep status
Current status: running
```

2. Run the following commands on the standby Collector node:
3. Log in to the master Insta node, and run the following commands:

```bash
> 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

# cli -t "en" "conf t" "show pm process collector" | grep status
  Current status: running
```

If the process is running, the command output is `Current status: running`.

```bash
(config) # insta infinidb get-status-info
```

The command output should show all modules in ACTIVE state.

It should also list all instances and Adaptor status as RUNNING.

4. Log in to the standby Insta node and repeat the same commands shown in step 3.

5. Run the following command to verify that Postgres is running on the master Insta node:

```bash
> en
# _shell
# ps -ef |grep pgsql
postgres 2990  1  0 Sep04 ?  00:00:01 /usr/pgsql-9.2/bin/postmaster -p 5432 -D /data/pgsql/9.2/data
```

6. Repeat step 5 on the standby Insta node.
Generate and Push 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.

Modifying IBs Manually

In addition to the necessary configurations done by the scripts, you might need to do some manual modifications of IBs.

1. Determine which additional entries you might need to add by viewing device groups list on the master Collector node:

```
# conf t
(config)# pmx
pm extension> subshell bulkstats
pm extension(bulkstats)> update all ibs from image
pm extension(bulkstats)> quit
pm extension> subshell aggregation_center
pm extension(aggregation center)> update all ibs from image
pm extension(aggregation center)> show ib deviceGroup.list
```

2. Make changes for core job on the master or standby Collector node:

```
[admin@host ~]# cd /opt/etc/scripts
[admin@host ~]# ./install_solution_config.sh
is tethering app enabled, enter (Y/N) : Y
is httperror app enabled, enter (Y/N) : Y
solutionConfig.json file is successfully copied
```

3. Create a file (/data/work/serverFile_tethering) to contain the details of the ASR gateways. The TAC, OS, and UA databases (the three reports associated with tethering) are created and stored in this file. The serverFile_tethering file contains the entries for the data transfer destination location.
**Note:** For the SCP protocol, the destination folder should be present on the destination server. This is not required for SFTP.

To create the file, log into the master Collector node:

```
> en
  _shell
  cd /data
  mkdir work
  cd work
  vi /data/work/serverFile_tethering
  192.168.156.96, admin, admin, /data/TTYT
```

Include an entry for each ASR gateway. The delimiter in this file must be ", " (comma followed by a space). Therefore, the file has the following format:

```
IP-address-of-gateway, ASR-gateway-user-login-name,
ASR-gateway-password, location-on-ASR-gateway-for-
databases-copies
```

For example:

```
192.168.1.1, admin, password, /data
```

4. Repeat the previous step on the standby Collector node.

**Configuring IBs for EDR**

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

<table>
<thead>
<tr>
<th>Sample Data Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC</td>
</tr>
<tr>
<td>Region</td>
</tr>
<tr>
<td>Area</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, GGSNIP is the management IP address. For SGSN, you might use SGSN, SGW, HSGW, or PDSN. In this case, SSGNIP is the service IP address.

To configure the IBs for EDR:
**Tip:** Repeat the `add` command to add the IP address of each node in turn.

1. Login to the master Collector node, and add Control or Internal IP(s) addresses of all Collector and UI nodes; that is, include all master and standby nodes of both collector and UI nodes:

   ```
   > en
   # conf t
   (config) # pmx
   pm extension> subshell aggregation_center
   pm extension (aggregation center)> add ib-destination-IP
   
   Control or Internal IP addresses of all master and all /standby collectors and UIs nodes
   ```

2. Enter the GGSN IPs and GGSN names:

   ```
   pm extension (aggregation center)> edit ib ipGgsn.map add
   ```

3. Enter the SGSN IPs and SGSN name:

   ```
   pm extension (aggregation center)> edit ib ipSgsn.map add
   ```

4. Enter the APN name and corresponding APN group:

   ```
   pm extension (aggregation center)> edit ib apnGroup.map add
   ```

5. Enter the RAT ID and RAT TYPE:

   ```
   pm extension (aggregation center)> edit ib ratidtype.map add
   ```

6. Default segments have only **Low**, **Active**, and **High** segments in the configuration, as shown in the following example:

   ```
   pm extension> subshell aggregation_center ` 
   pm extension (aggregation center)> show ib segment.map
   1 [524288000][High]
   ```
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 the BulkStat 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 (/).

- Files coming for BulkStats should contain the GatewayName delimited by an underscore (_). For example, GMPLAB1_20130912121500.

- The filename pattern provided here should be in sync with the Collector configurations.

- 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 (\_) and HTTP EDR files must contain string "http," delimited by an underscore (\_).

To configure gateways:

1. Add gateway information for each gateway (refer to guidelines above for clarification about input parameters):

```
> en
# conf t
(config)# pmx subshell aggregation_center
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 incoming-EDR-files-path-on-collector
bulkstat-file-path incoming-BS-files-path-on-collector
```

**Tip:** For bulkstat-schema-version, specify an integer only, for example use 15, do not use 15.0.

For example:

