Monitoring Java Management Extensions (JMX)

JMX Base Pack *BETA* PowerPack version 101

Table of Contents

Introduction 3
What is JMX? 3
What Does the JMX Base Pack *BETA* PowerPack Monitor? 4
Installing the JMX Base Pack *BETA* PowerPack 4
Configuration and Discovery 5
Prerequisites for Monitoring JMX Resources 5
Creating Credentials to Monitor JMX Resources 6
Creating a Credential to Monitor a Single Port 6
Creating a Credential to Monitor Multiple Ports 7
Discovering JMX Resources 8
Understanding the Dynamic Applications in the JMX Base Pack *BETA* PowerPack 9
Manually Aligning the "JMX: Inventory" Dynamic Application 9

Chapter 1

Introduction

Overview

This manual describes how to monitor Java Management Extensions (JMX) resources in SL1 using the *JMX Base Pack *BETA** PowerPack.

The following sections provide an overview of JMX resources and the *JMX Base Pack *BETA** PowerPack:

What is JMX? 3
*What Does the JMX Base Pack *BETA* PowerPack Monitor?* 4
*Installing the JMX Base Pack *BETA* PowerPack* 4

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

What is JMX?

Java Management Extensions (JMX) is a Java framework that is used for managing applications and other resources, which are represented by objects called Managed Beans (MBeans). The *JMX Base Pack *BETA** PowerPack is compatible with JMX resources from Oracle and IBM vendors.

What Does the JMX Base Pack *BETA* PowerPack Monitor?

To monitor JMX resources using SL1, you must install the *JMX Base Pack *BETA** PowerPack. This PowerPack enables you to collect data about JMX resources that are being run on HotSpot, JVM, or OpenJDK systems.

The *JMX Base Pack *BETA** PowerPack includes:

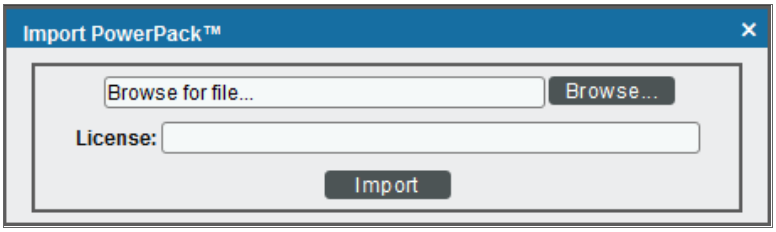
- Dynamic Applications to monitor JMX resources
- Two sample credentials that you can use to create your own JMX credentials

Installing the JMX Base Pack *BETA* PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *JMX Base Pack *BETA** PowerPack.

To download and install a PowerPack:

1. Download the PowerPack from the ScienceLogic Customer Portal.
2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*.
4. The **Import PowerPack** dialog box appears:



5. Click the **[Browse]** button and navigate to the PowerPack file.
6. When the **PowerPack Installer** modal page appears, click the **[Install]** button to install the PowerPack.

NOTE: If you exit the **PowerPack Installer** modal page without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPack Manager** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal page. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Chapter 2

Configuration and Discovery

Overview

The following sections describe how to configure and discover Java Management Extensions (JMX) resources for monitoring by SL1 using the *JMX Base Pack *BETA** PowerPack:

Prerequisites for Monitoring JMX Resources 5

Creating Credentials to Monitor JMX Resources 6

Creating a Credential to Monitor a Single Port 6

Creating a Credential to Monitor Multiple Ports 7

Discovering JMX Resources 8

*Understanding the Dynamic Applications in the JMX Base Pack *BETA* PowerPack* 9

Manually Aligning the "JMX: Inventory" Dynamic Application 9

Prerequisites for Monitoring JMX Resources

Before you can monitor JMX resources in SL1 using the *JMX Base Pack *BETA** PowerPack, you must have the following information:

- The IP address of the HotSpot, JVM, or OpenJDK system that uses the JMX resources you want to monitor
- The username and password for the system that you want to monitor
- The specific port numbers that you want to monitor

Creating Credentials to Monitor JMX Resources

To configure SL1 to monitor JMX resources on a HotSpot, JVM, or OpenJDK system, you must first create a credential that enables SL1 to communicate with that system. There are two ways you can do this:

- If you are monitoring only a single port on the system, you can create a Basic/Snippet credential to monitor that specific port.
- If you are monitoring more than one port on the system, you must create a SOAP/XML credential to monitor those specific ports.

