Splunk® Supported Add-ons
Splunk Add-on for MySQL released

Generated: 11/24/2022 10:20 am

Table of Contents

Overview

About the Splunk Add-on for MySQL

Version	3.1.0
Vendor Products	MySQL 5.7, 8.0.25, 8.0.29
Visible in Splunk Web	No. This add-on does not contain any views.

The Splunk Add-on for MySQL allows a Splunk software administrator to collect general logs, error logs, and slow query logs from MySQL servers and performance and configuration logs from local or remote MySQL Databases. This add-on provides the inputs and **CIM**-compatible knowledge to use with other Splunk apps, such as Splunk Enterprise Security and the Splunk App for PCI Compliance.

Splunk DB Connect version 3.5.1 or above is required to manage database connectivity. You must install and configure it before you can use this add-on to collect performance and configuration logs from a MySQL Database.

Splunk DB Connect versions 3.5.1 and lower do not support Splunk DB Connect templates that use the SHOW statement in their queries. For more information, see Configure Inputs for the Splunk Add-on for MySQL.

The Splunk Add-on for MySQL does not support versions 3.2.0 or earlier of Splunk DB Connect.

Download the Splunk Add-on for MySQL from Splunkbase at https://splunkbase.splunk.com/app/2848

Search the Splunk Community page for more information about this add-on.

Source types for the Splunk Add-on for MySQL

The Splunk Add-on for MySQL collects different events from different sources in MySQL Server. The add-on assigns different source types for each different log or event source.

There are two major groups of source types for the Splunk Add-on for MySQL. Each group depends on how events are collected:

- Collected through Splunk DB Connect (based on database queries)
- Collected through file monitoring (based on log files)

Log file source types

Data source	Source type	CIM Data Models
MySQL general log (file with general log content)	`mysql:generalQueryLog`	n/a
MySQL error log (file with error log content)	`mysql:errorLog`	n/a
MySQL Innodb status (regex matching Innodb status content from mysql:errorLog and redirecting to this source type)	`mysql:innodbStatus`	n/a

Data source	Source type	CIM Data Models
MySQL Slow Query Log (file with slow query log content)	`mysql:slowQueryLog`	Databases

Database entry source types

Data source	Collection method	Source type	CIM or ITSI data models
Logs from innodb_buffer_page database table	DB Connect	`mysql:innodb_buffer_page`	n/a
MySQL Innodb status	DB Connect	`mysql:innodbStatus`	n/a
MySQL role/account permission grant	DB Connect	`mysql:grants`	n/a
MySQL database threads/processes information	DB Connect	`mysql:databaseProcess`	Databases
MySQL process information	DB Connect	`mysql:processInfo`	Databases
MySQL system variables global settings	DB Connect	`mysql:variables`	ITSI Database
MySQL users	DB Connect	`mysql:user`	ITSI Database
Overall MySQL status	DB Connect	`mysql:status`	n/a
MySQL schema objects	DB Connect	`mysql:schemaObjectOverview`	n/a
Logs from database table	DB Connect	`mysql:database`	Databases
MySQL logs from general_log database table	DB Connect	`mysql:generalQueryLogDb`	ITSI Database
MySQL logs from slow_query database table	DB Connect	`mysql:slowQueryLogDb`	Databases
MySQL table status	DB Connect	`mysql:tableStatus`	ITSI Database
MySQL schema objects	DB Connect	`mysql:instance:stats`	ITSI Database
MySQL transactions	DB Connect	`mysql:transaction:stats`	ITSI Database
MySQL connections	DB Connect	`mysql:connection:stats`	ITSI Database
MySQL error log	DB Connect	`mysql:errorLogDb`	n/a
MySQL disk usage for all kinds of logs	DB Connect	`mysql:diskUsageDb`	n/a
MySQL summaries by stages	DB Connect	`mysql:userSummaryByStages`	n/a
Snapshot of which InnoDB locks transactions are waiting for	DB Connect	`mysql:innodbLockWaits`	n/a
MySQL global grants	DB Connect	`mysql:globalGrants`	n/a
MySQL events	DB Connect	`mysql:events`	n/a
MySQL loaded components	DB Connect	`mysql:components`	n/a
MySQL storage engines	DB Connect	`mysql:engines`	n/a

Release notes for the Splunk Add-on for MySQL

Version 3.1.0 of the Splunk Add-on for MySQL was released on July 18, 2022.

