Splunk® Supported Add-ons
Splunk Add-on for IBM WebSphere Application Server released
Generated: 5/29/2020 12:03 pm
Table of Contents

Overview................................................................................................................................................................................1
   About the Splunk Add-on for IBM WebSphere Application Server.........................................................................................1
   Source types for the Splunk Add-on for IBM WebSphere Application Server........................................................................1
   Release notes for the Splunk Add-on for IBM WebSphere Application Server........................................................................2
   Release history for the Splunk Add-on for IBM WebSphere Application Server.................................................................3

Installation.............................................................................................................................................................................8
   Hardware and software requirements for the Splunk Add-on for IBM WebSphere Application Server....................................8
   Installation overview for the Splunk Add-on for IBM WebSphere Application Server............................................................8
   Install the Splunk Add-on for IBM WebSphere Application Server.....................................................................................9

Configuration......................................................................................................................................................................11
   Configure IBM WebSphere to produce data for the Splunk Add-on for IBM WebSphere Application Server..........................11
   Configure JMX inputs for the Splunk Add-on for IBM WebSphere Application Server..........................................................12
   Configure global settings, HPEL inputs, and server log inputs for the Splunk Add-on for IBM WebSphere Application Server....13
   Configure monitor inputs for the gc.log and serverindex.xml logs.......................................................................................18
   Enable saved search for the Splunk Add-on for IBM WebSphere Application Server.............................................................19

Reference............................................................................................................................................................................21
   Lookups for the Splunk Add-on for IBM WebSphere Application Server................................................................................21
Overview

About the Splunk Add-on for IBM WebSphere Application Server

<table>
<thead>
<tr>
<th>Version</th>
<th>4.0.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Product(s)</td>
<td>IBM WebSphere Application Server versions 8.5.5 - 9.0.0</td>
</tr>
</tbody>
</table>

The Splunk Add-on for IBM WebSphere Application Server allows a Splunk software administrator to collect data from WebSphere Application Servers. The add-on can collect JMX metrics, HPEL logging events, and server logs, including status, trace, error, and exception logs.

After the Splunk platform indexes the events, you can analyze the data using the prebuilt panels included with the add-on. This add-on provides the inputs and CIM-compatible knowledge to use with other Splunk apps, such as Splunk Enterprise Security, the Splunk App for PCI Compliance, and Splunk IT Service Intelligence.

Download the Splunk Add-on for IBM WebSphere Application Server from Splunkbase at http://splunkbase.splunk.com/app/2789.

Discuss the Splunk Add-on for IBM WebSphere Application Server on Splunk Answers at http://answers.splunk.com/answers/app/2789.

Source types for the Splunk Add-on for IBM WebSphere Application Server

The Splunk Add-on for IBM WebSphere Application Server supplies or expects the following source types, depending on the data sources and collection methods that you configure: JMX events, HPEL logs, and other log files.

<table>
<thead>
<tr>
<th>Collection method</th>
<th>Source type</th>
<th>Description</th>
<th>CIM data models</th>
<th>ITSI data models</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk Add-on for JMX</td>
<td>ibm:was:jmx</td>
<td>JMX Events for WebSphere</td>
<td>JVM, Inventory, Performance</td>
<td>Application Server, OS</td>
</tr>
<tr>
<td>Local HPEL log collection</td>
<td>ibm:was:hpel</td>
<td>HPEL logging. Supported for IBM WebSphere Application Server version 8.X only.</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Local log file monitoring</td>
<td>ibm:was:manageprofiles</td>
<td>logs under manageprofile directory</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>ibm:was:serverStatus</td>
<td>server status logs</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>ibm:was:orbtrc</td>
<td>ORB trace logs</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>ibm:was:serverExceptionLog</td>
<td>Server exception logs</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>ibm:was:textLog</td>
<td>Logs in TextLog directory</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>ibm:was:derby</td>
<td>Derby database logs</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>ibm:was:ffdc</td>
<td>First Failure Data Capture logs</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>ibm:was:startServerLog</td>
<td>Start server logs</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>ibm:was:stopServerLog</td>
<td>Stop server logs</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Collection method</td>
<td>Source type</td>
<td>Description</td>
<td>CIM data models</td>
<td>ITSI data models</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------</td>
<td>----------------------</td>
<td>-----------------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>ibm:was:systemOutLog</td>
<td>System out logs</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>ibm:was:systemErrLog</td>
<td>System error logs</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>ibm:was:nativeStdOutLog</td>
<td>Native stdout logs</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>ibm:was:nativeStdErrLog</td>
<td>Native stderr logs</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>ibm:was:profileCreationLog</td>
<td>Profile creation logs</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>ibm:was:wsadminTraceout</td>
<td>wasadmin trace logs</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>ibm:was:profileManagementLog</td>
<td>Profile management logs</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>ibm:was:addNodeLog</td>
<td>App node addition logs</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>ibm:was:activityLog</td>
<td>Activity logs</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>ibm:was:httpErrorLog</td>
<td>http_error.log</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>ibm:was:httpLog</td>
<td>http_access.log</td>
<td>Inventory, Performance</td>
<td>Application Server, OS</td>
</tr>
<tr>
<td></td>
<td>ibm:was:serverIndex</td>
<td>serverindex.xml</td>
<td>Inventory</td>
<td>Application Server, OS</td>
</tr>
<tr>
<td></td>
<td>ibm:was:gcLog</td>
<td>Garbage collection log (gc.log)</td>
<td>Inventory, Performance</td>
<td>Application Server, OS</td>
</tr>
</tbody>
</table>

**Release notes for the Splunk Add-on for IBM WebSphere Application Server**

Version 4.0.1 of the Splunk Add-on for IBM WebSphere Application Server was released on March 14, 2020.

