Splunk: MySQL data connection setup

This document will detail the steps necessary for connecting to a Jamf Pro MySQL database as a Splunk data source.

One of the easier ways to get Jamf Pro data is to connect directly to the Jamf Pro's MySQL database. While the process for doing this is fairly straight forward, some of the steps are particular and should be done in a specific way. For example, allowing access to the MySQL database in a relatively secure fashion.

There are several steps to connecting Splunk to a database connection. Database connection add-ons and JDBC drivers need to be installed. User and connection information needs to configured. How often particular data is pulled and how it's organized within Splunk needs to be determined. While there are a lot of steps, none of them are insurmontable or very complicated.

Preparing MySQL

The first thing we have to do is prepare MySQL to both allow external connections in general and a specific user connection to gather data from MySQL. By default the Jamf Pro MySQL instance does not allow external connection or have users other than root and those used to connect to Jamf Pro.

Allowing connections to MySQL

By default, external connections are not enabled to a Jamf Pro MySQL instance. The default IP of the MySQL server is '127.0.0.1', so external requests aren't even seen. We must change the MySQL configuration file and restart so external connections are possible.

```
> cd /etc/mysql/mysql.conf.d
> sudo vi mysqld.cnf
```

The exact location of the 'mysqld.cnf' file that needs editing may vary, but it should be located somewhere in '/etc/mysql'.

Comment out 'bind-address'.

```
43 #opener
44 bind-address            = 127.0.0.1
45 #

to

43 #opener
44 #bind-address            = 127.0.0.1
45 #
```

Restart mysql.

```
> sudo service mysql restart
```

Create limited MySQL user

We should now create a MySQL user specifically for accessing MySQL from Splunk. There are a couple reasons for doing this. The first is to limit access to the databases and tables in MySQL. Splunk should only need access to the 'jamfsoftware' database and should only need 'read' (SELECT) access to tables within that database. Another reason is logging usage and access from Splunk. If all requests from Splunk come from specific users, it is easier to track any impact Splunk usage may have on the Jamf Pro instance.

First log in to MySQL. Where <admin> is a MySQL admin user or 'root

```
> mysql -u <admin> -p
```

Now create a new user. <host> can be an IP address or a FQDN .

```
: CREATE USER '<username>'@'<host>' IDENTIFIED BY '<password>';

examples
: CREATE USER 'splunk'@'foo.jamf.corp' IDENTIFIED BY 'jamf1234';
: CREATE USER 'splunk'@'10.20.30.40' IDENTIFIED BY 'jamf1234';
```

If SSL certificates are in use, the user can be created requiring their use for connections.

```
: CREATE USER '<username>'@'<host>' IDENTIFIED BY '<password>' REQUIRE
SSL;
```

Give the user access to specific databases and tables within MySQL.

```
: GRANT SELECT ON jamfsoftware.<table> TO '<username>'@'<host>';

examples:
: GRANT SELECT ON jamfsoftware.computers_denormalized TO
'splunk'@'foo.jamf.corp';
: GRANT SELECT ON jamfsoftware.mobile_devices_denormalized TO
'splunk'@'foo.jamf.corp';
: GRANT SELECT ON jamfsoftware.buildings TO 'splunk'@'foo.jamf.corp';
: GRANT SELECT ON jamfsoftware.departments TO
'splunk'@'foo.jamf.corp';
```

Note: While it is possible to grant a user access to all tables within a database with wildcards, doing so carries some risk. One could grant the user 'splunk' SELECT access to all tables and fields within the 'jamfsoftware' database. However this would include the 'users' table and all the Jamf Pro user subtables. When possible, MySQL users should only be granted the access required to produce the desired Splunk visualizations.

Create SSL cert for MySQL connection (ver. 5.6 and before, optional)

MySQL Documentation : creating ssl files

Connecting to a MySQL database remotely can be done several ways. Splunk uses a standard connection to the default MySQL port 3306. While this method works well, it is also insecure. Credentials to log in to MySQL are passed via an unencrypted connection and could be snooped. Luckily, there is a way to connect to MySQL via a secure encrypted connection.

Care should be taken protecting the certs, especially the private keys. With the private keys, anyone could generate client certs which could allow access to MySQL server.

This is the older, more complicated method for generating SSL certs for MySQL. With version 5.7 and newer there is a simpler method.

The steps below assume no certs are currently in use for MySQL.

First, create a certificate authority certificate.

```
> cd /etc/mysql
> mkdir certs && cd certs


> openssl genrsa 2048 > ca-key.pem
> openssl req -new -x509 -nodes -days 3600 -key ca-key.pem -out ca.pem
```

Follow the instructions presented

```
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or
a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:MN
Locality Name (eg, city) []:Frostbite Falls
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Mooseworks
Organizational Unit Name (eg, section) []:hats
Common Name (e.g. server FQDN or YOUR name) []:hats.moosensqurl.net
Email Address []:help@moosensqurl.net
```

Create server certificate. These are the certs that are used by the server to establish a secure connection.

Sign and add a passphrase for server certificate. 'server-cert.pem' is the public key. 'server-key.pem' is the private key.

```
> openssl req -newkey rsa:2048 -days 3600 -nodes -keyout
server-key.pem -out server-req.pem
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or
a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:MN
Locality Name (eg, city) []:Frostbite Falls
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Mooseworks
Organizational Unit Name (eg, section) []:hats
Common Name (e.g. server FQDN or YOUR name) []:hats.moosensqurl.net
Email Address []:help@moosensqurl.net

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:rocky001BullW
An optional company name []:Mooseworks


> openssl rsa -in server-key.pem -out server-key.pem
> openssl x509 -req -in server-req.pem -days 3600 -CA ca.pem -CAkey
ca-key.pem -set_serial 00001 -out server-cert.pem
```

Create client certificates. These are the certs that will be used remotely to log in to MySQL securely.

The client challenge password should be different from server challenge password. There could be multiple client certs for a single server cert.

```
> openssl req -newkey rsa:2048 -days 3600 -nodes -keyout
client-key.pem -out client-req.pem

-----
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or
a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:MN
Locality Name (eg, city) []:Frostbite Falls
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Mooseworks
Organizational Unit Name (eg, section) []:hats
Common Name (e.g. server FQDN or YOUR name) []:hats.moosensqurl.net
Email Address []:help@moosensqurl.net

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:boris991Natasha&
An optional company name []:Mooseworks


> openssl rsa -in client-key.pem -out client-key.pem
> openssl x509 -req -in client-req.pem -days 3600 -CA ca.pem -CAkey
ca-key.pem -set_serial 00001 -out client-cert.pem
```

Verify new certificates against certificate authority.

```
> openssl verify -CAfile ca.pem server-cert.pem client-cert.pem
  server-cert.pem: OK
  client-cert.pem: OK
```

Copy certs to MySQL data directory.

Find MySQL data directory

The MySQL data directory can be found with a command to mysql.

```
> mysql -u <admin user> -p -e 'SHOW VARIABLES WHERE Variable_Name LIKE "%dir"'
> cd /etc/mysql/certs


## if certs file doesn't exist is data directory
> sudo mkdir /var/lib/mysql/certs
> sudo chown mysql:mysql /var/lib/mysql/certs
> sudo cp ca.pem server-cert.pem server-key.pem /var/lib/mysql/certs


## change ownership of certs so MySQL can access them
> sudo chown -R mysql:mysql /var/lib/mysql/certs
```

Now configure MySQL to use the new certs. The location and name of the MySQL configuration file can vary by individual installation.

MySQL : Using secure connections

Find 'mysqld.cnf' files

> locate mysqld.cnf

```
> cd /etc/mysql/mysql.conf.d
> sudo vi mysqld.cnf
```

'mysqld.cnf'

```
[mysqld]
...
# mysql ssl certs
ssl-ca=/var/lib/mysql/certs/ca.pem
ssl-cert=/var/lib/mysql/certs/server-cert.pem
ssl-key=/var/lib/mysql/certs/server-key.pem
```

Restart mysql.

```
> sudo service mysql restart
```

Create SSL cert for MySQL connection (ver 5.7 and after, optional)

With version 5.7 of MySQL there is a much simpler method for generating SSL certs for use with MySQL. A single command will generate all required certificates in a specified directory. Care should be taken protecting the certs, especially the private keys. With the private keys, anyone could generate client certs which could allow access to MySQL server.

Generate certs.

```
> sudo mysql_ssl_rsa_setup --datadir=<mysql data directory> --verbose


## if certs file doesn't exist is data directory
> sudo mkdir /var/lib/mysql/certs
> sudo chown mysql:mysql /var/lib/mysql/certs


example:
> sudo mysql_ssl_rsa_setup --datadir=/var/lib/mysql/certs --verbose


2017-03-10 18:33:12 [NOTE]    Destination directory:
/var/lib/mysql/certs
2017-03-10 18:33:12 [NOTE]    Executing : openssl version
OpenSSL 1.0.2g  1 Mar 2016
2017-03-10 18:33:12 [NOTE]    Executing : openssl req -newkey rsa:2048
-days 3650 -nodes -keyout ca-key.pem -subj
/CN=MySQL_Server_5.7.17_Auto_Generated_CA_Certificate -out ca-req.pem
&& openssl rsa -in ca-key.pem -out ca-key.pem
Generating a 2048 bit RSA private key
.......................................+++
..........+++
writing new private key to 'ca-key.pem'
-----
writing RSA key
2017-03-10 18:33:12 [NOTE]    Executing : openssl x509 -sha256 -days
3650 -set_serial 1 -req -in ca-req.pem -signkey ca-key.pem -out ca.pem
Signature ok
subject=/CN=MySQL_Server_5.7.17_Auto_Generated_CA_Certificate
Getting Private key
2017-03-10 18:33:12 [NOTE]    Executing : openssl req -newkey rsa:2048
-days 3650 -nodes -keyout server-key.pem -subj
/CN=MySQL_Server_5.7.17_Auto_Generated_Server_Certificate -out
server-req.pem && openssl rsa -in server-key.pem -out server-key.pem
Generating a 2048 bit RSA private key
........+++
...............................+++
writing new private key to 'server-key.pem'
-----
writing RSA key
2017-03-10 18:33:12 [NOTE]    Executing : openssl x509 -sha256 -days
3650 -set_serial 2 -req -in server-req.pem -CA ca.pem -CAkey
ca-key.pem -out server-cert.pem
Signature ok
subject=/CN=MySQL_Server_5.7.17_Auto_Generated_Server_Certificate
```

```
Getting CA Private Key
2017-03-10 18:33:12 [NOTE]    Executing : openssl req -newkey rsa:2048
-days 3650 -nodes -keyout client-key.pem -subj
/CN=MySQL_Server_5.7.17_Auto_Generated_Client_Certificate -out
client-req.pem && openssl rsa -in client-key.pem -out client-key.pem
Generating a 2048 bit RSA private key
......................................................................
.................................................+++
......................................................................
..............................+++
writing new private key to 'client-key.pem'
-----
writing RSA key
2017-03-10 18:33:12 [NOTE]    Executing : openssl x509 -sha256 -days
3650 -set_serial 3 -req -in client-req.pem -CA ca.pem -CAkey
ca-key.pem -out client-cert.pem
Signature ok
subject=/CN=MySQL_Server_5.7.17_Auto_Generated_Client_Certificate
Getting CA Private Key
2017-03-10 18:33:12 [NOTE]    Executing : openssl verify -CAfile
ca.pem server-cert.pem client-cert.pem
server-cert.pem: OK
client-cert.pem: OK
2017-03-10 18:33:12 [NOTE]    Executing : openssl genrsa  -out
private_key.pem 2048
Generating RSA private key, 2048 bit long modulus
...........................+++
.......................................+++
e is 65537 (0x10001)
2017-03-10 18:33:12 [NOTE]    Executing : openssl rsa -in
```

```
private_key.pem -pubout -out public_key.pem
writing RSA key
2017-03-10 18:33:12 [NOTE]    Success!
```

Change ownership of certs so MySQL can access them.

```
> sudo chown -R mysql:mysql /var/lib/mysql/certs
```

Testing the connection

There are several tools for testing a MySQL connection to verify it functions. One could just try out the connection with Splunk. Splunk has a fairly robust connection tester. However other tools can also be used to test MySQL connections.