About this release

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

Splunk platform versions	8.1.x, 8.2.x, 9.0.x
CIM	5.0.1
ITSI	4.9.2
Platforms	Windows and Linux
Vendor Products	MySQL 5.7, 8.0.25, 8.0.29

New features

Version 3.1.0 of the Splunk Add-on for MySQL has the following new features.

- Support for MySQL 8.0.29.
- Support for CIM 5.0.1

Fixed issues

Version 3.1.0 of the Splunk Add-on for MySQL has the following fixed issues. If no issues appear, then none have been reported.

Known issues

Version 3.1.0 of the Splunk Add-on for MySQL has the following known issues. If no issues appear, then none have been reported.

Third-party software attributions

Version 3.1.0 of the Splunk Add-on for MySQL does not use any third-party libraries.

Release history for the Splunk Add-on for MySQL

Latest version

The latest version of the Splunk Add-on for MySQL is version 3.1.0. See Release notes for the Splunk Add-on for MySQL for the release notes of this latest version.

Version 3.0.0

Version 3.0.0 of the Splunk Add-on for MySQL was released on August 12, 2021.

About this release

Version 3.0.0 of the Splunk Add-on for MySQL is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	8.1.x, 8.2.x
CIM	14.20.0
ITSI	4.9.2
Platforms	Windows and Linux
Vendor Products	MySQL 5.7, 8.0.25

New features

Version 3.0.0 of the Splunk Add-on for MySQL has the following new features.

- Support for MySQL 8.0.25.
- Removed support for MySQL 5.6.
- Removed UI.
- Removed automation around creating monitor stanzas.
- Removed support for `mysqlbinlog` tool.
- Removed support for `mysqldiskusage` tool.
- Removed support for these source types:
    - mysql:errorLog:mysqld_safe
    - mysql:file_summary_by_instance
    - mysql:file_summary_by_event_name
    - mysql:hostSummary
    - mysql:events_waits_summary_global_by_event_name
    - mysql:events_waits_summary_by_user_by_event_name
    - mysql:events_statements_summary_by_user_by_event_name
    - mysql:events_statements_summary_by_host_by_event_name
    - mysql:events_statements_summary_by_digest
    - mysql:statementsWithRuntimesIn95Percentile
    - mysql:ioByThreadByLatency
    - mysql:userSummary
    - mysql:table_io_waits_summary_by_index_usage
    - mysql:schemaTableStatsBuffer
    - mysql:tableStatsBuffer
    - mysql:diskUsage
    - mysql:binLog

Fixed issues

Version 3.0.0 of the Splunk Add-on for MySQL has the following fixed issues. If no issues appear, then none have been reported.

Known issues

Version 3.0.0 of the Splunk Add-on for MySQL has the following known issues. If no issues appear, then none have been reported.

Third-party software attributions

Version 3.0.0 of the Splunk Add-on for MySQL does not use any third-party libraries.

Version 2.0.2

About this release

Version 2.0.2 of the Splunk Add-on for MySQL is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	7.1.x, 7.2.x, 7.3.x, 8.0.x
CIM	4.14
Platforms	Windows and Linux
Vendor Products	MySQL 5.6, 5.7

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

New features

Version 2.0.2 of the Splunk Add-on for MySQL has the following new features.

- Default support for Python3
- Enhanced python library structure

Fixed issues

Version 2.0.2 of the Splunk Add-on for MySQL has the following fixed issues. If no issues appear, then none have been reported.

Date resolved	Issue number	Description
2020-07-10	ADDON-26828	Addons unable to load UI or collect data on Splunk 8.0.4, 8.0.2004 and Splunk 8.0.5
2020-06-30	ADDON-26889, ADDON-26876, ADDON-26892	Fix UI and Data collection of Addon on Splunk 8.0.4 and 8.0.2004

Known issues

Version 2.0.2 of the Splunk Add-on for MySQL has the following known issues. If no issues appear, then none have been reported.

Third-party software attributions

Version 2.0.1 of the Splunk Add-on for MySQL incorporates the following third party software components:

- httplib2
- SortedContainers.
- Future.
- Configparser.

Version 2.0.1

Version 2.0.1 of the Splunk Add-on for MySQL was released on March 10, 2020.

About this release

Version 2.0.1 of the Splunk Add-on for MySQL is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	7.0.x, 7.1.x, 7.2.x, 7.3.x
CIM	4.14
Platforms	Windows and Linux
Vendor Products	MySQL 5.6, 5.7

New features

Version 2.0.1 of the Splunk Add-on for MySQL has the following new features.

