MURAL Software Installation Guide for Medium Pack with VMWare

Version 3.4.2

Published: 2015-01-30

Copyright © 2015, Cisco Systems, Inc.
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. CISCO DOES NOT WARRANT AGAINST INTERFERENCE WITH THE ENJOYMENT OF THE SOFTWARE OR AGAINST BREACH OF THE WARRANTY, IF ANY, INCLUDED IN THE SOFTWARE. FURTHERMORE, CISCO IS NOT LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOSS PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

MURAL Software Installation Guide for Medium Pack with VMWare

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

Installation Overview ................................................................. 9
Before You Begin ........................................................................ 9
System Components .................................................................... 10
Hardware .................................................................................... 12
Installation Package .................................................................... 13
Customer Information Questionnaire ........................................... 13
Installation Process Steps ............................................................. 13

Verifying UCS Hardware Configuration for MURAL ......................... 14
Before You Begin ........................................................................ 14
Reviewing Hardware Setup ........................................................... 14
Verifying Slot Assignments for Blades ......................................... 15
Verifying Physical Connections to the Fabric Interconnects .......... 17
Setting the Base Configuration for the UCS System ...................... 22

Configuring UCS for MURAL .......................................................... 25
Configuring Direct Attachments to External SANs ...................... 26
Configuring System Profiles for the Cisco UCS Manager ............... 40

Allocating Storage on the EMC .................................................... 45
EMC Hardware Installation Prerequisites ...................................... 47
Configuring IP Addresses for the EMC System ............................. 48

Installing Vmware on Bare Metal Servers ...................................... 49

Configuring the VCenter Server for Bare Metal Installation ........... 60
Accessing the VCenter Server ....................................................... 60
Creating a New DataCenter .......................................................... 61
MURAL Software Installation Guide for Medium Pack with VMWare

Validating Data on the Nodes ................................................................. 120
Validating Data on the Compute Blades (Data Nodes) ........................... 121
Validating Bulk Stats Data on the Insta Blade ..................................... 123
Starting UI Processes and Verifying Data ........................................... 124
Updating Whitelists ........................................................................... 126

Setting Up Offline Reports ................................................................. 128
Uncategorized URL, UA, and TAC Reports .......................................... 128
Tethering Reports ............................................................................. 128

Glossary ......................................................................................... 130
Installation Overview

This document describes how to install the Mobility Unified Reporting and Analytics (MURAL) application.

Before You Begin

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

- Linux operating system

Before you begin the installation, we recommend that you:

- Review the Release Notes for MURAL
- Locate the Customer Information Questionnaire (CIQ) for the deployment; see "Customer Information Questionnaire" on page 13
- Verify that each Fabric Interconnect is connected to the storage area network (SAN) controllers through fiber cables.
- Verify all that UCS B200 M2/M3 blade servers are physically installed in the UCS 5108 Blade Server Chassis and that the nodes of all types (Compute, UI/Caching, GCN, Insta, and so on) are connected to the UCS 6248 Fabric Interconnect. The number of each type of node depends on your deployment.

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

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

The figure depicts each type of node as a separate logical entity. In larger deployments there is often a separate blade for each type of node, whereas in smaller deployments a blade might host multiple types of nodes.

Medium Pack Setup

The MURAL system installation for the Medium Pack setup nodes topology is as follows:
**Note:** Throughout this document, master nodes and standby nodes shown above are referred as master GCN node and Standby GCN node, respectively. All references to Collector and Rubix nodes are referred to as the GCN node.

The MURAL platform (Medium Pack Setup) nodes perform the following functions:

- **GCN node**—In Medium Pack Setup, GCN node hosts GMS, Collector and Name Node components all together in one server. Medium Pack setup can be used where only a few gateways are connected to MURAL system. The GCN node cluster has two servers with 1+1 redundancy.

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

The Collector node cluster can have any number of servers, in pairs for master and standby and uses 1+1 redundancy, meaning there is a dedicated standby node for each master node. Both nodes run actively so if the master node fails, the standby node takes over transparently with
minimal delay. The number of paired Collector nodes in a cluster depends on the deployment.

- **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 months, 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 Server (GMS) node**—Provides centralized management of the other MURAL nodes, such as remote manufacturing of blades (installing the MURAL software), patch management, monitoring of all nodes and operations, and importing and running node configurations. GMS HA supported by GCN node cluster.

**Hardware**

The MURAL nodes are hosted on a UCS 5108 Blade Server Chassis that consists GCN, UI, Compute and Insta nodes. Data storage is provided by EMC storage devices.

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

The MURAL software installation package contains the following components:

- An ISO image file. For the image name and associated MD5 checksum, refer to the Release Notes.
- The file, which is used by the master GCN node. This sample configuration file provides configuration settings for your setup based on the network topology information in the Customer Information Questionnaire (CIQ).
- Any software patches that apply to the release. A complete list appears in the Release Notes.
- Management information bases (MIBs)

Customer Information Questionnaire

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

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

Installation Process Steps
Verifying UCS Hardware Configuration for MURAL

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

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

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

Before You Begin

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

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

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

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

Reviewing Hardware Setup

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

- "Verifying UCS Hardware Configuration for MURAL" on the previous page
- "Verifying Physical Connections to the Fabric Interconnects" on page 17

**Verifying Slot Assignments for Blades**

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

**Notes:**

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

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

**Double Chassis for a Standard MURAL Deployment**

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

![Chassis 1 Diagram]

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

The following figure and table depict sample slot assignments Chassis 2.
## Chassis Slot Node

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

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

### Verifying Physical Connections to the Fabric Interconnects

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

### Verifying Connections to the Management Network

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

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

Connecting First Chassis

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

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

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

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

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

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

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

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

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

### Table: Port Description

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

Setting the Base Configuration for the UCS System

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

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

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

2. For fabric A, set the following parameters:

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

Where:

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

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration method</td>
<td>console</td>
</tr>
<tr>
<td>This fabric interconnect will be added to the cluster</td>
<td>Y</td>
</tr>
<tr>
<td>Admin password of interconnect</td>
<td>admin-password</td>
</tr>
<tr>
<td>Mgmt0 IP address</td>
<td>Fab-B-management-port-IP-address</td>
</tr>
</tbody>
</table>
MURAL Software Installation Guide for Medium Pack with VMWare

Where admin-password is the same as what was used for Fabric A.

You can now log in to the management UI from a web browser at http://ip-address-of-cluster.
Configuring UCS for MURAL

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

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

- **ucs-config-version-number.txt** (where version-number is the most recent version available)—The configuration parameters in this file are used by the UCS configuration script. You must update this file with your local setup details.
- **ucs-config.exp**—Sets configuration parameters for the UCS Fabric Interconnects, servers, LAN, and SAN.

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

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

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

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

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

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

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

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

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

- "Setting Fabric Interconnects to FC Switching Mode" below
- "Creating VSANs for Zoning" on the facing page
- "Designating Storage Ports and Assigning Storage Cloud VSANs" on page 29
- "Confirming the Storage Port WWPN is Logged Into the Fabric Interconnects" on page 31
- "Creating Storage Connection Policies" on page 33
- "Creating SAN Connectivity Policy" on page 35
- "Configuring SAN Cloud Policy" on page 36
- "Creating vHBA Initiator Groups" on page 38
- "Verifying Service Profile Templates" on page 39
- "Configuring System Profiles for the Cisco UCS Manager" on page 40

Setting Fabric Interconnects to FC Switching Mode

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

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

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

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

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

---

**Creating VSANs for Zoning**

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

By convention, the name of a VSAN includes the associated ID, in the format `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 pop-up window, enter a VSAN name that complies with the restrictions listed above, and the fabric identifier used in Step 1.