One useful tool in this regard is 'Sequel Pro'. Available for macOS, ‘Sequel Pro’ allows creation of database connections, browsing through available databases, even running SQL commands against tables.

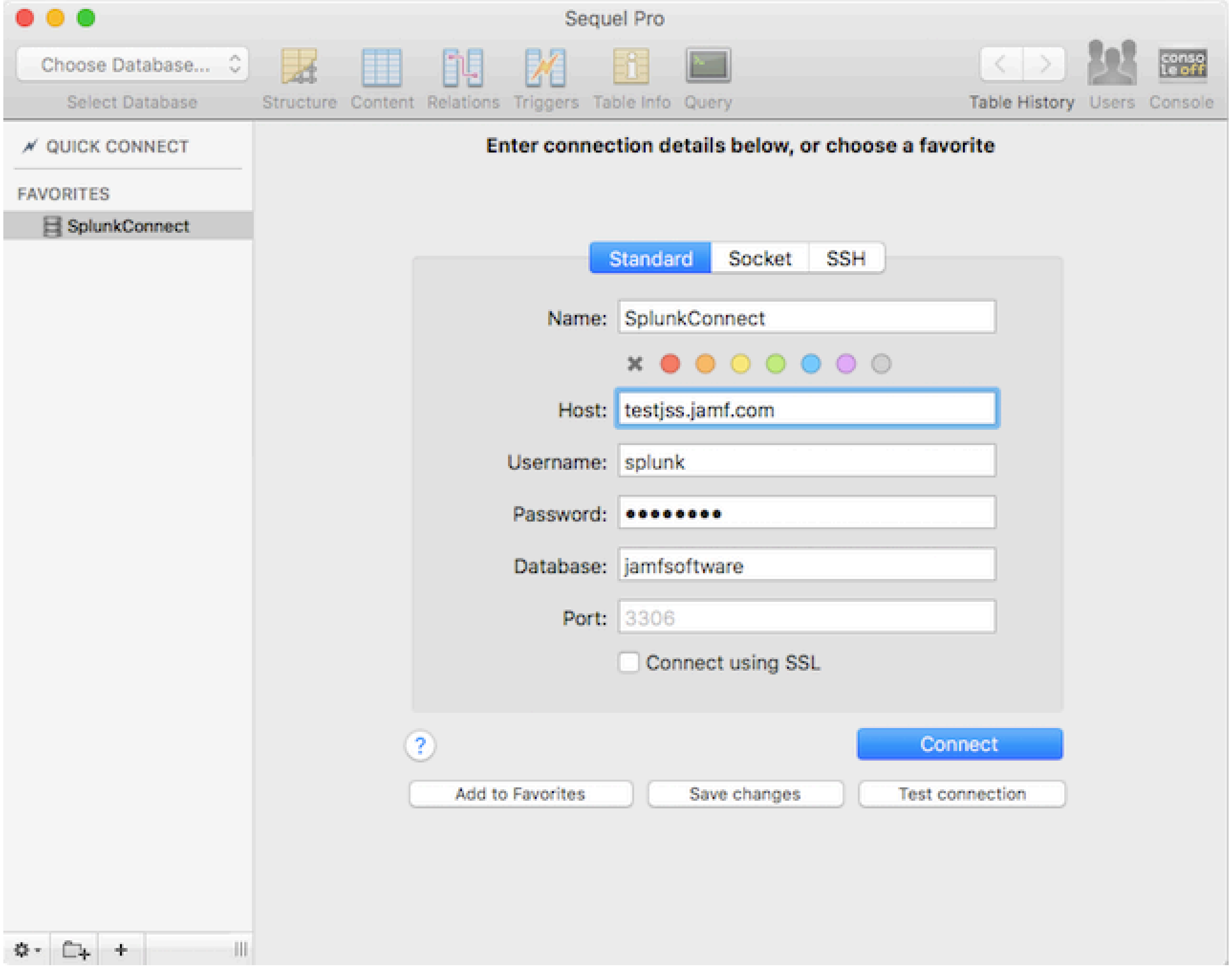
Sequel Pro

A more cross-platform solution would be MySQL's own tool, 'MySQL Workbench'. 'MySQL Workbench' has more functionality than 'Sequel Pro', but is often more complex to use.

MySQL Workbench

To demonstrate how to test a MySQL connection using 'Sequel Pro'.

First look at the basic connection screen.



Enter connection details below, or choose a favorite

Name: SplunkConnect

Host: testjss.jamf.com

Username: splunk

Password: •••••••••

Database: jamfsoftware

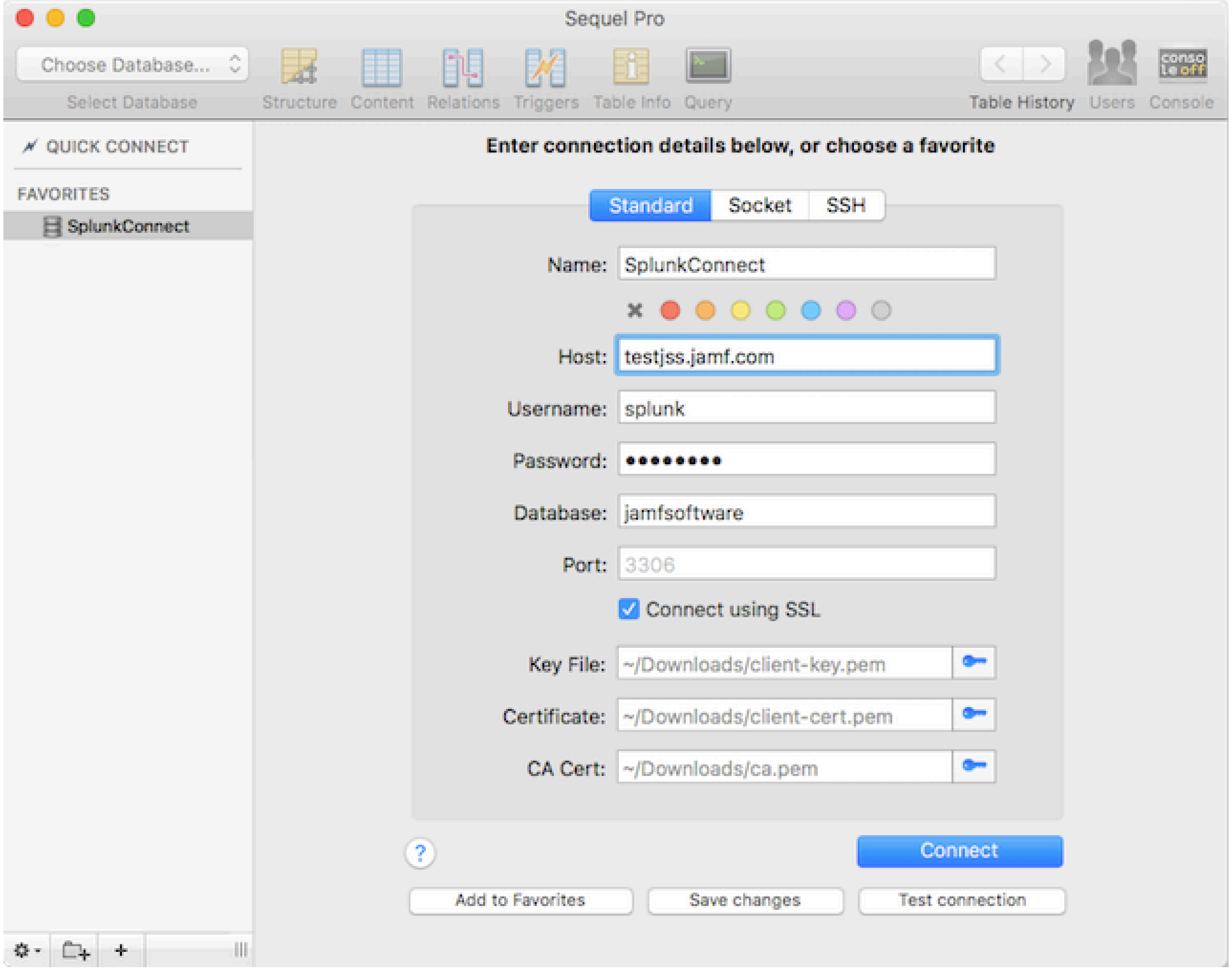
Port: 3306

☐ Connect using SSL

On this screen:

- **'Name'** is the label for the connection.
- **'Host'** is the fully qualified host name of the MySQL server.
- **'Username'** is the username used to log in to MySQL.
- **'Password'** is the password used to log in to MySQL.
- **'Database'** is an optional field. If a valid database name is entered here, when connecting to MySQL that database will automatically be opened. If left blank, a list of valid databases is shown on connection.
- **'Port'** is auto-populated with the default port for MySQL connections. It can be changed, but generally isn't.
- The **'Connect using SSL'** checkbox isn't required. However, connecting to MySQL via SSL is a good idea.

Using the certificates generated above, a secure connection to MySQL can be made.



Enter connection details below, or choose a favorite

Name: SplunkConnect

Host: testjss.jamf.com

Username: splunk

Password: ●●●●●●●●●

Database: jamfsoftware

Port: 3306

☑ Connect using SSL

Key File: ~/Downloads/client-key.pem

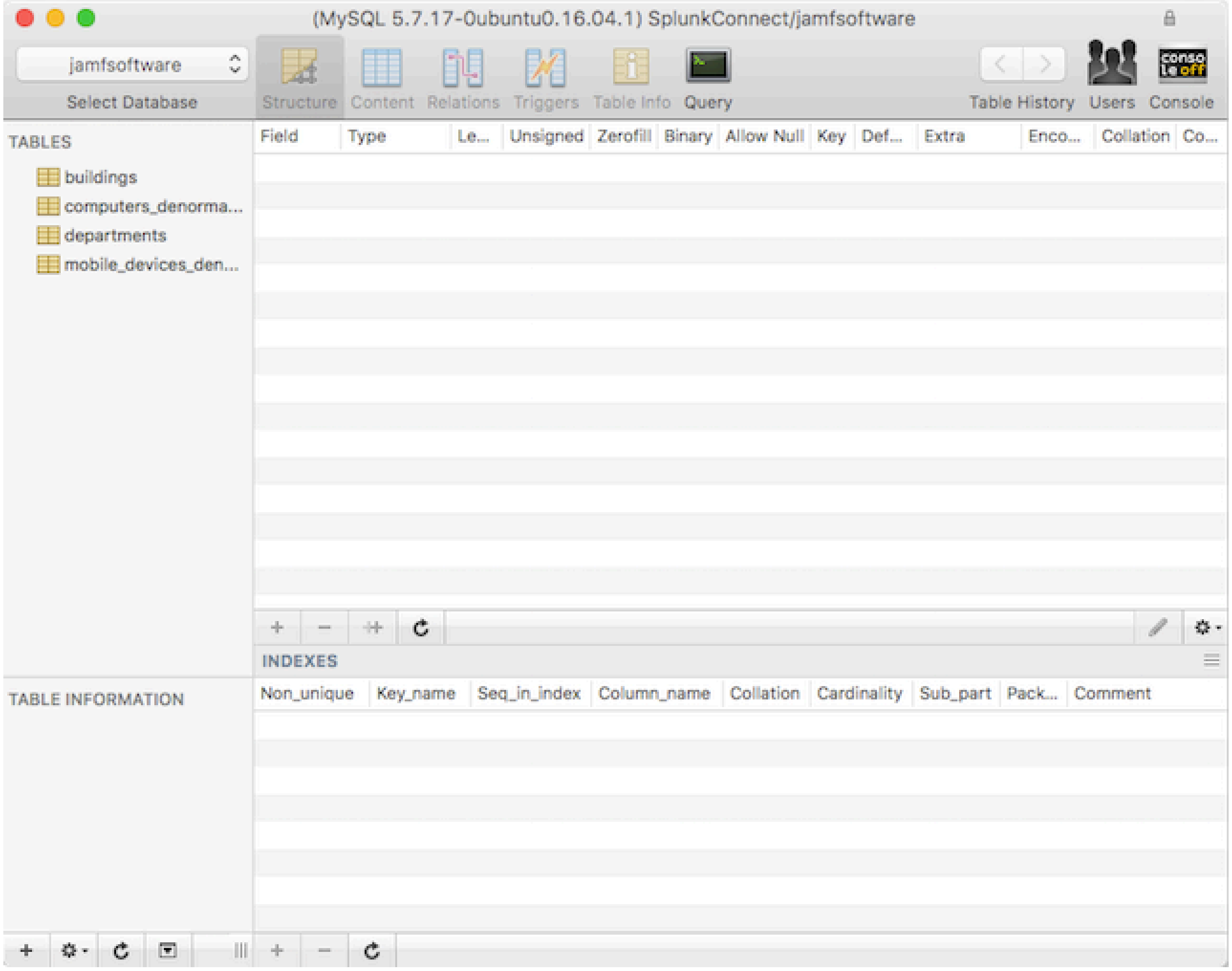
Certificate: ~/Downloads/client-cert.pem