```
pm extension (aggregation center)> add gateway name GMPLAB1
region EAST location USA
schema_version 15 ip 10.10.10.255
timezone America/Recife
edr-filename-pattern *_MURAL-edr_*_%MM%DD%YYYY%hh%mm%ss.*
bulkstat-filename-pattern
bulkstats_%YYYY%MM%DD%hh%mm%ss type HA edr-file-path
/California/edr111
bulkstat-file-path /California/bs111
```
Example output:

Adding IBs....
***************************************************************************Adding ib

dcRegionArea***************************************************************************

Adding in dcRegionArea.map
[dcRegionArea.map]:
   generated dc.id
   generated region.id
   generated area.id
   generated dcRegionArea.id.map

Summary:
--------
Successful IBs : 1 out of 1
Failed IBs : No id generation failures.
pushing ib [dc.id] to all IB destinations
pushing ib to ip 192.168.151.173
This product may be covered by one or more U.S. or foreign pending or issued patents listed at www.guavus.com/patents.

Guavus Network Systems NetReflex Platform

dc.id

    100%  133    0.1KB/s  00:00

This product may be covered by one or more U.S. or foreign pending or issued patents listed at www.guavus.com/patents.

Summary:
--------
Successful Transfers : 4 out of 4
Failed Transfers : No transfer failures.
pushing ib [region.id] to all IB destinations
pushing ib to ip 192.168.151.173
This product may be covered by one or more U.S. or foreign pending or issued patents listed at www.guavus.com/patents.

Guavus Network Systems NetReflex Platform

region.id

100% 86 0.1KB/s 00:00

**************************Added ib
dcRegionArea**************************

**************************Adding ib
gateway**************************
Adding in gateway.map
[key.map]:
  generated key.id.map
[gateway.map]:
  generated gateway_bs.id
  generated version_bs.id
  generated dc_bs.id
  generated region_bs.id
  generated area_bs.id
  generated gatewayRegionArea.id.map
[schema.map]:
  generated schema.id.map
[metric.map]:
  generated metric.id.map
[gatewayIDVersion.map]:

Summary:
Successful IBs : 5 out of 5
Failed IBs : No id generation failures.
pushing all ibs to all IB destinations
pushing ib to ip 192.168.151.173
This product may be covered by one or more U.S. or foreign pending or issued patents listed at www.guavus.com/patents.

Guavus Network Systems NetReflex Platform

gatewayIDVersion.map 100%  113  0.1KB/s  00:00
schemaIDToKeyID.map 100%  8018  7.8KB/s  00:00
Gateway_Schema_ASR.map 100%  1779KB  1.7MB/s  00:00
Gateway_Schema_GMPLAB1.map 100%  1779KB  1.7MB/s  00:00
Gateway_Schema_GMPLAB2.map 100%  1779KB  1.7MB/s  00:00
Gateway_Schema_NewDelhi.map 100%  1779KB  1.7MB/s  00:00
Gateway_Schema_gmplab1.map 100%  1779KB  1.7MB/s  00:00
Gateway_Schema_gmplab2.map 100%  1779KB  1.7MB/s  00:00
gatewaySchemaMetric.map 100%  10MB  10.4MB/s  00:00
key.id.map 100%  1375  1.3KB/s  00:00
key.map 100%  748  0.7KB/s  00:00
gateway_bs.id 100%  113  0.1KB/s  00:00
version_bs.id 100%  12  0.0KB/s  00:00
dc_bs.id 100%  113  0.1KB/s  00:00
region_bs.id 100%  31  0.0KB/s  00:00
area_bs.id 100%  34  0.0KB/s  00:00
gatewayRegionArea.id.map 100%  228  0.2KB/s  00:00
gateway.map 100%  178  0.2KB/s  00:00
schema.id.map 100%  1883  1.8KB/s  00:00
schema.map 100%  816  0.8KB/s  00:00
subschema_definition.list 100%  1007KB  1.0MB/s  00:00
metric.id.map 100%  679KB  679.1KB/s  00:00
metric.map 100%  471KB  471.1KB/s  00:00
This product may be covered by one or more U.S. or foreign pending or issued patents listed at www.guavus.com/patents.

Guavus Network Systems NetReflex Platform

_DONE

Summary:
========
Successful Transfers : 4 out of 4
Failed Transfers : No transfer failures.

Adding Gateway configs....

Name: gmplab2
Associated Region: EAST
Location: USA
Schema Version: 14
IP: 10.10.10.255
Timezone: America/Recife
Flow-EDR/Http-EDR Filename Pattern: %DC_MURAL-edr_*_%MM%DD%YYYY%hh%mm%ss*.gz
Bulkstat Filename Pattern: *_%YYYY%MM%DD%hh%mm%ss
Type: HA
Flow-EDR/Http-EDR Filename Path: /data/collector/California/edr111
Bulkstat Filename Path: /data/collector/Graham/bs111

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. Verify the IP addresses for all Collectors:

   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:
7. Generate and push all IBs:

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

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

pm extension > quit
(config) # write memory
```

