Monitoring Java Management Extensions (JMX)

JMX Base Pack PowerPack version 105

Table of Contents

Chapter 1

Introduction

Overview

This manual describes how to monitor Java Management Extensions (JMX) resources in Skylar One using the "JMX Base Pack" PowerPack.

This chapter covers the following topics:

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" PowerPack is compatible with JMX resources from Oracle and IBM vendors.

What Does the JMX Base Pack PowerPack Monitor?

To monitor JMX resources using Skylar One, you must install the "JMX Base Pack" 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" 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 PowerPack

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

TIP: By default, installing a new version of a PowerPack overwrites all content from a previous version of that PowerPack that has already been installed on the target system. You can use the ***Enable Selective PowerPack Field Protection*** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. For more information, see the section on *Global Settings*.

NOTE: For details on upgrading Skylar One, see the relevant *Skylar One Platform Release Notes*.

To download and install the PowerPack:

1. Search for and download the PowerPack from the **PowerPacks** page at the ScienceLogic Support Center (Skylar One > PowerPacks, login required).
2. In Skylar One, go to the **PowerPacks** page (System > Manage > PowerPacks).
3. Click the **[Actions]** button and choose *Import PowerPack*. The **Import PowerPack** dialog box appears.
4. Click **[Browse]** and navigate to the PowerPack file from step 1.
5. Select the PowerPack file and click **[Import]**. The **PowerPack Installer** modal displays a list of the PowerPack contents.
6. Click **[Install]**. The PowerPack is added to the **PowerPacks** page.

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

Chapter

2

Configuration and Discovery

Overview

This section describes how to configure and discover Java Management Extensions (JMX) resources for monitoring by Skylar One using the "JMX Base Pack" PowerPack.

This chapter covers the following topics:

Prerequisites for Monitoring JMX Resources

Before you can monitor JMX resources in Skylar One using the "JMX Base Pack" 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 Skylar One to monitor JMX resources on a HotSpot, JVM, or OpenJDK system, you must first create a credential that enables Skylar One 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.

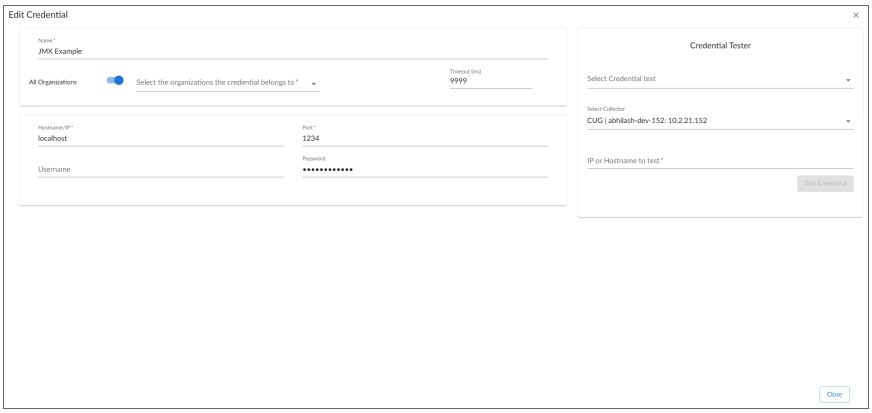
Creating a Basic/Snippet Credential to Monitor a Single Port

If you want to configure Skylar One 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" PowerPack to connect with the server or virtual machine running JMX and access the port specified.

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

To create a Basic/Snippet credential:

1. Go to the **Credentials** page (Manage > Credentials).
2. Locate the "JMX Example" credential, then click its **[Actions]** icon (⋮) and select *Duplicate* from the drop-down field. The "JMX Example copy" credential appears.
3. Click the **[Action]** icon (⋮) for the "JMX Example copy" credential, then select *Edit*. The **Edit Credential** page appears.



4. Enter values in the following fields:
    - ***Name***. Enter a new name for the credential. This field is required.
    - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***Select the organizations the credential belongs to*** drop-down field to align the credential with those specific organizations.
    - ***Timeout***. Enter the time, in milliseconds, after which Skylar One will stop trying to communicate with the JMX device. The default value is *30000*. This field is required.
    - ***Hostname/IP***. Enter the JMX url. The default is "%D".
    - ***Port***. Type the port number that you want to monitor.
    - ***Username***. Enter the username associated with the JMX administrator account.
    - ***Password***. Enter the password associated with the JMX administrator account.
5. Click **[Save & Close]**.

Creating a Basic/Snippet Credential to Monitor a Single Port in the Skylar One Classic User Interface

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

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

To create a Basic/Snippet credential in the classic user interface:

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]**.