CA Cert: ~/Downloads/ca.pem

Three certificates or encryption keys are needed by 'Sequel Pro' to establish a secure connection.

- The client private key file: **client-key.pem**
- The client certificate file: **client-cert.pem**
- The public certificate authority file: **ca.pem**

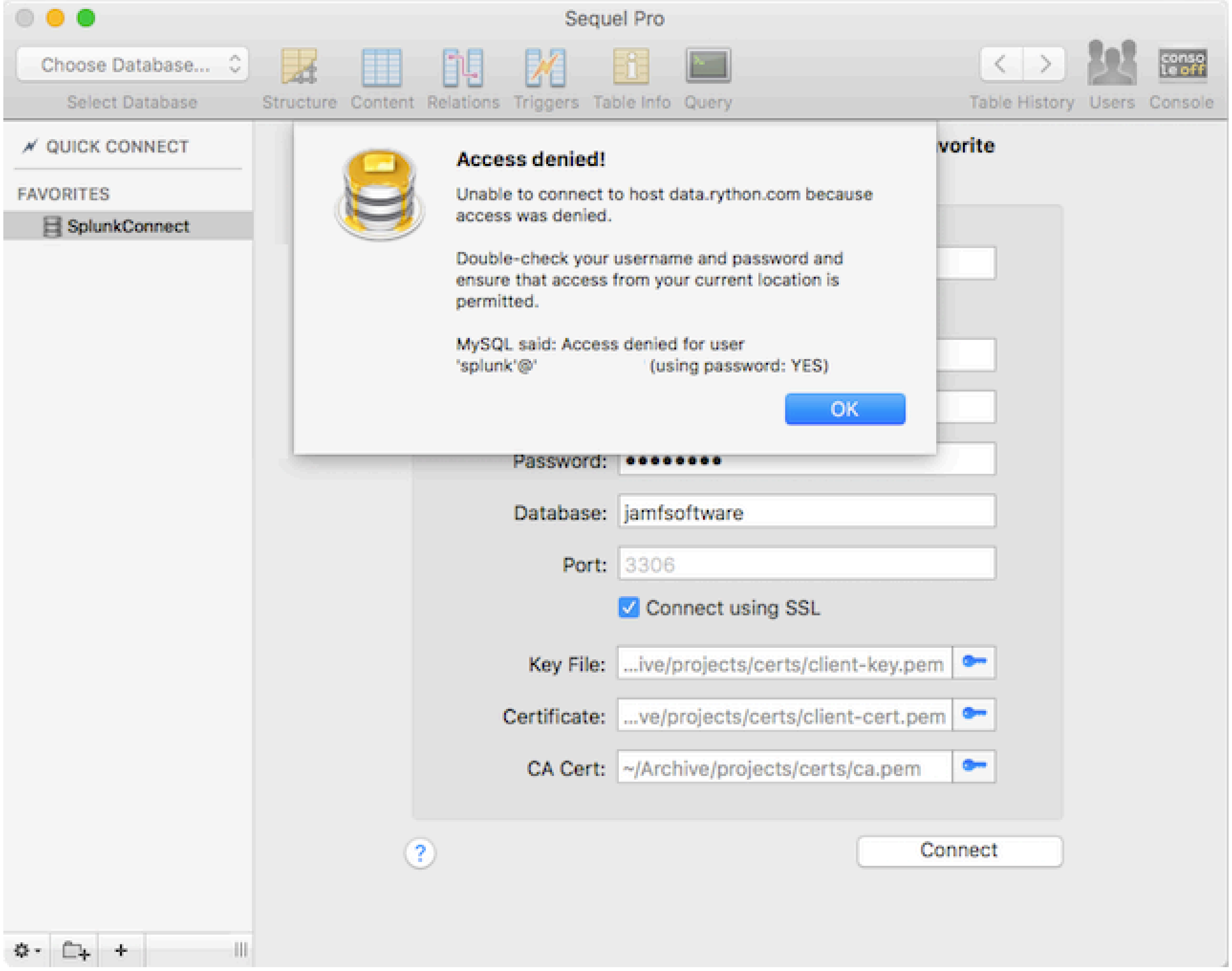
If a connection is successful, 'Sequel Pro' will show the databases and tables this user has access to. If the connection is set to automatically use a database, the available tables for that database will be shown.



General areas on this screen:

- **'Select Database'** shows this connection's available databases.
- **'Tables'** shows the database tables available to this connection.
- **'Table Information'** show some basic information for the selected table.
- The main panel can show multiple kinds of information about a table. In this case the **'Content'** of the database table is show.

If the connection fails, a message like the following will be displayed.



Access denied!

Unable to connect to host data.rython.com because access was denied.

Double-check your username and password and ensure that access from your current location is permitted.

MySQL said: Access denied for user 'splunk'@' (using password: YES)

Password: •••••••••

Database: jamfsoftware

Port: 3306

☑ Connect using SSL

Key File: ...ive/projects/certs/client-key.pem

Certificate: ...ve/projects/certs/client-cert.pem

CA Cert: ~/Archive/projects/certs/ca.pem

Connection failure can happen for many reasons. Some of them are:

- The username or password may be incorrect.
- The MySQL server may be down.
- The user's permissions may not allow a connection from the client system.
- The certificates may be invalid for the server system.

Using Spunk Enterprise

Splunk Enterprise needs some configuration and setup before it can connect to a MySQL database. By default it has no capability to use MySQL connections. It achieves these connections through a Splunk add-ons and JDBC libraries. This example uses Splunk Enterprise 6.5.2.

The base Splunk add-on for creating a variety of database connections is 'Spunk DB Connect'.

Splunk DB Connect add-on

Splunk Documentation: DB Connect add-on

A Spunk MySQL specific add-on is available, but it's primary purpose is accessing MySQL logs. Not general data pulls.

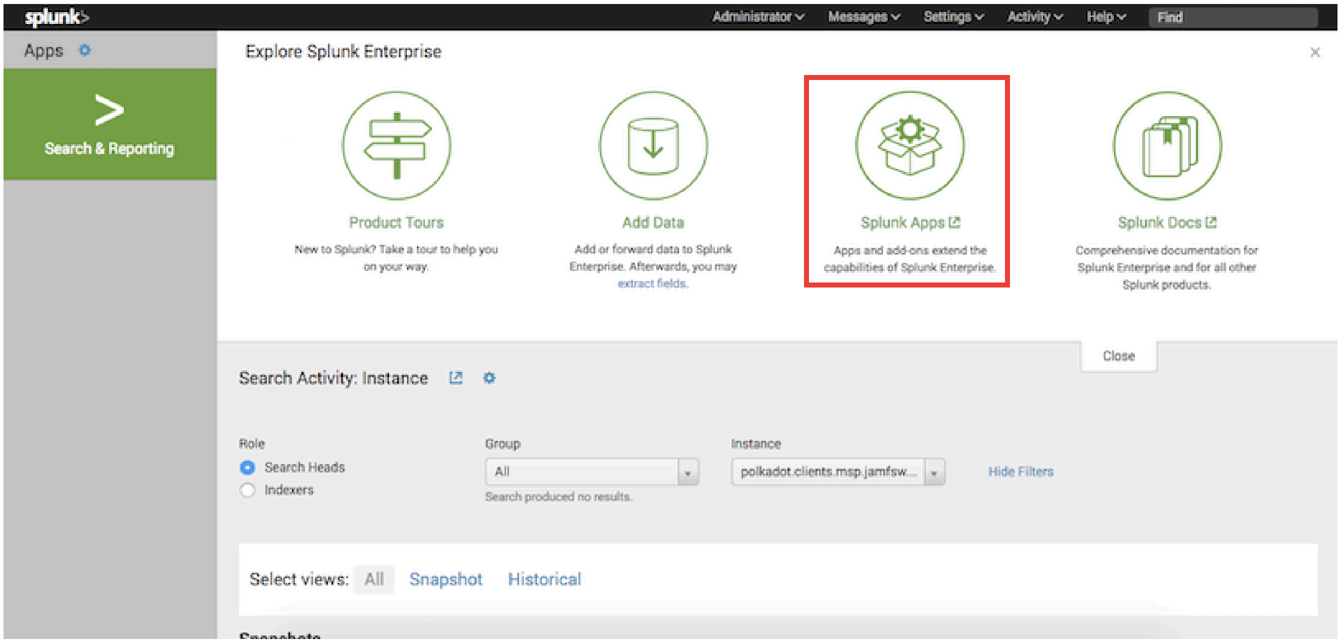
Splunk add-on for MySQL

Splunk Documentation : MySQL add-on

Set up DB add-on and JDBC library

First we need to install and setup the Spunk DB Connect add-on and the associate MySQL JDBC driver.

Download and install the 'Splunk DB Connect' add-on. Go to the 'Find More Apps' page in the apps section of Splunk Enterprise and search for 'mysql'.



Explore Splunk Enterprise

Product Tours: New to Splunk? Take a tour to help you on your way.

Add Data: Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Splunk Apps: Apps and add-ons extend the capabilities of Splunk Enterprise.

Splunk Docs: Comprehensive documentation for Splunk Enterprise and for all other Splunk products.