**Synchronize the EDR and BulkStats 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.

To fetch IBs for EDR data streams:

```
pmx
```

```
pm extension > subshell aggregation_center
pm extension (aggregation center) > fetch all ibs from inbox

Copying IB mobileappname.list [OK]
Copying IB segment.map [OK]
Copying IB apnGroup.map [OK]
Copying IB snAppCat.map [OK]
Copying IB privateKey.txt [OK]
Copying IB apnNetworkIB.map [OK]
Copying IB segment.txt [OK]
Copying IB dcNameClli.map [OK]
Copying IB ReservedNames.json [OK]
Copying IB collection_center.list [OK]
Copying IB ratidtype.map [OK]
Copying IB wngib.id.map [OK]
Copying IB pcsarange.list [OK]
Copying IB ServiceGateway.list [OK]
Copying IB dcRegionArea.map [OK]
```
Copying IB mobileappcategory.list [OK]
Copying IB model.list [OK]
Copying IB snAppIdStr.map [OK]
Copying IB UnresolvedTraps [OK]
Copying IB subdevice.id.mph [OK]
Copying IB ipGgsn.map [OK]
Copying IB keyword.list [OK]
Copying IB sp.list [OK]
Copying IB url.list [OK]
Copying IB ipSgsn.map [OK]
Copying IB SNMPRecordConverterConfig [OK]
Copying IB blacklist [OK]
Copying IB mobileapptype.list [OK]
Copying IB ivFile.txt [OK]
Copying IB smartDG.list [OK]
Copying IB ipProto.map [OK]
Copying IB mime.list [OK]
Copying IB topsubscriberib.id.map [OK]
Copying IB p2pCat.map [OK]
Copying IB tac_manuf_model.map [OK]
Copying IB subseg.id.map [OK]
Copying IB sp_url_cat.map [OK]
Copying IB symmetricKey.txt [OK]
Copying IB manufacturer.list [OK]
Copying IB IBStore.tab [OK]
Copying IB category.list [OK]
Copying IB ua_mobile_app.map [OK]
Copying IB subscriberib.id.map [OK]
Copying IB port_proto_app.map [OK]
Copying IB ua_manuf_model.map [OK]
Copying IB mobileapppname.id [OK]
Copying IB bytes.id [OK]
Copying IB segmentname.id [OK]
<table>
<thead>
<tr>
<th>Copying IB segment.id.map [OK]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copying IB apn.id [OK]</td>
</tr>
<tr>
<td>Copying IB group.id [OK]</td>
</tr>
<tr>
<td>Copying IB apnGroup.id.map [OK]</td>
</tr>
<tr>
<td>Copying IB snAppProtocolStr.id [OK]</td>
</tr>
<tr>
<td>Copying IB snAppCategory.id [OK]</td>
</tr>
<tr>
<td>Copying IB snAppCat.id.map [OK]</td>
</tr>
<tr>
<td>Copying IB ratid.id [OK]</td>
</tr>
<tr>
<td>Copying IB rattype.id [OK]</td>
</tr>
<tr>
<td>Copying IB ratidtype.id.map [OK]</td>
</tr>
<tr>
<td>Copying IB dc.id [OK]</td>
</tr>
<tr>
<td>Copying IB region.id [OK]</td>
</tr>
<tr>
<td>Copying IB area.id [OK]</td>
</tr>
<tr>
<td>Copying IB dcRegionArea.id.map [OK]</td>
</tr>
<tr>
<td>Copying IB mobileappcategory.id [OK]</td>
</tr>
<tr>
<td>Copying IB model.id [OK]</td>
</tr>
<tr>
<td>Copying IB snAppid.id [OK]</td>
</tr>
<tr>
<td>Copying IB snAppStr.id [OK]</td>
</tr>
<tr>
<td>Copying IB snAppIdStr.id.map [OK]</td>
</tr>
<tr>
<td>Copying IB ggsnip.id [OK]</td>
</tr>
<tr>
<td>Copying IB ggsn.id [OK]</td>
</tr>
<tr>
<td>Copying IB ipGgsn.id.map [OK]</td>
</tr>
<tr>
<td>Copying IB sp.id [OK]</td>
</tr>
<tr>
<td>Copying IB url.id [OK]</td>
</tr>
<tr>
<td>Copying IB sgsnip.id [OK]</td>
</tr>
<tr>
<td>Copying IB sgsn.id [OK]</td>
</tr>
<tr>
<td>Copying IB ipSgsn.id.map [OK]</td>
</tr>
<tr>
<td>Copying IB mobileapptype.id [OK]</td>
</tr>
<tr>
<td>Copying IB ipProtocolId.id [OK]</td>
</tr>
<tr>
<td>Copying IB ipProtocolStr.id [OK]</td>
</tr>
<tr>
<td>Copying IB ipProto.id.map [OK]</td>
</tr>
<tr>
<td>Copying IB mime.id [OK]</td>
</tr>
<tr>
<td>Copying IB p2pProtocolStr.id [OK]</td>
</tr>
</tbody>
</table>
Copying IB p2pCategory.id [OK]
Copying IB p2pCat.id.map [OK]
Copying IB manufacturer.id [OK]
Copying IB category.id [OK]
Copying IB Destport.id [OK]
Copying IB ipProtoStr.id [OK]
Copying IB appProtoStr.id [OK]
Copying IB port_proto_app.id.map [OK]