**About this release**

Version 4.0.1 of the Splunk Add-on for IBM WebSphere Application Server is compatible with the following software, CIM versions, and platforms.

<table>
<thead>
<tr>
<th>Splunk platform versions</th>
<th>7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIM</td>
<td>4.14 and above</td>
</tr>
<tr>
<td>Platforms</td>
<td>Platform independent</td>
</tr>
<tr>
<td>Vendor Products</td>
<td>IBM WebSphere Application Server versions 8.5.5 - 9.0.0</td>
</tr>
</tbody>
</table>

**New features**

Version 4.0.1 of the Splunk Add-on for IBM WebSphere Application Server has the following new features.

- Default support for Python3

**Fixed issues**

Version 4.0.1 of the Splunk Add-on for IBM WebSphere Application Server has the following fixed issues.

<table>
<thead>
<tr>
<th>Date resolved</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date filed</td>
<td>Issue number</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>2020-01-09</td>
<td>ADDON-24810</td>
<td>Addon requires restart to collect data for first time after installation</td>
</tr>
<tr>
<td>2018-01-30</td>
<td>ADDON-16900</td>
<td>Configuration page displays Read Operation Timed Out error while saving.</td>
</tr>
</tbody>
</table>

**Known issues**

Version 4.0.1 of the Splunk Add-on for IBM WebSphere Application Server has the following known issues.

**Third-party software attributions**

Version 4.0.1 of the Splunk Add-on for IBM WebSphere Application Server incorporates the following third-party software or libraries.

- Httplib2
- SortedContainers
- configparser
- future

**Release history for the Splunk Add-on for IBM WebSphere Application Server**

**Latest version**

The latest version of the Splunk Add-on for IBM WebSphere Application Server is version 4.0.1. See Release notes for the Splunk Add-on for IBM WebSphere Application Server for the release notes of this latest version.

**Version 4.0.0**

Version 4.0.0 of the Splunk Add-on for IBM WebSphere Application Server is compatible with the following software, CIM versions, and platforms.

<table>
<thead>
<tr>
<th>Splunk platform versions</th>
<th>7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIM</td>
<td>4.14 and above</td>
</tr>
<tr>
<td>Platforms</td>
<td>Platform independent</td>
</tr>
<tr>
<td>Vendor Products</td>
<td>IBM WebSphere Application Server versions 8.5.5 - 9.0.0</td>
</tr>
</tbody>
</table>

**New features**

Version 4.0.0 of the Splunk Add-on for IBM WebSphere Application Server has the following new features.

- Support for Python3
Fixed issues

Version 4.0.0 of the Splunk Add-on for IBM WebSphere Application Server has the following fixed issues.

<table>
<thead>
<tr>
<th>Date resolved</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-01-19</td>
<td>ADDON-23337</td>
<td>Splunk Add-on for IBM WebSphere Application Server 3.1.0 sourcetype not supported</td>
</tr>
</tbody>
</table>

Known issues

Version 4.0.0 of the Splunk Add-on for IBM WebSphere Application Server has the following known issues.

<table>
<thead>
<tr>
<th>Date filed</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-01-09</td>
<td>ADDON-24810</td>
<td>Addon requires restart to collect data for first time after installation</td>
</tr>
<tr>
<td>2018-01-30</td>
<td>ADDON-16900</td>
<td>Configuration page displays Read Operation Timed Out error while saving.</td>
</tr>
</tbody>
</table>

Third-party software attributions

Version 4.0.0 of the Splunk Add-on for IBM WebSphere Application Server incorporates the following third-party software or libraries.

- Httplib2
- SortedContainers
- configparser
- future

Version 3.1.0

Version 3.1.0 of the Splunk Add-on for IBM WebSphere Application Server is compatible with the following software, CIM versions, and platforms.

<table>
<thead>
<tr>
<th>Splunk platform versions</th>
<th>6.0 and above</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIM</td>
<td>4.2 and above</td>
</tr>
<tr>
<td>Platforms</td>
<td>Platform independent</td>
</tr>
<tr>
<td>Vendor Products</td>
<td>IBM WebSphere Application Server versions 7.0.0 - 8.5.5</td>
</tr>
</tbody>
</table>

Migration Guide

The Splunk Add-on for IBM WebSphere Application server replaces the Splunk App for WebSphere Application Server in its entirety. There is no backwards compatibility between this add-on and the old app and its two add-ons. If you have the old app and add-ons installed, uninstall or disable them and begin collecting new and historical data with this new add-on instead.

Upgrade Guide

The line breaker rule for the http_access.log and http_error.log logs has changed in the Splunk Add-on for IBM WebSphere Application Server version 3.1.0. If you had enabled http access logging and http error logging in IBM WebSphere and collected http_access.log and http_error.log using the Splunk Add-on for IBM WebSphere Application Server 3.0.0, you will need to fix the line breaks in the older data after upgrading to the Splunk Add-on for IBM WebSphere Application Server 3.1.0.
New features

Version 3.1.0 of the Splunk Add-on for IBM WebSphere Application Server has the following new features.