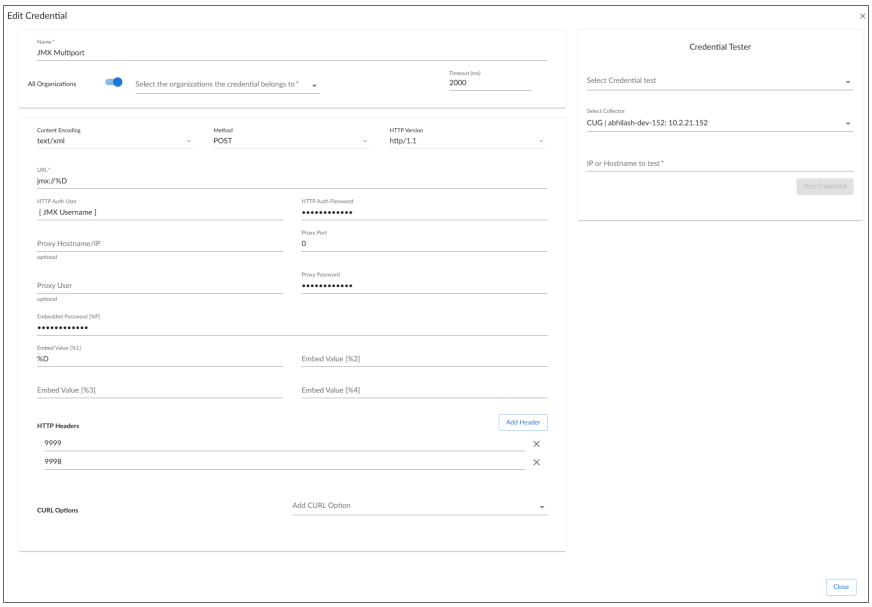
Creating a SOAP/XML Credential to Monitor Multiple Ports

To configure Skylar One to monitor a JMX system, you must first create a SOAP/XML credential. This credential allows the Dynamic Applications in the "JMX Base Pack" PowerPack to communicate with your JMX system.

The PowerPack includes an example SOAP/XML credential that you can edit and save for your own use.

To create a SOAP/XML credential:

1. Go to the **Credentials** page (Manage > Credentials).
2. Locate the "JMX Multiport" credential , then click its **[Actions]** icon () and select *Duplicate* from the drop-down field. The "JMX Multiport copy" credential appears.
3. Click the **[Action]** icon () for the "JMX Multiport copy" credential, then select *Edit*. The **Edit Credential** page appears.



4. Enter values in the following fields:
    - ***Name***. Enter a new name for the credential. This field is required.
    - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***Select the organizations the credential belongs to*** drop-down field to align the credential with those specific organizations.
    - ***Timeout***. Enter the time, in milliseconds, after which Skylar One will stop trying to communicate with the JMX device. The default value is *30000*. This field is required.
    - ***URL***. Keep the default url. The default url is "jmx://%D".
    - ***HTTP Auth User***. Enter the JMX username associated with the administrator account.
    - ***HTTP Auth Password***. Enter the password associated with the JMX administrator account.
    - ***Embedded Password [%P]***. Enter the embedded password associated with the JMX administrator account.
    - ***Embed Value [%1]***. Keep the default.
    - ***HTTP Headers***.Keep the default headers of "9999" and "9998".
5. Click **[Save & Close]**.

Creating a SOAP/XML Credential to Monitor Multiple Ports in the Skylar One Classic User Interface

If you want to configure Skylar One 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" 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

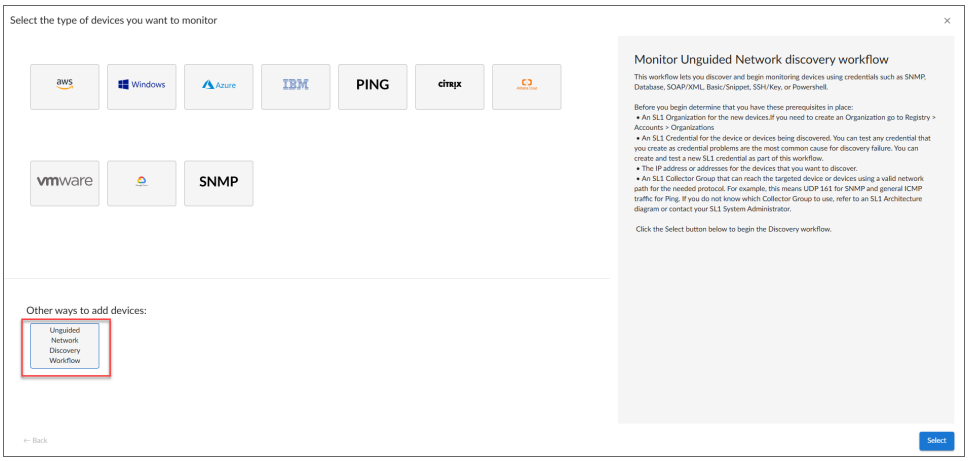
   - ***Add a header***. For each port that you want to monitor, click **[Add a header]** and then type the port number that you want to monitor in the blank field that appears.
4. For all other fields, keep the default value.
5. Click the **[Save As]** button, and then click **[OK]**.