The processes for creating both types of credentials are described in this section.

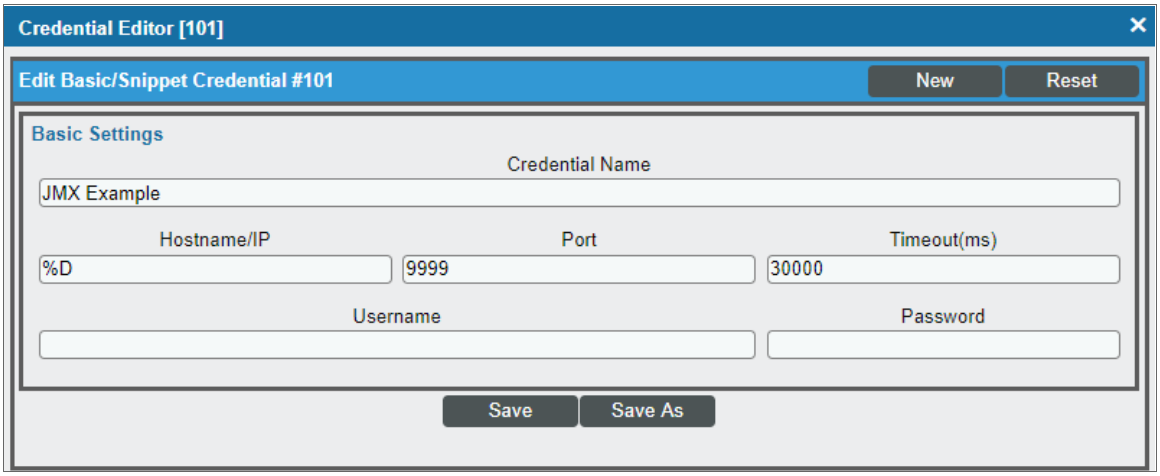
Creating a Credential to Monitor a Single Port

If you want to configure SL1 to monitor JMX resources on only a single port on a system, then you can create a Basic/Snippet credential to do so. This credential allows the Dynamic Applications in the *JMX Base Pack *BETA** PowerPack to connect with the server or virtual machine running JMX and access the port specified.

An example Basic/Snippet credential that you can edit for your own use is included in the PowerPack.

To create a Basic/Snippet credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **JMX Example** credential, and then click its wrench icon (). The **Edit Basic/Snippet Credential** modal page appears:



3. Complete the following fields:
   - ***Credential Name***. Type a new name for the credential.
   - ***Hostname/IP***. Type the IP address of the JMX system that you want to monitor, or type "%D".
   - ***Port***. Type the port number that you want to monitor.
   - ***Timeout(ms)***. Keep the default value.

- ***Username***. Type the username that is used to access the system that you want to monitor.
- ***Password***. Type the password that is used to access the system that you want to monitor.

