xMatters *(IT)* engine

FOR HP OPERATIONS MANAGER FOR LINUX

This manual provides information about xMatters. Every effort has been made to make it as complete and accurate as possible; however, the information it contains is subject to change without notice and does not represent a commitment on the part of xMatters No part of this document may be reproduced by any means without the prior written consent of xMatters

Wednesday, November 12, 2014

Contacting xMatters, inc.:

You can visit the xMatters web site at: http:///www.xmatters.com

xMatters, inc.
Corporate Headquarters
12647 Alcosta Blvd, Suite 425
San Ramon, CA 94583
Telephone: 925.226.0300
Facsimile: 925.226.0310

Client Assistance:

Email: support@xmatters.com
International: +1 925.226.0300 and press 2
US/CAN Toll Free: +1 877.XMATTRS (962.8877)
EMEA: +44 (0) 20 3427 6333
Australia/APJ Support: +61-2-8038-5048 opt 2

Other Resources:

Join the xMatters Community: http://community.xMatters.com

This integration was designed and tested on an unmodified version of HP Operations Manager for Linux software, and this document describes how to configure xMatters to integrate with the default installation. If you have customized or altered your instance of HPOM for Linux, this integration may need to be modified for your deployment. Please note that these integration changes are not part of the services offered by xMatters Technical Support, but can be performed through xMatters's Professional Services department. For more information, contact your xMatters Sales representative.

Table of Contents

Chapter 1: Introduction

Welcome to xMatters (IT) for HP Operations Manager for Linux. This document describes how to install and configure the xMatters (IT) for HP Operations Manager for Linux software integration. The intended audience for this document is experienced consultants, system administrators and other technical readers.

1.0 Summary

xMatters is an interactive alerting application, designed to capture and enrich important events, to route those events to the right person on any communication device, and to give that person the ability to solve, escalate, or enlist others to resolve the events remotely.

xMatters allows you to take critical business information and contact the right people via voice phone, SMS, two-way pagers, instant message, and email.

Through integration modules, xMatters can become the voice and interface of an automation engine or intelligent application (the Management System, such as HP Operations Manager for Linux software). When HPOM for Linux detects something that requires attention, xMatters places phone calls, sends pages, messages, or emails to the appropriate personnel, vendors or customers.

xMatters is also persistent, escalating through multiple devices and personnel until someone accepts responsibility or resolves the problem. Once contacted, xMatters gives the notified person instant two-way communication with HP Operations Manager for Linux software. Responses are executed immediately on HPOM for Linux, enabling remote resolution of the event.

This integration supports event notifications (from HPOM for Linux to xMatters) through the use of web service calls via the xMatters integration agent. It also supports inbound actions (from xMatters to HPOM for Linux) to update events remotely.

You will need to modify this configuration to suit your particular business requirements and adjust it to suit your expected loads. For example, the default integration features automatic status annotations to the original event; in a high-volume production system, this can significantly affect performance. Consider your expected volume of injected events and your server capacity when designing your own integration with xMatters.

1.0.1 Benefits

With the xMatters integration, the appropriate technician can be notified directly via voice, email, pager, BlackBerry, or other device. Information about the failure will be presented to the event resolver and decisions can be made in real-time.

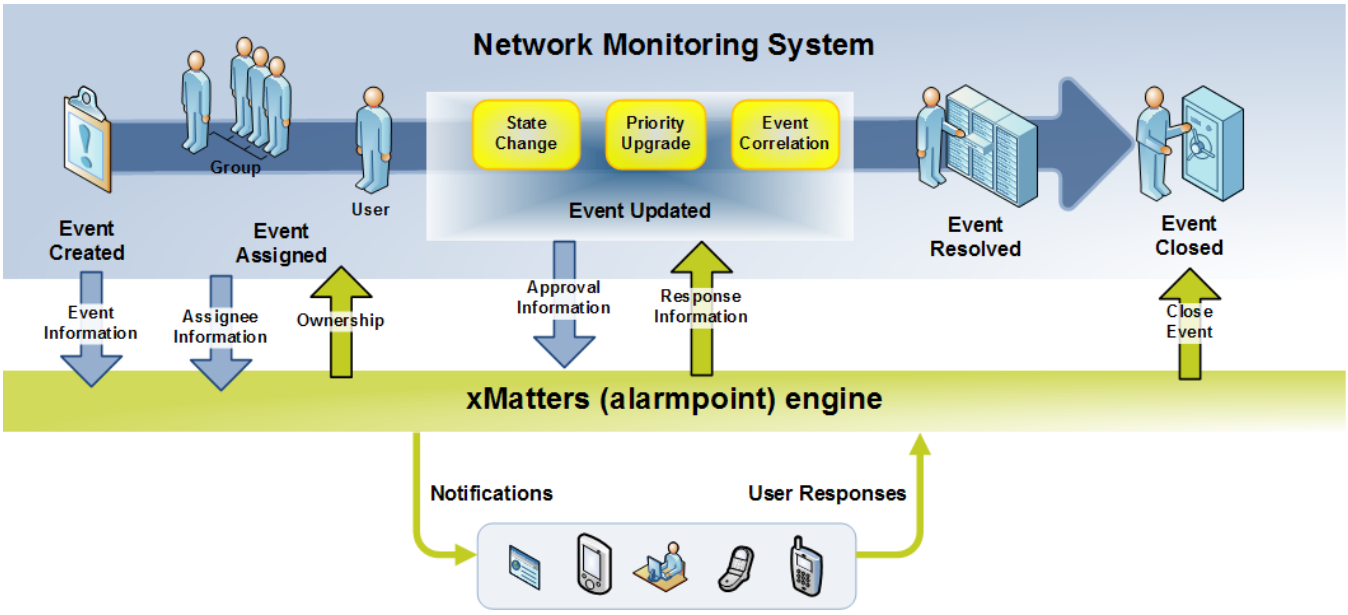
Once a response is selected on the recipient's remote device, xMatters will update the HPOM for Linux event in real-time. The benefit is that this process is immediate – significantly faster than the time required for staff to notice the failures or malfunctions, determine who is on call, and manually notify the right person. In addition, the ability to take simple actions on the event from any device gives the event resolver a quick way to deal with many issues and communicate to other team members the current state of the event.

During the process, every notification, response, and action is logged in xMatters. In addition, xMatters automatically annotates the original event with status information.

The xMatters product features a self-service web user interface to allow accurate assignment of responsible personnel for each job. xMatters also includes a Subscription panel that allows both managed and self-subscription to HPOM for Linux events.

1.0.2 Information Workflow

The following diagram provides an example of a standard workflow in a network monitoring system, and how information from the management system can be passed into xMatters relevance engine:

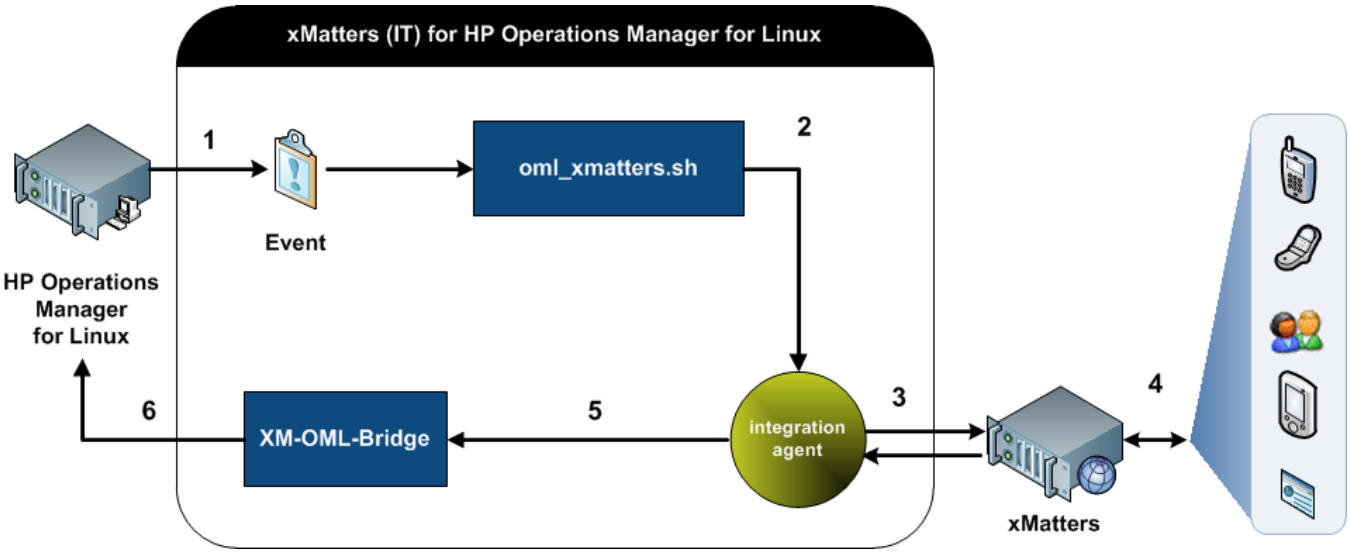


1.0.3 Integration Architecture

The software components in this integration include:

- xMatters relevance engine
- HP Operations Manager for Linux software
- xMatters integration agent

The following diagram illustrates the software processes used by this integration:



The number for the following steps correspond to the numbers in the diagram:

1. A new HPOM for Linux event occurs that requires notification via xMatters.
2. The om_xmatters.sh script processes the event and forwards it to the integration agent via the APClient.bin.
3. The integration agent injects the event content into xMatters.
4. xMatters sends a notification to the appropriate users or users on their preferred devices, and returns the response information to the integration agent.
5. The integration agent's response actions script sends a request, based on the response choice, to HPOM for Linux using the XM-OMU-Bridge application.
6. The event is updated in HPOM for Linux.

1.1 System Requirements

The following products must be installed and operating correctly prior to integration:

- xMatters relevance engine 5.1 (patch 001 or later).
- xMatters integration agent 5.1 (patch 003 or later)
- HP Operations Manager for Linux software 9.1

1.1.1 Operating Systems

The following component versions, operating systems and databases are supported by this integration.

Integration Component	Version	Operating System	Database
xMatters relevance engine	5.1 patch 001	Linux CentOS 5.3 (validated) Microsoft Windows 2008 R2	Oracle 11g (validated) SQL Server 2008
xMatters integration agent	5.1 patch 003	Linux CentOS 5.3 (validated) Microsoft Windows 2008 R2	
HP Operations Manager for Linux software	9.1	Linux CentOS 5.3 (validated) All operating systems supported by the xMatters integration agent	

1.2 Conventions and Terminology

This section describes how styles are used in the document, and provides a list of definitions.

1.2.1 Conventions

Some instructions appear in the following format: **MENU > OPTION**; for example, **File > Open** means click the **File** menu, and then click the **Open** menu option.

Words in **bold** typically reference text that appears on the screen. Words in `monospace` font represent the following:

- text that must be typed into the computer
- directory and file names
- code samples

Directory paths

This document uses the following shorthand placeholders to refer to the installation locations of the software components.