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

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

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

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

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

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

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

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

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

![Configure Unified Ports](image)

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

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

4. Wait until all Fabric Interconnects have rebooted.

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

6. In the main pane, make the following settings:

   a. In the Actions box, select Configure as FC Storage Port.

   b. In the Properties box, select the appropriate VSAN from the VSAN drop-down menu. In the following figure, vsan3010 is selected for Fabric Interconnect A.
7. Repeat Step 6 for **FC Port 32**.

8. Click **Save Changes**.

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

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

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

To confirm the storage port is logged into the Fabric Interconnects, perform the following steps:

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

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

```
hostname# connect nxos
```

Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2013, Cisco Systems, Inc. All rights reserved.
Note: You can run `?` in the prompt to get help.

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

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

The resulting output may resemble:

```
zoneset name hostname-vsan-3010-zoneset vsan 3010
 zone name hostname_A_8_U11_vHBA-A vsan 3010
   * fcid 0x6c0000 [pwnn 20:00:00:05:ad:1e:11:2f]
   * fcid 0x6c00ef [pwnn 50:06:01:68:3e:e0:0a:6b]
   * fcid 0x6c01ef [pwnn 50:06:01:60:3e:e0:0a:6b]

zone name hostname_A_7_GMS1_vHBA-A vsan 3010
   * fcid 0x6c0003 pwnn 20:00:00:05:ad:1e:11:4f
   * fcid 0x6c00ef [pwnn 50:06:01:68:3e:e0:0a:6b]
   * fcid 0x6c01ef [pwnn 50:06:01:60:3e:e0:0a:6b]

zone name hostname_A_6_INSTA1_vHBA-A vsan 3010
   * fcid 0x6c0004 [pwnn 20:00:00:05:ad:1e:11:7f]
   * fcid 0x6c00ef [pwnn 50:06:01:68:3e:e0:0a:6b]
   * fcid 0x6c01ef [pwnn 50:06:01:60:3e:e0:0a:6b]

zone name hostname_A_5_INSTA2_vHBA-A vsan 3010
   * fcid 0x6c0005 [pwnn 20:00:00:05:ad:1e:11:5f]
   * fcid 0x6c00ef [pwnn 50:06:01:68:3e:e0:0a:6b]
   * fcid 0x6c01ef [pwnn 50:06:01:60:3e:e0:0a:6b]
```

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

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

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

6. Run the **exit** command.

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

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

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

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

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

**Creating Storage Connection Policies**

Create a storage connection policy for each Fabric Interconnect.

To create storage connection policies, perform the following steps:

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

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

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

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

**Path**—`FI-ID`

**VSAN**—The VSAN created for the Fabric Interconnect in "Creating VSANs for Zoning" on page 27, such as `vsan3010` for Fabric Interconnect A

For example,

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

3. Repeat Step 2 for port 32.

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

The following example figure shows the result for Fabric Interconnect A. The settings from Step 2 are recorded in the **Fc Target Endpoints** box.
Creating SAN Connectivity Policy

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>Name</th>
<th>vhBA-A</th>
</tr>
</thead>
<tbody>
<tr>
<td>WWNN Assignment:</td>
<td>wnnn-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.
The following screen shows an example of two vHBAs initiator groups within one SAN connection policy. The section after the screen details the steps for creating a VHBA initiator group.

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 theSANtab 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. SelectSAN 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.

Copyright © 2015, Cisco Systems, Inc.
The following figure shows a vHBA configuration within a service template.

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

Configuring System Profiles for the Cisco UCS Manager

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

Ethernet Adapter Policy

Configure the Ethernet adapter policy for all Ethernet interfaces.

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

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

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

   **Note:** Ensure that the Resources and Options values are set correctly, as recommended in the table.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmit Queues</td>
<td>1</td>
</tr>
<tr>
<td>Transmit Checksum Offload</td>
<td>Enabled</td>
</tr>
<tr>
<td>Receive Queues</td>
<td>8</td>
</tr>
<tr>
<td>Receive Checksum Offload</td>
<td>Enabled</td>
</tr>
<tr>
<td>Ring Size</td>
<td>Default</td>
</tr>
<tr>
<td>Ring Size</td>
<td>Default</td>
</tr>
<tr>
<td>Completion Queues</td>
<td>9</td>
</tr>
<tr>
<td>Completion Queues</td>
<td>Default</td>
</tr>
<tr>
<td>Interrupts</td>
<td>16</td>
</tr>
<tr>
<td>Hyper Threading</td>
<td>Default</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>Execute Disable Bit</td>
<td>Default</td>
</tr>
<tr>
<td>Interrupt Coalescing type</td>
<td>Min</td>
</tr>
<tr>
<td>Interrupt Coalescing type</td>
<td>Min</td>
</tr>
<tr>
<td>Interrupt Timer</td>
<td>350</td>
</tr>
<tr>
<td>Interrupt Timer</td>
<td>350</td>
</tr>
</tbody>
</table>

**Bios Policy (Processor Page)**

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

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

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

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turbo Boost</td>
<td>Disabled</td>
</tr>
<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>
</tbody>
</table>
### Field Name | Field Value
---|---
Direct Cache Access | Enabled
Processor C State | Disabled
Processor C1E | Enabled
Processor C3 Report | Default
Processor C6 Report | Default
Processor C7 Report | Default
CPU Performance | hpc
Max variable MTRR Setting | Default

**Specifying Boot Order of Devices**

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

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

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

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

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

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

To set the RAID policy, perform the following steps:

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

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

3. In the Properties box, select **RAID 1 Mirrored** from the **Mode** drop-down
MURAL Software Installation Guide for Medium Pack with VMWare

menu, as shown in the figure:

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

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

Verify Zoning/FLOGI on the Fabric Interconnect

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

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

   **Note:** In the following output and figures, the identifiers are examples only and are different in your deployment. Also, the term 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]
```
Run the `show zoneset active` command again for the other Fabric Interconnect:

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

The resulting output may resemble:

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

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

4. Verify the zoning using UCS Manager.

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

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

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

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

**EMC Hardware Installation Prerequisites**

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

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

- The SPS is connected to the storage processor (SP) management ports according to the instructions in the EMC Unisphere installation guide, using the cables provided with the product.

- Power cords are connected for the following components according to the instructions provided in the EMC Unisphere installation guide.
  
  - From SPS A and SPS B to SP A and SP B
  
  - From SPS A and SPS B to power distribution units (PDUs)

- The Fibre Channel SFP+ transceiver, included with the hardware, is installed in ports 4 and 5 of both SP A and SP B.

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

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

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

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

**Configuring IP Addresses for the EMC System**

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

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

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

Proceed to next section once UCS and EMC hardware configurations are completed.
Installing Vmware on Bare Metal Servers

Download Vmware images (ESXI OS 5.5 and VCenter Server) onto a windows machine. Attach the image to DRAC of a blade so that blade can boot up with the new iso image.

To install the Vmware image on the blades:

1. Click **Add Image**...

2. Open the file named **VMware-VMvisor-Installer-5.5.0.update01-1623387.x86_64**

3. In the navigation bar, press Reset.

4. A warning pops-up. Select the radio button of **Power Cycle** and click **OK**.

5. Click **OK** in the next warning window.
6. In the MSDOS screen, select EFI:Cisco vKVM-Mapped vDVD1.22 CDROM File1 as the boot device.

![Image of boot device selection]

7. Wait while the system loads. When the window resembles the one shown below, press **Enter** to continue with the installation.

![Image of VMware ESXi 5.5.8 installation window]

8. rest
9. If a VMFS interface was previously installed on this drive, you will see an error message. Select the option to **Install ESXi, overwrite VMFS datastore**.

10. Press **F11** to accept the End user License Agreement.

11. Select the **US Default** keyboard layout.

12. Enter the password _____.

13. Press **F11** to confirm the installation.

14. When the installation is complete, the message on your screen will
MURAL Software Installation Guide for Medium Pack with VMWare

15. Remove the installation disk and reboot as directed.

To remove the disk, go back to the KVM console and uncheck the box for the vmware disk, under the **Mapped** column.

A warning pops-up. Acknowledge it by clicking **Yes**.

16. When the system reboots it prompts you for a Login name and password.

Use login name **root** and the same password you used in step 12.
17. Use arrow keys to select **Configure management Network**, and press **Enter**.

18. Modify the following settings to match your configuration:

   a. **IP Configuration:**
      - IP Address
      - Subnet Mask
      - Default Gateway

   b. **DNS Configuration:**
      - Primary DNS Server
      - Hostname

19. Press **Esc** to exit, and when prompted press **Y** to save your changes and
restart the management network.

20. Use arrow keys to select **Troubleshooting Options**, and press **Enter**.

21. **Enable/Disable SSH**.

Once VMware OS is installed on all the blades, you need to install VMware VCenter Server on a Windows machine. VCenter server is required so that all blades running VMware OS can be managed centrally and in turn Virtual Machines can be managed on them. The user account on the windows machine should have administrator privileges. Latest version of Adobe Flash must be installed on the windows machine.

Download VCenter Server from VMware website. The file would be a iso file. Mount it on a windows box and run the installation. Follow the below screenshots so as to install VCenter server.

1. Run **autorun.exe** when prompted.

2. When the installer opens, choose to do a **Custom Install**.
3. Click **vCenter Single Sign-On** in the grey navigation bar at left. Then click the **Install** button.

4. Click **Next** to begin the installation.

5. On the next slide, ensure the checkbox for **Add guavus.com as a native Active Directory identity source** is marked. Click **Next** again.

6. Select the radio button for **vcenter Single Sign-On for your first vCenter Server**. Click **Next** again.

7. Enter your password (twice) for the Administrator account of the vsphere.local domain. Click **Next** again.

8. Designate a site name, for example, **Default-First-Site**. Click **Next** again.

9. Enter the HTTPS port number as shown below. Click **Next** to continue.
10. If necessary, you can change the destination folder for **vCenter Single Sign-On**. Then click **Next** to complete the installation.

11. Review the installation details as shown below. If they are correct, click **Install**. If not, click **Back** to change the settings as needed.
12. When the Single Sign-On installation is complete, the Install Wizard returns you to the main screen. Select **vSphere Web Client** from the grey toolbar on the left and then click **Install**.

13. Click next until you reach the **Configure Ports** slide. Enter values for the HTTP and HTTPS ports and click **Next**.

14. When prompted to enter your sign-on information, enter:
   - SSO administrator user name: **administrator@vsphere.local**
   - SSO administrator password: **Admin@123**
Click **Next**.

15. You will be prompted with an SSH key. Accept it.

16. Click **Install Certificates**.

17. Click **Finish**.

18. When the Web Client installation is complete, the Install Wizard returns you
to the main screen.

19. Run installations for the following features with the default values in the wizard:
   
   a. **vCenter Inventory Service**
   
   b. **vCenter Server**
Configuring the VCenter Server for Bare Metal Installation

Accessing the VCenter Server

Installation of VCenter Server along with its various components is complete. Now VCenter server can be accessed from any client machine which is reachable from this windows machine, where VCenter server has been installed.

Use the below URL to access VCenter Server:

IP_Addr: IP Address of the windows machine, where VCenter server has been installed.

The Vmware UI which opens up, prompts you to provide authentication details. Enter Admin@123 as the password.

The following nine steps are all required to properly configure VMware.

1. Create a DataCenter for the VM environment. See "Configuring the VCenter Server for Bare Metal Installation" above.
2. Add Host Machines running Vmware OS under the DataCenter object. See "Configuring the VCenter Server for Bare Metal Installation" above.
3. Create a Virtual Machine on any of the host machines. See "Configuring the VCenter Server for Bare Metal Installation" above.
4. Create a template out of the host machine. See "Creating a VM on a Host Machine" on page 62.
5. Deploy virtual machines on each host machine out of the template created. Repeat "Cloning a VM Template to a Host" on page 69 as needed until all VMs have been created.
6. Create VMDK image required for powering up a VM from installing 3.10.1 OS on a blade. See "Creating and Deploying VMFS Disks " on page 71.
7. Add Physical Disks (rootfs and datafs) on each virtual machine. See "Configuring the VCenter Server for Bare Metal Installation" above.
8. Add external Storage Disks (assigned to host machines) on each virtual machine. See "Creating Datastores for VM External Storage" on page 74.
9. Apply final configurations and power up the Virtual Machine. See "Special Configuration for Insta" on page 78.

Creating a New DataCenter

1. Navigate to the server you want to create the DataCenter under.

2. Right-click on the server name and click **New Datacenter....**

Adding Host Machines

Adding an ESXi host to vCenter server requires configuring the hostname/IP address of the host and its credentials in the vCenter server. To add the host to a datacenter, follow these steps:

1. Go to the **Hosts** section under the newly created vCenter.

2. Create a new host and enter the hostname/IP address.
3. Click **Next** through the rest of the default settings to complete the **Add Host** wizard.

**Creating a VM on a Host Machine**

Establish a network using a VMKernel adaptor and a virtual switch:

- The VMKernel adaptor provides network connectivity for the ESXi host and handle standard infrastructure traffic of vMotion, IP storage, Fault Tolerance logging, and Virtual SAN.

- A vSphere standard switch is used to provide network connectivity to hosts and virtual machines. A standard switch can bridge traffic internally between virtual machines in the same VLAN and link to external networks. Create a new vSphere standard switch when creating a new VMKernel adaptor or separately.

To create the new Virtual Machine, follow these steps:

1. Click **VCenter > Virtual Machines** and follow the wizard to create Virtual machine/s on Hosts added in the datacenter.
2. Add a name to the Virtual Machine.

3. Select the datastore to store the VM configuration files.

4. Select the compatibility versions.
5. Select the OS type.

6. Change the CPU to 12 and Cores per socket as 6. Remove the HDD and click Next.
7. Click Finish to create a Virtual Machine.

**Configuring VM through vApp Properties**

The last step in a VM deployment is setting the configuration parameters which help auto configuration of VM at its first boot. This is possible with the help of vApp properties previously set in VM Template. vApp properties configure a VM by creating a runtime environment called Open Virtualization Format (OVF) environment which works on simple mechanism of key/value pairs. These key/value pairs are called OVF properties.

To enable a VM to self-configure using VApp, perform the following steps:

1. Define OVF properties on the VM.

2. Setup the OVF environment transport to carry the settings into the virtual machine.

3. Write glue code to access and apply the information inside the VM.

Modify the VM created above and change its vApp Options as shown in the following steps.
1. Customize the values of these four parameters for the VM:
   a. interface_name = eth0  
   b. ipaddr = 192.168.147.120/24  
   c. ipgw = 192.168.147.1  
   d. gmsauthkey = aaaa

2. Go to **OVF settings > OVF environment transport** and check the box next to **ISO image**.
Creating a VM Template for Cloning

A VM Template is a master copy of a virtual machine that can be used to create many clones. When you clone a virtual machine, you create a copy of the entire virtual machine, including its settings, any configured virtual devices, installed software, and all the contents of the virtual machine's disks. We always have the option to change some of the guest OS settings.

To create a VM Template:

1. Create a VM Template. "Creating a VM Template" below "Creating a VM on a Host Machine" on page 62
2. Clone the VM to a host using the VM Template.

Creating a VM Template

Create the VM Template without any disks in it. Upload the pre-manufactured disks later when a VM is deployed from the template.

1. Clone the VM created as a template by clicking **VCenter > Virtual Machines > VM1.** Select **Clone to Template.**

2. Enter the name **VM-Template** and select a datacenter. Click **Next.**

3. Double-click on the datacenter to use for this VM.
4. Select a storage location to be used as a default for the template. Click **Next**.

5. Customize entries for the following four properties:
   - interface_name
   - ipaddr
   - ipgw
   - gmsauthkey
Click **Next**.

6. Click **Next** and **Finish** to unique ID and prefix the complete the Template for deploying Virtual Machines.

**Cloning a VM Template to a Host**

Now you can deploy a VM on any added host using the template created in the section above.

1. Navigate to **VCenter > VM Templates > Template-1**. Click **Actions** and select **Deploy VM from this Template**.

2. Enter a name for the new VM. In this example, it was **VM-100**. Click **Next**.
3. Select a datacenter for the new VM. Click Next.

4. From the drop-down menu for Select virtual disk format, select Same format as source. Click Next.

5. Change the values for ipaddr and ipgw if necessary. If not, click Next.
6. Click **Next** and **Finish** to deploy a new VM on the host machine.

7. Repeat these steps to create virtual machines on each host.

**Creating and Deploying VMFS Disks**

A VMFS disk is necessary when deploying VMs in vSphere® environment. The default deployment of all VMs consists of two vdisks: **rootfs** the **datafs**.

The process to create VM raw disks has been changed for VMFS disks also. These disks can be uploaded to the VMware datastores. This will also handle the upgrade process as the new rootfs can be uploaded anytime later without changing the datafs.

To manufacture a VM with VMWARE_2D model, create a rootfs.vmdk of 17G, and a datafs.vmdk of default size 50G, use the following steps:

1. Manufacture a blade with 3.6.rc1 image (not with Vmware image) and run the enable command from shell prompt:

   ```
   > en
   ```

2. Download the vmdk files (rootfs.vmdk and datafs.vmdk) from the ftp server location which has been shared along with the image.

3. Attach the vmdks to each VM as Existing Hard Disk. See "Configuring the VCenter Server for Bare Metal Installation" on page 60.
**Adding a Local Disk to a VM**

1. Edit Virtual Machine Settings on which local disk needs to be added.

2. In this view, select the `datafs.vmdk` file, and click **OK**.
3. Repeat the last two steps to add `rootfs.vmdk` as another **Existing Hard Disk**.

4. The snapshot of both the disks added should resemble the following images.

**Datafs Disk**
Creating Datastores for VM External Storage

1. Go to **vCenter > Datastores**.

2. Click **Actions > Create New Datastore**.

3. A wizard opens. Select the Datacenter to hold the new Datastore and click **Next**.
4. Select the radio button for **VMFS** and click **Next**.

5. Enter a name for the new datastore. In this case, **Storage_Collector_147-12** was used.

6. Select the radio button for **VMFS 5** and click **Next**.
7. For the partition settings, select **Use all available partitions** from the drop-down menu and set the size as **1024 GB**. Click **Next**.

8. Review the settings and click **Finish** to complete the wizard, so that External Storage gets formatted with VMFS partition which can be used for a VM.
Assigning External Storage to VM

1. Edit Virtual Machine Properties and select a New Device.

2. From the drop down menu select New Hard Disk and click Add.

3. Change the location of New Hard Disk by selecting Browse from the drop down menu and selecting the Storage created in the previous section.

4. The final settings of the New Hard Disk should look like as below as
specifying the disk space required for that VM. If it is a 1 TB LUN and you are creating 2 VM's assign 500 GB to each VM. Disk provisioning should be **Thick provision eager zeroed**.

![Screenshot of VM settings with SCSI Bus Sharing](image)

**Special Configuration for Insta**

Insta requires same disk to be shared between both the Master and Standby node. VMware provides support for disk sharing by setting the **SCSI Bus Sharing** option of SCSI controller to **Physical** and thick provisioning of the disk. The following screenshot shows a sample VM settings with SCSI Bus Sharing:
1. Verify settings match those in the screenshot below.

![Screenshot of VM Template Edit Settings](image)

2. Verify settings match those in the screenshot below.
3. Once these settings are complete, the VM and is ready to be powered on and used.
Configuring GC Virtual Machine

The following steps are required to configure the VM so that GMS processes can be started.

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

   For a complete list of patches and installation instructions, refer to the MURAL Release Notes, 3.4.

2. Start the GMS server:

   ```
   # cli -m config
   (config)# postgres dbroot /data/pgsql
   (config)# postgres mode external
   (config)# pm process psqlqd restart
   (config)# pm process gms_server restart
   (config)# write memory
   (config)# quit
   ```

3. Check the status of the GMS server by running the following command:

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

   The resulting output may resemble:

   ```
   Current status: running
   ```

4. Create soft links to copy all the required profiles, as:

   ```
   # _shell
   cd /config/gms/Profiles/Custom/
   pwd
   /config/gms/Profiles/Custom
   ln -s /opt/deployment/GMS_
   ```
ln -s /opt/deployment/GMS_Templates/collector/Feed/bulkstats/collector_adaptor_bulkstats_template.xml .
ln -s /opt/deployment/GMS_Templates/collector/Feed/edrhttp_edrflow/collector_adaptor_edrhttp_edrflow_template.xml .
ln -s /opt/deployment/GMS_Templates/hadoop/dfs_template.xml .
ln -s /opt/deployment/GMS_Templates/insta/App/bulkstats/insta_mural_bulkstats_flat.xml .
ln -s /opt/deployment/GMS_Templates/insta/App/dpi/insta_mural_dpi_flat.xml .
ln -s /opt/deployment/GMS_Templates/oozie/App/bulkstats/workflow_bulkstat_mural_with_timeout.xml .
ln -s /opt/deployment/GMS_Templates/oozie/App/dpi/workflow_dpi_with_timeout_jobs.xml .