<table>
<thead>
<tr>
<th>Date</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-10-19</td>
<td>ADDON-6104</td>
<td>Modifications to support integration with ITSI including two new data sources: <em>gc.log</em> and <em>serverindex.xml</em>. These new sources are mapped to the Application Server and OS ITSI data models. Other sources are also mapped to the Application Server and OS ITSI data models. In addition, some sources are mapped to the Inventory and Performance CIM data models. See the source types table for more information.</td>
</tr>
<tr>
<td>2016-03-16</td>
<td>ADDON-8323</td>
<td>Add saved search Server Index - WAS Inventory Lookup to generate a lookup file that is used to correlate data from multiple logs and populate certain fields in the events.</td>
</tr>
</tbody>
</table>

Fixed issues

Version 3.1.0 of the Splunk Add-on for IBM WebSphere Application Server has the following fixed issues.

<table>
<thead>
<tr>
<th>Date</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-02-27</td>
<td>ADDON-7977</td>
<td>tag=performance should contain response_code field.</td>
</tr>
<tr>
<td>2016-02-27</td>
<td>ADDON-7980</td>
<td>ip_address field is not extracted.</td>
</tr>
<tr>
<td>2015-09-14</td>
<td>ADDON-6384</td>
<td>If Splunk Add-on for JMX version 3.1.0 or later is used with the Splunk Add-on for IBM WebSphere Application Server version 3.0.0 or later, the source type override in the Splunk Add-on for IBM WebSphere Application Server incorrectly assigns the source type as jmx instead of ibm:was:jmx. Workaround: specify a source type of ibm:was:jmx in the JMX input.</td>
</tr>
<tr>
<td>2015-06-10</td>
<td>ADDON-4216</td>
<td>Data inputs page appears to allow you to configure new inputs, but its only purpose is to allow you to easily enable the HPEL data collection input, which requires no additional configuration in this page.</td>
</tr>
</tbody>
</table>

Known issues

Version 3.1.0 of the Splunk Add-on for IBM WebSphere Application Server has the following known issues.

<table>
<thead>
<tr>
<th>Date</th>
<th>Defect number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-01-13</td>
<td>ADDON-5325</td>
<td>requireClientCert=true in server.conf is not supported by add-ons using modular inputs and REST. If this setting is enabled in server.conf, communication is broken between the modular input and splunkd and the add-on stops collecting data. The following error appears in the splunkd.log: &quot;SSL3_GET_CLIENT_CERTIFICATE:peer did not return a certificate.&quot; The workaround is to set requireClientCert=false.</td>
</tr>
<tr>
<td>2015-06-29</td>
<td>ADDON-4360</td>
<td>The &quot;HPEL logs start date&quot; field in the setup page or the start_date argument in ibm_was.conf can only be configured before you enable the input for the first time. If you need to change it after enablement, see &quot;Change the HPEL data collection start time&quot; in the Troubleshooting topic.</td>
</tr>
<tr>
<td>2015-06-23</td>
<td>ADDON-4321/ ADDON-4204</td>
<td>Some files collected via the monitor input have invalid source type names such as responseFile-too_small.</td>
</tr>
<tr>
<td>2015-06-10</td>
<td>ADDON-4218</td>
<td>Any messages shown on the setup page after saving continue to show until you click on save again.</td>
</tr>
<tr>
<td>2015-06-09</td>
<td>ADDON-4206</td>
<td>JMX input throws errors &quot;ERROR - Error executing JMX stanza...&quot; because the Splunk Add-on for JMX queries attributes that the WAS MBean does not implement. Can be safely ignored.</td>
</tr>
</tbody>
</table>
Third-party software attributions

Version 3.1.0 of the Splunk Add-on for IBM WebSphere Application Server incorporates the following third-party software or libraries.

- Httplib2
- SortedContainers

Version 3.0.0

Version 3.0.0 of the Splunk Add-on for IBM WebSphere Application Server has the same compatibility specifications as version 3.1.0.

Migration Guide

The Splunk Add-on for IBM WebSphere Application server replaces the Splunk App for WebSphere Application Server in its entirety. There is no backwards compatibility between this add-on and the old app and its two add-ons. If you have the old app and add-ons installed, uninstall or disable them and begin collecting new and historical data with this new add-on instead.

New features

Version 3.0.0 of the Splunk Add-on for IBM WebSphere Application Server has the following new features.

<table>
<thead>
<tr>
<th>Date</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>07/01/15</td>
<td>ADDON-1324</td>
<td>New Splunk-supported add-on that replaces the Splunk App for WebSphere Application Server and brings it up to date through version 8.5.5, including support for High Performance Extensible Logging (HPEL) in WAS 8.x.</td>
</tr>
</tbody>
</table>

Known issues

Version 3.0.0 of the Splunk Add-on for IBM WebSphere Application Server has the following known issues.

<table>
<thead>
<tr>
<th>Date</th>
<th>Defect number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-01-13</td>
<td>ADDON-5325</td>
<td>requireClientCert=true in server.conf is not supported by add-ons using modular inputs and REST. If this setting is enabled in server.conf, communication is broken between the modular input and splunkd and the add-on stops collecting data. The following error appears in the splunkd.log: &quot;SSL3_GET_CLIENT_CERTIFICATE:peer did not return a certificate.&quot; The workaround is to set requireClientCert=false.</td>
</tr>
<tr>
<td>09/14/15</td>
<td>ADDON-5524/ADDON-6384</td>
<td>If version 3.1.0 of the Splunk Add-on for JMX is used with the Splunk Add-on for IBM WebSphere Application Server version 3.0.0, the source type override in the Splunk Add-on for IBM WebSphere Application Server incorrectly assigns the source type as jmx instead of ibm:was:jmx. Workaround: specify a source type of ibm:was:jmx in the JMX input.</td>
</tr>
<tr>
<td>06/29/15</td>
<td>ADDON-4360</td>
<td>The &quot;HPEL logs start date&quot; field in the setup page or the start_date argument in ibm_was.conf can only be configured before you enable the input for the first time. If you need to change it after enablement, see &quot;Change the HPEL data collection start time&quot; in the Troubleshooting topic.</td>
</tr>
<tr>
<td>06/23/15</td>
<td>ADDON-4321/ADDON-4204</td>
<td>Some files collected via the monitor input have invalid source type names such as responseFile-too_small.</td>
</tr>
</tbody>
</table>
Version 3.0.0 of the Splunk Add-on for IBM WebSphere Application Server incorporates the following third-party software or libraries.