Discovering JMX Resources

To monitor your JMX system, you must run a discovery session to discover the server on which JMX is installed.

To create and run a discovery session that will discover a JMX appliance:

1. Go to the **Devices** page () or the **Discovery Sessions** page (Devices > Discovery Sessions) and click the **[Add Devices]** button.
2. Click the **[Unguided Network Discovery Workflow]** button. Additional information about that requirements for discovery appears in the **General Information** pane to the right.



3. Click **[Select]**. The three-step wizard appears starting with the **[Step 1 Basic Information]** tab.
4. Complete the following fields:
    - ***Discovery Session Name***. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab.
    - ***Description***.Optional. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the **[Discovery Sessions]** tab.
    - ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered devices.
5. Click **[Next]**. The **[Step 2 Credential Selection]** tab of the wizard appears.
6. On the **[Credential Selection]** tab, locate and select the SOAP/XML credential you created for JMX appliances.
7. Click **[Next]**. The **[Step 3 Discovery Session Details]** tab of the wizard appears.
8. Complete the following fields:
    - ***List of IP/Hostnames***. Type the IP address for the JMX appliance.
    - ***Which collector will discover these devices?***. Required. Select an existing collector to monitor the discovered devices.
    - ***Run after save***. Toggle on (blue) to run this discovery session as soon as you save the session.
    - ***Advanced options***. Click the down arrow (⌄) to complete the following fields:
        - ***Discover Non-SNMP***. Toggle on (blue) to enable this setting.
        - ***Model Devices***. Toggle on (blue) to enable this setting.
        - ***Select Device Template***. If you configured a JMX device template, select it here. Otherwise, leave the default selection.
9. If you enabled the ***Run after save*** option, click the**[Save and Run]** button. The discovery session will run and the **Discovery Logs** page will display any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page will include a link to the **Device Investigator** page for the discovered device.

10. If you did not enable the ***Run after save*** option, click the **[Save and Close]** button. The **Discovery Sessions** page (Devices > Discovery Sessions) will display the new discovery session.

Discovering JMX Resources in the Skylar One Classic User Interface

To discover JMX resources:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery or System > Manage > Discovery in the classic user interface).
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 PowerPack

In most cases, the Dynamic Applications in the "JMX Base Pack" 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" 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 Skylar One 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.

> **NOTE:** Memory pools such as PermGen, Code Cache, or Survivor Spaces are not supported in Java 8 and any Dynamic Application or Collection Object which use such pools is expected to return a message of "No Data" when running on Java version 8 and later.

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" 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 (Devices > Classic 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.

Chapter 3

Executing the Skylar One Agent with JMX

Overview

NOTE: Only the Linux agent supports monitoring with JMX Dynamic Applications.

This section provides an overview of local Agent execution on JMX devices.

This chapter covers the following topics:

What is a Skylar One Agent?

The ***Skylar One agent*** is a program that you can install on a device monitored by Skylar One (formerly SL1). There is a Windows agent, an AIX agent, a Solaris agent, and a Linux agent. The agent collects data from the device and pushes that data back to Skylar One.

Similar to a Data Collector or Message Collector, the agent collects data about infrastructure and applications.

You can configure an agent to communicate with either the Message Collector or the Compute Cluster.

NOTE: The following minimum agent versions are required for Skylar One 12.5.1 and later:

- **Windows** version 154
- **Linux** version 196
- **AIX** version 196
- **Solaris** version 196

Users who require agent-based log collection on a device with a Windows agent or a Linux agent must have the minimum Windows agent or Linux agent version. If you do not have the minimum required agent versions, ScienceLogic recommends that you upgrade using the **[Upgrade]** button on the **Agents** page (Devices > Agents), or by downloading and upgrading the agent manually. For more information, see the section on *Upgrading an Agent*.