ln -s /opt/deployment/GMS_Templates/oozie/App/dynamicWhitelisting/workflow_dynamic_whitelisting_with_timeout.xml .
ln -s /opt/deployment/GMS_Templates/oozie/App/tethering/workflow_tethering_with_timeout.xml .
ln -s /opt/deployment/GMS_Templates/oozie/Feed/edrhttp_edrflow/workflow_edrhttp_edrflow_with_timeout.xml .
ln -s /opt/deployment/GMS_Templates/postgres/postgresql_mural.xml .
ln -s /opt/deployment/GMS_Templates/rubix/bulkstats/rubix_bulkstats_mural.xml .
ln -s /opt/deployment/GMS_Templates/rubix/dpi/rubix_atlas_distributed_mural.xml .
ln -s /opt/deployment/GMS_Templates/rubix/rge/rubix_rge_mural.xml .
ln -s /opt/deployment/GMS_Templates/solution/solution_solution_
Verifying XML Settings

Click on the name of a chassis to see more details and verify settings.

The hardware type, chassis number and chassis logical name are displayed, as well as the list of nodes (blades) in each slot.

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

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

Understanding LUN SCSI and Block IDs

The number of LUNs, and therefore the number of SCSI/Block IDs, assigned to each node depends on the type of node:

- **GC nodes** – Each GC node has three assigned Block IDs:
  - GMS – pgsql database to store GMS and Zabbix data and MURAL UI users related data (like user permissions, etc).
  - Collector – EDR/Bulkstat raw data files received from ASR
  - Rubix – Storing offline reports.

- **Compute nodes** – Each node has one Block IDs assigned.

- **Insta node** - Insta node has two SCSI IDs, assigned as dbroot1 and dbroot2

  **Important:** Ensure that SCSI IDs (like 0:0, 0:1, etc) are only used for Insta node. All other nodes use device Block IDs (like /dev/sda, /dev/sdb, etc created corresponding to SCSI IDs 0:0, 0:1 and so on).

If you are at a stage where UCS configuration is not yet fully set up, then you can use a dummy WWID for each blade. However, if you have configured both UCS and EMC, you must enter the actual WWID, which you can find as described below.
Verifying Server Details Tab

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

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

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

2. In the Chassis box, select the chassis.

3. The Slot section lists the nodes (blades) in each slot. Select a node to verify or modify its WWID values.

Set the following values:
- Slot 1

- Slot 3
- Slot 5
- Slot 6
MURAL Software Installation Guide for Medium Pack with VMWare

### Slot

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Host Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>VDN2</td>
</tr>
<tr>
<td>5</td>
<td>VInsta1</td>
</tr>
<tr>
<td>6</td>
<td>VInsta2</td>
</tr>
<tr>
<td>7</td>
<td>VRubix1</td>
</tr>
<tr>
<td>8</td>
<td>VRubix2</td>
</tr>
</tbody>
</table>

### Interface Members

<table>
<thead>
<tr>
<th>Mac_Address</th>
<th>Ifc_Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:50:56:87:42:37</td>
<td>eth0</td>
</tr>
<tr>
<td>00:50:56:87:60:7a</td>
<td>eth1</td>
</tr>
</tbody>
</table>

### Storage

**FC Zone / iSCSI Initiator Zone:**

**Storage Type:** FC/Device

<table>
<thead>
<tr>
<th>Storage_WWID</th>
<th>Mount_Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0</td>
<td>/dev/root</td>
</tr>
<tr>
<td>0 1</td>
<td>/dev/root2</td>
</tr>
<tr>
<td>1 0 1</td>
<td>/data/pgsql</td>
</tr>
</tbody>
</table>

- Slot 7
Verifying Networks Tab

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

1. Under the Networks tab, verify the following fields for the Management Network:
   - Network Name
   - Network IP Address: prefix and subnet
   - Interface Type
   - Network Interface
   - Network Range

Copyright © 2015, Cisco Systems, Inc.
Verifying Global Settings Tab

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

In Starter pack setup, all the nodes have only one Management IP address. GMS and Insta clusters also have one Virtual IP address, each from the same Management Network. GCN, UI and Insta clusters also have one Virtual IP address, each from the same Management Network.

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

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

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

4. NTP version

Verifying Nodes Tab

Define the IP address and subnet mask of each node.
MURAL Software Installation Guide for Medium Pack with VMWare

<table>
<thead>
<tr>
<th>Chassis LogicalName</th>
<th>Slot Number</th>
<th>Node Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM-1</td>
<td>1</td>
<td>VGC1</td>
</tr>
<tr>
<td>VM-1</td>
<td>2</td>
<td>VGC2</td>
</tr>
<tr>
<td>VM-1</td>
<td>3</td>
<td>VDN1</td>
</tr>
<tr>
<td>VM-1</td>
<td>4</td>
<td>VDN2</td>
</tr>
<tr>
<td>VM-1</td>
<td>5</td>
<td>Vmsta1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Name</th>
<th>Network IP</th>
<th>Network Subnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>External</td>
<td>192.165.147.62</td>
<td>24</td>
</tr>
<tr>
<td>Data</td>
<td>10.10.10.62</td>
<td>24</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chassis LogicalName</th>
<th>Slot Number</th>
<th>Node Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM-1</td>
<td>4</td>
<td>VDNZ</td>
</tr>
<tr>
<td>VM-1</td>
<td>5</td>
<td>Vmsta3</td>
</tr>
<tr>
<td>VM-1</td>
<td>6</td>
<td>Vmsta2</td>
</tr>
<tr>
<td>VM-1</td>
<td>7</td>
<td>VRubix1</td>
</tr>
<tr>
<td>VM-1</td>
<td>8</td>
<td>VRubix2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Name</th>
<th>Network IP</th>
<th>Network Subnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>External</td>
<td>192.168.147.64</td>
<td>24</td>
</tr>
<tr>
<td>Data</td>
<td>10.10.10.64</td>
<td>24</td>
</tr>
</tbody>
</table>
Verifying Clusters Tab
Verifying Applications Tab and Specifying Component Profiles

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

- Collector GMS Cluster with the following values:

  This template configures HDFS on the cluster.

<table>
<thead>
<tr>
<th>App Name</th>
<th>App Profile</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMS</td>
<td>gms_default_without_nbi_template</td>
<td>Clusters—GMS Cluster</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Application Instance = 1</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>postgres_custom_mural</td>
<td>Clusters—GMS Cluster</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Application Instance = 1</td>
</tr>
</tbody>
</table>

- Collector Cluster with the following values:
<table>
<thead>
<tr>
<th>App Name</th>
<th>App Profile Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collector</td>
<td>collector_custom_adaptor_bulkstats_template</td>
</tr>
<tr>
<td></td>
<td>Clusters = COL-CLUS</td>
</tr>
<tr>
<td></td>
<td>Application Instance = 1</td>
</tr>
<tr>
<td></td>
<td>Change the format of the following values to</td>
</tr>
<tr>
<td></td>
<td>/data/collector/bulkstats_files/gateway_name:</td>
</tr>
<tr>
<td></td>
<td>- BulkStats file input directory, specified by</td>
</tr>
<tr>
<td></td>
<td>adaptor.bulkStats.input.fileConfig.</td>
</tr>
<tr>
<td></td>
<td>bulkStatsFile1.inputDirectory</td>
</tr>
<tr>
<td></td>
<td>Change the format of the following values to</td>
</tr>
<tr>
<td></td>
<td>/data/collector/bulkstats_files_backup/gateway_name:</td>
</tr>
<tr>
<td></td>
<td>- BulkStats filebackup directory, specified by</td>
</tr>
<tr>
<td></td>
<td>adaptor.bulkStats.input.fileConfig.</td>
</tr>
<tr>
<td></td>
<td>bulkStatsFile1.backupDirectory</td>
</tr>
</tbody>
</table>
### Collector

**App Name**: Collector  
**Settings**
- **App Profile**: collector_custom_adaptor_edrhttp_edrflow_template
- **Clusters** = COL-CLUS
- **Application Instance** = 1
- **adaptor.edrflow.numThreads** = 8 for 24 CPU, 11 for 32 CPU
- **adaptor.edrhttp.numThreads** = 8 for 24 CPU, 11 for 32 CPU

Configure the default name, or at least remove the `-` in front of "edr", for the following two values:

- **%DC_MURAL-edr_**
- ***_%MM%DD%YYYY%hh%mm%ss*.gz**

- adaptor.edrhttp.input.fileConfig.httpfile.fileNameFormat
- adaptor.edrflow.input.fileConfig.flowfile.fileNameFormat

Refer to the [table](#) to set the gateway names, filename formats, and transfer filename format.

### solution

**App Name**: solution

**Settings**
- **App Profile**: solution_custom_mural
- **Clusters** = COL-CLUS
- **Application Instance** = 1
- **Client name** = CISCO
- **isStarterPack** = false
- **timeZone** = Refer to the [table](#) for valid values. The selected time zone is automatically applied to all the jobs.
<table>
<thead>
<tr>
<th>App Name</th>
<th>App Profile</th>
<th>Settings</th>
</tr>
</thead>
</table>
| DFS      | dfs_custom_template | **Clusters** = COL-CLUS  
**Application Instance** = 1  
hadoop.mapred.min.split.size = 134217728 |
| Hive     | hive_custom_mural | **Clusters** = COL-CLUS  
**Application Instance** = 1 |
| Workflow | workflow_custom_dynamic_whitelisting_with_timeout  
workflow_custom_dpi_with_timeout_jobs  
workflow_custom_bulkstat_mural_with_timeout  
workflow_custom_edrhttp_edrflow_with_timeout  
workflow_custom_tethering_with_timeout | **Clusters** = COL-CLUS  
**Application Instance** = 1 |

When you set the value for `timeZone`, ensure that the value is the same as what was used in the UI templates. The following table lists the different `timeZone` values that can be used.