pm extension (aggregation center)>

pm extension (aggregation center) > quit

pm extension > quit

COL-02 [COL-VIP: standby] (config) # write mem

COL-02 [COL-VIP: standby] (config) #

**Fetching BulkStats IBs**

To configure your MURAL environment to evaluate BulkStats data, go to the bulkstats PMX subshell and fetch the IBs from the inbox:

```plaintext
(config) # pmx
pm extension> subshell bulkstats
pm extension (bulk stats) > fetch allibs from inbox
Copying IB gatewaySchemaMetric.map [OK]
Copying IB gatewayIDVersion.map [OK]
Copying IB key.map [OK]
Copying IB gateway.map [OK]
Copying IB schema.map [OK]
Copying IB subschema_definition.list [OK]
Copying IB metric.map [OK]
Copying IB cube_names.list [OK]
Copying IB key.id.map [OK]
Copying IB gateway_bs.id [OK]
Copying IB version_bs.id [OK]
Copying IB dc_bs.id [OK]
Copying IB region_bs.id [OK]
```
Copy IB area bs.id [OK]
Copy IB gatewayRegionArea.id.map [OK]
Copy IB schema.id.map [OK]
Copy IB metric.id.map [OK]

**Create File for Uncategorized URL, UA, and TAC Reports**

To create the file needed for reports for uncategorized URLs, UAs, and TACs:

1. Create a file on the master Collector node containing the destination information, to which the uncategorized URL, UA, and TAC reports will be copied, as shown:

   **File**: /data/work/serverFile_uncatReports

   "serverFile_uncatReports" contains the entry for data transfer destination. This file has the following format:

   **Example:**

   192.168.156.96, admin, password, /data/offline_uncat_reports

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

2. Log in to the master Collector node:

   ```
   > en
   # _shell
   # cd /data
   # cd work
   # vi /data/work/serverFile_uncatReports
   ```

   192.168.156.96, admin, password, /data/TTYT

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

3. Create the same file on the standby Collector node.
Single Certificate Installation

This section provides instructions for generating and installing a common certificate for all Tomcat processes on the distributed Rubix setup. The example shown is based on generating and using a certificate with the Microsoft CA. However, when deploying the MURAL application, you can use any third party CA (Verisign, for example).

Note: MURAL supports the Mozilla Firefox and Chrome browsers.

Backing Up and Generating the Keystore Files

1. Log in to the master Rubix node and make a backup of the original keystore.

   ```
   mv /data/apache-tomcat/apache-tomcat-7.0.27/keystore /data/apache-tomcat/apache-tomcat-7.0.27/keystore_orig
   ```

2. Generate the new keystore file following the steps below:

   ```
   cd /usr/java/latest/bin/
   ./keytool -keysize 2048 -genkey -alias tomcat -keyalg RSA -keystore keystore
   ```

The keytool command prompts for the following values:

- **password**—rubix123
- **first and last name**—The fully-qualified domain name, or URL, you are securing. If you are requesting a wildcard certificate, add an asterisk (*) to the left of the common name where you want the wildcard; for example, 
  ```
  ```
- **Organizational Unit**—Optional
- **Organization**—The full legal name of your organization (for example, CompanyName)
- **City/Locality**—Name of the city in which your organization is registered/located; do not abbreviate
Cisco MURAL Software Installation Guide

- **State/Province**—Name of state or province where your organization is located; do not abbreviate
- **Country Code**—The two-letter International Organization for Standardization (ISO) format country code for where your organization is legally registered.

Enter keystore password:
Re-enter new password:
What is your first and last name?
   [Unknown]: *.companyname.com
What is the name of your organizational unit?
   [Unknown]:
What is the name of your organization?
   [Unknown]: Company Name
What is the name of your City or Locality?
   [Unknown]: Boston
What is the name of your State or Province?
   [Unknown]: Massachusetts
What is the two-letter country code for this unit?
   [Unknown]: US
Is CN=*.companyname.com, OU=Unknown, O=Guavus, L=Gurgaon, ST=Haryana, C=IN correct?
   [no]: yes
Enter key password for <tomcat>
   (RETURN if same as keystore password):
   [admin@UI-147-17 bin]#

3. Run the following command to create a CSR file called **csr.csr**:

   [admin@UI-147-17 bin]# ./keytool -certreq -keyalg RSA -alias tomcat -file csr.csr -keystore keystore

   When prompted for the keystore password, type the same password as for the last prompt in step 2.