4. Click the **[Save As]** button, and then click **[OK]**.

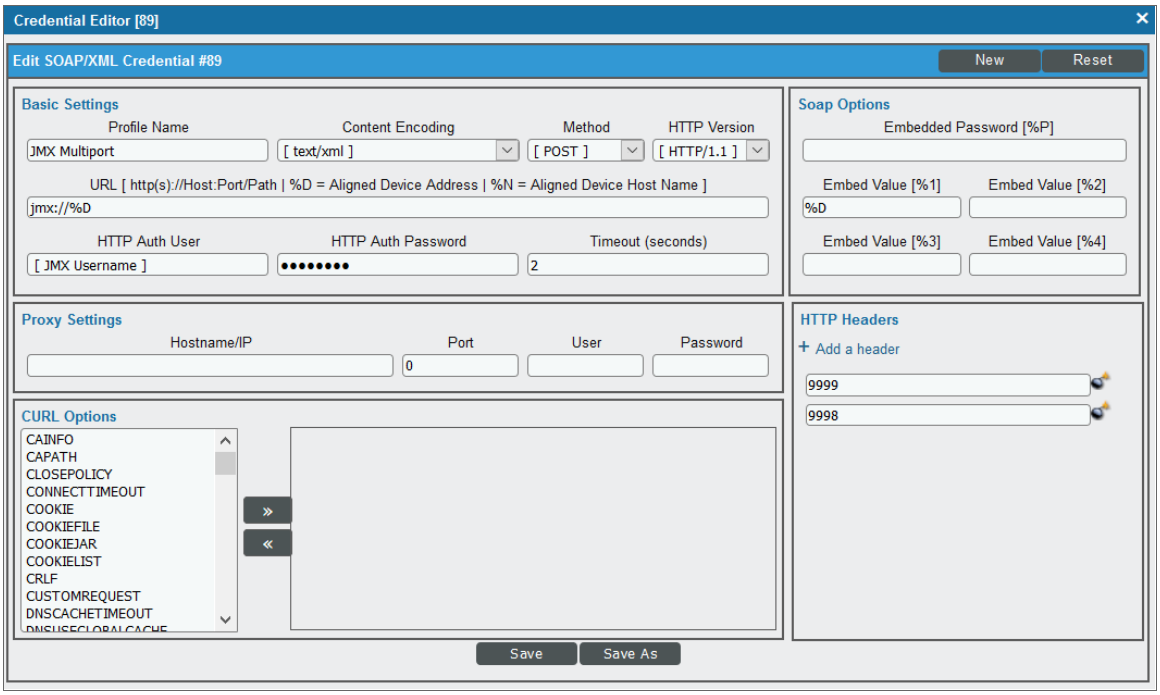
Creating a Credential to Monitor Multiple Ports

If you want to configure SL1 to monitor JMX resources on more than one port on a system, then you must create a SOAP/XML credential to do so. This credential allows the Dynamic Applications in the *JMX Base Pack *BETA** PowerPack to connect with the server or virtual machine running JMX and access all of the ports specified.

An example SOAP/XML credential that you can edit for your own use is included in the PowerPack.

To define a SOAP/XML credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **JMX Multiport** credential and click its wrench icon (). The **Credential Editor** modal page appears:



3. Enter values in the following fields:

Basic Settings

- ***Profile Name***. Type a new name for the credential.
- ***URL***. Keep the default value of "jmx://%D".
- ***HTTP Auth User***. Type the username that is used to access the system that you want to monitor.

- ***HTTP Auth Password***. Type the password that is used to access the system that you want to monitor.

SOAP Options

- ***Embed Value [%1]***. Type the IP address of the JMX system that you want to monitor, or type "%D".