<table>
<thead>
<tr>
<th>TimeZone String</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>US/Central</td>
<td>United States Central Standard Time</td>
</tr>
<tr>
<td>US/Eastern</td>
<td>United States Eastern Standard Time</td>
</tr>
<tr>
<td>US/Pacific</td>
<td>United States Pacific Standard Time</td>
</tr>
<tr>
<td>America/Lima</td>
<td>Peru</td>
</tr>
<tr>
<td>Chile/EasterIsland</td>
<td>Chile</td>
</tr>
<tr>
<td>Africa/Johannesburg</td>
<td>South Africa</td>
</tr>
<tr>
<td>Asia/Manila</td>
<td>Philippines</td>
</tr>
</tbody>
</table>
### Time Zone String

<table>
<thead>
<tr>
<th>Time Zone String</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egypt</td>
<td>Egypt</td>
</tr>
<tr>
<td>Europe/Amsterdam</td>
<td>Netherlands</td>
</tr>
<tr>
<td>Europe/Dublin</td>
<td>Ireland</td>
</tr>
<tr>
<td>UTC</td>
<td>Universal Co-ordinated Time</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Filename Pattern</th>
<th>Regex in Wrapper CLI</th>
<th>Regex in Collector Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gatewayname_(multiple strings separated by underscore or hyphen or both)_flow_timestamp_str4.gz</td>
<td><em>_</em><em>*</em><em>%MM%DD%YYYY%hh%mm%ss_</em>.gz</td>
<td>%DC_<em>_</em><em>*</em>%MM%DD%YYYY%hh%mm%ss*.gz</td>
</tr>
<tr>
<td><strong>Example</strong>: Gatewayname_str1_str2_str3_flow_timestamp_str4.gz</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Timestamp</strong>: MMDDYYYYhhmmss</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gatewayname_(multiple strings separated by underscore or hyphen or both)_flow_timestamp_str4_str5.gz</td>
<td><em>_</em><em>*</em><em>%MM%DD%YYYY%hh%mm%ss_</em>_.gz</td>
<td>%DC_<em>_</em><em>*</em>%MM%DD%YYYY%hh%mm%ss*.gz</td>
</tr>
<tr>
<td><strong>Example</strong>: Gateway name_str1_str2_str3_flow_timestamp_str4_str5.gz</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Timestamp</strong>: MMDDYYYYhhmmss</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Filename Pattern</td>
<td>Regex in Wrapper CLI</td>
<td>Regex in Collector Configuration</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>Gatewayname_(multiple strings separated by underscore or hyphen or both)_flow_string_timestamp_string.gz</td>
<td>* * * <em>%MM%DD% YYY%hh%mm%ss</em>*_.gz</td>
<td>%DC_* _ _ _ _%MM%DD% YYY%hh%mm%ss*.gz</td>
</tr>
<tr>
<td>Example: Gatewayname_str1_str2_str3_flow_str4_timestamp_str5.gz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timestamp: MMDDYYYYhhmmss</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gatewayname_(multiple strings separated by underscore or hyphen or both)_flow_string_timestamp_string.gz</td>
<td>* * <em>%MM%DD %YYYY%hh%mm%ss</em>*_.gz</td>
<td>%DC_* _ _ _ _%MM%DD %YYYY%hh%mm%ss*.gz</td>
</tr>
<tr>
<td>Example: Gatewayname_str1_str2_str3_flow_str4_timestamp_str5_str6.gz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timestamp: MMDDYYYYhhmmss</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gatewayname_(multiple strings separated by underscore or hyphen or both)_flow_string_timestamp_string.gz</td>
<td>* <em>%YYYY%MMDD% hh%mm%ss</em>*_.gz</td>
<td>%DC_* _ _ _ _%YYYY%MMDD% hh%mm%ss*.gz</td>
</tr>
<tr>
<td>Example: Gatewayname_str1_str2_str3_flow_str4_timestamp_str5_str6.gz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timestamp: YYYYMMDDhhmmss</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Filename Pattern

<table>
<thead>
<tr>
<th>Filename Pattern</th>
<th>Regex in Wrapper CLI</th>
<th>Regex in Collector Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gatewayname_(multiple strings separated by underscore or hyphen or both)_flow-string_timestamp_string.gz</td>
<td><em>_</em><em>*</em>-%MM%DD %YYYY%hh %mm%ss_*_.gz</td>
<td>%DC_<em>_</em>-<em>_%MM%DD %YYYY%hh %mm%ss</em>.gz</td>
</tr>
<tr>
<td>Example: Gatewayname_str1_str2_str3_flow-str4_timestamp_str5_str6.gz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timestamp: MMDDYYYYhhmmss</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**

- It is mandatory to send gateway name as the first substring followed by an underscore.
- You can replace 'http' with 'flow'.
- If the timestamp is in the MMDDYYYYhhmmss format, set the %MM%DD%YYYY%hh%mm%ss parameter in the Regex pattern.
- If the timestamp is in the YYYYMMDDhhmmss format, set the %YYYY%MM%DD%hh%mm%ss parameter in the Regex pattern.

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

Later in this installation procedure you will change the Oozie start time and start all of the jobs.

- Rubix with the following values:

  Ensure that Rubix Atlas and Launcher profiles are added to the application instance 1 and the remaining profiles are added to the application instance 2.
### MURAL Software Installation Guide for Medium Pack with VMWare

<table>
<thead>
<tr>
<th>App Name</th>
<th>App Profile</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution</td>
<td>solution_custom_mural</td>
<td></td>
</tr>
<tr>
<td><strong>Application Instance = 2</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Clusters = RUBIX-CLUS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Client name = cisco</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>isStarterPack = false</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>timeZone</strong> = Refer to the table for valid values. The selected time zone is automatically applied to all the required UI applications.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Rubix | rubix_custom_atlas_distributed_mural | |
| **Application Instance = 1** | |
| **Clusters = RUBIX-CLUS** | |

| Rubix | rubix_custom_rge_mural |
| | rubix_custom_bulkstats_mural |
| | rubix_custom_cacheless_mural |
| **Application Instance = 2** | |
| **Clusters = RUBIX-CLUS** | |

Set the following property values:

- For profile **rubix_custom_atlas_distributed_mural**, set:
  - `application.atlas.rubixFQDN = Default or per requirement`
  - `application.atlas.rgeSolutionURL = Default or per requirement`
  - `application.atlas.anomalySolutionURL = Only if the Anomaly feature is enabled`
  - `application.atlas.bulkStatsURL = Default or per requirement`
application.atlas.sessionCookieDomain = Default or per requirement

application.atlas.cachePresistToDisk = false (if no extra lun for disk caching)

application.atlas.numOwners = 2

- For profile rubix_custom_bulkstats_mural, set:

  application.bulkstats.sessionCookieDomain = Default or per requirement

  application.bulkstats.cachePresistToDisk = false (if no extra lun for Disk caching)

  application.bulkstats.numOwners = 2

- For profile rubix_custom_cacheless_mural, set:

  application.reportAtlas.sessionCookieDomain = Default or per requirement

  application.reportAtlas.timeZone = Same as set in Workflow template

- For profile rubix_custom_rge_mural, set:

  application.rge.sessionCookieDomain = Default or per requirement

  application.rge.mailHost = e.g. - mx1.cisco.com

  application.rge.mailSender = e.g. support@cisco.com

  application.rge.mailPort = 25

For example,
Insta Cluster with the following values:

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

Compute Cluster with the following values:

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

<table>
<thead>
<tr>
<th>App Name</th>
<th>App Profile</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute</td>
<td>compute_default_template</td>
<td>Application Instance = 1 Clusters = DN-CLUS</td>
</tr>
</tbody>
</table>
**Applying Profile Settings**

Apply the above profile settings by following these steps:

1. Select the **Applications** tab:

2. Start with the **Available Profiles** section:
   a. For **Application Name**, select the name of the system component from the drop-down menu.
   b. For **Application Profile**, select the profile you want to attach to the system component.

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

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

5. Attach the profiles as required.

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

**Validating the XML Configuration**

To validate the GMS configuration, perform the following steps:

1. Click **Validate** on the bottom bar of the GMS interface.
   
   If any field or value entered is incorrect, a list of errors is displayed.

2. For each error, click the error and then the **Go** button to display the entry in the GMS configuration that is causing the error.
3. Correct any errors by following the steps in "Verifying XML Settings " on page 83

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

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

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

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

This section explains how to use GMS Lite to manufacture the nodes, instead of manually manufacturing them individually.

Applying Patches on MURAL nodes

Download the patches from the FTP server to the master GCR VM in the `/data` directory. Apply all patches applicable for respective MURAL nodes.

Note: See the release notes for software version 3.4 for a complete list of patches and installation instructions.

Activating the XML File

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