4. Open the CSR file, and copy all of the text.

   [admin@UI-147-17 bin]# vi csr.csr
5. Paste all of the text into the online request form, as described in the following steps, and complete your application.

**Downloading the Signed Certificate**

2. Enter your username and password.
3. From the list of tasks, select **Request a certificate**.
4. Select **Advanced Certificate Request** from the next screen.
5. On the next screen, **Submit a Certificate Request or Renewal Request**, enter the CSR generated above (in the csr.csr file) and select **Web Server** from the Certificate Template.
6. Click **Download certificate** to download the CA certificate.

   The certificate you requested is issued.

7. Rename the downloaded file to **tomcat.cer**.
8. Place the file **tomcat.cer** on the same path on the server where the keystore is generated: `/usr/java/latest/bin/`

   ```
   scp tomcat.cer admin@172.16.10.0:/usr/java/latest/bin
   ```

**Downloading the CA Certificate**

2. Enter your username and password.
3. From the list of tasks, select the task **Download a CA certificate, certificate chain, or CRL**.
4. On the next screen, select **Download CA certificate**.
5. Rename the downloaded file to **root.cer** and place the file on the same path on the server where the keystore is generated:

   `/usr/java/latest/bin/`

   ```
   scp root.cer admin@172.16.10.0:/usr/java/latest/bin
   ```

6. Click on the **Install CA certificate** link.

   **Note:** This option should be used on all client machines to install the CA certificate on the client, which will be able to identify the
7. Click all the check boxes and then click **OK**.

**Note:** If the CA certificate is already installed, the following message is displayed:

![Alert](image)

**Installing the Signed Certificate in the Keystore**

For the CA GUAVUS-MX1-CA, the root (CA) certificate and signed certificates (downloaded using the steps given above) need to be added to keystore.

1. Using keytool, enter the following commands to install the signed certificates and root certificate

   Enter the keystore password and type **yes** to accept the certificate:

   ```bash
   [admin@UI-147-17 bin]# ./keytool -import -alias root -keystore keystore
   -trustcacerts -file root.cer
   ```

   Enter keystore password:

   Owner: CN=Guavus-MX1-CA, DC=guavus, DC=com
   Issuer: CN=Guavus-MX1-CA, DC=guavus, DC=com
   Serial number: 7570961243691e8641088832d6c218a5
   Certificate fingerprints:
   Signature algorithm name: SHA1withRSA
   Version: 3
   Extensions:
   #1: ObjectId: 2.5.29.19 Criticality=true
   BasicConstraints:[
   CA:true
PathLen:2147483647
]
#2: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [ 
  DigitalSignature
  Key_CertSign
  Crl_Sign
]
#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [ 
  KeyIdentifier [ 
    0000: D4 DA C9 FC FB AF 5E 32 BF C0 A3 F1 6F 03 39 C3
    ......^2....o.9.
    0010: 29 36 84 7D )6..
  ]
]
#4: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
Trust this certificate? [no]: yes
Certificate was added to keystore

2. Install the signed certificate:

[admin@UI-147-17 bin] # /keytool -import -alias tomcat -keystore keystore -trustcacerts -file tomcat.cer

3. Enter the keystore password.

The certificate reply was installed in keystore

4. Copy the new keystore to the apache-tomcat-7.0.27 directory for all EDRs, Bulkstats and RGE on both master and standby machines.

[admin@UI-147-17 bin] # cp keystore /data/apache-tomcat/apache-tomcat-7.0.27/
[admin@host apache-tomcat-7.0.27] # scp keystore admin@192.168.147.20:/data/apache-tomcat/apache-tomcat-7.0.27/

**Note:** 192.168.147.20 is the management IP address of the standby Rubix node.

5. Verify that the keystorePass in server.xml of all Tomcat processes is the same as the keystore password given above:
# vi /data/apache-tomcat/apache-tomcat-7.0.27/conf/server.xml

```xml
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
  maxThreads="150" scheme="https" secure="true"
  keystoreFile="keystore"
  keystorePass="rubix123"
  clientAuth="false" ciphers="SSL_RSA_WITH_RC4_128_MD5,
  SSL_RSA_WITH_RC4_128_SHA" sslProtocol="TLS" />
```
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

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

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`

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 /`  
   `UsePAM no`  
   `PasswordAuthentication yes`

3. Run the `pm process sshd restart` command:

   `# en`  
   `> conf t`  
   `(config)> pm process sshd restart`  
   `(config)> _shell`  
   `# mount -o remount,ro /`

4. Repeat steps 1 through 3 on the standby Collector node.
Ingesting the 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.

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 the System Installations

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

Validating Data on the Collector Nodes

1. Login to the master Collector node:

```
> en
# __shell
```

2. Run the following two commands:

```
# 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
```

If the Collector node is receiving data in the expected format, it retains the data in HDFS.

**Note:** Specify the year, month day, hour, and minute for which data is being sent to the MURAL system; minutes are always in multiples of 5 - 00,05,10,....55.