- Httplib2
- SortedContainers
Installation

Hardware and software requirements for the Splunk Add-on for IBM WebSphere Application Server

Dependencies

The Splunk Add-on for IBM WebSphere Application Server supports multiple data inputs, each capable of collecting different data from your WAS. For more information about which kind of data you can collect with which input, refer to the source types page.

If you want to collect data from the HPEL interface or by monitoring log files, you must install a Splunk Enterprise forwarder or single instance directly on the machine running your WebSphere application server, so it can access the logs locally.

If you want to collect JMX data, install the Splunk Add-on for Java Management Extensions (JMX) on your data collection node.

Note: To collect JMX data from an IBM WebSphere application server, you need to install the IBM JDK or JRE, which you can download here: http://www.ibm.com/developerworks/java/jdk/eclipse/. Put the JDK or JRE bin directory in the system path to make sure that the JMX data collection uses this IBM version of the Java runtime.

Sizing guidelines

The Splunk Add-on for IBM WebSphere Application Server has no specific sizing guidelines for JMX or file monitoring inputs. For HPEL interface inputs, the add-on can concurrently collect metrics from twenty WebSphere profiles without performance implications.

Splunk platform requirements

Because this add-on runs on the Splunk platform, all of the system requirements apply for the Splunk software that you use to run this add-on.

• For Splunk Enterprise system requirements: see System Requirements in the Splunk Enterprise Installation Manual.
• For Splunk Light system requirements: see System Requirements in the Splunk Light Installation Manual.
• If you are managing on-premises forwarders to get data into Splunk Cloud, see System Requirements in the Splunk Enterprise Installation Manual, which includes information about forwarders.

Installation overview for the Splunk Add-on for IBM WebSphere Application Server

To install and configure the Splunk Add-on for IBM WebSphere Application Server on your supported platform:


2. Install the Splunk Add-on for IBM WebSphere Application Server.
3. **Configure your WebSphere application server** to enable server file system logs, HPEL logs, and/or JMX data.

4. On the part of your Splunk Enterprise architecture that is performing data collection for the add-on, configure the inputs that you want to use:
   
   - configure JMX inputs
   - configure HPEL and log file monitor inputs
   - configure monitor inputs for gc.log and serverindex.xml

5. If you plan to use the Splunk Add-on for IBM WebSphere Application Server with IT Service Intelligence (ITSI), **enable the saved search for the Splunk Add-on for IBM WebSphere Application Server**.

### Install the Splunk Add-on for IBM WebSphere Application Server

**Installation instructions**

See Installing add-ons in *Splunk Add-Ons* for detailed instructions describing how to install a Splunk add-on in the following deployment scenarios:

- single-instance Splunk Enterprise
- distributed Splunk Enterprise
- Splunk Cloud
- Splunk Light

**Deployment notes**

There are three different inputs in this add-on. You can choose to use one or several of them. Keep these requirements in mind as you choose how to install the add-on in your environment.

- The JMX input depends on the Splunk Add-on for JMX, which must be installed on a heavy forwarder or single-instance Splunk Enterprise.
- The HPEL interface modular input must be enabled on a forwarder or single-instance Splunk Enterprise that is installed directly on the machine running your WebSphere application server. This input requires Python. You can configure the input either using the UI or using configuration files. Light forwarders or heavy forwarders are supported. Universal forwarders are not supported.
- The file monitoring inputs must be enabled on a forwarder or single-instance Splunk Enterprise that is installed directly on the machine running your WebSphere application server. This input does not require Python. You can configure the input either using the UI or using configuration files. Universal forwarders, light forwarders, or heavy forwarders are all supported.

If you have many WebSphere application server instances, consider using an aggregator between the WebSphere application servers and the Splunk platform. In this configuration scenario, you can install a Splunk forwarder and the Splunk Add-on for IBM WebSphere Application Server on the aggregation server rather than on each WebSphere application server to monitor the HPEL and local server logs.
Distributed deployments

Use the tables below to determine where and how to install this add-on in a distributed deployment of Splunk Enterprise.

Where to install this add-on

This table provides a quick reference for installing this add-on to a distributed deployment of Splunk Enterprise.

<table>
<thead>
<tr>
<th>Splunk instance type</th>
<th>Supported</th>
<th>Required</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Heads</td>
<td>Yes</td>
<td>Yes</td>
<td>Install this add-on to all search heads where IBM WebSphere knowledge management is required.</td>
</tr>
<tr>
<td>Indexers</td>
<td>Yes</td>
<td>Conditional</td>
<td>Not required if you use heavy forwarders to collect data. Required if you use universal or light forwarders to collect data.</td>
</tr>
<tr>
<td>Heavy Forwarders</td>
<td>Yes</td>
<td>Conditional</td>
<td>Required for the JMX input. Optional for HPEL and file monitoring inputs. The HPEL and file monitoring inputs must be enabled on a forwarder that is installed directly on the machine running your WebSphere application server.</td>
</tr>
<tr>
<td>Universal Forwarders</td>
<td>Yes</td>
<td>Conditional</td>
<td>Not supported for JMX inputs or HPEL inputs. Supported for file monitoring inputs. The file monitoring inputs must be enabled on a forwarder that is installed directly on the machine running your WebSphere application server. Python scripts are not supported.</td>
</tr>
<tr>
<td>Light Forwarders</td>
<td>Yes</td>
<td>Conditional</td>
<td>Not supported for JMX inputs. Supported for HPEL and file monitoring inputs. The HPEL and file monitoring inputs must be enabled on a forwarder that is installed directly on the machine running your WebSphere application server.</td>
</tr>
</tbody>
</table>

Distributed deployment feature compatibility

This table provides a quick reference for the compatibility of this add-on with Splunk distributed deployment features.