The xMatters installation folder is referred to throughout the documentation as `<xMHOME>`**.**

The default location is `/opt/xmatters/`

The xMatters integration agent installation folder is referred to throughout the documentation as `<IAHOME>`**.**

The default location is `/opt/xmatters/integrationagent`

1.2.2 Terminology

The following terms are used through the xMatters documentation.

Documentation terminology

Term	Meaning
Event	An *event* refers to any situation or item of interest detected by the management system, and which requires attention. Event is also used to refer to the incident or situation as it progresses through the xMatters system, from injection to notification to resolution. Each event must generate at least one alert or notification. Event can also be a generic term used to refer to an incident, change request, message, or other specific item within the management system. Whenever possible, these situations are referred to using the management system's preferred terminology, but can also collectively be called events.
Management system	A *management system* is any sort of IT service management software, and with which xMatters can combine; i.e., a synonym for HPOM for Linux.
Device	The medium through which a recipient is contacted by xMatters is referred to as a *Device*; i.e., email, pager, phone, etc.
User	In xMatters, people who can receive notifications are called *Users*. Each person in the xMatters system is defined by a set of User details, including ID number, user name, login password, and so on.
Group	*Groups* are used to collect and organize Users and Devices into notification schedules. For a complete explanation of Groups in xMatters, see the *xMatters user guide*.

Chapter 2: Installation and Configuration

This chapter provides information about installing the xMatters (IT) for HP Operations Manager for Linux integration. This chapter also contains complete instructions on how to configure xMatters, HPOM for Linux, and the integration components.

2.1 Installing the integration

The instructions in this chapter do not include information on how to install xMatters relevance engine, the xMatters integration agent, or HP Operations Manager for Linux software. These components must be installed according to their related documentation, and operating properly before you can proceed with the integration.

Note: *For more information about installing xMatters relevance engine and other xMatters products, refer to the xMatters web site at http:///www.xmatters.com.*

To begin installing and configuring the installation, extract the integration archive file to a location on your management server.

2.1.1 Integration components

The following table describes some of the notable components in the integration archive:

Integration components

Component Name	Description
install_xmatters_hp_oml_ RHEL.sh	This script automates much of the installation and configuration steps for the integration.
om_xmatters.sh	This wrapper script takes the parameters used by HPOM for Linux for calling xMatters, and translates them into the parameters required by xMatters.
	This program translates requests generated from xMatters and passed by the integration agent into queries that can be responded to by a HPOM for Linux server.

2.1.2 Running the integration installer

This integration includes a script to automate many of the steps required to install the integration on the management server.

Note: *Ensure that your HPOM for Linux instance is running properly before running the installation script.*

To run the automated install script:

1. Navigate to the directory where you extracted the integration archive file and locate the installation file, `install_ xmatters_hp_oml_RHEL.sh`.
2. Open the file in a text editor and verify that the paths at the beginning of the file are valid for your environment.
   - If you accepted the default paths when installing all of the related components, those paths should match the defaults in the installation script.
3. Verify that the specified user and group match a user and group installed on your system, and that HPOM for Linux users who will be interacting with messages sent into xMatters are members of the specified group.
   - The defaults in the script should match a default xMatters application.
4. After ensuring that the variables in the script match your environment, and that HPOM for Linux is running properly, you can execute the script.
   - This may require that you set the execute permission on the script before you can run it. For example:

```
chmod u+x install_xmatters_hp_oml_RHEL.sh
./install_xmatters_hp_oml_RHEL.sh
```

Watch the outcome of the script to make sure that everything ran properly. If any issues occurred, you may need to open the script and run each process within separately, one at a time.

Testing the Bridge installation

To ensure that the Bridge program was installed successfully, run the following command:

```
<IAHOME>/bin/XM-OMU-Bridge -u xMattersOM -p xMattersOM --validate
```

If the provided credentials are valid, you should see: `ValidateCredentials:true`

If the Bridge is working properly, this command returns "Total:", followed by the number of active messages that this user can see.

2.1.3 Installing the integration service and updating the integration agent

If you have more than one integration agent providing the "hpoml-1-0-1" service, repeat the following steps for each one. If you are not certain of the settings required in this section, consult your HPOM for Linux administrator.

To install the integration service:

1. Open the `<IAHOME>\integrationservices\hpoml-1-0-1\oml-config.js` file and modify the following variables to match your HPOM for Linux installation:

Property	Description
OML_URL	The URL at which the integration agent can contact the HPOM for Linux API.
OML_USER	The HPOM for Linux user to use for API calls.
OML_PASSWORD_FILE	Location of the file containing the API user's password; for instructions on how to set the password for this user, see "Setting API user password", below.
DEDUPLICATOR_FILTER	Name of the filter in the `<IAHOME>/conf/deduplicator-filter.xml` file; default is hpoml-1-0-1.

2. Restart the integration agent.

Setting API user password

This integration includes an encrypted file, located in the `<IAHOME>\conf` folder, that stores the password for the API user required for the management system. You will need to update the file with the correct password for the OML_USER variable specified in the `oml-config.js` file.

Password file name:

- `hpoml.pwd` stores the password for the OML_USER user used by the hpoml-1-0-1 integration service. If you change the name of this file, you must also update the `oml-config.js` file to point to the correct password file.

To specify the API user password:

1. Open a command prompt, and then navigate to `<IAHOME>\bin`.
2. Run the following command, where <new_password> is the password for the user specified in the `oml-config.js` file, <old_password> is the existing password (the default value for a newly installed integration is "password"), and <filename> is the name of the password file (`hpoml.pwd`).

```
iapassword.bat --new <new_password> --old <old_password> --file conf/<filename>.pwd
```

2.1.4 Installing voice files

These files must be installed into any xMatters deployment running a voice Device Engine. For more information, refer to the *xMatters installation and administration guide*.

This integration provides a complete set of English voice files.

To install the voice files:

1. Determine the value of the File Identifier associated with your Company.
   - To find your Company's File Identifier, log into the xMatters web user interface as the Super Administrator, and view the target Company's Details page (**Admin** tab **> Companies > Company name**).
2. Copy the contents of the `\components\xmatters\vox\` folder from the extracted integration archive to the following node installs folder:

```
<xMHOME>\node\phone-engine\Datastore\<FILE_IDENTIFIER>\
```

For example, if you were installing the integration for the Default Company on an out-of-the-box deployment, the installation path for the voice files would be as follows:

```
<xMHOME>\node\phone-engine\Datastore\1\hpoml-1-0-1\recordings\english\phrases
```

2.1.5 Validate installation

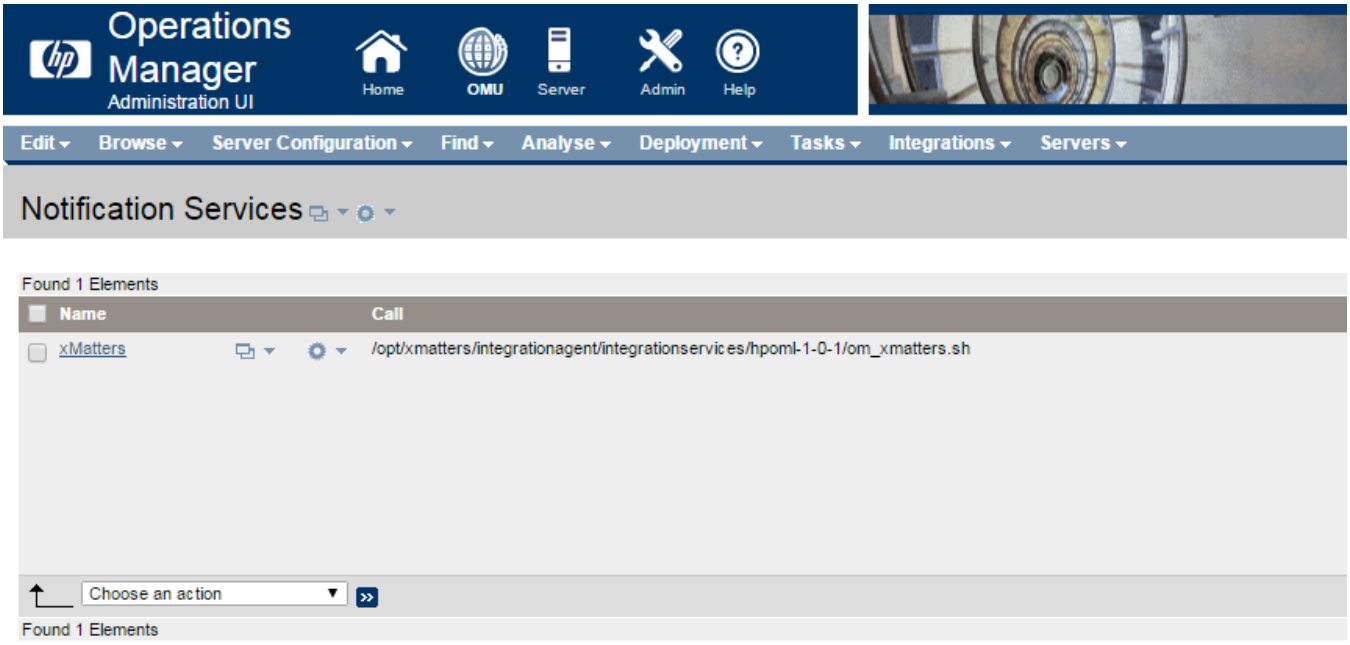
After installing the integration components and configuring xMatters, you can use the steps in the following sections to validate the installation with your HPOM for Linux installation.

To begin, start the Operations Manager Administration UI. Execute the steps in the following sections and ensure that your screens match or resemble the examples shown.

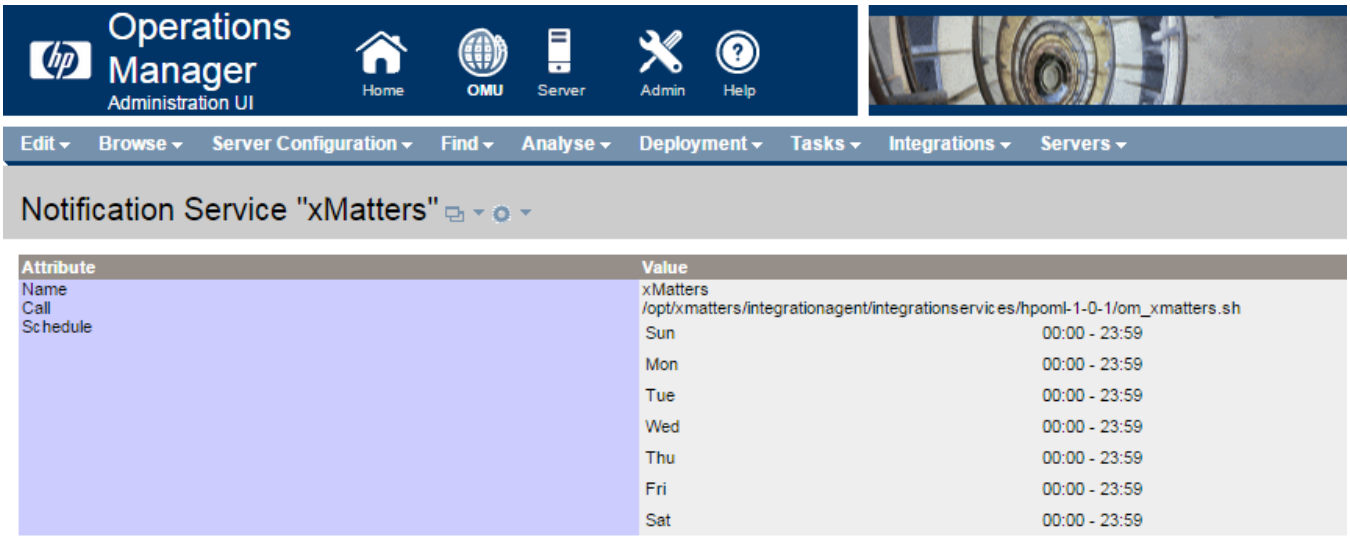
2.1.6 Notification Service

To verify that the notification service has been configured:

1. In the Operations Manager Administration UI, on the HPOM for Linux Configuration page, click the **All Notification Services** link.
   - HPOM for Linux displays the Notification Services page, indicating that xMatters is the Notification Service, and that it is scheduled to be active 24 hours a day, 7 days a week:



2. Click the **xMatters** link to display the Notification Server details.
   - The path displayed in the Notification Server details dialog box should be identical to the path on which `om_xmatters.sh` was installed. Verify that the path is correct.