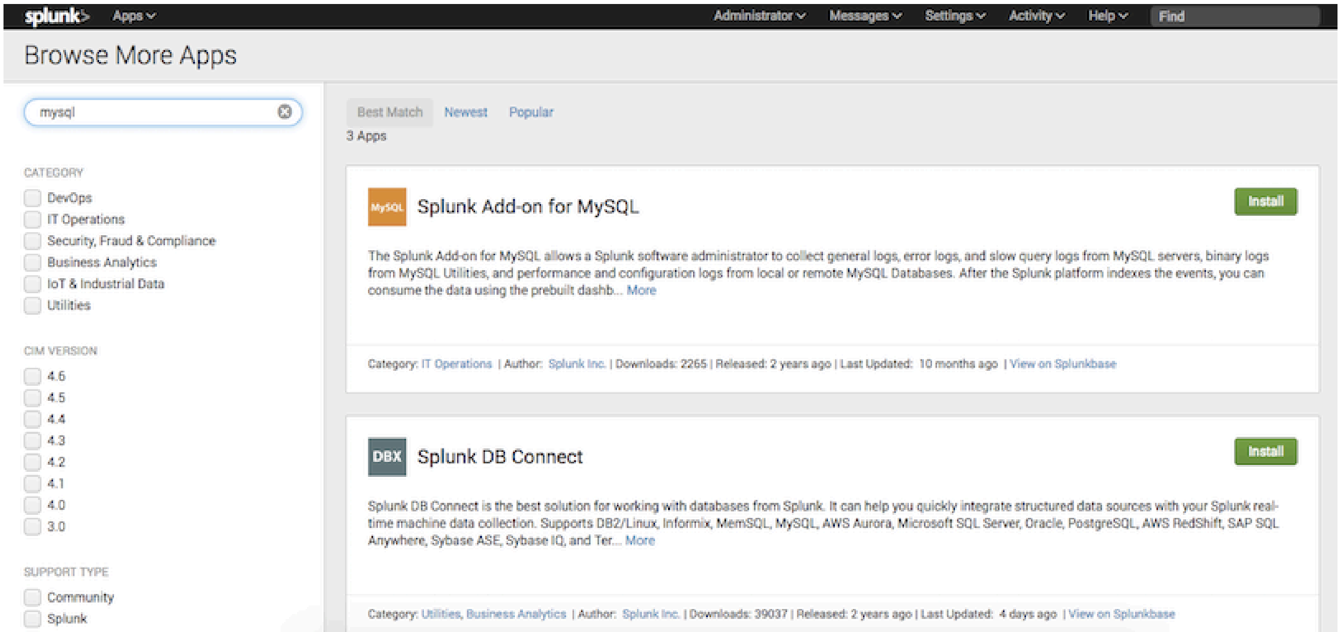
Search Activity: Instance

Role: ● Search Heads ○ Indexers

Group: All — Search produced no results.

Instance: polkadot.clients.msp.jamfsw...

Select views: All | Snapshot | Historical



Browse More Apps

Search: mysql

3 Apps

CATEGORY
- □ DevOps
- □ IT Operations
- □ Security, Fraud & Compliance
- □ Business Analytics
- □ IoT & Industrial Data
- □ Utilities

CIM VERSION
- □ 4.6
- □ 4.5
- □ 4.4
- □ 4.3
- □ 4.2
- □ 4.1
- □ 4.0
- □ 3.0

SUPPORT TYPE
- □ Community
- □ Splunk

Splunk Add-on for MySQL

The Splunk Add-on for MySQL allows a Splunk software administrator to collect general logs, error logs, and slow query logs from MySQL servers, binary logs from MySQL Utilities, and performance and configuration logs from local or remote MySQL Databases. After the Splunk platform indexes the events, you can consume the data using the prebuilt dashb... More

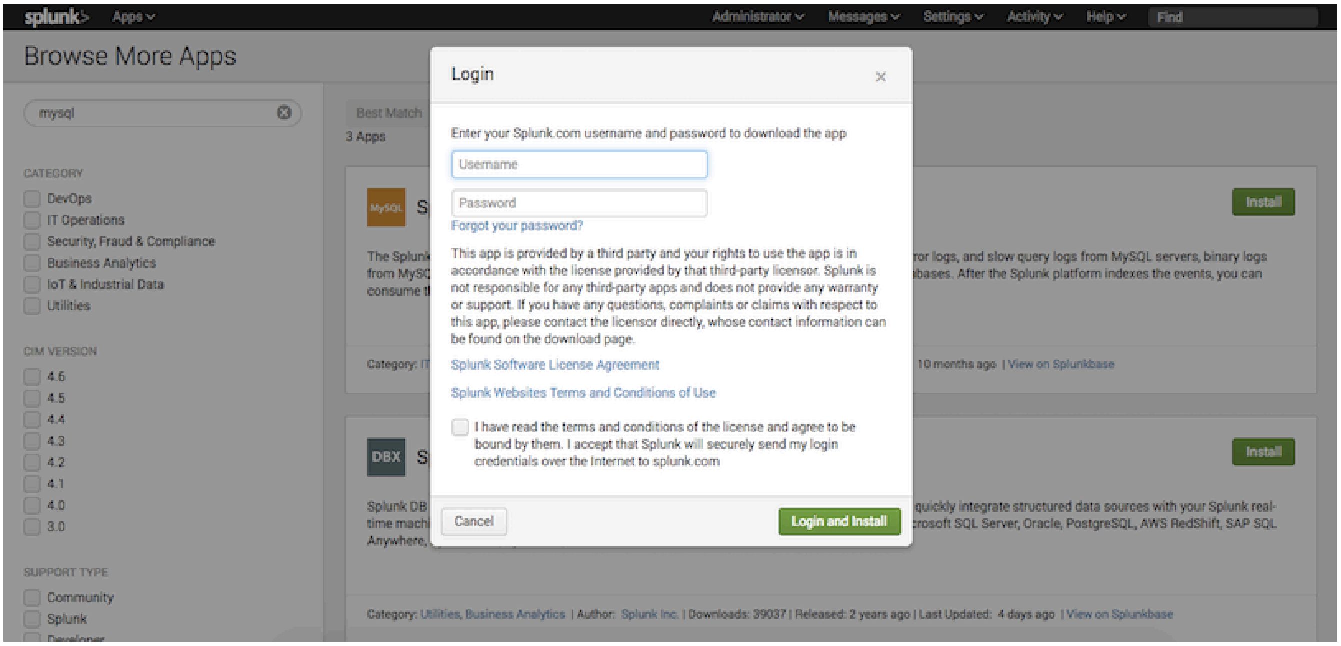
Category: IT Operations | Author: Splunk Inc. | Downloads: 2265 | Released: 2 years ago | Last Updated: 10 months ago | View on Splunkbase

Splunk DB Connect

Splunk DB Connect is the best solution for working with databases from Splunk. It can help you quickly integrate structured data sources with your Splunk real-time machine data collection. Supports DB2/Linux, Informix, MemSQL, MySQL, AWS Aurora, Microsoft SQL Server, Oracle, PostgreSQL, AWS RedShift, SAP SQL Anywhere, Sybase ASE, Sybase IQ, and Ter... More

Category: Utilities, Business Analytics | Author: Splunk Inc. | Downloads: 39037 | Released: 2 years ago | Last Updated: 4 days ago | View on Splunkbase

SplunkBase, a location for Splunk add-ons and apps, requires a login to download and install the 'DB Connect' add-on. Use your Splunk.com credentials here or create an an account. Once the add-on is installed, a restart of Spunk.



Login

Enter your Splunk.com username and password to download the app

Username

Password

Forgot your password?

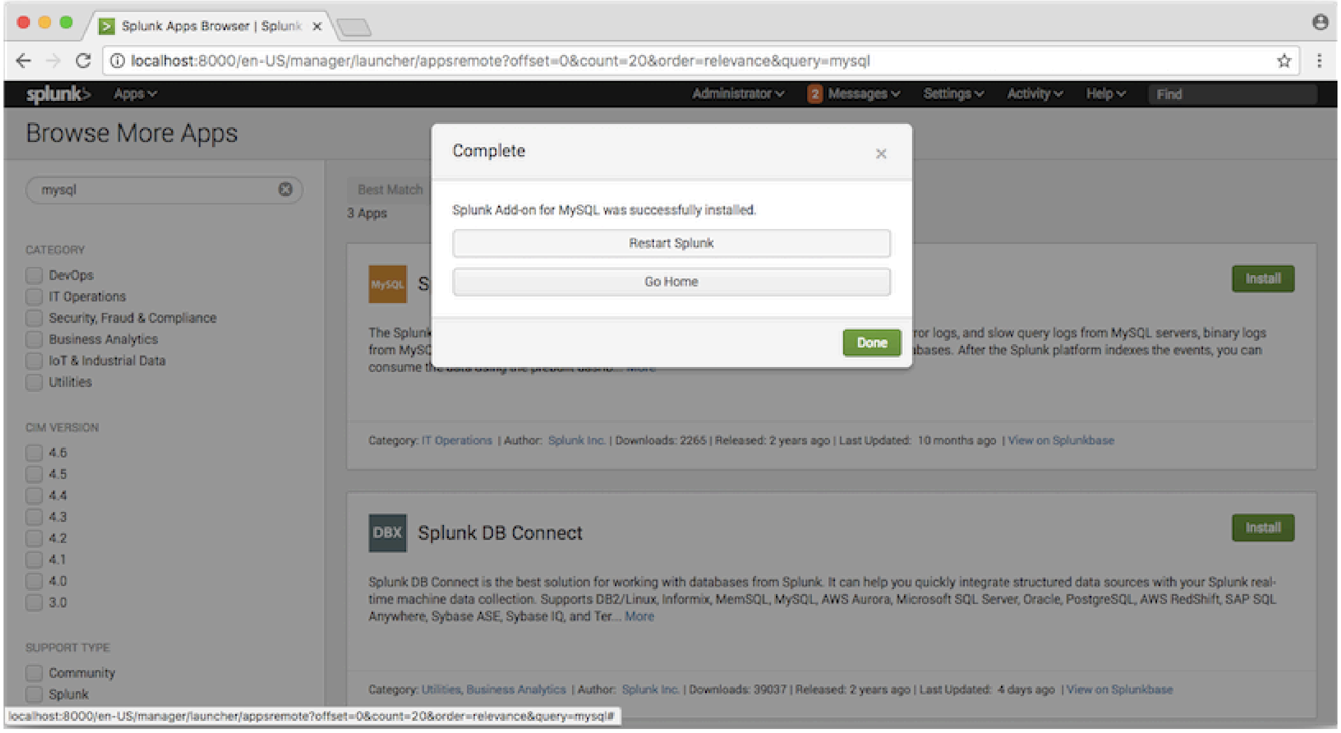
This app is provided by a third party and your rights to use the app is in accordance with the license provided by that third-party licensor. Splunk is not responsible for any third-party apps and does not provide any warranty or support. If you have any questions, complaints or claims with respect to this app, please contact the licensor directly, whose contact information can be found on the download page.

Splunk Software License Agreement

Splunk Websites Terms and Conditions of Use

□ I have read the terms and conditions of the license and agree to be bound by them. I accept that Splunk will securely send my login credentials over the Internet to splunk.com

Category: Utilities, Business Analytics | Author: Splunk Inc. | Downloads: 39037 | Released: 2 years ago | Last Updated: 4 days ago | View on Splunkbase


Splunk Apps Browser | Splunk
localhost:8000/en-US/manager/launcher/appsremote?offset=0&count=20&order=relevance&query=mysql
splunk> Apps
Administrator 2 Messages Settings Activity Help Find
Browse More Apps
mysql
CATEGORY
DevOps
IT Operations
Security, Fraud & Compliance
Business Analytics
IoT & Industrial Data
Utilities
CIM VERSION
4.6
4.5
4.4
4.3
4.2
4.1
4.0
3.0
SUPPORT TYPE
Community
Splunk
Best Match
3 Apps
Install
Install
Restart Splunk
Go Home
Done
localhost:8000/en-US/manager/launcher/appsremote?offset=0&count=20&order=relevance&query=mysql#

Complete

Splunk Add-on for MySQL was successfully installed.