<table>
<thead>
<tr>
<th>Distributed deployment feature</th>
<th>Supported</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Head Clusters</td>
<td>Yes</td>
<td>You can install this add-on on a search head cluster for all search-time functionality, but only configure inputs on forwarders to avoid duplicate data collection. Before installing this add-on to a cluster, make the following changes to the add-on package: 1. Remove the eventgen.conf file and all files in the samples folder 2. Remove the inputs.conf file.</td>
</tr>
<tr>
<td>Indexer Clusters</td>
<td>Yes</td>
<td>Before installing this add-on to a cluster, make the following changes to the add-on package: 1. Remove the eventgen.conf file and all files in the samples folder 2. Remove the inputs.conf file.</td>
</tr>
<tr>
<td>Deployment Server</td>
<td>No</td>
<td>Supported for deploying unconfigured add-on only. Using a deployment server to deploy the configured add-on to multiple forwarders acting as data collectors causes duplication of data.</td>
</tr>
</tbody>
</table>
Configuration

Configure IBM WebSphere to produce data for the Splunk Add-on for IBM WebSphere Application Server

The Splunk Add-on for IBM WebSphere Application Server allows you to collect three different data types from your WAS instances:

- server file system logs
- HPEL interface logs for applications
- JMX metrics

You need to configure your IBM WebSphere application servers to produce these logs using the WebSphere administrative console.

Enable server file system logs

Enable PMI metrics

You can configure Performance Monitoring Infrastructure (PMI) metrics in IBM WebSphere to control the number of Mbeans the Splunk Add-on for IBM WebSphere Application Server can collect. Although the basic Mbeans used for AppServer data model mapping for ITSI can be retrieved without enabling PMI metrics in IBM WebSphere, you can collect additional Mbeans by configuring PMI according to your needs.

To enable all PMI metrics, log in to the WebSphere administrative console and navigate to Servers > Server Types > WebSphere application servers > <server_name>. Click the Configuration tab then click Performance Monitoring Infrastructure (PMI). Check Enable Performance Monitoring Infrastructure and select All under Currently monitored statistic set.


Enable verbose garbage collection

Log in to the WebSphere administrative console and navigate to the Java Virtual Machine: Servers > Server Types > WebSphere application servers > <server_name> > Server Infrastructure > Java and Process Management > Process definition > Java Virtual Machine. Enable verbose garbage collection and specify the gc.log file path. The log path must be under the ${SERVER_LOG_ROOT} directory. For example: /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/server1. For more information, see the IBM documentation: http://www-01.ibm.com/support/docview.wss?uid=swg21114927.

Enable http access logging and http error logging

Login into the WebSphere administrative console and navigate to Servers > Server Types > WebSphere application servers > <server_name> > Troubleshooting > NSCA access and HTTP error logging. On the NSCA access and HTTP error logging screen, enable the following:

- Enable logging service at server start-up
- Enable access logging
Enable error logging

Turn on HPEL logging

To turn on High Performance Extensible Logging (HPEL) logging for your WebSphere applications, follow the instructions in the IBM documentation that match your WAS version. This link leads to instructions for version 8.5.5: http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.multiplatform.doc/ae/trrb_compToHPEL.html

Enable JMX in WebSphere

To extract JMX metrics for your WebSphere application server using the Splunk Add-on for JMX, you must first enable the JMX connector in WebSphere. Follow this detailed walkthrough for instructions on how to do this in WebSphere version 8.5: https://www.splunk.com/en_us/blog/tips-and-tricks/enabling-jmx-in-websphere-application-server.html

Configure JMX inputs for the Splunk Add-on for IBM WebSphere Application Server

The Splunk Add-on for IBM WebSphere Application Server relies on the Splunk Add-on for Java Management Extensions (JMX) to collect JMX metrics. The Splunk Add-on for IBM WAS provides a `jmx_templates.conf` that the Splunk Add-on for JMX can invoke.

Note: To collect JMX data from an IBM WebSphere application server, you need to install the IBM JDK or JRE, which you can download here. Put the JDK or JRE bin directory in the system path to make sure that the JMX data collection uses this IBM version of the Java runtime.

1. Install the Splunk Add-on for JMX on the Splunk Enterprise instance responsible for JMX data collection, usually a heavy forwarder. This add-on can collect JMX metrics locally or remotely.