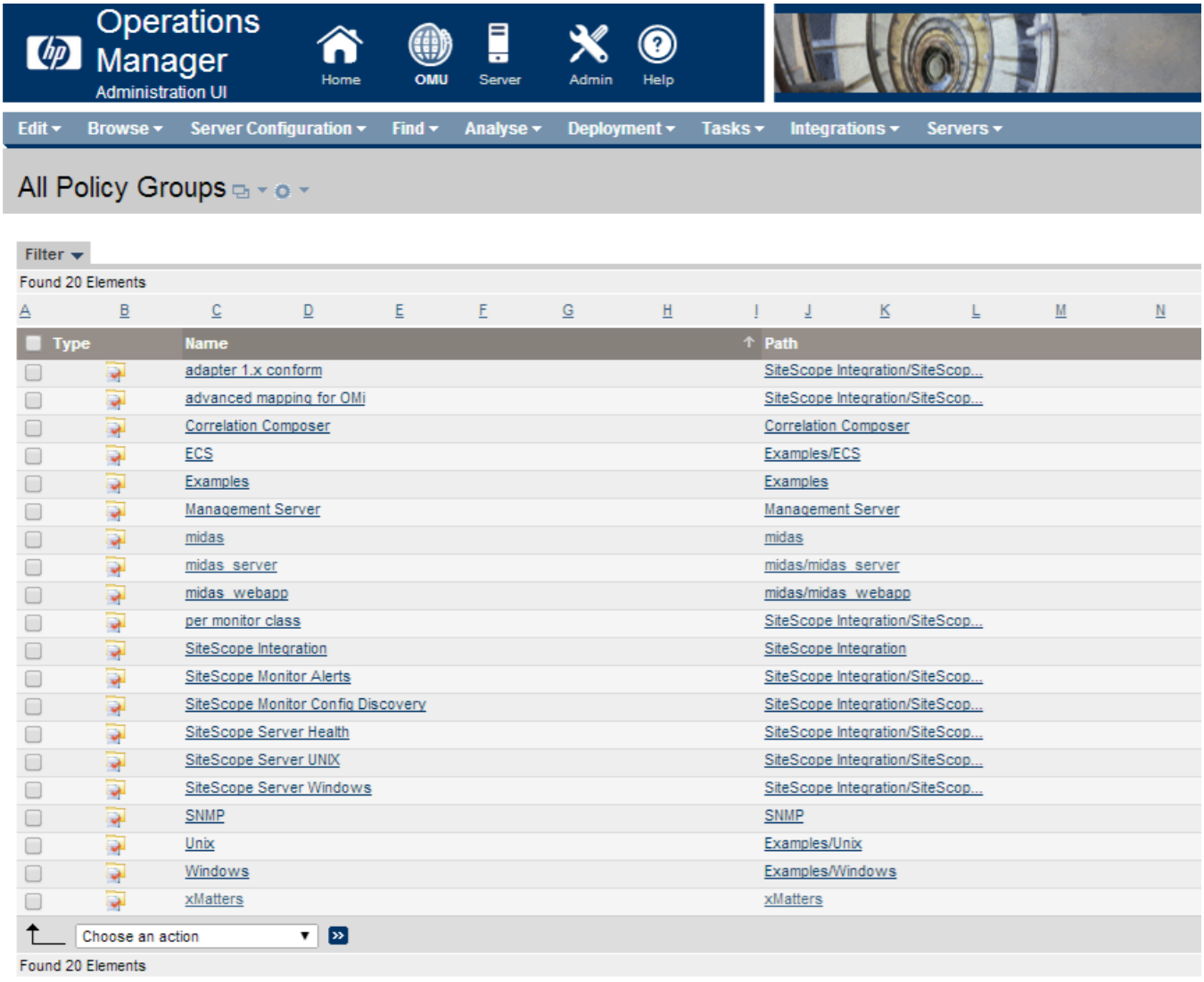


3. Click the **OMU** link to return to the Configuration page.

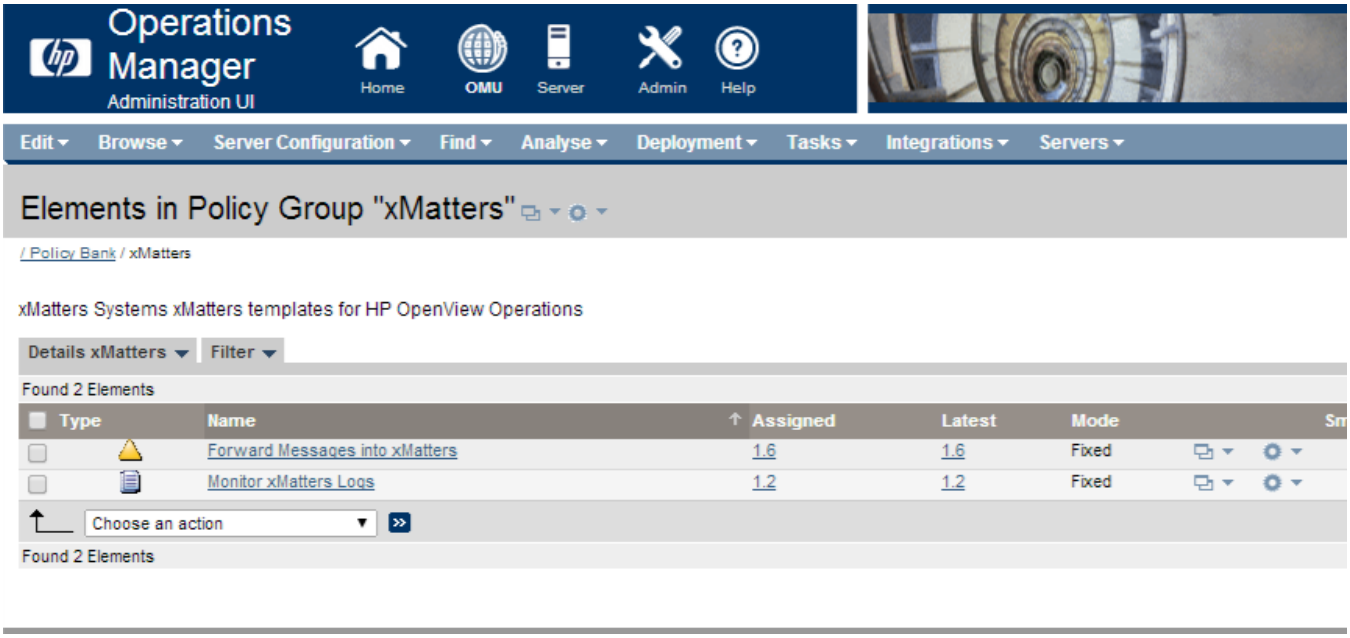
2.1.7 Message Policies

To verify the message policies:

1. On the HPOM for Linux Configuration page, click **Show All**.
   - HPOM for Linux displays the list of Policy Groups:



2. Click **xMatters**, and verify that the xMatters Policy Group contains two Policies:

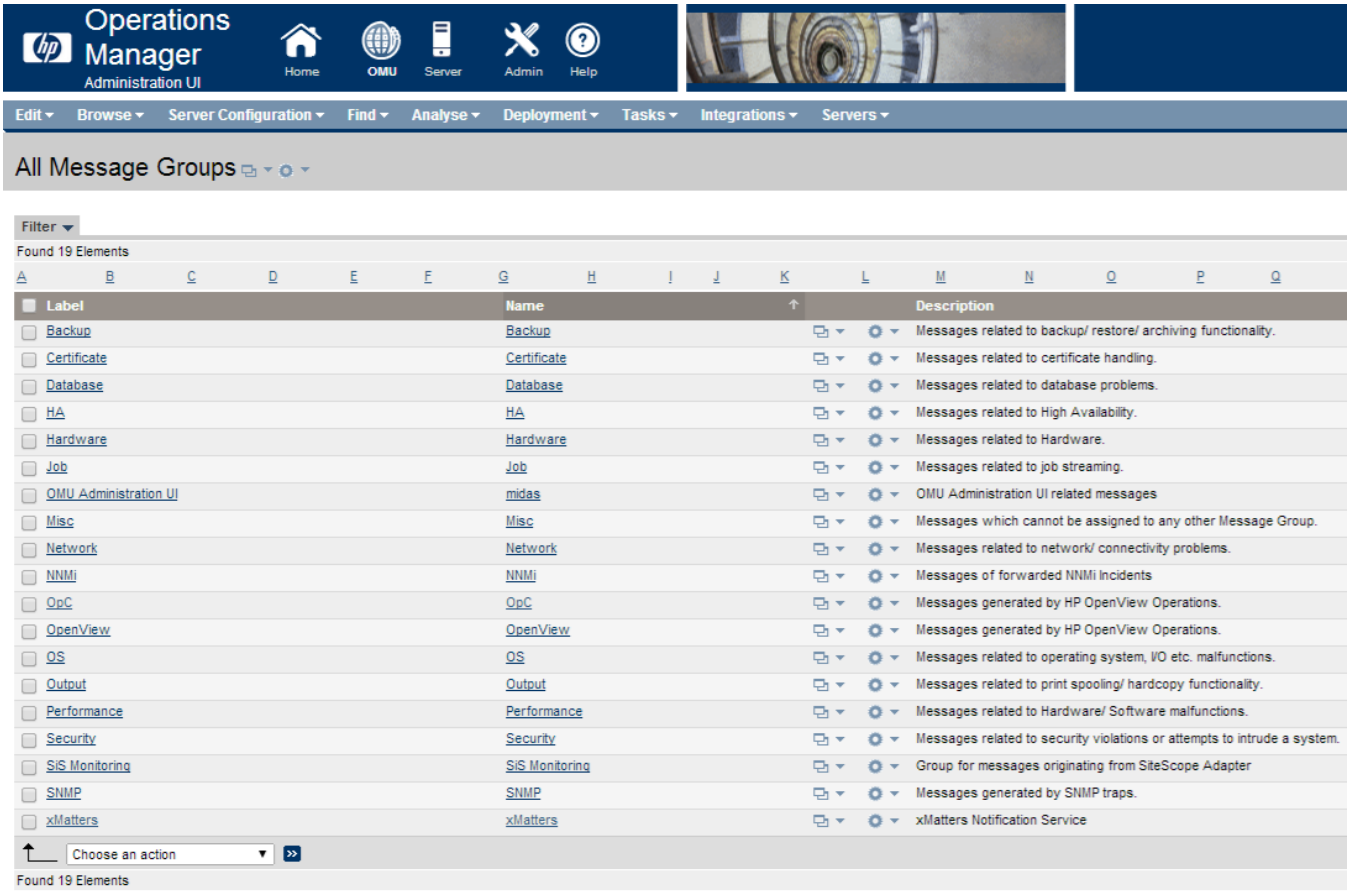


3. Click the **OMU** link to return to the Configuration page.

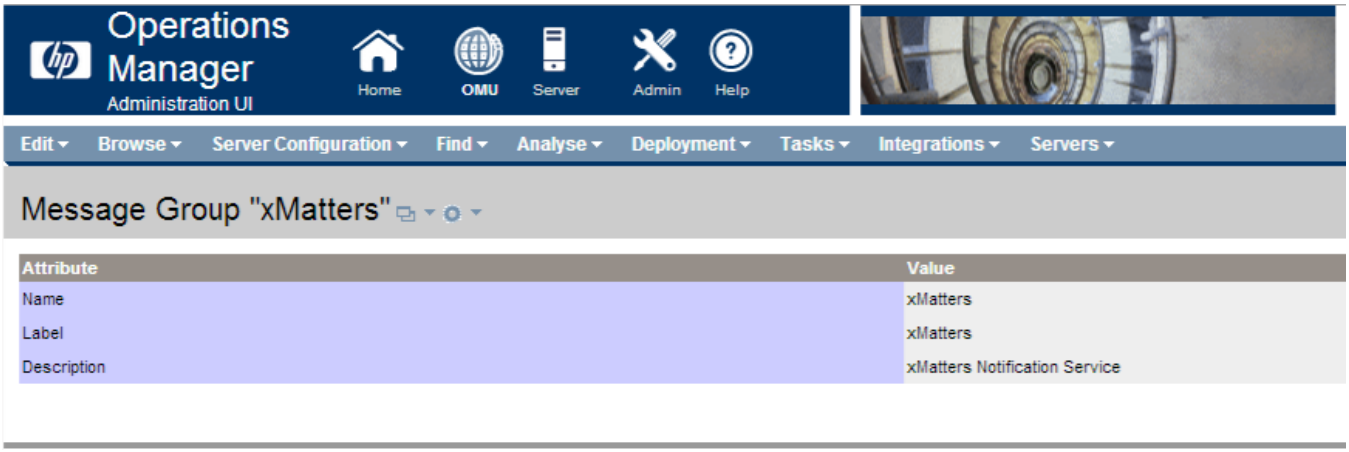
2.1.8 Message Group

To verify the message group:

1. On the HPOM for Linux Configuration page, click the **All Message Groups** link.
   - HPOM for Linux displays the list of Message Groups:



2. On the All Message Groups page, click **xMatters**, and verify the xMatters Message Group:

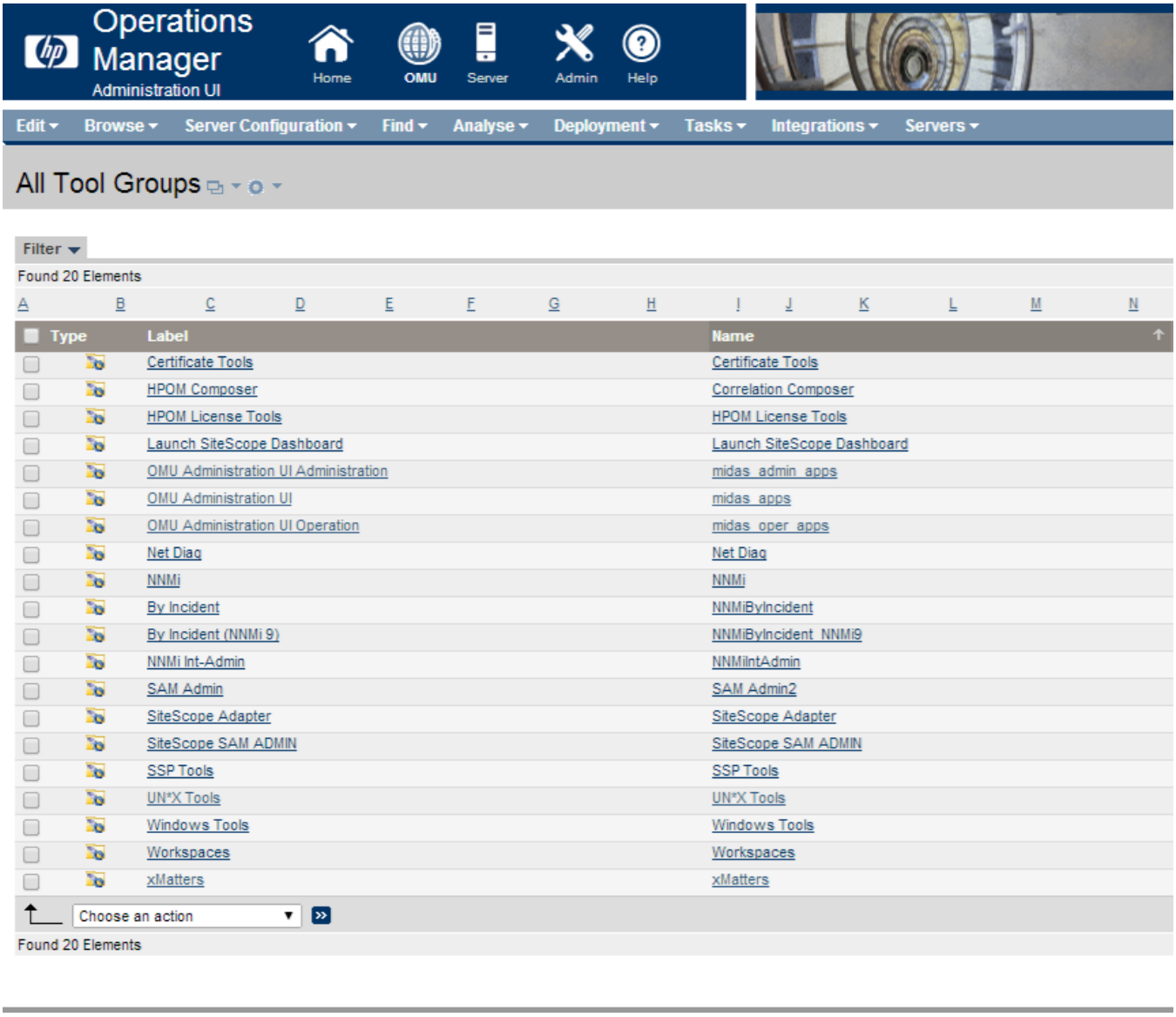


3. Click the **OMU** link to return to the Configuration page.

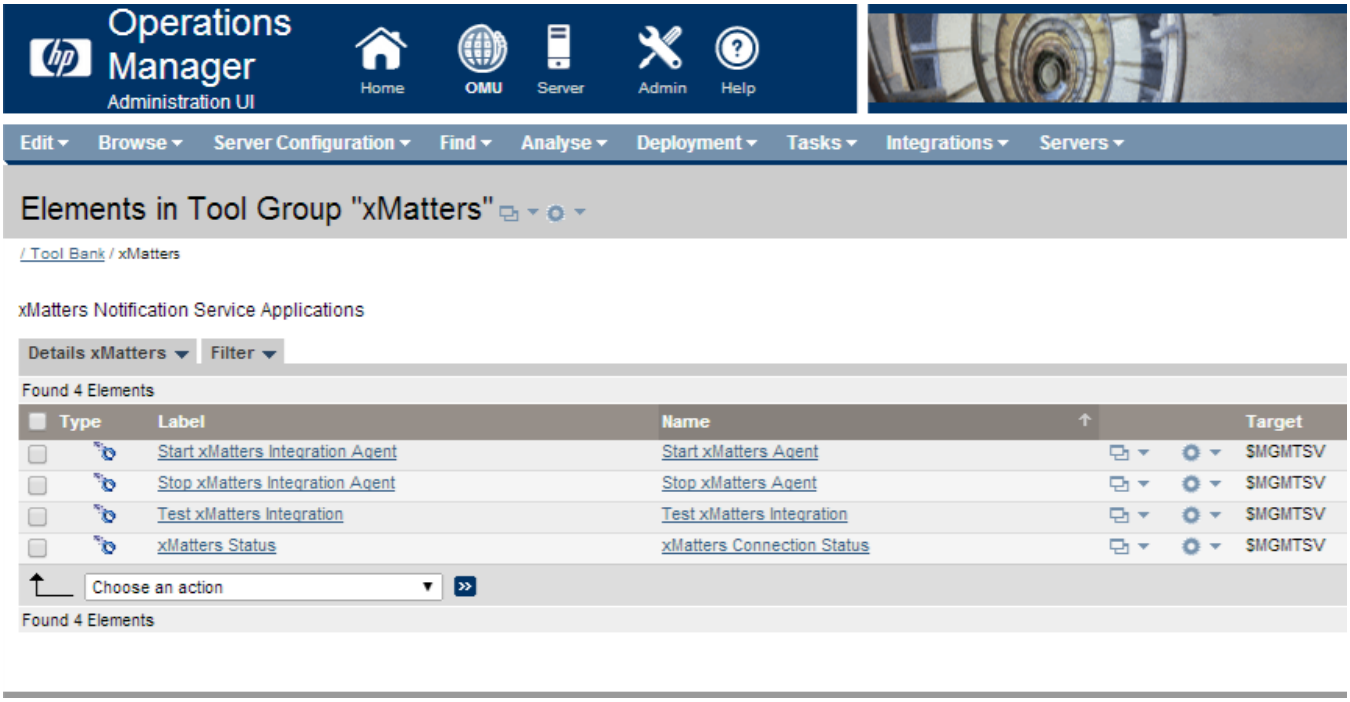
2.1.9 Tools

To verify the tools:

1. On the Configuration page, click the **All Tool Groups** link.
   - HPOM for Linux displays the list of tool groups:



2. Click **xMatters**, and verify that the xMatters tool group contains the following tools:
   - **xMatters Status**: runs an `iadmin.sh` get-status command, which returns the status of the integration agent and the connection to the xMatters Server.
   - **Start xMatters Integration Agent**: starts the integration agent.
   - **Stop xMatters Integration Agent**: stops the integration agent.
   - **Test xMatters Integration**: generates a test message and sends it to the Operations Group in xMatters. (For information about using this tool, see "Triggering a notification" on page 21.)