```bash
> en
# _shell
```

2. Activate the xml file on this VM

```bash
(config)# gms config muralMediumPack_Vmware.xml.xml activate
```

Modifying Templates

Following values have to be modified in attached templates as per the site requirement.

- If URL to be used is https://abc.mural.com, then `sessionCookieDomain` should be `.mural.com` and `FQDN` should be `abc.mural.com`.

- The time zone of location of the ASR. For more information, see the "Verifying Applications Tab and Specifying Component Profiles" section in "Verifying XML Settings " on page 83.

Installing GC Nodes

Run the following commands to bring up various clusters.
1. Log into the first GC node where GMS is running and run the install command.

```
(config)# install appliance cluster cluster-name VMGC-CLUS node VGC1
```

This installation takes 1.5-2 hours. Periodically check the installation status by running:

```
[CLUSTER: master] (config)# install appliance show installation-status cluster VMGC-CLUS node VGC1
```

The resulting output may resemble:

```
VGC1 : Node successfully installed
```

2. Install the 2nd GC node.

```
(config)# install appliance cluster cluster-name VMGC-CLUS node VGC2
(config)# install appliance show installation-status cluster VMGC-CLUS node VGC2
```

The resulting output may resemble:

```
VGC2 : Node successfully installed
```

3. Install the DN cluster.

```
(config)# install appliance cluster cluster-name VDN-CLUS
Installation in progress, check VDN1_cmc.log file for more details
Installation in progress, check VDN2_cmc.log file for more details
```

This installation takes 20-30 minutes. Periodically check the installation status by running:

```
(config)# install appliance show installation-status cluster VDN-CLUS
```

---

108

Copyright © 2015, Cisco Systems, Inc.
The resulting output may resemble:

<table>
<thead>
<tr>
<th>Node</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDN1</td>
<td>Node successfully installed.</td>
</tr>
<tr>
<td>VDN2</td>
<td>Node successfully installed.</td>
</tr>
</tbody>
</table>

4. Install the Insta cluster.

```
(config)# install appliance cluster cluster-name VMINSTA-CLUS
Installation in progress, check VInsta1_cmc.log file for more details
Installation in progress, check VInsta2_cmc.log file for more details
```

This installation takes 45-60 minutes. Periodically check the installation status by running:

```
(config)# install appliance show installation-status cluster VMINSTA-CLUS
```

The resulting output may resemble:

<table>
<thead>
<tr>
<th>Node</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>VInsta1</td>
<td>Node successfully installed</td>
</tr>
<tr>
<td>VInsta2</td>
<td>Node successfully installed</td>
</tr>
</tbody>
</table>

5. Install the Rubix cluster.

```
VGC1 [VMGC-CLUS: master] (config)# install appliance cluster cluster-name VMRUBIX-CLUS
Installation in progress, check VRubix1_cmc.log file for more details
Installation in progress, check VRubix2_cmc.log file for more details
VGC1 [VMGC-CLUS: master] (config)# install appliance show installation-status cluster VMRUBIX-CLUS
```

The resulting output may resemble:

<table>
<thead>
<tr>
<th>Node</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRubix1</td>
<td>Node successfully installed</td>
</tr>
<tr>
<td>VRubix2</td>
<td>Node successfully installed</td>
</tr>
</tbody>
</table>

After installing the GC node, perform the steps in "Repairing HDFS" below.
Reparing HDFS

1. To repair HDFS, log in to the master GC node and execute the following commands:

   ```console
   [admin@host ~]# pmx
   Welcome to pmx configuration environment.
   pm extension> subshell hadoop
   pm extension (hadoop)> repair hdfs
   Safe mode is OFF
   The filesystem under path '/' is HEALTHY
   pm extension (hadoop)> quit
   pm extension> quit
   ```

2. To ensure that Hadoop is not in the safe mode, execute the following commands:

   ```console
   [admin@host ~]# hadoop dfsadmin -report
   ```

3. To make the performance related changes, execute the following commands on both the master and the standby GC nodes:

   ```text
   > en
   # conf t
   (config) #internal set modify -
   /tps/process/hadoop/attribute/mapred.reduce.tasks/value value
   string 8
   (config) #wr mem
   (config) #pm process tps restart
   ```

1. If the Anomaly detection feature is enabled, run the following commands in both the GCR nodes for CoreJob solution config.

   a. Enter the pmx oozie subshell environment.

      ```console
      (config)# pmx
      pm extension> subshell oozie
      ```

   b. Exit the oozie subshell using the `quit` command.
c. Apply one more setting and write changes to memory before restarting processes.