2. Go to your WebSphere installation directory and navigate to `$WAS_ROOT/WebSphere/AppServer/runtimes`.

3. Copy these three files to `$SPLUNK_HOME/etc/apps/Splunk_TA_jmx/bin/lib`:

   ```
   • com.ibm.ws.admin.client_*.jar
   • com.ibm.ws.ejb.thinclient_*.jar
   • com.ibm.ws.orb_*.jar
   ```

4. After copying, verify the files successfully copied to your `$SPLUNK_HOME/etc/apps/Splunk_TA_jmx/bin/lib` directory before continuing. For example, if you run the command `ls /opt/splunk/etc/apps/Splunk_TA_jmx/bin/lib/com.ibm*`, you should see something similar to:

   ```
   /opt/splunk/etc/apps/Splunk_TA_jmx/bin/lib/com.ibm.ws.admin.client_8.5.0.jar
   /opt/splunk/etc/apps/Splunk_TA_jmx/bin/lib/com.ibm.ws.ejb.thinclient_8.5.0.jar
   /opt/splunk/etc/apps/Splunk_TA_jmx/bin/lib/com.ibm.ws.orb_8.5.0.jar
   ```

5. Restart the Splunk platform.

6. Go to Splunk Web and access the configuration pages for the Splunk Add-on for JMX, either by clicking on the name in the left nav, or going to Apps > Manage Apps, then clicking Launch app in the row for Splunk Add-on for JMX.

7. Click Add Server to add a new JMX server.
8. Enter a **Name** and an optional **JVM Description** for your server.

9. For **Connection Type**, choose **Use URL directly** from the dropdown menu.

10. Enter the URL in this format:
    
    service:jmx:iiop://<hostname>/jndi/corbaname:iiop://hostname:9100/WsnAdminNameService#JMXConnector

    **Note:** `<hostname>` is the hostname of the running application server. Use the hostname instead of the IP address. If the hostname cannot be resolved through DNS, add the hostname to the hosts file. You can find the hostname for the application server through WAS administration console.

11. Click **Create**.

12. Navigate to the task configurations by clicking **Configurations > Tasks**.

13. Click **Add Task** to create a new JMX task.

14. Enter a **Name** and optional **Description** for your task, then select the server that you just configured.

15. On the **Templates** tab, select one or more of the predefined templates to collect the data that you want.

16. On the **Settings** tab, set the source type to `ibm:was:jmx`.

17. Click **Create** to enable your JMX input.

For more information about configuring JMX inputs, refer to "Configure inputs for the Splunk Add-on for JMX" in the *Splunk Add-on for Java Management Extensions* manual.

**Configure global settings, HPEL inputs, and server log inputs for the Splunk Add-on for IBM WebSphere Application Server**

Configuring your HPEL inputs and your file monitor inputs for your server log files requires several steps. You can perform all of this configuration in Splunk Web on your data collection nodes or by using a combination of configuration files.

**Prerequisite:** Ensure you have configured your IBM WebSphere application servers to enable logging for the logs you want to collect with the add-on as described in Configure IBM WebSphere to produce data for the Splunk Add-on for IBM
Configure HPEL and server log inputs using Splunk Web

Follow these steps to configure your global settings and your HPEL and/or server log inputs using the Splunk Web setup UI.

**Configure global settings**

1. In Splunk Web, click **Apps > Manage Apps**.

2. Click **Set up** under **Actions** in the row for Splunk Add-on for IBM WebSphere Application Server.

3. In the Global Settings section, enter your **WebSphere Application Server installation directory**.

   **Note:** On Windows, WebSphere installation path should include all spaces. For example: `C:\Program Files (x86)\IBM\WebSphere`.

4. (Optional) Select an **index** and a **log level**, if you wish to override the defaults.

5. If you do not want to configure either HPEL or log file monitoring inputs, you can skip to the end of the form and **Save**.

**Configure HPEL data collection**

1. If you have configured your WebSphere application server to turn on HPEL logging, keep **Enable HPEL data collection** checked. It is checked by default.

   **Note:** This page allows you to configure the settings for your HPEL data collection, but the input itself remains inactive until you enable it under **Settings > Data inputs** in a later step.

2. (Optional) Enter a comma-separated list of **Profiles to exclude from HPEL data collection**.

3. (Optional) Enter a **HPEL logs start date** if you want to collect historical HPEL logs. The default start date is one day ago.

   **Note:** You cannot change this start date after the input is enabled for the first time. If you make a mistake and need to configure a different start date after the input is enabled, see Change the HPEL data collection start time in the Troubleshooting topic.

4. (Optional) Specify the level of HPEL logs to collect, either by entering an **HPEL log level** or by setting a **min** and **max** log level to create a range.

   **Note:** Any value in the HPEL log level overrides the min and max. If you choose to configure a min and max, ensure the min is a lower level than the max. If the min is set to a higher level than the max, the add-on will not collect any HPEL log data.

5. (Optional) Configure a collection interval. The default is 60 seconds.

6. If you do not want to configure file monitoring, click **Save**, then skip to **Enable HPEL inputs** below.
Configure file monitor settings

This creates all of the file monitor inputs for the server file system logs with the exception of the gc.log and serverindex.xml logs. You must manually create these two file monitor inputs as described in Configure monitor inputs for gc.log and serverindex.xml.

1. To enable file monitoring, click **Enable data collection from WAS log files.**

   **Note:** This page allows you to configure the settings for your file monitoring, but the input itself remains inactive until you validate and restart in a later step.

2. (Optional) Customize the whitelist regex to specify which log files the add-on should monitor. This field expects Splunk's file whitelist regex formatting. For detailed instructions, see Whitelist or blacklist specific incoming data in the *Getting Data In* manual, part of the Splunk Enterprise documentation.

3. (Optional) Customize the list of directories to exclude from file monitoring. You can use standard PCRE-compliant regex to define a blacklist in this field.

4. Click **Save.**

**Validate and enable the file monitoring**

If you configured file monitor inputs in the setup page, validate that they were created successfully before restarting the Splunk platform to activate them.

1. Go to **Settings > Data inputs > Files & directories.**

2. Click **App** in the column headings to organize the results by app name, then scroll to **Splunk_TA_ibm-was** in that column.