3. Click the **OMU** link to return to the Configuration page.

2.2 Configuring xMatters

The following sections describe how to configure xMatters to combine with HPOM for Linux.

2.2.1 Importing Event Domain and scripts

The integration package includes an XML file that was created using the xMatters "Export Integration" feature; this greatly simplifies the xMatters configuration process by enabling you to create the integration Event Domain, configure the predicates and Event Domain Constants, and import the integration script package in a single step.

To import the integration Event Domain package:

1. Log in to xMatters as a Company Administrator, and click the **Developer** tab.
2. In the Domains menu on the left side of the screen, click **Event Domains**.
3. On the Event Domains page, click **Import New**.
4. On the Import Integration page, click **Browse**, and then locate the `components\xmatters\event-domain\XM-HP-OM-L.xml` file extracted from the integration archive.
5. Click **Open**, and then click **Upload**.

xMatters imports the integration configuration settings and displays the new hpoml-1-0-1 Event Domain.

Defining the integration services

For the installation to be successful, the integration service name must match the name specified in the `hpoml.xml` file installed on the integration agent.

To define an Integration Service:

1. In xMatters, on the Event Domains page, click the **hpoml-1-0-1** Event Domain.
2. On the Event Domain Details page, in the Integration Services area, click **Add New**.

3. Enter the following information into the form:
   - **Name**: hpoml-1-0-1
   - **Description**: HPOM for Linux Integration Service
   - **Path**: *Not required. (This field is used by the xMatters mobile access component, which is not included in this integration.)*
4. Click **Save**.

Specifying connection parameters

Once you have imported the Event Domain package and configured the Integration Service, you must specify an xMatters address that is reachable from within a notification so that responses can be processed.

To specify the connection constants:

1. On the Event Domains page, in the Domains menu, click **Event Domain Constants**.
2. In the **Event Domain** drop-down list, select **hpoml-1-0-1**, and then click **Continue**.
   - xMatters displays the pre-configured Event Domain Constants for the integration:
3. In the Event Domain Constants list, specify the correct values for the following constants (click the name of a constant to edit its value and description):

Constant Name	Default Value	Description
xmattersurl	http://localhost:8888	Used to specify the address of the xMatters web server. The links provided in notification content use this value to locate the xMatters web server which would process the response. For these links to work, this address must be reachable from the Device where the User will receive the notification; normally, this is the IP address or fully-qualified host name of the xMatters web server.
bespushurl	http://localhost:8888/static	Used to specify the address of the BES device server.

Note: *For more information about the Event Domain Constants included in the integration and how to configure them to suit your deployment, see "Defining Event Domain Constants" on page 26.*

2.2.2 Adding the Web Service User

This integration requires a Web Service User to query for events to be injected to xMatters. The following steps describe how to configure the default Web Service User, IA_User, for this integration.

To set up a Web Service User:

1. In xMatters, click the **Users** tab, and then click **Find Web Service Users**.
2. On the Find Web Services Users page, click **All**.
3. In the returned search results, locate and click **IA_User**.
4. On the Details for IA_User page, confirm that the list of Allowed Web Services includes the **Query Incident** web service; if Query Incident is not listed in the Allowed Web Services list, select it in the Denied Web Services list, and then click **Add**.
5. Click **Save**.

2.3 Configuring Subscriptions

The following sections describe how to manage subscriptions in xMatters, including instructions on how to configure a Subscription panel and assign subscriptions to users.

To allow users to subscribe to specific criteria on injected events, you must configure a subscription panel, which requires the following steps:

- Define the Event Domain predicates
- Define a Subscription Domain
- Create a Subscription
- Create a Fail-Safe Group

Defining Event Domain predicates

The default integration configuration uses the following Event Domain predicates to which you can subscribe:

- source_node
- application
- severity
- source_node_text
- message_group
- object

These predicates are automatically created in the Event Domain when importing the Event Domain package, as described in "Importing Event Domain and scripts" on page 13. To modify these predicates, or to add other predicates that you consider important, see "Modifying Event Domain predicates" on page 26.

2.3.1 Defining a Subscription Domain

The Subscription Domain is the reference point for Subscriptions, and allows you to control who can create Subscriptions, how recipients can respond to Subscription notifications, and which Event Domain predicates can be used to create a Subscription. You must create a Subscription Domain before you can create Subscriptions.

To create a Subscription Domain:

1. On the Developer tab, the Developer menu, click **Subscription Domains**.
2. On the Subscription Domains page, click the **Add New** link.
3. In the **Event Domain** drop-down list, select **hpoml-1-0-1**, and then click **Continue**.
4. On the Subscription Domain Details page, in the **Name** field, type `hpoml-1-0-1`.
   - By default, Subscriptions are non-FYI (i.e., they support response options). To disable two-way Subscription notifications, select the **One-Way** check box. Note that you will not be prompted to enter response choices for one-way Subscriptions.
5. In the **Type of Management** drop-down list, select **Both**.
6. Leave the **Custom Page URL** field blank, and click **Continue**.
7. On the Select Appropriate Response Choices page, specify the available responses for this Subscription, and then click **Continue**.
   - By default, the scripts support the following response choices: "Acknowledge", "Own", “Ignore”, and “Annotate”. To enable two-way communications for Subscriptions, define all response choices on the Select Appropriate Response Choices page.

8. On the Select Appropriate Predicates page, add all of the predicates to the **Applied Predicates** list, and then click **Continue**.
9. On the Select Roles page, specify the Roles you want to be able to create Subscriptions on the Domain, and then click **Save**.

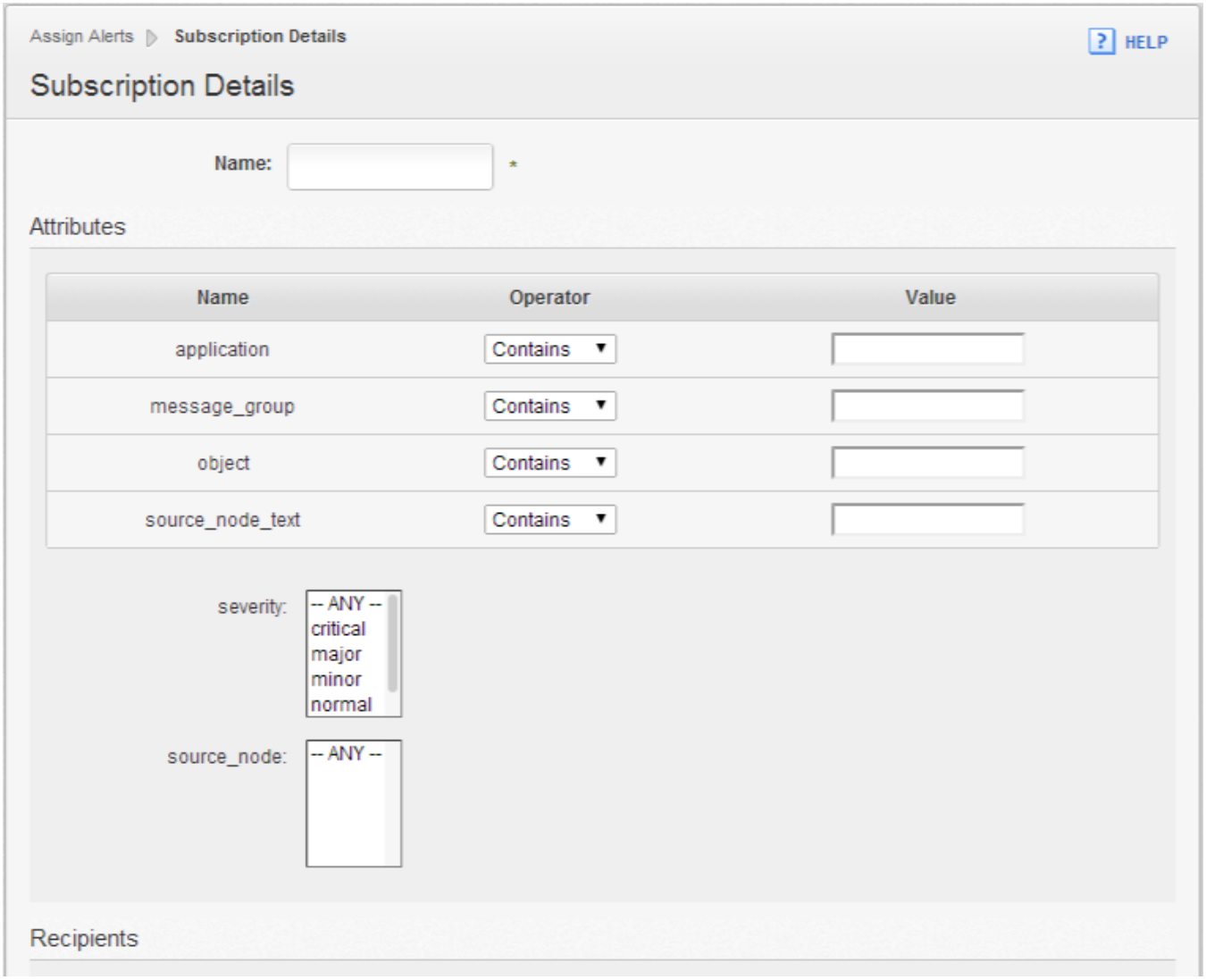
Note: *For more information about working with Event and Subscription Domains, see the* xMatters installation and administration guide.

2.3.2 Creating a Subscription

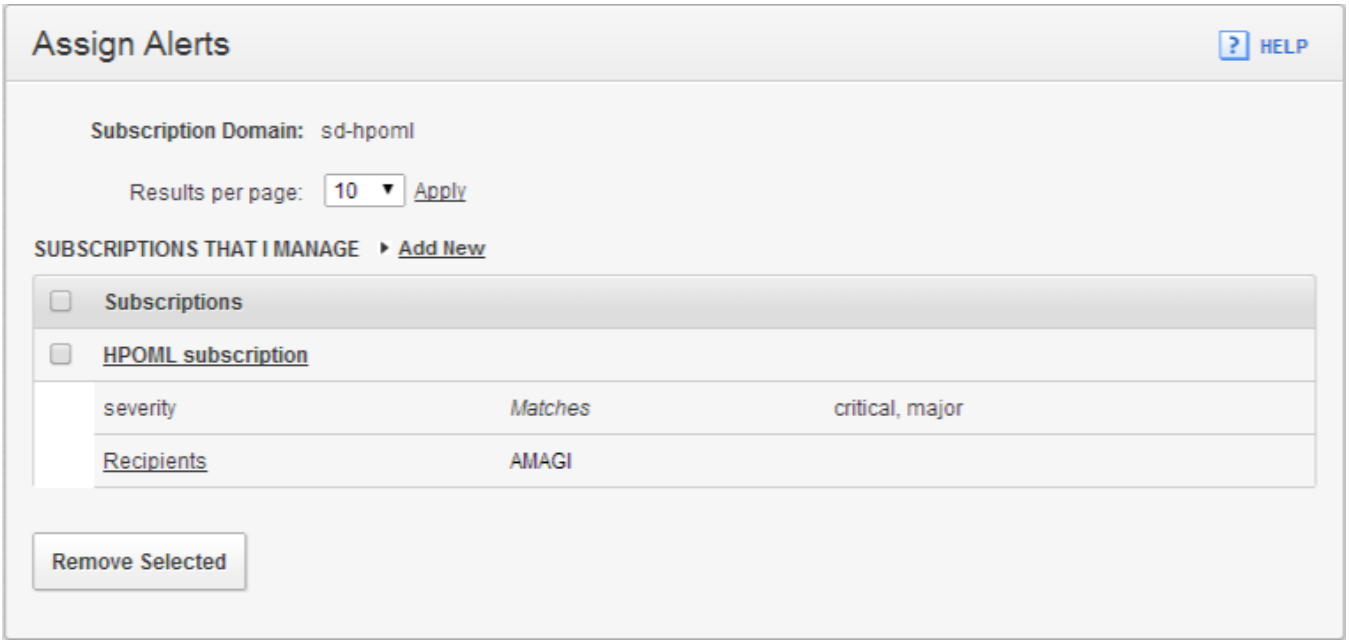
You can now subscribe to HPOM for Linux events that match specific criteria. For example, you could configure a subscription that would send a notification to a specific User each time an event entered the system that was of critical severity.