- Default support for Python3

Fixed issues

Version 2.0.1 of the Splunk Add-on for MySQL has the following fixed issues. If no issues appear, then none have been reported.

Known issues

Version 2.0.1 of the Splunk Add-on for MySQL has the following known issues. If no issues appear, then none have been reported.

Date filed	Issue number	Description
2020-06-01	ADDON-26889, ADDON-26876, ADDON-26892	Fix UI and Data collection of Addon on Splunk 8.0.4 and 8.0.2004

Third-party software attributions

Version 2.0.1 of the Splunk Add-on for MySQL incorporates the following third party software components:

- Httplib2 Python library
- SortedContainers.
- Future.
- Configparser.

Version 2.0.0

Version 2.0.0 of the Splunk Add-on for MySQL was released on January 24, 2020.

About this release

Version 2.0.0 of the Splunk Add-on for MySQL is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x
CIM	4.14
Platforms	Windows and Linux
Vendor Products	MySQL 5.6, 5.7

New features

Version 2.0.0 of the Splunk Add-on for MySQL has the following new features.

- Support for Python3
- Support for Splunk DB Connect 3

Fixed issues

Version 2.0.0 of the Splunk Add-on for MySQL has the following fixed issues. If no issues appear, then none have been reported.

Known issues

Version 2.0.0 of the Splunk Add-on for MySQL has the following known issues. If no issues appear, then none have been reported.

Date filed	Issue number	Description
2020-06-01	ADDON-26889, ADDON-26876, ADDON-26892	Fix UI and Data collection of Addon on Splunk 8.0.4 and 8.0.2004

Third-party software attributions

Version 2.0.0 of the Splunk Add-on for MySQL incorporates the following third party software components:

- Httplib2 Python library
- SortedContainers.
- Future.
- Configparser.

Version 1.1.0

Version 1.1.0 of the Splunk Add-on for MySQL is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.6.x, 7.0.x, 7.1.x, 7.2.x
CIM	4.11
Platforms	Windows and Linux
Vendor Products	MySQL 5.6, 5.7

New features

Version 1.1.0 of the Splunk Add-on for MySQL has the following new features.

Date	Issue number	Description
2016-03-31	ADDON-7312	Update add-on to support ITSI integration. Add new source types and provide mapping to the ITSI Database module.

Fixed issues

Version 1.1.0 of the Splunk Add-on for MySQL has the following fixed issues.

Date	Issue number	Description
2016-02-03	ADDON-7654	The field "uptime" in source type `[mysql:status]` is not extracted as expected.

Known issues

Version 1.1.0 of the Splunk Add-on for MySQL has the following known issues.

Date	Issue number	Description
2016-04-19	ADDON-8226	The show statement in a Splunk search (for example, `show tables`) works if the add-on is configured in the Splunk Add-on for MySQL setup UI (wherein the `inputs.conf` for DB Connect is generated automatically) or if the add-on is configured directly in the `inputs.conf` of DB Connect. However it does not work when DB Connect inputs are configured through the DB Connect web UI. Workaround: Use the latest version of DB Connect (2.1.3 or later) and add `enable_query_wrapping = 0` to the corresponding connection stanza in the `local/db_connections.conf`.

2016-04-05	ADDON-8578	Failure to get events for `sourcetype=mysql:processInfo` when sql_mode "ONLY_FULL_GROUP_BY" is on. See workaround in Troubleshooting section.
2016-03-01	ADDON-8064	Queries on mysql_variables fails if @@global.show_compatibility_56 is not set. See workaround in Troubleshooting section.
2016-02-23	ADDON-7922	DB Connect Query results in error when querying for Username field. See workaround in Troubleshooting section.
2015-12-18	ADDON-4936	In search results, some events are displayed on multiple lines instead of one continuous line.
2016-01-30	ADDON-8695	FIPS mode is not supported by this add-on. For a workaround, see Add-ons and FIPS mode in the *Splunk Add-ons* manual.

Note: Versions 3.0.3 and earlier of Splunk DB Connect do not support a new installation of the Splunk Add-on for MySQL. To configure inputs using versions 3.0.3 and earlier of Splunk DB Connect, see Use the Splunk DB Connect GUI to configure your database inputs for details.

Third-party software attributions

Version 1.1.0 of the Splunk Add-on for MySQL incorporates the Httplib2 Python library and SortedContainers.

Version 1.0.0

Version 1.0.0 of the Splunk Add-on for MySQL has the same compatibility specifications as version 1.1.0.

New features

Version 1.0.0 of the Splunk Add-on for MySQL has the following new features.