3. Review the list of directories being monitored to ensure it is as you expect. If you need to make corrections, return to the setup page to adjust your whitelist and blacklists.

4. If you are satisfied with the list of directories being monitored, restart the Splunk platform to start the file monitoring inputs.

If you plan to use the Splunk Add-on for IBM WebSphere Application Server with ITSI, create inputs for the gc.log and serverindex.xml logs. See Configure monitor inputs for gc.log and serverindex.xml.

**Enable HPEL inputs**

If you configured HPEL input settings, activate the HPEL input.

1. Go to **Settings > Data inputs.**

2. Click **Splunk Add-on for IBM WebSphere Application Server.**

3. Under Status, click **Enable.**

Your HPEL data collection is active.
## Configure HPEL and server log inputs using configuration files

Follow these steps to configure your global settings and your HPEL and/or server log inputs using the configuration files.

**Configure global settings, file monitor settings, and HPEL settings in local/ibm_was.conf**

1. Copy `$/SPLUNK_HOME/etc/apps/Splunk_TA_ibm-was/default/ibm_was.conf` to `$/SPLUNK_HOME/etc/apps/Splunk_TA_ibm-was/local/`

2. Provide the root installation directory of your IBM WebSphere application server for the argument `was_install_dir`.

3. All other parameters are optional. Refer to the table for information about each one.

<table>
<thead>
<tr>
<th>Section</th>
<th>Argument</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>index</td>
<td>The index in which to store data collected with the Splunk Add-on for IBM WebSphere Application Server.</td>
<td>main</td>
</tr>
<tr>
<td></td>
<td>was_install_dir</td>
<td>Required. The installation directory of your IBM WebSphere application server. On Windows, the WebSphere installation path should include all spaces. For example: <code>C:\Program Files (x86)\IBM\WebSphere</code>.</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>log_level</td>
<td>The logging verbosity for the add-on.</td>
<td>INFO</td>
</tr>
<tr>
<td>File monitor</td>
<td>file_whitelist</td>
<td>The whitelist of log files to be monitored. This argument expects Splunk's file whitelist regex formatting. For detailed instructions, see “Whitelist or blacklist specific incoming data” in the Getting Data In manual, part of the Splunk Enterprise documentation.</td>
<td>`.txt*$</td>
</tr>
<tr>
<td></td>
<td>exclude_dirs</td>
<td>The directories to exclude from monitoring, separated by commas.</td>
<td>java,jre,postinstall,deploytool,eclipse64,docs,help,lib,Plugins,plugins,properties,javascript,lafiles</td>
</tr>
<tr>
<td></td>
<td>was_file_monitor_enabled</td>
<td>Enable data collection from WAS log files. Change to 1 and run the <code>was_inputs_gen.py</code> script to create the monitor inputs based on the parameters defined in this file.</td>
<td>0</td>
</tr>
<tr>
<td>HPEL</td>
<td>excluded_profiles</td>
<td>Profiles to exclude from HPEL data collection separated by commas. For example, MyProfile.*,OtherProfile.</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>start_date</td>
<td>HPEL logs start date (UTC) in &quot;MM/dd/yy H:m:s:S&quot; format. For example, 6/29/15 00:00:00:000. Note that you can configure this only before you enable the input for the first time.</td>
<td>1 day ago</td>
</tr>
<tr>
<td></td>
<td>level</td>
<td>Set a single log level to collect from the HPEL log data. This argument overrides any values in <code>min_level</code> and <code>max_level</code>.</td>
<td>None</td>
</tr>
</tbody>
</table>
### Argument Description Default

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>min_level</td>
<td>Set a minimum log level to collect from the HPEL log data. Ensure the min_level is set to a lower level than max_level to define a valid range.</td>
<td>INFO</td>
</tr>
<tr>
<td>max_level</td>
<td>Set a maximum log level to collect from the HPEL log data. Ensure the max_level is set to a higher level than min_level to define a valid range.</td>
<td>FATAL</td>
</tr>
<tr>
<td>duration</td>
<td>The collection interval for the HPEL input.</td>
<td>60</td>
</tr>
<tr>
<td>hpe1_collection_enabled</td>
<td>A toggle that activates the settings in this section if the HPEL data input itself is enabled in local/inputs.conf. You still need to enable the input there manually.</td>
<td>1</td>
</tr>
</tbody>
</table>

**Generate your local/inputs.conf**

The add-on includes a Python script named `was_inputs_gen.py` that automatically generates an `inputs.conf` file using the parameters specified in the `ibm_was.conf`. The resulting `local/inputs.conf` file contains all the file monitoring stanzas specified by your whitelist and blacklist statements, as well as a modular input stanza for the HPEL input, if you kept it enabled in the `ibm_was.conf`.

Python scripts are not supported on universal forwarders.

**usage:** `was_inputs_gen.py [-h] [--was_install_dir WAS_INSTALL_DIR] [--index INDEX] [--exclude_dirs EXCLUDE_DIRS] [--file_whitelist FILE_WHITELIST]`

**optional arguments:**
- `-h, --help` show this help message and exit
- `--was_install_dir WAS_INSTALL_DIR` The root installation directory of WebSphere Application Server
- `--index INDEX` Splunk index to hold the data
- `--exclude_dirs EXCLUDE_DIRS` The directories which should be excluded for monitoring. Separated by comma.
- `--file_whitelist FILE_WHITELIST` The whitelist of log files to be monitored. Refer to [http://docs.splunk.com/Documentation/Splunk/latest/data/Specifyinputpathswithwildcards](http://docs.splunk.com/Documentation/Splunk/latest/data/Specifyinputpathswithwildcards) for more details

You can run the script with parameters passed in the CLI. For example:

```python
python was_inputs_gen.py --was_install_dir /opt/IBM/WebSphere --index was
```

The parameters specified in the CLI have the highest priority, then the configuration in `local/ibm_was.conf`, and `default/ibm_was.conf` has the lowest priority.