To create a Subscription:

1. On the Alerts tab, in the Alerts menu, click **Assign Alerts**.
2. Select the **hpoml-1-0-1** Subscription Domain, and click the **Add New** link.
3. On the Subscription Details page, specify a name for the Subscription, and set the Subscription criteria and recipients using the fields of the subscription panel.



4. In the Recipients area, click the links to add recipients.
5. When you are satisfied with the subscription details, click **Save** to create the Subscription.



Creating a fail-safe Group

If an event is submitted to xMatters when the fail-safe functionality is enabled, and there is no subscription that matches the event, xMatterssends the notification to the fail-safe recipient. The fail-safe recipient is typically a Group, but can be configured as a User.

To create a fail-safe Group:

1. In xMatters, click the Groups tab.
2. Create a new Group named HPOML FailSafe, with at least one User as a Team member to receive notifications.

For more information about creating Groups and Teams, see the xMatters user guide.

Note: *If you want to use an existing Group or a different Group name, modify the value for the failsafegroup Event Domain Constant. You can also eliminate notifying any fail-safe group by setting the failsafe constant to* disabled. *For more information, see "Configuring the Event Domain" on page 25.*

2.4 Configuring HPOM for Linux

The following sections describe how to configure HPOM for Linux to combine with xMatters.

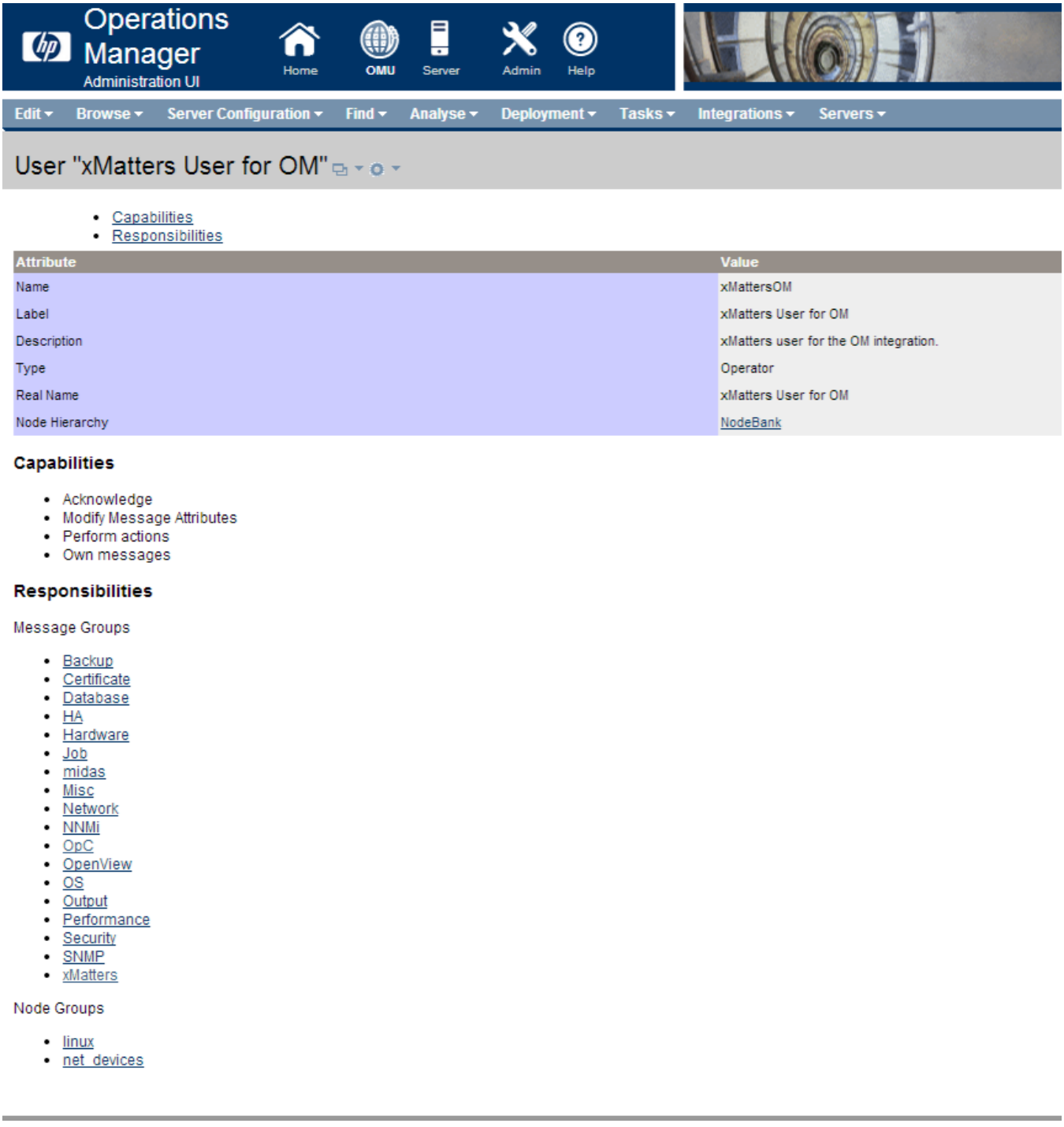
1. Assign the xMatters Policy Group to the nodes and node groups in your system that you want to cause notifications to be injected into xMatters.
2. Defgine the nodes and node groups that should be handled by the xMatters OM User by modifying the user profile and changing the list for the xMatters Policy Group.
3. Distribute the configuration changes, particularly the policies, to the nodes in your system..

2.4.1 Verifying the HPOM for Linux User

The user defined in this section is automatically configured during the installation of xMatters, and is the key user for the integration. The user is responsible for all interaction between HPOM for Linux and the integration agent.

To verify the xMatters OML user:

1. Log into the xMattersOM Administrator Console, and click **All Users**.
2. Verify that the xMatters User exists, and has the following properties and capabilities:



3. Verify that the user has all of the appropriate responsibilities to interact with all messages that are sent to xMatters for notification.
4. Click the **OMU** link to return to the Configuration page.

After you have verified the xMatters user, it is recommended that you change its password or login ID. Note that the password must also be changed in the xMatters Action Scripts. For more information, see "Configuring HPOM for Unix to Use a Different User" on page 32.

At this point, all the files necessary for the default integration are in their required locations on the management server. The next step in the validation is to configure HPOM for Linux to use the files properly:

1. Assign the xMatters Message Group to the nodes in your system that you want to cause notifications to be injected into xMatters.
2. Define the nodes that should be handled by the xMatters User Profile by modifying the profile and changing the list for the xMatters Message Group.
3. Assign the xMatters User Profile to the appropriate users in your system. Ensure they have responsibility for the correct set of nodes.
4. Distribute the configuration changes, particularly the Message Policies, to the agents in your system.

2.4.2 Enabling Policy Conditions

Although a number of sample policies with notifications enabled are provided, you must enable your policies to inject messages into xMatters. This is done via the standard notification interface.

Note: *Do not submit all events for notification. Tailor the policies to fit your specific business requirements and the capacity of your HPOM for Linux server, xMatters server and communications infrastructure.*

To enable a particular policy condition for notification:

1. On the Configuration page, click **Show All**.
2. Click the **Actions** icon for the policy you want to edit, and then select **Edit** from the drop-down list.
3. On the Edit Policy page, click the **Conditions** tab, and then expand the condition you want to enable.
4. On the Actions tab, select the **Notification** check box.
5. Click the **Custom Attributes** tab.
6. In the drop-down list, select **D_Add attribute**.
7. In the **Name** field, type `person_and_group_id`.
8. In the **Value** field, type the target name of the recipient who should receive notifications for this condition.
   - This target name is usually the name of a group in xMatters.
9. In the drop-down list, select **D_Add attribute**.
10. In the **Name** field, type `Destination`.
11. In the **Value** field, type `xMatters`.
12. Click **Save**.

Update the Policy version on your Nodes and Node Groups, and then deploy the configuration.

Custom "recipient" attribute

By creating a "recipients" custom parameter, you can set the xMatters recipient (or a comma-delimited list of recipients) that should be targeted for notification whenever HPOM for Linux generates a message that matches that condition.

Once the parameter is placed on the condition, the Input Action Script for the integration automatically directs the notification to the correct recipient in xMatters. There is no need to adjust the scripts in the Developer IDE, as they are already set up to accommodate this particular custom field.

Typically, the recipient identified in the Condition's attribute will be an xMatters group, but could be a dynamic team, user, or any other type of recipient.

Using the Message Policies

Sample Policies are provided with notification enabled; these provide support for the Test xMatters Integration Tool and for monitoring various failure conditions in xMatters. You can use these Policies as a basis for customizing your Message Policies to monitor any problems in your network for which you want to use xMatters to notify people about the issue.

2.4.3 Adding a Destination Column

The default Policies and Conditions provided with this integration include a Destination attribute. If you add another column to the All Active Messages pane in the HPOM Java Console to display the Destination property, you can easily determine which messages are being sent to xMatters.

To add a Destination column:

1. Launch the HPOM for Linux Java Console.
2. In the All Active Messages pane, right-click one of the column headings, and then select **Customize Message Browser Columns**.
3. In the Customize Message Browser Columns dialog box, click the **Custom** tab.
4. In the Available Custom Message Attributes area, select the **Destination** check box, and then type `Destination` in the label field.
5. Click **Add**, and then click **OK**.
6. The All Active Messages pane will now display "xMatters" in the Destination column for all messages sent to xMatters:

Chapter 3: Integration Validation

After configuring xMatters and HPOM for Linux, you can validate that communication is properly configured. It is recommended that you start the components in the following order:

- HP Operations Manager for Linux software
- xMatters relevance engine
- xMatters integration agent

Consult the respective user manuals for details on starting these applications.