These directories and files are updated continuously as the data keeps coming in.

3. Run the following command:

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

If the Collector is receiving data in the expected format, it will retain the data in HDFS.
Note: Specify the year, month, day, hour, and minute for which data is being sent to the MURAL system; minutes are always in multiples of 5 - 00,05,10,....55.

Setting the Data Start Time

To set the data start time in the configuration:

1. Log in to the GMS server:

   ```
   > en
   # _shell
   # mount -o remount,rw /
   # cd /opt/deployment/Mural_setStartTime/
   # ./setOozieTime --dataStartTime data-start-time --node collector-mgmt-IP --password admin-password --verbose
   ```

2. Execute the script to set the data start times to the time from which EDR and BulkStats data starts coming into the Hadoop system from the previous section, "Data Validation on the Collector Node."

   For example, if EDR and Bulk Stats 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 --verbose
   ```

   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 Collector nodes.

Starting the Data Processing

Log in to the master Collector/Name 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.

**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.

*Note:* Wait two hours after completing the above steps before doing the checks described in this section. This allows sufficient time for the jobs that process the collector data to start, and the **done.txt** files to be updated.

**Validating EDR Data**

All commands in this section are to be executed on the master Collector node.

1. Check the last timestamp for EDR data cubes being generated by the EDR job from the master Collector node.

```
> en
# _shell
[admin@collector-1 0000041-121020165932574-oozie-admi-W]
# hadoop dfs -text /data/EDR/done.txt 2>/dev/null
```

2. Check the last timestamp for CubeExporter data cubes being exported.

```
[admin@collector-1 0000041-121020165932574-oozie-admi-W]
# hadoop dfs -text /data/CubeExporter/done.txt 2>/dev/null
```

3. Check the last timestamp for BulkStat Cubes being generated by the BulkStat Job:

```
[admin@host ~]
# hadoop dfs -text /data/BulkStat/done.txt 2>/dev/null
# hadoop dfs -text /data/BSAgg15min/done.txt 2>/dev/null
```

4. Check the last timestamp for BulkStat data cubes being exported.

---

*Copyright © 2014, Cisco Systems, Inc.*
Validating Data on the Insta Blades

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

```
INSTA-01 [INSTA-CLUST: master] > en MUR-INSTA-01 [INSTA-CLUST: master] # _shell
[admin@MUR-INSTA-01 ~]# cli -t "en" "conf t" "show runn full" |
grep "insta instance 0 cubes-database" | awk -F ' ' '{print $5}'
DATABASE_MURAL
```

2. Connect to idbmysql and select the database:

```
[admin@MUR-INSTA-01 ~]# idbmysql
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 151
Server version: 5.1.39 MySQL Embedded / Calpont InfiniDB Enterprise 2.2.9.1-1 GA (Commercial)
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql>
mysql> use DATABASE_MURAL;
Database changed
```

3. Get the value for the **mints** and **maxts** field for -1 aggregation level and 60 minute bin class:

```
mysql> select * from bin_metatable;
+-------------------------+-------------------------+-------------------------+-------------------------+-------------------------+
| binclass | aggregationinterval | mints | maxts | bintype |
+-------------------------+-------------------------+-------------------------+-------------------------+-------------------------+
```
4. Convert the date format Run the `date` command with the value of `maxts` captured from the step above. The example shows the user has processed data from Oct 13 11:00 to Oct 18 21:00.

```
[admin@MUR-INSTA-01 ~]# date -d @1350126000 Sat Oct 13 11:00:00 UTC 2012
[admin@MUR-INSTA-01 ~]# date -d @1350594000 Thu Oct 18 21:00:00 UTC 2012
```

Validating Bulk Stats Data on the Insta Blade

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

```
INSTA-01 [INSTA-CLUST: master] > en
INSTA-01 [INSTA-CLUST: master] # _shell
[admin@INSTA-01 ~]# cli -t "en" "conf t" "show runn full" | grep "insta instance 1 cubes-database" | awk -F ' ' '{print $5}' 'bulkstats
```

2. Connect to `idbmysql` and select the database:

```
[admin@host ~]# idbmysql
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 151
```
3. Select the data from the table. Run the following command to get the value for the **mints** and **maxts** field for 900 aggregation interval:

```
mysql> select * from bin_metatable;
+-----------------+-----------------+------------------+------------------+-------------------|
| binclass | aggregationinterval | mints | maxts |
| binType | |
+-----------------+-----------------+------------------+------------------+-------------------|
| 5min | -1 | 0 | 0 |
| NULL | |
| 5min | 900 | 1364713200 | 1367293500 | |
| NULL | |
| 5min | 3600 | 1364713200 | 1365004800 | |
| NULL | |
| 5min | 86400 | 1364688000 | 1364860800 | |
| 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. This shows we have processed data from 132

Copyright © 2014, Cisco Systems, Inc.
Starting UI Processes and Verifying Data

These final steps include starting the UI processes and verifying the data on the UI. 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 and start the EDR process:

   ```
   > en
   # conf t
   (config) # pm process rubix restart
   (config) # rubix modify-app atlas enable
   (config) # rubix modify-app atlas modify-instance 1 enable
   ```

2. Log in to the standby UI node and start the EDR process:

   ```
   > en
   # conf t
   (config) # pm process rubix restart
   (config) # rubix modify-app atlas enable
   (config) # rubix modify-app atlas modify-instance 1 enable
   ```

   **NOTE:** Wait for two minutes before moving to the next step.

3. Login to Master UI node and start other processes:

   ```
   (config) # rubix modify-app bulkstats enable
   (config) # rubix modify-app bulkstats modify-instance 1 enable
   ```
NOTE: Wait for two minutes before issuing the following commands.

```
(config) # rubix modify-app reportAtlas enable
(config) # rubix modify-app reportAtlas modify-instance 1 enable
```

NOTE: Wait for two minutes before issuing the following commands.

```
(config) # rubix modify-app rge enable
(config) # rubix modify-app rge modify-instance 1 enable
```

NOTE: Wait for two minutes before moving to the next step.

4. Login to the Standby UI node and start the other processes:

```
(config) # rubix modify-app bulkstats enable
(config) # rubix modify-app bulkstats modify-instance 1 enable
```

NOTE: Wait for two minutes before issuing the following commands.

```
(config) # rubix modify-app reportAtlas enable
(config) # rubix modify-app reportAtlas modify-instance 1 enable
```

NOTE: Wait for two minutes before issuing the following commands.

```
(config) # rubix modify-app rge enable
(config) # rubix modify-app rge modify-instance 1 enable
```

5. Access the UIs by going to the URL https://domain-name:8443/ through your browser.
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:

<table>
<thead>
<tr>
<th>URL</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://demo.cisco.com:8443/">https://demo.cisco.com:8443/</a></td>
<td>Username: admin&lt;br&gt;Password: admin123</td>
</tr>
</tbody>
</table>

**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.

Click the following ports once and accept the certificates:

<table>
<thead>
<tr>
<th>URL</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://domainName:20443/">https://domainName:20443/</a></td>
<td></td>
</tr>
<tr>
<td><a href="https://domainName:30443/">https://domainName:30443/</a></td>
<td></td>
</tr>
</tbody>
</table>

For example:

<table>
<thead>
<tr>
<th>URL</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://demo.cisco.com:20443/">https://demo.cisco.com:20443/</a></td>
<td></td>
</tr>
<tr>
<td><a href="https://demo.cisco.com:30443/">https://demo.cisco.com:30443/</a></td>
<td></td>
</tr>
</tbody>
</table>

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

```

1381518310,1381518337,1000000018,70000,29,20000,20000,182,36,iax,27.9.126.155,2,1,FromMobile,,,2.2.2.1,27.23.157.2,1381518337,1381518337,10,Sushfone-2,231-10-1073-10065,43769,1985,rb31,,2
```
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

Sample:

```plaintext

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,Ssuffix-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:

```plaintext
edr-format edr-flow-format
attribute sn-start-time format seconds priority 1
rule-variable ip subscriber-ip-address priority 4
attribute sn-subscriber-port priority 6
attribute sn-start-time format seconds priority 10
```
attribute sn-charge-volume ip pkts uplink priority 12
attribute sn-charge-volume ip pkts downlink priority 13
attribute sn-charge-volume ip bytes uplink priority 14
attribute sn-charge-volume ip bytes downlink priority 15
attribute sn-direction priority 21
rule-variable bearer ggsn-address priority 23
rule-variable bearer 3gpp2 bsid priority 24
attribute sn-flow-start-time format seconds priority 26
attribute sn-flow-end-time format seconds priority 27
attribute sn-flow-id priority 28
attribute sn-closure-reason priority 29
attribute radius-calling-station-id priority 30
rule-variable p2p protocol priority 31
rule-variable bearer 3gpp imsi priority 35
attribute radius-called-station-id priority 40
rule-variable ip server-ip-address priority 60
attribute sn-server-port priority 70
attribute sn-app-protocol priority 80
attribute sn-parent-protocol priority 81
rule-variable ip protocol priority 82
attribute sn-volume-amt ip bytes uplink priority 100
attribute sn-volume-amt ip bytes downlink priority 110
attribute sn-volume-amt ip pkts uplink priority 120
attribute sn-volume-amt ip pkts downlink priority 130
rule-variable bearer 3gpp charging-id priority 140
rule-variable bearer 3gpp imei priority 141
rule-variable bearer 3gpp rat-type priority 142
rule-variable bearer 3gpp user-location-information priority 143
rule-variable bearer 3gpp sgsn-address priority 144
rule-variable traffic-type priority 160
rule-variable voip-duration priority 170
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
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 43.

The master General Management Server (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 EMC setup.
- 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
   
   `/data/mfgcd-guavus-x86_64-20140315-133212.iso`

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

   ```
   # md5sum /data/mfgcd-guavus-x86_64-20140315-133212.iso
   48fc39f77bc7ab8847ca2f7a684d2ace /data/mfgcd-guavus-x86_64-20140315-133212.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.