To use the script:
1. After you finish configuring the `ibm_was.conf` in your local directory, run `was_inputs_gen.py`, located in `$SPLUNK_HOME/etc/apps/Splunk_TA_ibm-was/bin`.

2. Open the resulting file to validate the results are what you expected.

3. Restart the Splunk platform to allow the inputs to take effect.

   **Note:** If you want to create inputs for the `gc.log` and `serverindex.xml` logs, don't restart the Splunk platform yet. See Configure monitor inputs for `gc.log` and `serverindex.xml`.

**Validate the inputs**

To validate that all of the inputs you configured are working correctly, go to the Search and Reporting app and search for the source types listed on the source types page that match the inputs that you configured.

**Configure monitor inputs for the `gc.log` and `serverindex.xml` logs**

If you plan to use the Splunk Add-on for IBM WebSphere Application Server with IT Service Intelligence (ITSI), you need to create inputs for the `gc.log` and `serverindex.xml` logs. Although you can use the setup page to generate inputs for most of the local server logs, you must manually create monitor inputs for the `gc.log` and `serverindex.xml` logs. You can use either Splunk Web to create the monitor inputs or configure `inputs.conf` directly.

**Configure Monitoring through Splunk Web**

Configure file monitoring inputs on your data collection node for the `gc.log` and `serverindex.xml` logs.

1. Log into Splunk Web.

2. Select Settings > Data inputs > Files & directories.

3. Click New.

4. Click Browse next to the File or Directory field.

5. Navigate to directory of your `gc.log`, and click Next.

6. In the Sourcetype field, select `ibm:was:gcLog`, and click Next.

7. Click Review.

8. After you review the information, click Submit.

9. Repeat the steps above for the `serverindex.xml` and assign a source type of `ibm:was:serverIndex`.

**Configure inputs.conf**

You can configure the monitor inputs in the `inputs.conf` file instead of using Splunk Web. After setting up the add-on, using either the setup page or using the configuration files and running the python script, a `local/inputs.conf` file gets generated for you. Edit this file to add the file monitor inputs.
1. Using a text editor, open the $SPLUNK_HOME/etc/apps/Splunk_TA_ibm-was/local/inputs.conf file.

2. Add the following stanzas and lines, replacing `<server_name>`, `<cell_name>`, and `<node_name>` with the appropriate values for your environment, and save the file:

   ```conf
   [monitor:///opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/<server_name>/gc.log]
   sourcetype = ibm:was:gcLog
   disabled = 0
   [monitor:///opt/IBM/WebSphere/AppServer/profiles/AppSrv01/config/cells/$<cell_name>/nodes/$<node_name>/serverindex.xml]
   sourcetype = ibm:was:serverIndex
   disabled = 0
   ``

3. Restart the Splunk platform in order for the new inputs to take effect.

**Validate inputs for gc.log and serverindex.xml**

After you configure monitoring, verify that data from the two sources is being ingested into the Splunk platform by using the following search commands and verifying that one or more events is returned.

```
sourcetype=ibm:was:gcLog
sourcetype=ibm:was:serverIndex
```

**Enable saved search for the Splunk Add-on for IBM WebSphere Application Server**

The Splunk Add-on for IBM WebSphere Application Server includes a preconfigured lookup generation saved search that you need to enable if you are using this add-on with Splunk IT Service Intelligence. This saved search is based on the data collected through JMX and file based logs. You need to configure JMX inputs, configure server log inputs, and configure monitor inputs for the gc.log and serverindex.xml logs in order to collect the data. After the data has been indexed by the Splunk platform, manually run the saved search in order to populate the lookup file then set a frequency to run it that matches the frequency of configuration changes in your environment.

<table>
<thead>
<tr>
<th>Saved search name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Index - WAS Inventory Lookup</td>
<td>Generates the <code>ibm_was_inventory.csv</code> lookup file. Populates the <code>appserver_port_number</code> and <code>application_server</code> fields in the events.</td>
</tr>
</tbody>
</table>

You can review and enable the saved search either in Splunk Web or in the configuration files.

**Access and enable saved search in Splunk Web**

To access and enable the saved search in Splunk Web:

1. Go to **Settings > Searches, reports, and alerts**.

2. Set the app context to **Splunk Add-on for IBM WebSphere Application Server**.

3. Click **Enable** next to **Server Index - WAS Inventory Lookup**.
**Access and enable saved search in `savedsearches.conf`**

To access and enable the saved search in the configuration files:

1. Go to `$SPLUNK_HOME/etc/apps/Splunk_TA_tomcat/default/savedsearches.conf`.
2. Copy the file to `/local`.
3. In the local copy, change `disabled = 1` to `disabled = 0`.  


Reference

Lookups for the Splunk Add-on for IBM WebSphere Application Server

The Splunk Add-on for IBM WebSphere Application Server has one lookup. The lookup file is located in $SPLUNK_HOME/etc/apps/Splunk_TA_ibm-was/lookups.

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibm_was_inventory.csv</td>
<td>Generated from Server Index - WAS Inventory Lookup saved search. Links the events from JMX and the events from file based logs and populates the appserver_port_number and application_server fields in all events.</td>
</tr>
</tbody>
</table>