
IBM DataPower Add-on for Splunk Documentation

Release 1.0.0

Diogo Silva

May 17, 2020

1	About the IBM DataPower Add-on for Splunk	1
2	Release notes	3
2.1	About this release	3
2.2	New features	3
2.3	Fixed issues	3
2.4	Known issues	3
3	Hardware and software requirements	5
3.1	IBM DataPower setup requirements	5
3.2	Splunk platform requirements	5
4	Installation	7
4.1	Install the IBM DataPower Add-on for Splunk	7
5	Configuration	9
5.1	Splunk	9
5.2	IBM DataPower	9
6	Troubleshooting	11
7	Support	13
7.1	Bugs & Support Issues	13
8	Indices and tables	15

About the IBM DataPower Add-on for Splunk

Version	1.0.0
Vendor Products	IBM DataPower 7.5 or newer
Visible in Splunk Web	No. This add-on contains no dashboards.

The IBM DataPower Add-on for Splunk brings field extractions from IBM DataPower syslog data to Splunk platform. This add-on does not collect any data.

Download the [IBM DataPower Add-on for Splunk](#) from Splunkbase.

For a summary of new features, fixed issues, and known issues, see [Release Notes for the IBM DataPower Add-on for Splunk](#).

For information about installing and configuring the IBM DataPower Add-on for Splunk, see [Installation and configuration overview for the IBM DataPower Add-on for Splunk](#).

See [Questions related to IBM DataPower Add-on for Splunk](#) on Splunk Answers.

2.1 About this release

Version 1.0.0 of the IBM DataPower Add-on for Splunk is compatible with the following software, CIM versions, and platforms.

Splunk software versions	7.1 or later
CIM	4.7 or later
Platforms	Platform independent
Vendor Products	IBM DataPower 7.5 or newer

2.2 New features

Version 1.0.0 of the IBM DataPower Add-on for Splunk contains the following new features.

2.3 Fixed issues

Version 1.0.0 of the IBM DataPower Add-on for Splunk contains the following fixed issues.

Date resolved	Issue number	Description
---------------	--------------	-------------

2.4 Known issues

Version 1.0.0 of the IBM DataPower Add-on for Splunk has the following known issues.

Date filed	Issue number	Description
------------	--------------	-------------

Hardware and software requirements

To install and configure the IBM DataPower Add-on for Splunk, you must have the admin role in the Splunk platform.

3.1 IBM DataPower setup requirements

3.2 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. If you plan to run this add-on entirely in Splunk Cloud, there are no additional Splunk platform requirements. 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.

4.1 Install the IBM DataPower Add-on for Splunk

- Get the IBM DataPower Add-on for Splunk by downloading it from [Splunkbase](#) or browsing to it using the app browser within Splunk Web.
- Determine where and how to install this add-on in your deployment, using the tables on this page.
- Perform any prerequisite steps before installing, if required and specified in the tables below.
- Complete your installation.

4.1.1 Distributed deployments

Reference the tables below to determine where and how to install this add-on in a distributed deployment of Splunk Enterprise or any deployment for which you are using forwarders to get your data in. Depending on your environment, your preferences, and the requirements of the add-on, you may need to install the add-on in multiple places.

Where to install this add-on

Unless otherwise noted, all supported add-ons can be safely installed to all tiers of a distributed Splunk platform deployment. See [Where to install Splunk add-ons](#) in Splunk Add-ons for more information.

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

Splunk platform component	Supported	Required	Comments
Search Heads	Yes	Yes	Install this add-on to all search heads.
Indexers	Yes	Optional	Required for the parsing operations (sourcetype renaming) if the data is not coming from a heavy forwarder.
Heavy Forwarders	Yes	Yes	Required for the parsing operations (sourcetype renaming).
Universal Forwarders	No	No	This add-on requires heavy forwarders.

Distributed deployment compatibility

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

Distributed deployment feature	Supported	Comments
Search Head Clusters	Yes	You can install this add-on on a search head cluster for all search-time functionality.
Indexer Clusters	Yes	
Deployment Server	Yes	Supported for deploying via Deployment server

4.1.2 Installation walkthroughs

The Splunk Add-Ons manual includes an [Installing add-ons](#) guide that helps you successfully install any add-on to your Splunk platform. For a walkthrough of the installation procedure, follow the link that matches your deployment scenario:

- [Single-instance Splunk Enterprise](#)
- [Distributed Splunk Enterprise](#)
- [Splunk Cloud](#)

5.1 Splunk

- Configure a new index (e.g. netwaf) for the new logs

The IBM DataPower Add-on contains two base sourcetypes: - `ibm:datapower:syslog` - this should be used if you are sending data via UDP - `ibm:datapower:syslog:tcp` - this should be used if you are sending data via TCP

The reason behind having multiple base sourcetypes is due to the fact that DataPower logs different timestamp formats depending on how you are sending the logs. - Sending data via UDP doesn't allow for much configuration and the timestamp will look something like "Jul 10 10:45:32". - Sending data via TCP allows for extra time granularity since you can choose to include the microseconds and time zone. It will look something like "2019-07-10T10:45:32.123415+01:00".

5.1.1 Receiving syslogs on Splunk

NOTE: Its recommended to use a separate and dedicated syslog solution (e.g. rsyslog, syslog-ng, etc) for data persistence before forwarding it to Splunk. - Configure new TCP port (e.g. 514) pointing to the new index using the "ibm:datapower:syslog:tcp" sourcetype

5.1.2 Monitoring log files

- Configure a new file monitor input pointing to the new index using the "ibm:datapower:syslog:tcp" sourcetype

5.2 IBM DataPower

- Configure syslog outputs

For more information please refer to the [IBM DataPower documentation](#).

CHAPTER 6

Troubleshooting

7.1 Bugs & Support Issues

You can file bug reports on our [GitHub issue tracker](#) and they will be addressed as soon as possible. **Support is a volunteer effort** and there is no guaranteed response time.

CHAPTER 8

Indices and tables

- `genindex`
- `modindex`
- `search`