For more information, see the ***Monitoring with the Skylar One Agent*** manual

The Credential for the Skylar One Agent

To monitor JMX with the Skylar One agent, you will need to create a Basic/Snippet or a SOAP/XML credential.

To create the Basic/Snippet credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the ***Actions*** button and select the ***Create Basic/Snippet*** credential. The **Create New Basic/Snippet Credential** modal page appears.
3. For monitoring JMX with the Skylar One agent, provide values in the following fields:
   - ***Credential Name***. Type a name for the credential.
   - ***Hostname/IP***. Type "%D",
   - ***Port***. Type "9999". Ports are not used for monitoring the Skylar One agent with JMX, but there must be a numerical value in this field.
   - ***Username***. Type the username associated with the Java process(es) to be monitored on the agent device.
4. Click the **[Save As]** button, and then click **[OK]**.

You can also use a SOAP/XML credential. To create the credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the JMX credential you created when *configuring the PowerPack* and then click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal page appears.
3. For monitoring JMX with the Skylar One agent, the only fields you will need to configure are the ***Profile Name*** and ***HTTP Auth User*** fields. The ***HTTP/Auth User*** should be the username associated with the Java process(es) to be monitored on the agent device.

NOTE: The port fields in the ***HTTP Headers*** section are not used for monitoring with the Skylar One agent.

4. Click the **[Save As]** button so you do not save over your original JMX credential.

Configuring the Skylar One Agent for JMX

After discovery there are two ways to configure the Skylar One Agent to monitor JMX:

- Manually aligning Dynamic Applications to the Linux agent device
- Configuring a Device Template

Manually Aligning Dynamic Applications for Monitoring with the Skylar One Agent

Once you have discovered the JMX device that you want to monitor with the Skylar One Agent, you can manually align the relevant Dynamic Applications to that device.

NOTE: All Dynamic Applications included in the "JMX Base Pack" are supported for Agent monitoring **except** "JMX: Inventory" as it does not specify any JMX MBeans to be collected.

To manually align the Dynamic Applications:

1. Find the JMX device you want to monitor with the Skylar One Agent in the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface) and click its wrench icon (🔧).
2. From the **Device Properties** page, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
3. On the **Dynamic Application Collections** page, click the **[Actions]** button and then select *Add Dynamic Application*. The **Dynamic Application Alignment** pane appears.
4. In the ***Dynamic Applications*** field, select the JMX Dynamic Applications you want to align to your device.
5. In the ***Credentials*** field, select the Basic/Snippet or SOAP/XML credential you created for monitoring JMX with the Skylar One agent.
6. Click **[Save]**. The Dynamic Application appears on the **Dynamic Application Collections** page.

Configuring a Device Template for Monitoring with the Skylar One Agent

A ***device template*** allows you to save a device configuration and apply it to multiple devices. You can create a device template for the *JMX Base Pack* PowerPack to use when executing the Skylar One Agent

with JMX. If you apply this device template during discovery, Skylar One aligns the appropriate Dynamic Applications to the discovered JMX device.

To create the device template:

1. Go to the **Configuration Templates** page (Devices > Templates, or Registry > Devices > Templates in the classic user interface).
2. Click the **[Create]** button. The **Device Template Editor** page appears.
3. Supply a name for the template in the ***Template Name*** field.
4. Click the **[Dyn Apps]** tab. The **Editing Dynamic Application Subtemplates** page appears.
5. To add a Dynamic Application to the template, go to the ***Subtemplate Selection*** and click on the plus-sign (+). Then search for the JMX Dynamic Applications you want to align to your device, and select those Dynamic Applications in the ***Dynamic Application*** field.
6. To remove a Dynamic Application listed in the ***Subtemplate Selection*** section on the left side of the page, click its delete icon ( ) and then click **[OK]** when asked to confirm.
7. Once you have finished adding Dynamic Applications, click the **[Save]** button.

NOTE: JMX Dynamic Applications are snippet-based applications that specify JMX MBeans in one or more collection objects. Only the collection objects which are of the format `jmx://<MBean information>` will be collected. Any collection objects which are not in the format "`jmx://...`" will be ignored. The Dynamic Application snippet will **not** be executed when it is run on the Agent. The JMX Mbeans will be queried exactly as specified in the collection objects and any pre- or post-processing steps added to the snippet will be ignored **except** for the time-conversion functions `time_duration_to_str` and `unix_time_to_sl1_timestamp`, which will be applied after data is collected. The user can also specify the optional `time_unit` argument which is applied with the `time_duration_to_str` conversion.

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

International: +1-703-354-1010