HTTP Headers

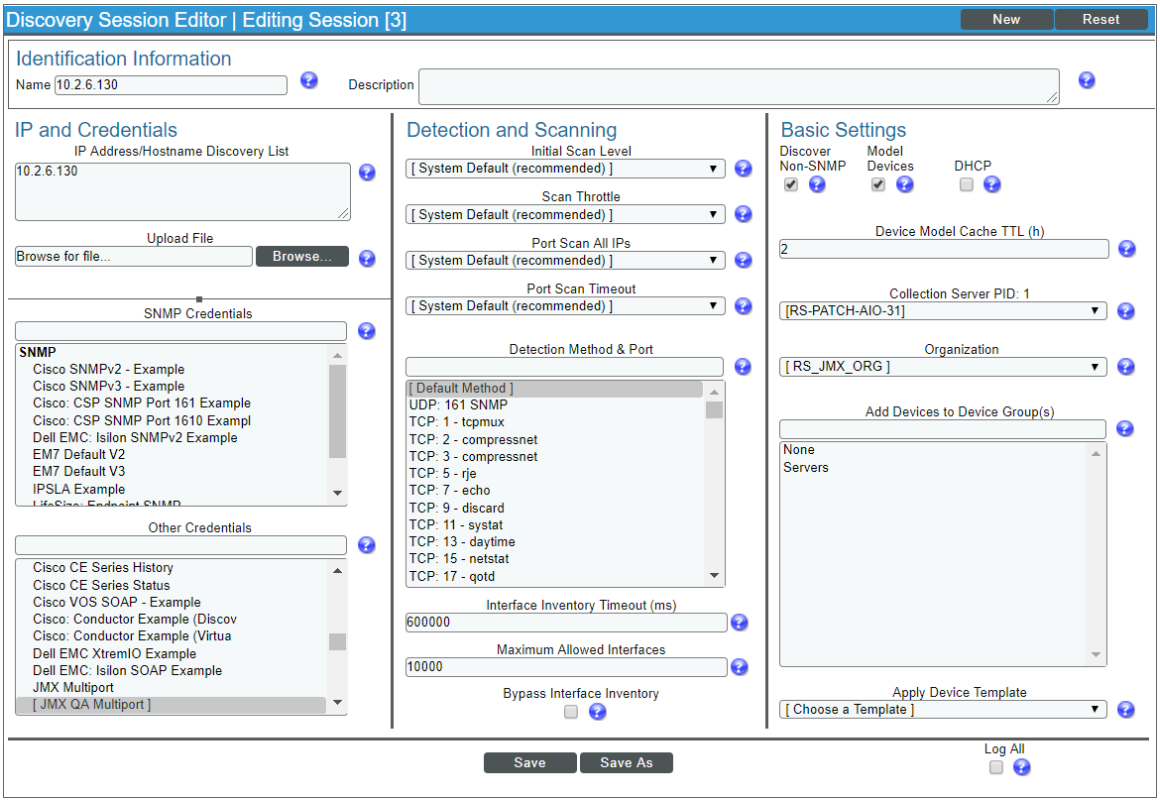
- ***Add a header***. For each port that you want to monitor, click **[Add a header]** and then type the port number that you want to monitor in the blank field that appears.

4. For all other fields, keep the default value.
5. Click the **[Save As]** button, and then click **[OK]**.

Discovering JMX Resources

To discover JMX resources:

1. Go to the **Discovery Control Panel** page (System > Manage > Discovery).
2. In the **Discovery Control Panel**, click the **[Create]** button. The **Discovery Session Editor** page appears.
3. On the **Discovery Session Editor** page, complete the following fields:



- ***Name***. Type a name for the discovery session.

- ***IP Address/Hostname Discovery List***. Type the hostname or IP address of the system that you want to monitor.
- ***Other Credentials***. Select the credential that you created for monitoring JMX resources.
- ***Discover Non-SNMP***. Select this checkbox.
- ***Model Devices***. Select this checkbox.

4. Optionally, you can enter values in the other fields on this page. For more information about the other fields on this page, see the ***Discovery & Credentials*** manual.
5. Click the **[Save]** button to save the discovery session and then close the **Discovery Session Editor** window.
6. The discovery session you created appears at the top of the **Discovery Control Panel** page. Click its lightning-bolt icon ( ) to run the discovery session.
7. The **Discovery Session** window appears. When the system is discovered, click the device icon ( ) to view the **Device Properties** page for the system.

Understanding the Dynamic Applications in the JMX Base Pack *BETA* PowerPack

In most casesFor the most part, the Dynamic Applications in the *JMX Base Pack *BETA** PowerPack align to MBeans that are exposed in the server being monitored. A single MBean will generally have a performance Dynamic Application and a configuration Dynamic Application aligned to it. However, the "JMX: Base Configuration (Sample)" and "JMX: Base Performance (Sample)" Dynamic Applications provide an overview of the server metrics and thus span multiple MBeans.