Date	Issue number	Description
08/20/15	ADDON-603	New add-on providing inputs and CIM normalization for MySQL.

Known issues

Version 1.0.0 of the Splunk Add-on for MySQL has the following known issue.

Date	Issue number	Description
2016-01-30	ADDON-7646	FIPS mode is not supported by this add-on. For a workaround, see Add-ons and FIPS mode in the *Splunk Add-ons* manual.

Third-party software attributions

Version 1.0.0 of the Splunk Add-on for MySQL incorporates the Httplib2 Python library and SortedContainers.

Installation and Configuration

Hardware and software requirements for the Splunk Add-on for MySQL

Enable MySQL logs

You need to enable the following MySQL logs. If any of the logs are not enabled, they will not be collected. Refer to the following instructions for information:

Version 5.7

- Slow query log: https://dev.mysql.com/doc/refman/5.7/en/slow-query-log.html
- General query log: https://dev.mysql.com/doc/refman/5.7/en/query-log.html
- Error log: https://dev.mysql.com/doc/refman/5.7/en/error-log.html

Version 8.0.x

- Slow query log: https://dev.mysql.com/doc/refman/8.0/en/slow-query-log.html
- General query log: https://dev.mysql.com/doc/refman/8.0/en/query-log.html
- Error log: https://dev.mysql.com/doc/refman/8.0/en/error-log.html

Splunk DB Connect

You must have Splunk DB Connect installed to your heavy forwarders to collect MySQL performance and configuration logs with this add-on. The Splunk Add-on for MySQL works with DB Connect versions 3.5.1 and later. See Deploy and Use Splunk DB Connect in the *Splunk DB Connect* manual for information.

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 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 MySQL

Install and configure this add-on on your supported platform.

1. Download the add-on from Splunkbase.

2. Determine where and how to install this add-on in your deployment, using the tables in the following steps.

3. Install the Splunk Add-on for MySQL.

4. Configure inputs for the Splunk Add-on for MySQL.

Install the Splunk Add-on for MySQL

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

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 instance type	Supported	Required	Comments
Search Heads	Yes	Yes	Install this add-on to all search heads where MySQL knowledge management is required.
Indexers	Yes	Conditional	Not required if you use heavy forwarders to monitor MySQL log files directly on MySQL machines. This is required if you use universal or light forwarders for monitor inputs.
Heavy Forwarders	Yes	Supported for monitor inputs only. Forwarder needs to be installed directly on the MySQL server for file monitoring of local logs.	The forwarder doing the data collection needs to be installed directly on the MySQL server for file monitoring of local logs.
Universal Forwarders	Yes	No	Supported for monitor inputs only. Forwarder needs to be installed directly on the MySQL server for file monitoring of local logs.
Light Forwarders	No	No	This add-on does not support light forwarders because Splunk recommends using the Splunk Web user interface to perform the setup and authentication with MySQL.

Distributed deployment feature 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	
Indexer Clusters	Yes	

Distributed deployment feature	Supported	Comments
Deployment Server	Conditional	Supported for deploying the configured add-on to multiple forwarders for local data collection using file monitoring. Not supported for DB Connect inputs.

Installation walkthroughs

The *Splunk Add-Ons* manual includes an Installing add-ons guide that helps you successfully install any Splunk-supported 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

Migrate Splunk add-on for MySQL version 3.0.0 to 3.1.0

There are no additional steps required to upgrade the Splunk Addon for MySQL from v3.0.0 to v3.1.0. If you want to use the file monitoring feature, see how to Monitor Files and Directories with Splunk Web.

Migrate Splunk add-on for MySQL version 2.0.2 to 3.0..0

The Splunk Add-on for MySQL version 3.0.0 no longer supports automation for input creation in DB Connect. This only affects the automation for new servers, but all currently created inputs (whether they were created by automation or otherwise) in DB Connect will remain. If you want to use the file monitoring feature, see how to Monitor Files and Directories with Splunk Web.

We no longer support these source types:

- mysql:errorLog:mysqld_safe
- mysql:file_summary_by_instance
- mysql:file_summary_by_event_name
- mysql:hostSummary
- mysql:events_waits_summary_global_by_event_name
- mysql:events_waits_summary_by_user_by_event_name
- mysql:events_statements_summary_by_user_by_event_name
- mysql:events_statements_summary_by_host_by_event_name
- mysql:events_statements_summary_by_digest
- mysql:statementsWithRuntimesIn95Percentile
- mysql:ioByThreadByLatency
- mysql:userSummary
- mysql:table_io_waits_summary_by_index_usage
- mysql:schemaTableStatsBuffer
- mysql:tableStatsBuffer
- mysql:diskUsage
- mysql:binLog

Inputs from previous versions of the Splunk add-on for MySQL will continue to work as designed. Both CIM mappings and extractions will work as expected. Splunk best practice is to add the new inputs as then they will be properly extracted.