Category: IT Operations | Author: Splunk Inc. | Downloads: 2265 | Released: 2 years ago | Last Updated: 10 months ago | View on Splunkbase

Splunk DB Connect

Splunk DB Connect is the best solution for working with databases from Splunk. It can help you quickly integrate structured data sources with your Splunk real-time machine data collection. Supports DB2/Linux, Informix, MemSQL, MySQL, AWS Aurora, Microsoft SQL Server, Oracle, PostgreSQL, AWS RedShift, SAP SQL Anywhere, Sybase ASE, Sybase IQ, and Ter... More

Category: Utilities, Business Analytics | Author: Splunk Inc. | Downloads: 39037 | Released: 2 years ago | Last Updated: 4 days ago | View on Splunkbase

One Splunk restarts, the JDBC driver for MySQL needs to be installed. The Splunk DB add-on uses Java and JDBC to manage database connections. If Java is not installed on the system Splunk Enterprise is running on, it will have to be installed.

Splunk Documentation : Database driver installation

Download the MySQL JDBC driver from MySQL.

MySQL JDBC driver

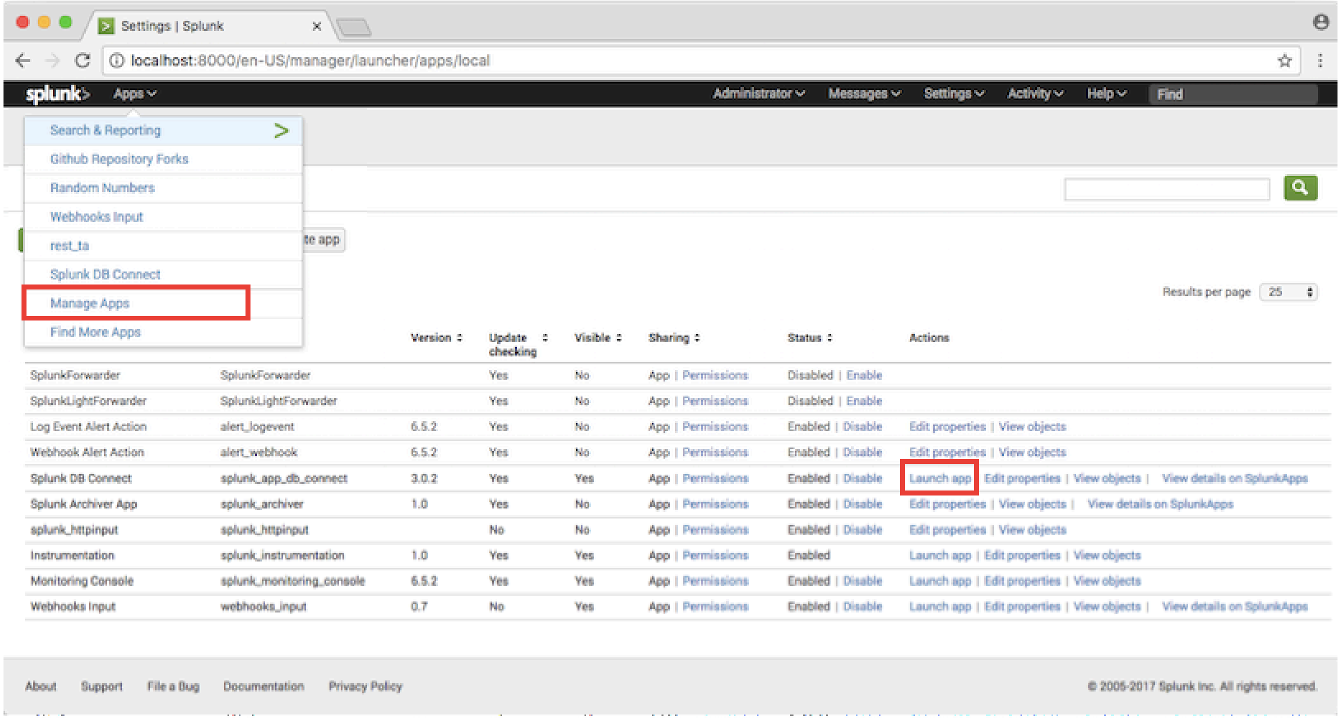
The driver is a jar and cross platform. After unarchiving the jar file, copy it to appropriate location in the Splunk application path. Later, when we are configuring the Splunk DB Connection app, we'll be able to verify the library is installed and functioning correctly.

```
> cp <mysql jdbc driver> <splunk
home>/etc/apps/splunk_app_db_connect/drivers/


ex.
(on macOS)
> cp mysql-connector-java-5.1.41-bin.jar
/Applications/Splunk/etc/apps/splunk_app_db_connect/drivers/


(on linux)
> cp mysql-connector-java-5.1.41-bin.jar
/opt/splunk/etc/apps/splunk_app_db_connect/drivers/
```

Configure the DB Connection add-on

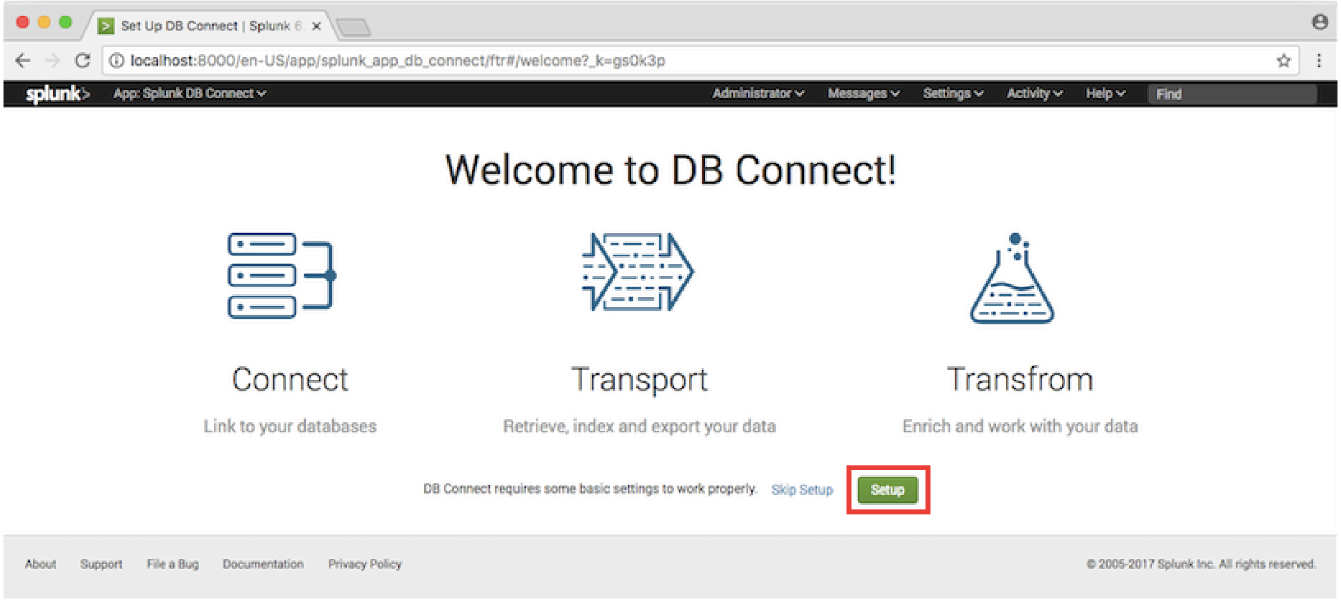
Now we can configure the Splunk DB Connection add-on.

The add-on can be seen and configured on the 'Manage Apps' screen. Select 'Launch App' from 'Spunk DB Connect' line. Or select 'Spunk DB Connect' from apps menu.



		Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App | Permissions	Disabled | Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App | Permissions	Disabled | Enable	
Log Event Alert Action	alert_logevent	6.5.2	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Webhook Alert Action	alert_webhook	6.5.2	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Splunk DB Connect	splunk_app_db_connect	3.0.2	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View objects | View details on SplunkApps
Splunk Archiver App	splunk_archiver	1.0	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects | View details on SplunkApps
splunk_httpinput	splunk_httpinput		No	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Instrumentation	splunk_instrumentation	1.0	Yes	Yes	App | Permissions	Enabled	Launch app | Edit properties | View objects
Monitoring Console	splunk_monitoring_console	6.5.2	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View objects
Webhooks Input	webhooks_input	0.7	No	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View objects | View details on SplunkApps

From the initial apps page, select setup. The location of the Java JRE and JVM options need to be set. We can also check on the status of the MySQL JDBC drivers.



Welcome to DB Connect!

Connect

Link to your databases

Transport

Retrieve, index and export your data

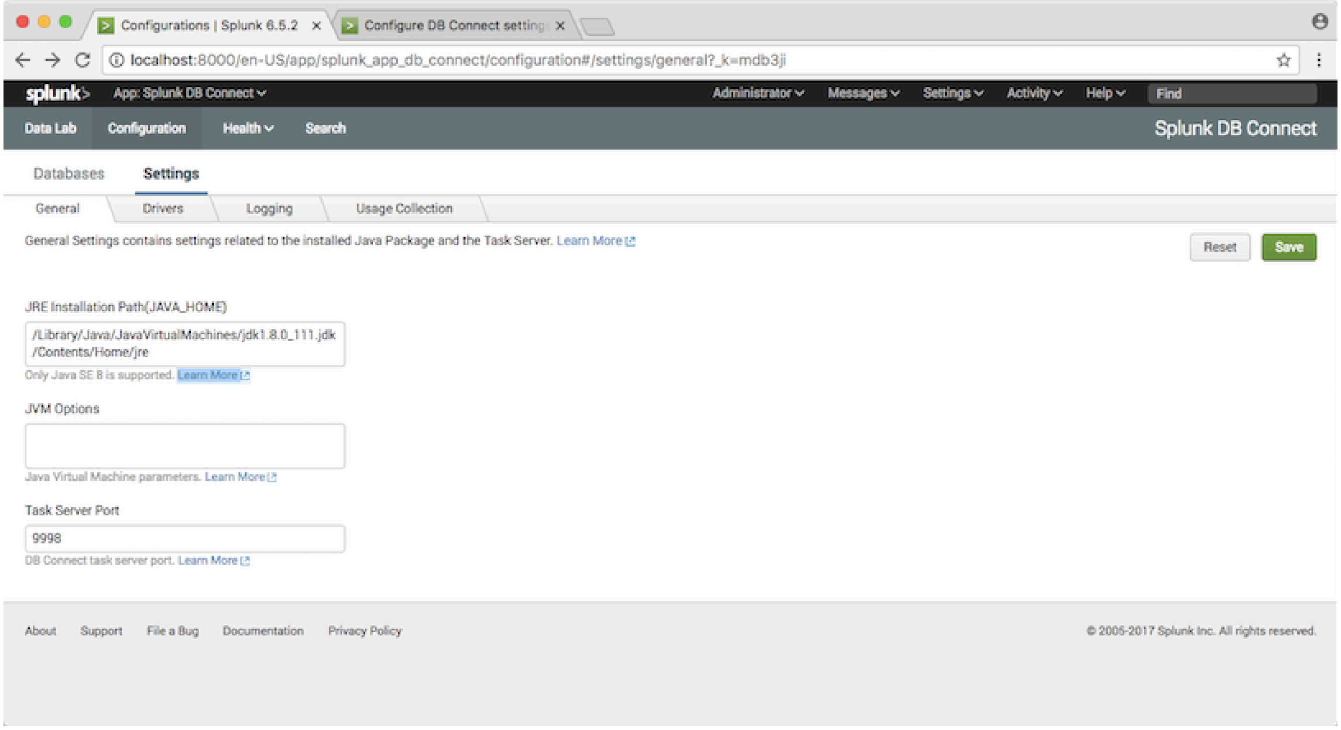
Transfrom

Enrich and work with your data

DB Connect requires some basic settings to work properly.

© 2005-2017 Splunk Inc. All rights reserved.