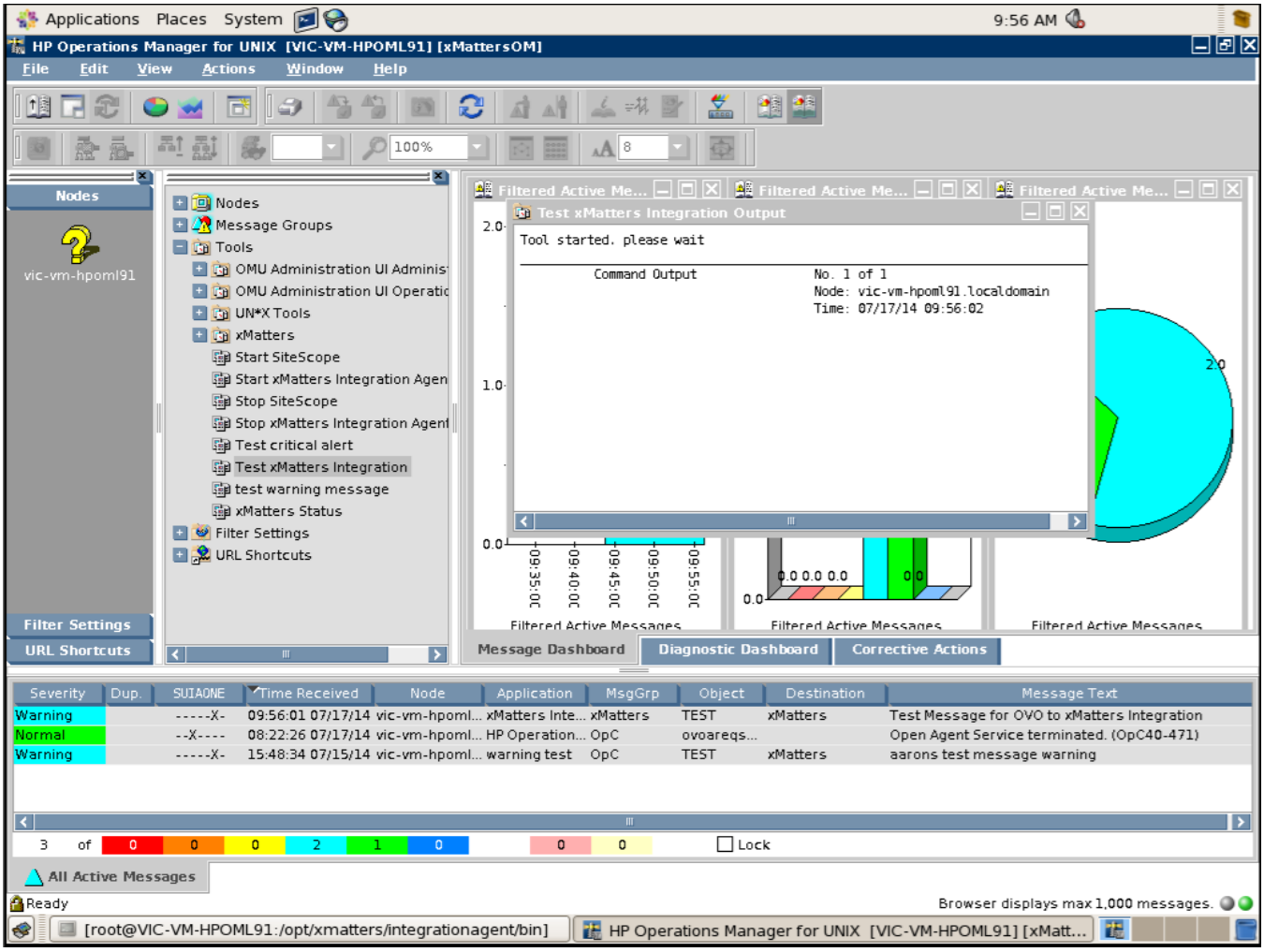
The following sections will test the combination of xMatters and HPOM for Linux for notification delivery and response, and Subscription Panel functionality.

3.1 Triggering a notification

In this example, the Test Tool included with the integration is used to trigger a CRITICAL event in HPOM for Linux. The xMatters policy detects that a CRITICAL event has occurred, and sends notifications to xMatters.

To trigger a CRITICAL event:

1. Open the HPOM for Linux Console, and expand the tree in the left pane (**Tools > xMatters**) to display the test tool.
2. Double-click **Generate a Critical Test Message to xMatters**.
3. Select the check box next to the Management Server you want to use.
4. Click **Next**, and then click **Launch**.
    - The Nodes area displays the CRITICAL event:



3.2 Responding to a notification

This section describes how to respond to a notification from xMatters. In the following example, the notification is received as an email message, but the process is similar for all Devices.

To respond to a notification:

1. Opening the notification displays its details:

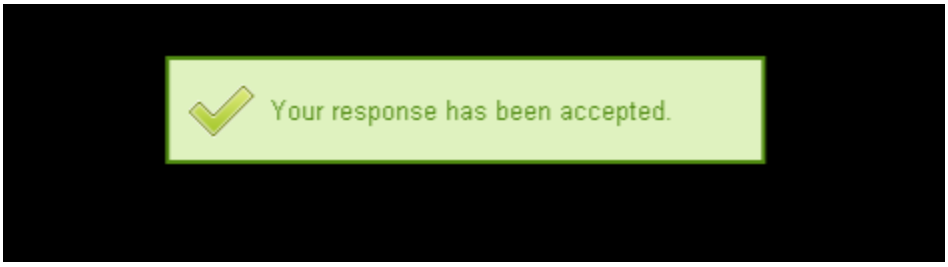
(x) matters
The relevance engine company.

HP Operations Manager Linux - Automated Notification	
Time of Event:	Wednesday, 31 Dec 1969 16:00:00 GMT-0800
Target:	AMAGI|Work Email
Severity:	warning
Node:	vic-vm-hpoml91.localdomain
Application:	xMatters Integration Test
Message Group:	xMatters
Object:	TEST
Description:	Test Message for OVO to xMatters Integration
Message GUID:	3ba7ea8e-0dd3-71e4-13fa-c0a89f990000

Provided you can connect to the xMatters Web Server, you can respond by selecting one of the following links:

1. Acknowledge
2. Own
3. Ignore
4. Change Sev Critical
5. Change Sev Major
6. Change Sev Minor
7. Change Sev Warning
8. Change Sev Normal

2. To respond to the notification, the user clicks a response choice such as "Own", and xMatters updates the event in HPOM for Linux.



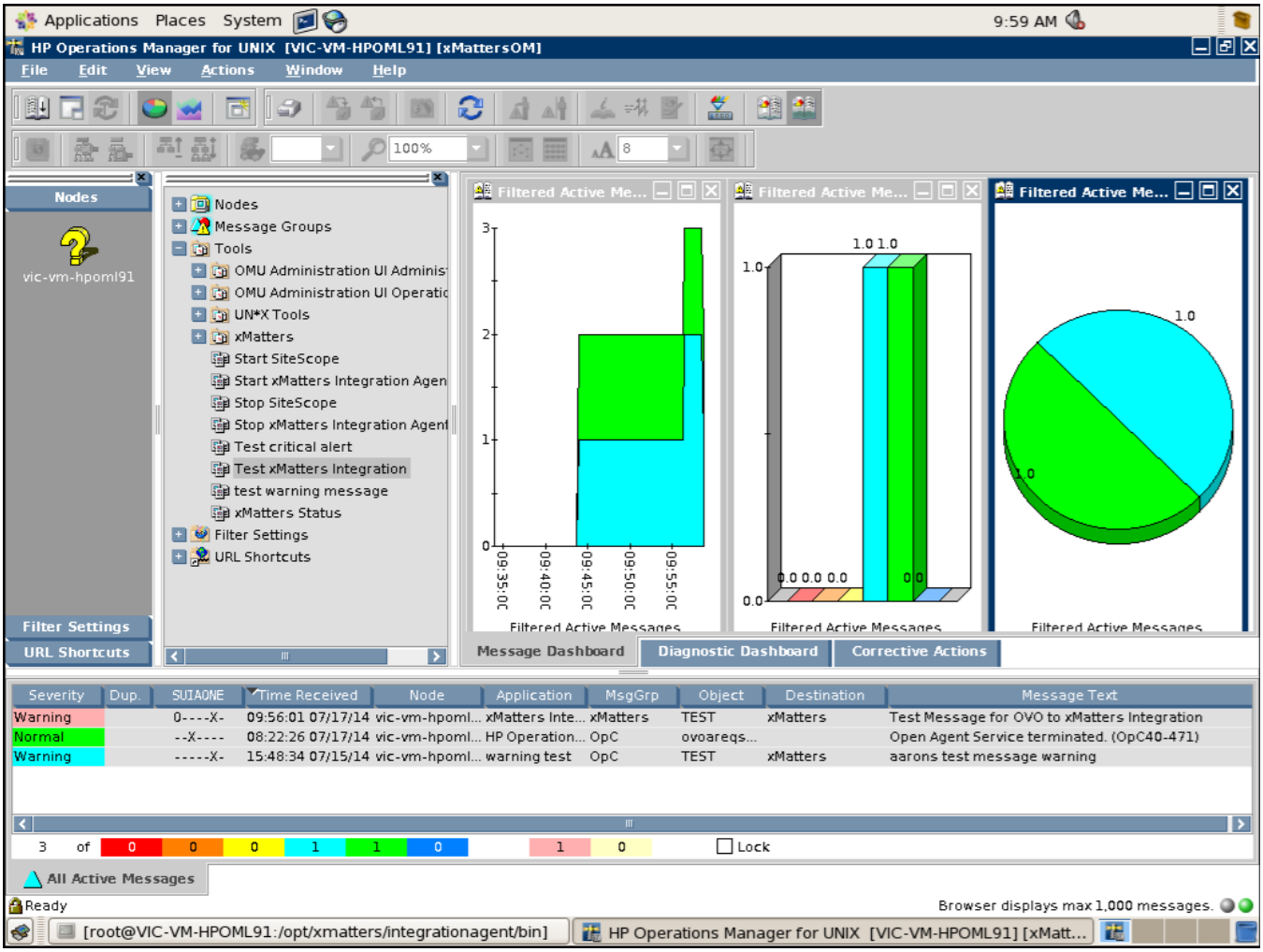
For more information about response choices, and changing the options available to Users, see "Response Choices" on page 29.

3.3 Viewing response results

In the HPOM for Linux Console, the message will now be displayed as "Owned" in the message pane.

To view the notification results:

1. Right-click **Nodes**, and then select **View > Filter Active Messages.**
2. Select the message from the list, and view the **Properties** tab:



3. To display the messages annotated to the event, click the **Annotations** tab:

Chapter 4: Optimizing and Extending the Integration

This section describes some of the available methods you can use to optimize or extend the xMatters (IT) for HP Operations Manager for Linux integration.

4.1 Manually configuring xMatters

This integration includes an exported version of the Event Domain, including constants and predicates. You must import this package to create and configure the required Event Domain and scripts; the following sections describe how to manually configure and verify these components after you have imported them.