Click **OK** to clear the keyboard access warning message that appears.

The console for the port opens.

4. 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. Access 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 **Enter Setup** to open the setup utility.

9. 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.
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
```

Output similar to the following traces the manufacturing process.

```
Running /etc/in it .d/rcS .d/S34automf g
- Automatic manufacture is not enabled. Type ‘automf g’ to start it.

BusyBox v1.00 (2010.12.03-23:16+0000) Built-in shell (ash)
Enter ‘help’ for a list of built-in commands.

-sh: can’t access tty: job control turned off

Processing /etc/profile... Done

# manufacture.sh -v -t -f /mnt/cdrom/image.img
====== Starting manufacture at YYYYMMDD-hhmmss
```
Called as: /sbin/manufacture.sh -v -t -f /mnt/cdrom/image.img

Manufacture script starting

Model selection

Product model (‘?’ for info) ( DESKTOP VM VM_2D 1D 2D 3D 4D 2D_EXT4)
[2D]: 2D

== Using model: 2D

Kernel type selection

Kernel type (uni smp) [smp]:
== Using kernel type: smp

Layout selection

Layout (STD) [2D]:
== Using layout: 2D

Partition name-size list selection

Partition name-size list [VAR 40960 SWAP 40960 ]:
== Using partition name-size list: VAR 40960 SWAP 40960

Device list selection

Device list [/dev/sda /dev/sdb]
== Using device list: /dev/sda /dev/sdb

Interface list selection
Interface list [eth0 eth1]:
== Using interface list: eth0 eth1

Interface naming selection
Interface naming [none]:
== Using interface naming: none
== Smartd enabled

CMC server settings
Enable CMC server (yes no) [yes]: no
== CMC server enabled: no

CMC client settings
Enable CMC client (yes no) [yes]: no
== CMC client enabled: no
== CMC client auto-rendezvous enabled: no
== CMC server address for rendezvous: (none)

Cluster settings
Enable cluster (yes no) [no]: no
== Cluster enable: no
Cluster ID:

Number Start End Size File system Name Flags
1 0.02MiB 30000MiB 30000MiB ext3 primary

Writing partition table to DISICZ
Disk dev: /dev/sdb

Copyright © 2014, Cisco Systems, Inc.
Sector size (logicalphysical): 512B,512B
Partition Table: gpt
Number Start End Size File system Name Flags
1 0.002MiB 5232MiB 5232MiB ext3 primary

== Making filesystems
== Creating ext3 filesystem on /dev/sda2 for BOOT1
== Creating ext3 filesystem on /dev/sda3 for BOOT2
== Creating ext3 filesystem on /dev/sda1 for BOOTMGR
== Creating ext3 filesystem on /dev/sda8 for CONFIG
== Nothing to do on /dev/sda9 for HA
== Creating ext3 filesystem on /dev/sda5 for ROOT1
== Creating ext3 filesystem on /dev/sda6 for ROOT2
== Making swap on /dev/sda7 for SWAP
Setting up swapspace version 1, size = 42952404 kB
== Creating ext3 filesystem on /dev/sda10 for VAR

== CMC server address for rendezvous: (none)

-------------------------------------------
Cluster settings
-------------------------------------------
== Cluster enable: no
Cluster ID:
== Cluster ID: (none)
Cluster description:
== Cluster description: (none)
Cluster interface:
== Cluster interface: (none)
Cluster master virtual IP address [0.0.0.0]:
== Cluster master virtual IP address: 0.0.0.0
Cluster master virtual IP masklen [0]:
== Cluster master virtual IP masklen: 0
Cluster shared secret:
== System successfully imaged
  Writing Host ID: 3b0455ef813d
== Zeroing the destination partition disk /dev/sda9 with dd
== Calling imgverify to verify manufactured system
== Using layout: ZD
Using dev list: /dev/sda /dev/sdb
== 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 YYYYMMDD–hhmmss
— Manufacture done.
#

11. In the UCS-KVM Launch Manager, navigate to **KVM Console > Virtual Media** and click the check box in the **Mapped** column of the ISO image file, to remove the check and unmount the file.

12. Run the **reboot** command to reboot the node with the new ISO image.
13. Use SSH to log in to the master GMS blade as user admin. Continue to "Setting Up the Master GMS Node" on page 55.
# 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.
Cisco MURAL Software Installation Guide

**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.

**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.

**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.
GMS node  General Management Server. 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).
Cisco MURAL Software Installation Guide

**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.
<table>
<thead>
<tr>
<th><strong>Uplink Rate</strong></th>
<th>The average bytes sent from the mobile device out to the Internet during a selected interval.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Uplink Tonnage</strong></td>
<td>The total amount of data sent from the mobile device out to the Internet.</td>
</tr>
</tbody>
</table>

**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.