Select 'Settings:General' from 'Configuration'. Fill in the path of the JRE and any JVM options that will be used. If the JRE was installed when the DB Connection app was installed, the option '-Ddw.server.applicationConnector[0].port=9998' and the 'Task Server Port' should be filled in automatically by Splunk. Save the changes.



General Settings contains settings related to the installed Java Package and the Task Server. Learn More

JRE Installation Path(JAVA_HOME)

/Library/Java/JavaVirtualMachines/jdk1.8.0_111.jdk/Contents/Home/jre

Only Java SE 8 is supported. Learn More

JVM Options

Java Virtual Machine parameters. Learn More

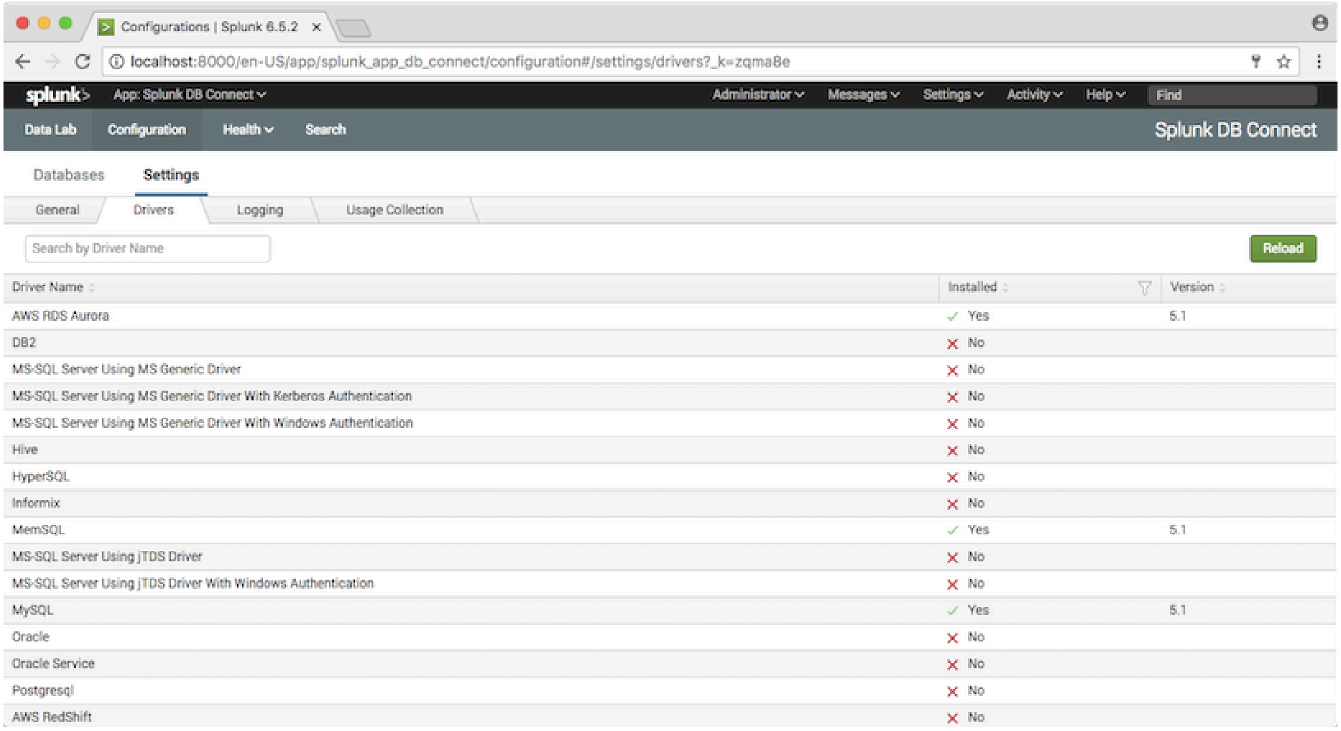
Task Server Port

9998

DB Connect task server port. Learn More

© 2005-2017 Splunk Inc. All rights reserved.

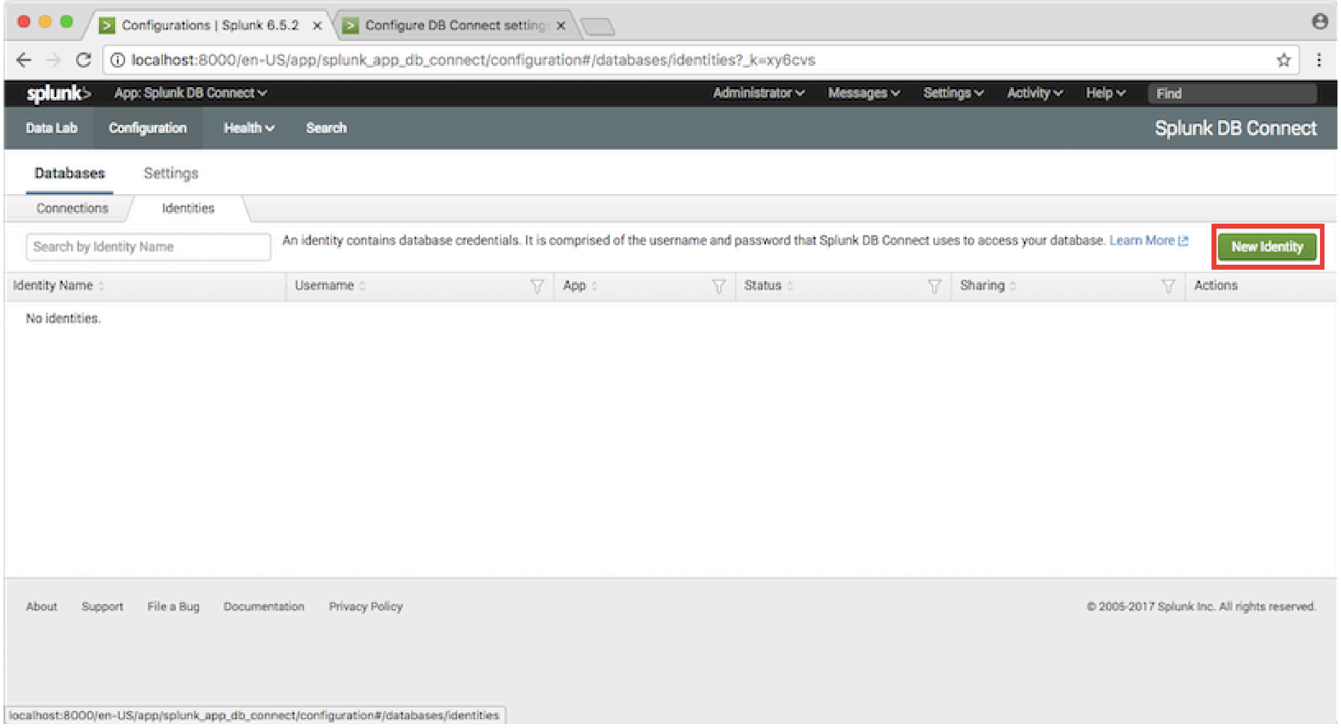
By selecting the 'Drivers' tab the status of the MySQL JDBC driver can be checked.



Driver Name	Installed	Version
AWS RDS Aurora	✓ Yes	5.1
DB2	✗ No	
MS-SQL Server Using MS Generic Driver	✗ No	
MS-SQL Server Using MS Generic Driver With Kerberos Authentication	✗ No	
MS-SQL Server Using MS Generic Driver With Windows Authentication	✗ No	
Hive	✗ No	
HyperSQL	✗ No	
Informix	✗ No	
MemSQL	✓ Yes	5.1
MS-SQL Server Using jTDS Driver	✗ No	
MS-SQL Server Using jTDS Driver With Windows Authentication	✗ No	
MySQL	✓ Yes	5.1
Oracle	✗ No	
Oracle Service	✗ No	
Postgresql	✗ No	
AWS RedShift	✗ No	

Create connection to JSS MySQL server

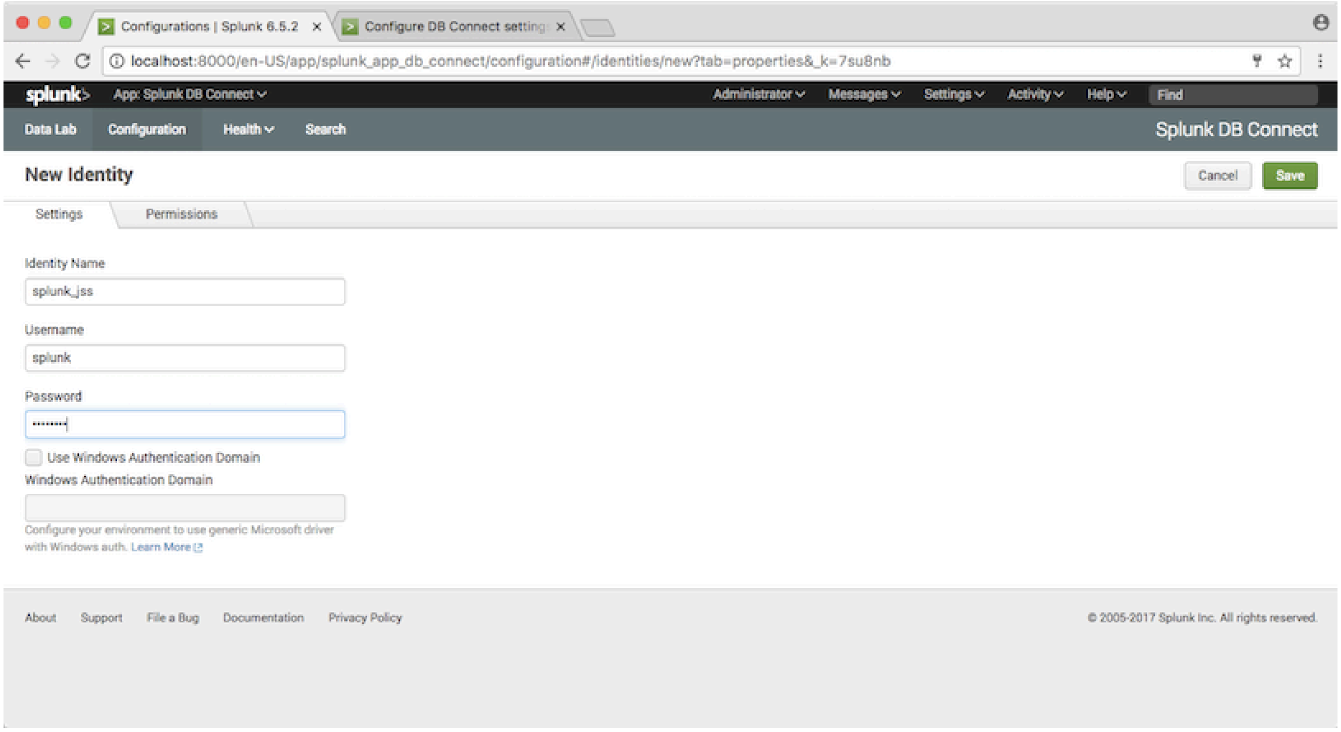
Now that all the drivers and support software is in place, a connection to a Jamf Pro MySQL server can be created.
First an 'identity' or login credentials need to be set up. This will be the credentials of the MySQL user set up earlier. Select 'Configuration:Settings:Identities' from the menu tabs and create a 'New Identity'.



An identity contains database credentials. It is comprised of the username and password that Splunk DB Connect uses to access your database. Learn More

No identities.

Fill in the username and password for the Splunk MySQL user and save. Default permissions should not need to be changed.