Configure inputs for the Splunk Add-on for MySQL

To gather data from MySQL, the Splunk Add-on for MySQL leverages Splunk DB Connect.

Set up the database connection

1. Download the connector driver for MySQL database from https://dev.mysql.com/downloads/connector/j/

2. Place the driver file called `mysql-connector-java*.jar` in `$SPLUNK_HOME/etc/apps/splunk_app_db_connect/drivers/` on the part of your Splunk Enterprise architecture performing the data collection.

3. Still on the part of your Splunk Enterprise architecture performing data collection, go to Splunk DB Connect in Splunk Web.

4. Create an identity for establishing a connection to a database. Make sure the DB user for this identity has access to MySQL information_schema, performance_schema and mysql schemas.

Use the Splunk DB Connect GUI to create a database connection

To create a database connection to the MySQL using the Splunk DB Connect GUI:

refer to the "Create and manage database connections" in the Splunk DB Connect manual for step-by-step instructions for using the GUI to set up a new database connection.

Configure the inputs using the Splunk DB Connect GUI

If you want to create MySQL database input, choose the template created for '*Splunk Add-on for MySQL* under Template field of DB Connect.

Configure the inputs using the Splunk DB Connect v3.5.1 or lower

> For cloud environment, please contact Splunk Cloud SRE

1. Configure the Splunk Add-on for MySQL, if you have not done so already.
2. Copy the following text:

```
[<input_name>]
batch_upload_size = 1000
connection = <connection>
description = Query all database instances in a MySQL box
disabled = 0
fetch_size = 300
index = <index>
index_time_mode = current
input_type = event
```

```
interval = 86400
max_rows = 0
mode = batch
query = show databases;
query_timeout = 30
sourcetype = mysql:database
template_name = mysql:database
source = <source>

[<input_name>]
batch_upload_size = 1000
connection = <connection>
description = Query innodb engine of the database
disabled = 0
fetch_size = 300
index = <index>
index_time_mode = current
input_type = event
interval = 120
max_rows = 0
mode = batch
tail_rising_column_number =
query = SHOW ENGINE INNODB STATUS;
query_timeout = 30
sourcetype = mysql:innodbStatus
template_name = mysql:innodbStatus
source = <source>

[<input_name>]
batch_upload_size = 1000
connection = <connection>
description = Query all of the current running process of the database
disabled = 0
fetch_size = 300
index = <index>
index_time_mode = current
input_type = event
interval = 120
max_rows = 0
mode = batch
tail_rising_column_number =
query = SHOW FULL PROCESSLIST;
query_timeout = 30
sourcetype = mysql:databaseProcess
template_name = mysql:databaseProcess
source = <source>

[<input_name>]
batch_upload_size = 1000
connection = <connection>
description = Query grant actions in the database
disabled = 0
fetch_size = 300
index = <index>
index_time_mode = current
input_type = event
interval = 300
max_rows = 0
mode = batch
tail_rising_column_number =
query = SHOW GRANTS;
query_timeout = 30
```

```
sourcetype = mysql:grants
template_name = mysql:grants
source = <source>
```

3. Navigate to $SPLUNK_HOME/etc/apps/Splunk_TA_mysql/local, and open db_inputs.conf.
4. Paste your copied MySQL inputs to In db_inputs.conf.
5. For each of your mysql inputs, change each mention of <input_name>, <connection>, <index> and <source> to appropriate values for each parameters.
6. Save your changes.
7. Restart your Splunk platform deployment.

Troubleshooting

Troubleshoot the Splunk Add-on for MySQL

General troubleshooting

For helpful troubleshooting tips that you can apply to all add-ons, see Troubleshoot add-ons in *Splunk Add-ons*. For additional resources, see Support and resource links for add-ons in *Splunk Add-ons*.

To check for DB Connect errors, you can perform this search of the DB Connect internal logs:

```
index=_internal sourcetype=dbx* state=error
```

DB Connect does not collect data

If DB Connect doesn't collect anything, make sure that you installed Splunk DB Connect, configured its java path, and installed the MySQL JDBC before doing the setup for the Splunk Add-on for MySQL.