```
(config)# internal set delete -
/tps/process/oozie/jobs/CleanupAnomaly5weekly/actions/CleanAnomalyAction/attribute/cleanupDatasets/values/anomaly_Agg_daily
(config)# write memory
(config)# pm process tps restart
```
Generating and Pushing the Information Bases

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

Configuring IBs for EDR

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

<table>
<thead>
<tr>
<th>DC</th>
<th>Area</th>
<th>Region</th>
<th>GGSN</th>
<th>GGSNIP</th>
<th>SGSN</th>
<th>SGSNIP</th>
<th>SGSNIP</th>
<th>APN</th>
<th>APN</th>
<th>GROUP</th>
<th>GROUP</th>
<th>RATTID</th>
<th>RATTYPE</th>
<th>3G</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>USA</td>
<td>MW</td>
<td>GGSN</td>
<td>Kansas-GGSN</td>
<td>SGSN</td>
<td>2.2.2.1</td>
<td>SGSNIP</td>
<td>CYBERCITY</td>
<td>APN</td>
<td>broadband</td>
<td>GROUP</td>
<td>broadband</td>
<td>RATTID</td>
<td>RATTYPE</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:

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

   ```
   > en
   # conf t(config)# pmx
   pm extension> subshell aggregation_center
   pm extension (aggregation center)> update all ibs from image
   ```

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

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

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

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

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

Where `ib-file-name` is:

- ipGgsn
- ipSgsn
- apnGroup

The resulting output may resemble:

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

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

5. To configure the IBs for BulkStats:

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

### Configuring DCs and Gateways For All IBs

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

- The filename pattern provided here should be in sync with the Collector configurations. For guidelines on the regex value to be used for the filename format, see the "Verifying Applications Tab and Specifying Component Profiles" section in "Verifying XML Settings" on page 83. Refer to the values in the Wrapper CLI column for sample filename formats.

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

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

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

To configure gateways:

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

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

2. Verify the new gateway has been added:

pm extension (aggregation_center)> show gateways

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

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

Example:
pm extension (aggregation center)> set collector IPs
192.168.1.1,192.168.2.2

Note: These are internal IP addresses.

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

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

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

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

6. Push the gateway configuration to all the Collectors:

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

7. Generate and push all IBs:

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

8. Generate and push IBs on Bulkstats:

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

9. Write changes to memory:

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

**Synchronize the IBs on the GC VM Node**

After the above `push` command completes, run the following command on the node from the CLI configure terminal.

1. Go to the `bulkstats` subshell.

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

2. Fetch all IBs.

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

3. Go to the `aggregation_center` subshell.
4. Fetch all IBs for EDR data streams.

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

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

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

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

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

Setting Up a New User for the ASR in the Collectors

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

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

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

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

2. Edit `/etc/ssh/sshd_config` to set the following parameters:

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

3. Set the sshd_config file attribute as immutable.

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

Verify the sshd_config file attribute as below.

```
# lsattr /var/opt/tms/output/sshd_config
-----i-------- /var/opt/tms/output/sshd_config
```

4. Run the `sshd` restart command:
5. Repeat steps 1 through 3 on the standby Collector node.

## Ingesting Data Into the System

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

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

**GW_Name** would be the gateway you added up while configuring the GCU.

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

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

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

Validating Data on the Nodes

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

   ```
   > en
   # _shell
   ```

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

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

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

Setting the Data Start Time

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

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

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

2. Execute the setOozieTime script to set the time at which EDR and BulkStats data starts coming into the Hadoop directories listed in "Validating Data on the Nodes" above.
For example, if EDR and Bulkstats data starts coming into the Hadoop system from April 1, 2013, 06:00 onwards, run the following scripts with the start_time value as "2013-04-01T06:00Z":

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

**Note:** Enter minutes as a multiple of 5. For example, "2013-04-01T06:00Z."

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

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

**Starting the Data Processing**

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

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

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

**Note:** It may take approximately 20 minutes to start all the jobs, depending upon what all applications are enabled.

**Validating Data on the Compute Blades (Data Nodes)**

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

**Caution:** Wait two hours after completing the steps in "Starting the Data Processing" above. This allows sufficient time for the jobs that process the collector data to start, and the done.txt files to be updated. Not waiting could result in the checks failing.
MURAL Software Installation Guide for Medium Pack with VMWare

### Validating EDR Data

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

   ```
   > en
   # _shell
   ```

2. Check the last timestamp for the Core job.

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

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

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

4. Check the last timestamp for CubeExporter data cubes.

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

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

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

### Validating Insta Data

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

   ```
   > en
   # _shell
   # cli -t "en" "conf t" "show runn full" |
   grep "insta instance 0 cubes-database" | awk -F ' ' '{print $5}'
   database_mural
   ```

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

   ```
   # idbmysql
   Welcome to the MySQL monitor. Commands end with ; or \g.
   ...
MURAL Software Installation Guide for Medium Pack with VMWare

mysql> use database_mural;
Database changed

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

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

Press Ctrl+D to exit

mysql> Bye

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

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

```
# date -d @1406710800
Wed Jul 30 09:00:00 UTC 2014
# date -d @1409295600
Fri Aug 29 07:00:00 UTC 2014
```

**Validating Bulk Stats Data on the Insta Blade**

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

```
> en
# _shell
# cli -t "en" "conf t" "show runn full" | grep "insta instance 1 cubes-database" | awk -F ' ' '{print $5}
'bulkstats
```
2. Open the `idbmysql` user interface and select `bulkStats` as the database.

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

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

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

```sql
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.

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

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

**Starting UI Processes and Verifying Data**

Starting the UI processes and verify UI data. Ensure that the URL is set up in the DNS for the production system.
Starting the Rubix Tomcat Instance on Both UI Nodes

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

1. Log in to the master UI node.

   ```
   > en
   # conf t
   ```

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

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

   Check the tomcat process status using command:

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

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

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

   ```
   (config)# pm process rubix restart
   (config)# rubix modify-app ApplicationName enable
   (config)# rubix modify-app ApplicationName modify-instance 1 enable
   ```

   Where **ApplicationName** is replaced by the following applications in the same order:

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

   Check the tomcat process status using command:

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

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

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

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

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

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

Visit the following ports once and accept the certificates:

```
https://domainName:20443/
https://domainName:30443/
```

For example:

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

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

**Updating Whitelists**

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

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

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

Uncategorized URL, UA, and TAC Reports

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

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

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

   For example,

   ```text
   192.168.156.96, admin, admin@123, /data/offline_uncat_reports
   ```

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

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

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

3. Create the `serverFile_uncatReports` file:

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

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

4. Create the same file on the standby node.

Tethering Reports

Create a file called `serverFile_tethering` with details of the ASR 5000 gateways, where the TAC, OS or UA databases, created as a result of tethering processing, need to be pushed.
1. The `serverFile_tethering` file contains the entries for the data transfer destination location. This file has the following format:

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

Where:

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

2. Log in to the master node:

   ```
   > en
   # _shell
   ```

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

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

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

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

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

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

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

   This file can have multiple rows of this kind.
# 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**
The cluster of nodes consisting of the Collector nodes in active/standby High Availability clustering.

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

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

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

**D**

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

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

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

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

**F**

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

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

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

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

**H**

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

**I**

**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.

**M**

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

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

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

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

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

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

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

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.

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.

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)

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

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

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

**V**

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

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

**W**

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

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

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

**Z**

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