Configurations | Splunk 6.5.2
Configure DB Connect setting
localhost:8000/en-US/app/splunk_app_db_connect/configuration#/identities/new?tab=properties&_k=7su8nb
splunk>
App: Splunk DB Connect
Administrator
Messages
Settings
Activity
Help
Find
Data Lab
Configuration
Health
Search
Splunk DB Connect
Cancel
Save
Settings
Permissions
About
Support
File a Bug
Documentation
Privacy Policy
© 2005-2017 Splunk Inc. All rights reserved.

New Identity

Identity Name: splunk_jss

Username: splunk

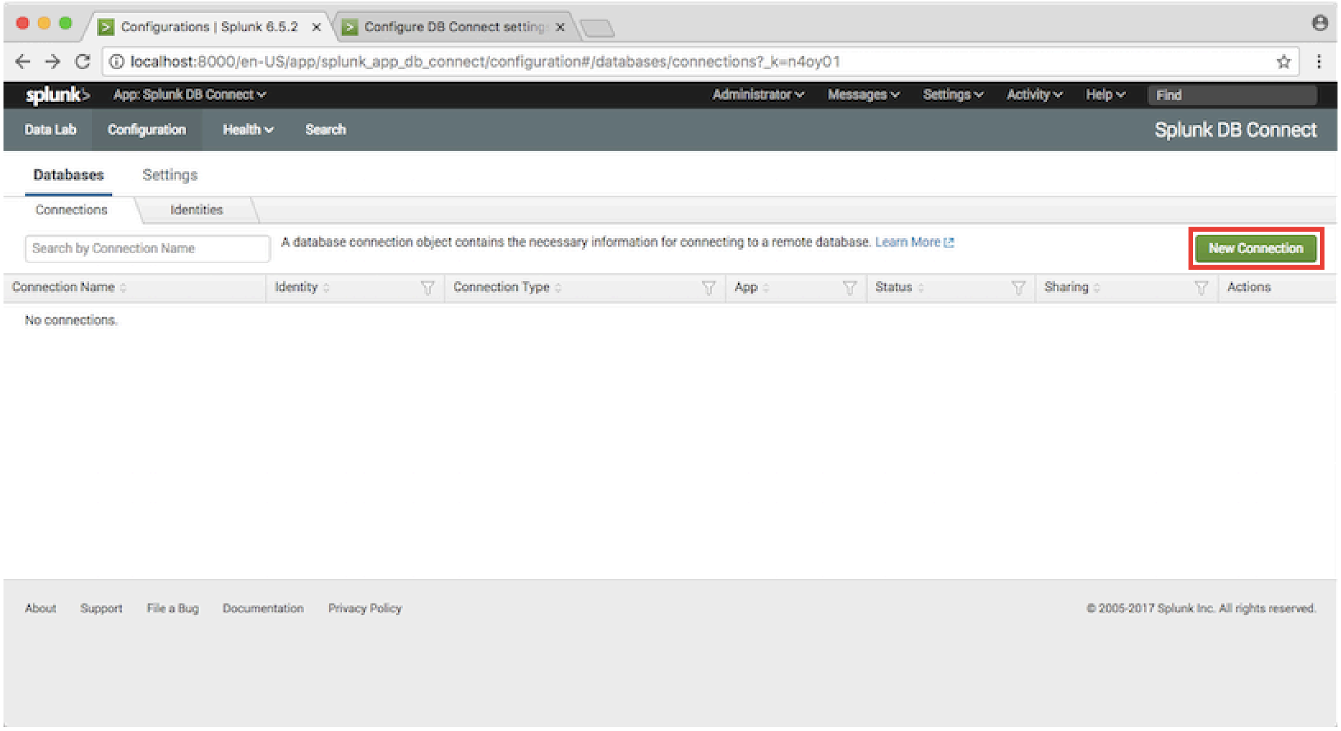
Password: ••••••••

☐ Use Windows Authentication Domain

Windows Authentication Domain:

Configure your environment to use generic Microsoft driver with Windows auth. Learn More

With the identity just creates, set up a new database connection to a Jamf Pro MySQL. First select 'Configuration:Databases:Connections' from the menu tabs. Then select 'New Connection'.

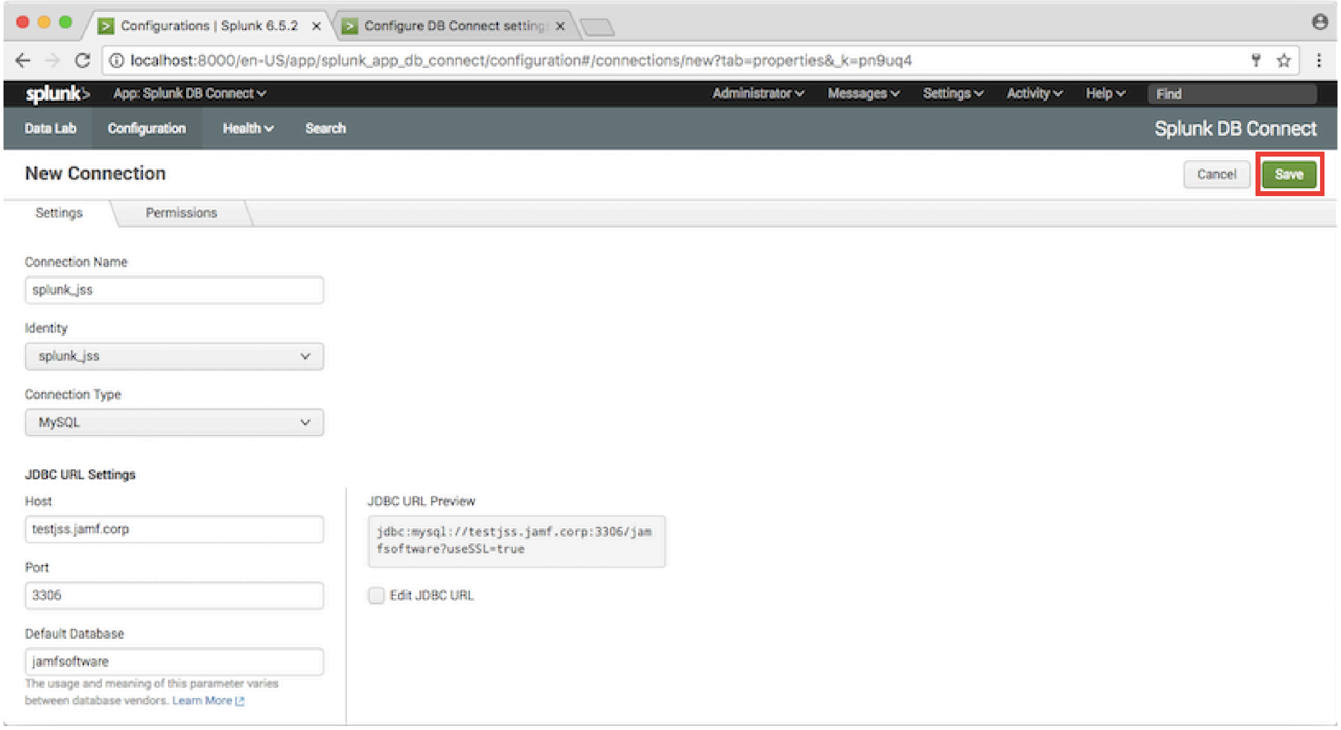


A database connection object contains the necessary information for connecting to a remote database. Learn More

Connection Name	Identity	Connection Type	App	Status	Sharing	Actions
No connections.						

Now fill in the fields with the values of the identity just created and the connection information to a Jamf Pro MySQL server. The JDBC connection string preview will be auto-populated as information is filled in. If SSL connections are being used, that option can be selected. 'Read Only' for the database should also be turned on. With Splunk we are only interested in aggregating data, not altering it.

Save the new connection when done.



Configurations | Splunk 6.5.2
Configure DB Connect setting
localhost:8000/en-US/app/splunk_app_db_connect/configuration#/connections/new?tab=properties&_k=pn9uq4
splunk>
App: Splunk DB Connect
Administrator
Messages
Settings
Activity
Help
Find
Data Lab
Configuration
Health
Search
Splunk DB Connect
Cancel
Save
Settings
Permissions

New Connection

Connection Name: splunk_jss

Identity: splunk_jss

Connection Type: MySQL

JDBC URL Settings

Host: testjss.jamf.corp

Port: 3306

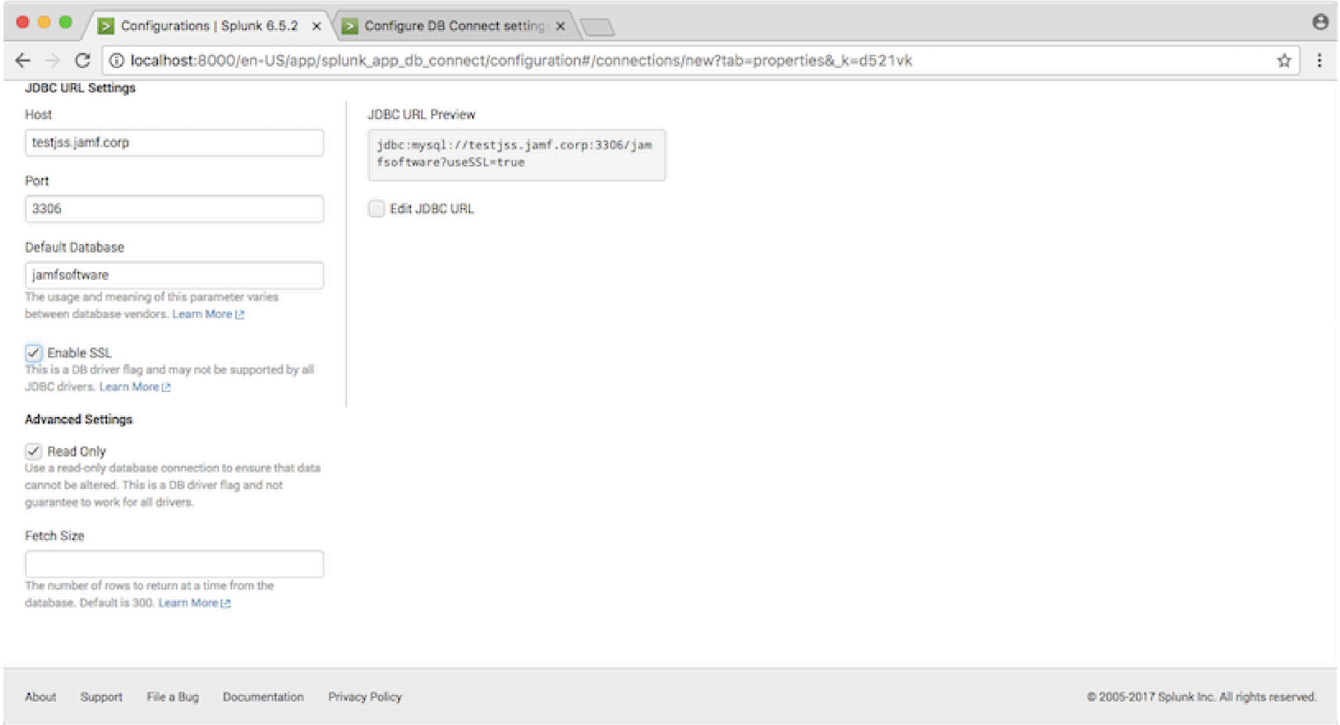
Default Database: jamfsoftware

The usage and meaning of this parameter varies between database vendors. Learn More

JDBC URL Preview

```
jdbc:mysql://testjss.jamf.corp:3306/jamfsoftware?useSSL=true
```

☐ Edit JDBC URL



Configurations | Splunk 6.5.2
Configure DB Connect setting
localhost:8000/en-US/app/splunk_app_db_connect/configuration#/connections/new?tab=properties&_k=d521vk
About
Support
File a Bug
Documentation
Privacy Policy
© 2005-2017 Splunk Inc. All rights reserved.