4.1.1 Configuring Users

Each xMatters User that will be notified and respond to notifications must be configured to allow xMatters to communicate with HPOM for Linux as that User. Note that each User must also be configured in HPOM for Linux.

To configure a User:

1. In xMatters, click the **Users** tab.
2. Use the Find Users page to locate the User you want to configure and view their details.
3. In the Common Tasks pane, click **User Devices**.
4. Verify that an appropriate Device exists and that it is enabled.
5. Click **Save**.

Note: *If you have no Users in the system, you can use the default demonstration User, "bsmith". If this User does not exist, create a User with the User ID "bsmith", and add a virtual text phone Device. For more information and instructions on how to perform these tasks, refer to the* xMatters user guide.

4.1.2 Configuring the Event Domain

By default this integration is set up to use an Event Domain of "hpoml-1-0-1"; it is strongly recommended that you use this default Event Domain. For the integration to be successful, the Event Domain name must match the value in the integration agent configuration file for the integration service (i.e., the <domain> tag in `hpoml.xml`).

The xMatters relevance engine web server must be running to perform this portion of the integration.

To define an Event Domain:

1. Log in to xMatters as a Company Administrator, and click the **Developer** tab.
2. In the Developer menu on the left side of the screen, click **Event Domains**.
3. On the Event Domains page, click **hpoml-1-0-1**.
4. Verify the following information:
   - **Name**: hpoml-1-0-1
   - **Description**: HPOM for Linux Integration
   - **Script Package**: HP Operations Manager for Linux
5. Click **Save**.

Once you have verified the Event Domain, you can add the integration service, as described in "Defining the integration services" on page 13.

Modifying Event Domain predicates

The default predicates for the integration are automatically created in the Event Domain when importing the Event Domain package, as described in "Importing Event Domain and scripts" on page 13. The following instructions are included to explain how to add or modify these predicates, and explain how the default configuration relates to event details in HPOM for Linux.

To define Event Domain predicates:

1. In xMatters, click the **Developer** tab.
2. On the Event Domains page, click hpoml-1-0-1.
3. On the Event Domain Details page, click **Add New**.
4. Add the following predicates to the Event Domain:

Event Domain predicates

Predicate	Type	Important	Values
source_node	List	Yes	Populate with a list of the source nodes in your HPOM for Linux.
application	Text	Yes	
severity	List	Yes	A list of severity levels; possible values are: • normal • warning • minor • major • critical
source_node_text	Text		
message_group	Text		
object	Text		

Note: *For more information about populating list values for the NODE, NODE_GROUPS, MSG_OBJECT, and MSG_SOURCE predicate, see .*

Defining Event Domain Constants

Company Administrators and Developers can create Event Domain Constants that will be available in scripting for all event objects associated with an Event Domain.This integration uses Event Domain Constants to define custom values for the integration script package.

The integration script package uses the names of the constants defined in the table below to look up the values; it is strongly recommended that you use the names specified, or speak to your xMatters client assistance representative before changing these values.

Note: *The values for the xmattersurl and bespushurl constants should be modified to specify the address of the xMatters web server (to enable the HMTL response options) and the BES device server.*

To add an Event Domain Constant:

1. In xMatters, click the **Developer** tab, and then, in the menu on the left side of the screen, click **Event Domain Constants**.
2. In the **Event Domain** drop-down list, select **hpoml-1-0-1**.
3. On the Event Domain Constants page, click **Add New**.
4. Define a **Constant Name**, **Value**, and **Description** for the new constant, according to the table below.
5. Click **Save**.
6. Repeat the above steps for each of the constants you want to add.
    - Note that if the constants are not defined in the web user interface, the scripts will use the values listed in the Default Values column of the following table.

Note: *Shaded rows indicate **mandatory** settings that are specific to your deployment. You must change the default settings to match your instance.*

Event Domain Constants

Constant Name	Default Value	Description
xmattersurl	http://localhost:8888	Used to specify the address of the xMatters web server. The links provided in notification content use this value to locate the xMatters web server which would process the response. For these links to work, this address must be reachable from the Device where the User will receive the notification; normally, this is the IP address or fully-qualified host name of the xMatters web server.
bespushurl	http://localhost:8888/static	Used to specify the address of the BES device server. Populates the `$main.bes_pushurl` parameter.
forcefyi	disable	Force notifications to be informational only (FYI), rather than requiring responses; this overrides the fyi behaviour specified on the injected event. Possible values: • **disable**: Nothing is forced. • **on**: Notifications are forced to be FYI. • **off**: Notifications are forced not to be FYI.
failsafegroup	HPOML FailSafe	The fail-safe recipient to notify, typically a group. The fail-safe group identifies the recipient that will be notified if an event is injected to xMatters relevance engine and no subscriptions exist that match the event. Set this constant if you want to change the failsafe group from HPOML FailSafe to another group defined in xMatters.

Constant Name	Default Value	Description
failsafe	enabled	Controls fail-safe functionality, notifying the fail-safe recipient via EMAIL under certain circumstances; possible values are: • **enabled**: Notify if no subscriptions match or no notifiable recipients. • **for-subscriptions**: Notify if subscription functionality is enabled AND no subscriptions match. • **for-recipients**: Notify if no notifiable recipients. • **disabled**: Disable fail-safe functionality.
overridetimeframes	false	Override Recipients Device Timeframes.
useemergencydevices	false	Force the use of emergency Devices.
trackdelivery	true	Track when each device is delivered to. Setting this to false may give a performance advantage, but you lose any information about whether a delivery was successful or not.
annotate	true	Enables submission of annotations back to the management system.
subscriptionannotate	true	Enables submission of Subscription annotations back to the management system.
tracksubscriptiondelivery	true	Track when each device is delivered to for Subscriptions. Populates the `$track_subscriptionDelivery` parameter.
timeout	259200	Amount of time (in seconds) the event is allowed to run before timing out. 259200 seconds = 72 hours.
maxinvalidresponses	3	Specifies the maximum number of invalid responses allowed before notification is no longer requeued.
enablehtmlemail	true	Enables HTML email functionality.
uselogo	true	Set this if you want the logo displayed within HTML email notifications.
useurlalias	false	Indicates how Response Choices are presented to xMatters to ensure that the user is authenticated in the correct company so the notification can be updated.
debug	false	Indicates whether to use the debug level for logging messages.
enablesubscriptions	true	Indicates whether to enable processing of Subscriptions on incoming events.
subscriptionfyi	false	Indicates whether Subscriptions should be forced to be informational only (FYI).
numericpagernumber	555-1212	The callback number to be used as the subject for outgoing notifications to numeric pagers.

4.2 Response Choices

This integration allows recipients to respond to notifications with several default choices, some of which are injected back to the HPOM for Linux server, updating the original event. Users notified on email devices also have the ability to respond with an extra annotation message which will be logged in the original event.

The following is a list of the default response choices available with the integration and their associated actions on the xMatters Event and the HPOM for Linux event:

Response Choice	xMattersAction	HPOM for Linux Update	Default Device Availability
Acknowledge	Delinks everyone from the xMatters event (deletes/terminates the event), and halts notifications from being delivered. **Note**: If FYI Subscriptions are being delivered, they are allowed to finish.	Removes the message for the active messages browser view and puts it in the acknowledged message browser.	Email, BES, Browser. For other non-FYI mobile devices an Acknowledge is represented as an Ack.
Own	Delinks all users other than the responder from the event, not allowing them to submit responses. The owner will not be notified further, but has the ability to affect the event by responding on one of their Devices or from the browser. For example, a User owns the event in xMatters, and then changes the severity of the event. They may also acknowledge or annotate the owned event.	The owner gains exclusive read/write access to the message. Other users can see the message, but have limited access.	All non-FYI devices.
Ignore	Signifies that the User rejects the notification. The rejection causes the action script to escalate to the next recipient in the Group.	A reject message is sent back to HPOM for Linux and logged as an Annotation; it has no effect on the state of the message.	Email, BES and Browser. For other non-FYI mobile Devices an Ignore is represented as an Ign.
Change Severity	Halts delivery of notifications to any other Devices the responding User may have configured. Delinks all Users other than the User changing the severity.	Handles the changing of the message severity. Possible severities: • Critical • Major • Minor • Warning • Normal	Email, BES and Browser. If notified on a phone Device, the option to change severity is provided as a phone menu. (Can only change the severity up or down, but have unlimited number of times to do so; i.e., it requires four times to go from critical to warning.)

Response Choice	xMattersAction	HPOM for Linux Update	Default Device Availability
Annotate	Halts delivery of notifications to any other Devices the responding User may have configured.	Allows the User to provide a message to be posted to the annotation of the message. When an annotation is provided the state of the message does not change.	This functionality is available for text-based Devices only.

4.2.1 Responses for FYI notifications

FYI notifications do not have any response choices available, except for FYI notifications sent to voice Devices. Voice FYI notifications offer the following response choices so that Users can navigate between multiple notifications. (This navigation is not required on other Devices.)

Voice Device responses for FYI notifications

Response	Description
Delete	Removes the notification from the User's list. This option is most likely to be selected.
Save	Saves the notification and stops attempting to deliver it to the User's other Devices. Users may select this option to delay listening to the notification when it is delivered, and access the details by calling in, or via the xMatters web user interface, at a later time.
Repeat	Replays the notification content.

4.3 Altering the duration of events

You can modify the amount of time xMatters will send out notifications for a particular event before it times out by changing the "timeout" Event Domain Constant. This constant stores the number of seconds the notifications will be allowed to continue before timing out.

For example, if you wanted to change the event duration to two hours, you could change the value for the timeout constant to **7200**.

Note: *For more information about working with Event Domain Constants, see "Configuring the Event Domain" on page 25.*

4.4 Uninstalling

For instructions on removing an xMatters deployment, refer to the *xMatters installation and administration guide*.

Chapter 5: Configuration Variable Reference

This section outlines and describes the configuration variables available in the initial PROCESS Action Script.

Note that many of the configuration variables are configurable using the Event Domain Constants, as described in "Configuring the Event Domain" on page 25; those variables are not listed here.

5.1 Global configuration variables

These variables are available throughout the script package, and are parameters of the “main” object. The value assigned to each variable is its default value within the script.

Gobal variables

Variable	Description
$main.use_logFile = false	Specify whether to use an alternate log file for debugging messages. This variable is ignored unless $main.debug is also set to true.
$main.logFile = "../logs/"	Defines the file used to log debugging information (only if $main.use_logfile is set to true).
$main.logo_alt_text = “[If the logo does not appear you may be blocking images or you may be outside a firewall. If the latter, the links will not work for responding and you should respond by replying to this email as described below.]”	The alternate text to display if the HTML email logo is unavailable. **Note**: If the logo does not display, it is unlikely that the HTML_form_url is valid and responses will not be injected from HTML Devices (email and BES).

www.xMatters.com

12647 ALCOSTA BLVD., SUITE #425 SAN RAMON CA 94583 USA | P: 1-877-xMattrs + 1.877.962.8877
CENTRAL COURT 25 SOUTHAMPTON BUILDINGS, LONDON WC2A 1AL UK | P: +44 (0) 800 652 7711