If you collect the same data from different ports, then the configuration Dynamic Applications in the *JMX Base Pack *BETA** PowerPack will display the data for each port separately in the Configuration Report. Performance Dynamic Applications will display the metrics for all ports monitored by a particular Dynamic Application as different lines on its corresponding performance graph. If a performance collection is disabled on the server being monitored, the corresponding metric in SL1 will appear as a zero value.

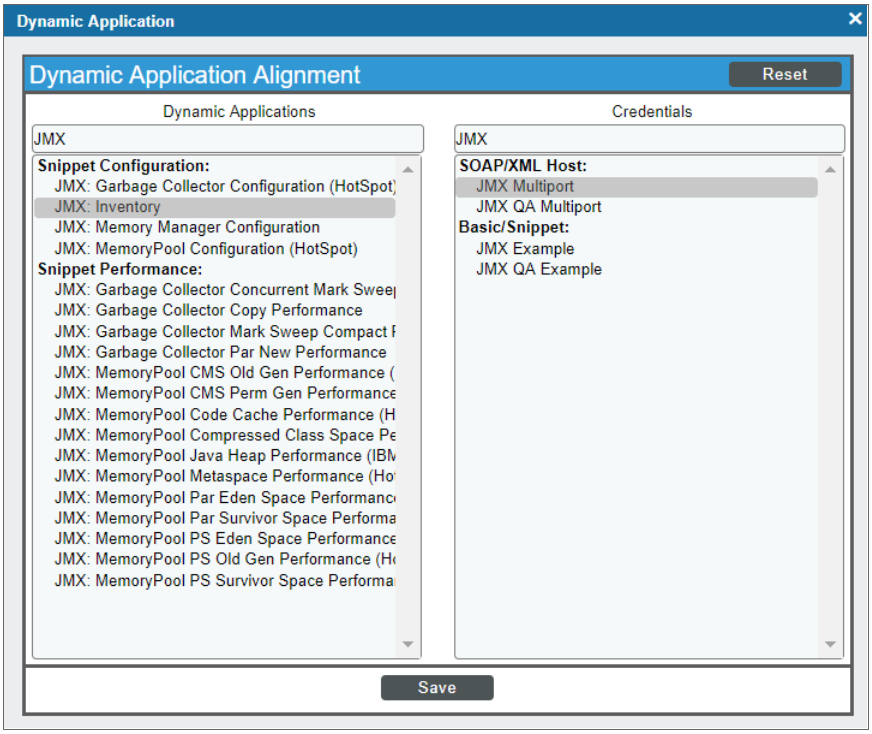
Dynamic Applications with names appended by "(IBM)" are used to collect data from IBM servers, while those appended by "(HotSpot)" collect data from servers that are using HotSpot or OpenJDK. Dynamic Applications with names that are not appended by "(IBM)" or "(HotSpot)" are compatible with both. However, some of these Dynamic Applications, such as "JMX: Memory Configuration", might collect more or different data from one source over the other, depending on the detail of the server type being monitored. This behavior is expected.

Manually Aligning the "JMX: Inventory" Dynamic Application

The "JMX: Inventory" Dynamic Application is not automatically aligned to your JMX system during discovery because of the possible load it can place on the Data Collector in some situations. This Dynamic Application provides a list of all JMX values that the system exports and their most recent values. You can then use that information to check that all necessary values are available for the system or create a new Dynamic Application to collect specific metrics that are not collected by other Dynamic Applications in the *JMX Base Pack *BETA** PowerPack. If you want to use the "JMX: Inventory" Dynamic Application, you must manually align it to your JMX system.

To manually align the "JMX: Inventory" Dynamic Application:

1. From the **Device Properties** page (Registry > Devices > wrench icon) for the JMX system, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. Click the **[Action]** button and then click *Add Dynamic Application*. The **Dynamic Application Alignment** page appears.
3. In the ***Dynamic Applications*** field, select the "JMX: Inventory" Dynamic Application.
4. In the ***Credentials*** field, select the credential you created for monitoring JMX resources.



5. Click the **[Save]** button.

© 2003 - 2019, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010