JDBC URL Settings

Host: testjss.jamf.corp

Port: 3306

Default Database: jamfsoftware

The usage and meaning of this parameter varies between database vendors. Learn More

☑ Enable SSL

This is a DB driver flag and may not be supported by all JDBC drivers. Learn More

Advanced Settings

☑ Read Only

Use a read-only database connection to ensure that data cannot be altered. This is a DB driver flag and not guarantee to work for all drivers.

Fetch Size:

The number of rows to return at a time from the database. Default is 300. Learn More

JDBC URL Preview

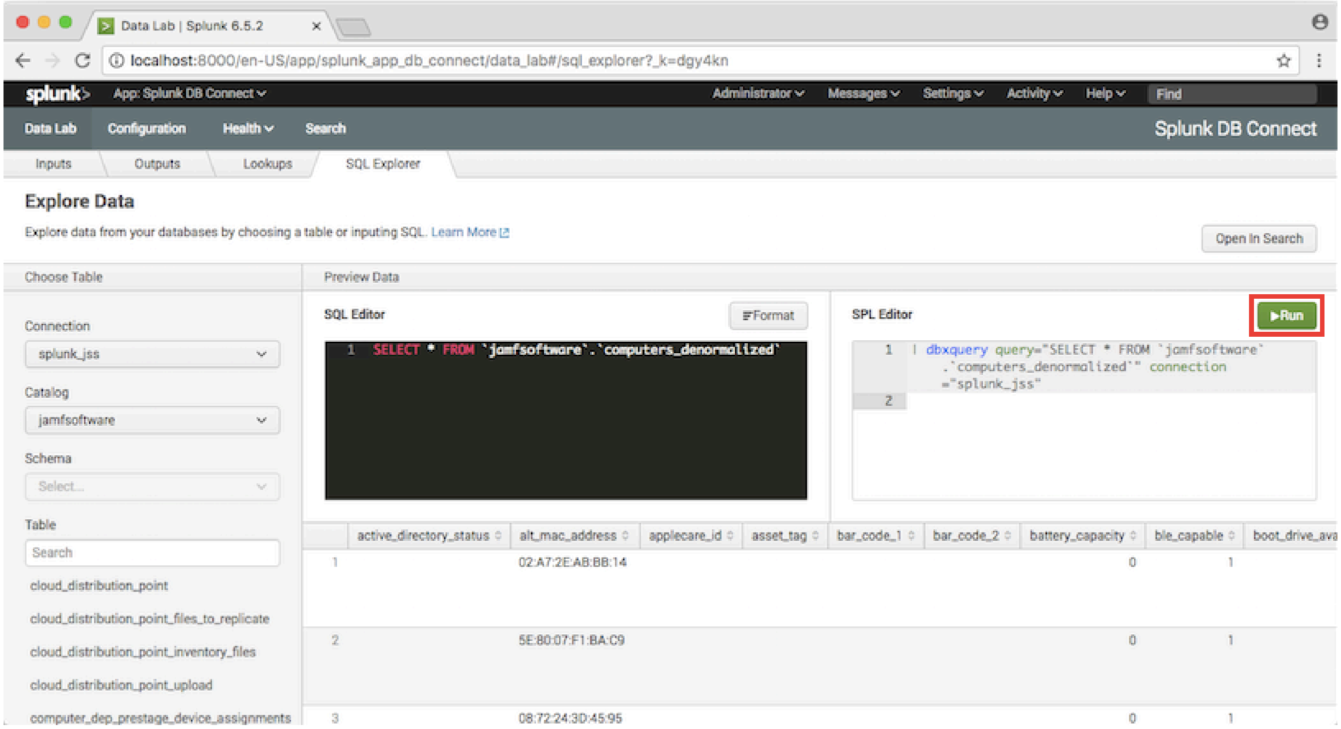
```
jdbc:mysql://testjss.jamf.corp:3306/jamfsoftware?useSSL=true
```

☐ Edit JDBC URL

Using the MySQL connection in Splunk

Splunk provides an SQL Explorer tool as a way of testing connections and possible data feeds.

Select 'Data Lab:SQL Explorer' from the menu tabs. The previously created 'splunk_jss' connection can be used, selecting catalogs (databases), tables, and specific SQL as appropriate. When a query is constructed, select 'Run'.



localhost:8000/en-US/app/splunk_app_db_connect/data_lab#/sql_explorer?_k=dgy4kn

Explore Data

Explore data from your databases by choosing a table or inputing SQL. Learn More

Choose Table

Connection: splunk_jss

Catalog: jamfsoftware

Schema: Select...

Table: Search

cloud_distribution_point

cloud_distribution_point_files_to_replicate

cloud_distribution_point_inventory_files

cloud_distribution_point_upload

computer_dep_prestage_device_assignments

Preview Data

SQL Editor

```
SELECT * FROM `jamfsoftware`.`computers_denormalized`
```

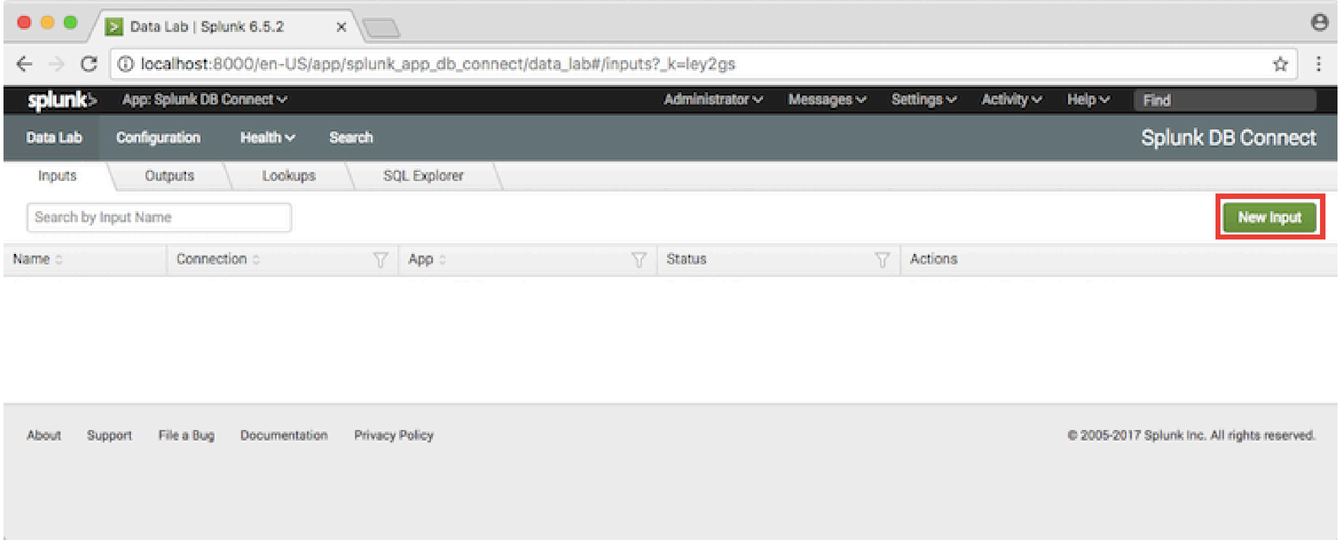
SPL Editor

```
| dbxquery query="SELECT * FROM `jamfsoftware`
    .`computers_denormalized`" connection
    ="splunk_jss"
```

	active_directory_status	alt_mac_address	applecare_id	asset_tag	bar_code_1	bar_code_2	battery_capacity	ble_capable	boot_drive_ava
1		02:A7:2E:AB:BB:14					0	1	
2		5E:80:07:F1:BA:C9					0	1	
3		08:72:24:3D:45:95					0	1	

The MySQL connection can also be used to create data inputs into Splunk. The data from these input can be searched, aggregated, visualized, or used any other way data can be used in Splunk. A Splunk input from a database connection is a four step process, though not all the steps will be filled out.

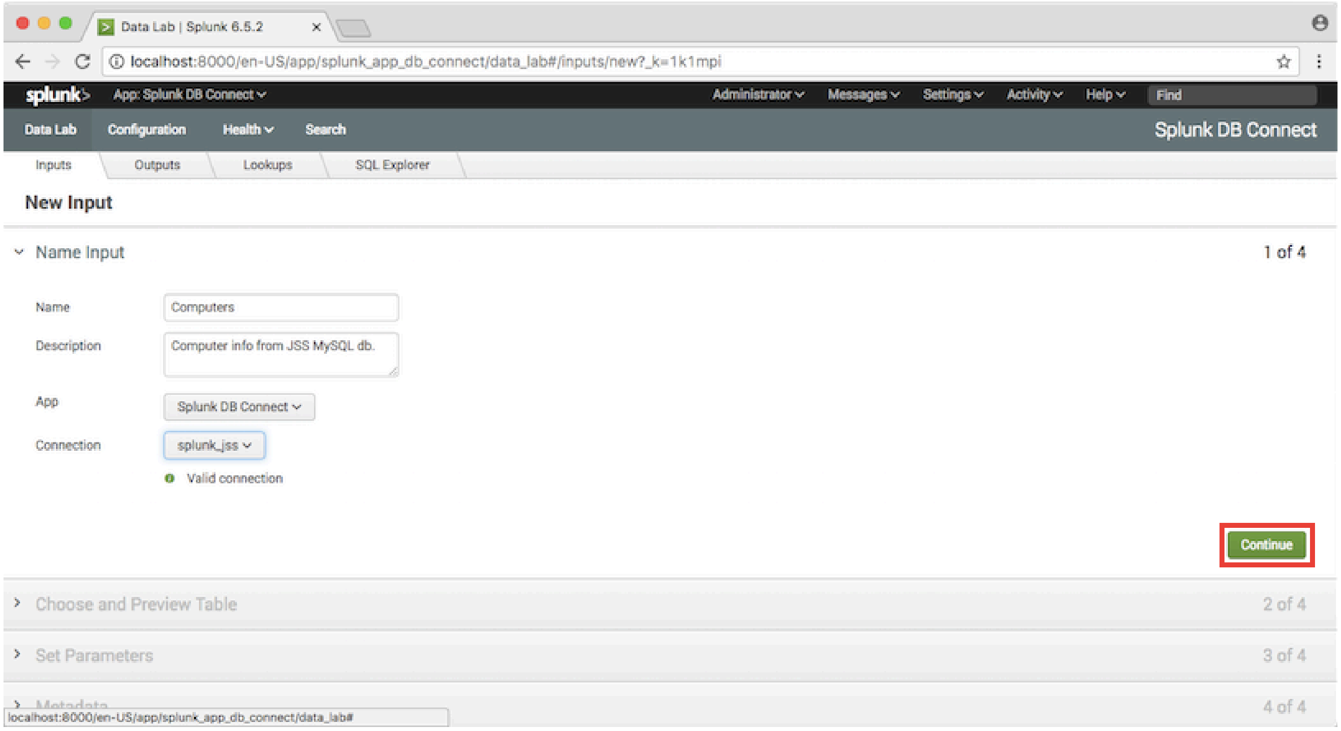
First select 'Data Lab:Inputs' from the menu tabs. Create a 'New Input'.



localhost:8000/en-US/app/splunk_app_db_connect/data_lab#/inputs?_k=ley2gs

Name	Connection	App	Status	Actions

The first step is to name the input, give it a short description, then select which app and database connection it uses. In this example the app is the 'Splunk DB Connect' add-on and the connection is the 'spunk_jss' connection created earlier. Once the information is filled out, select 'Continue'.



New Input

Name Input 1 of 4

Name: Computers

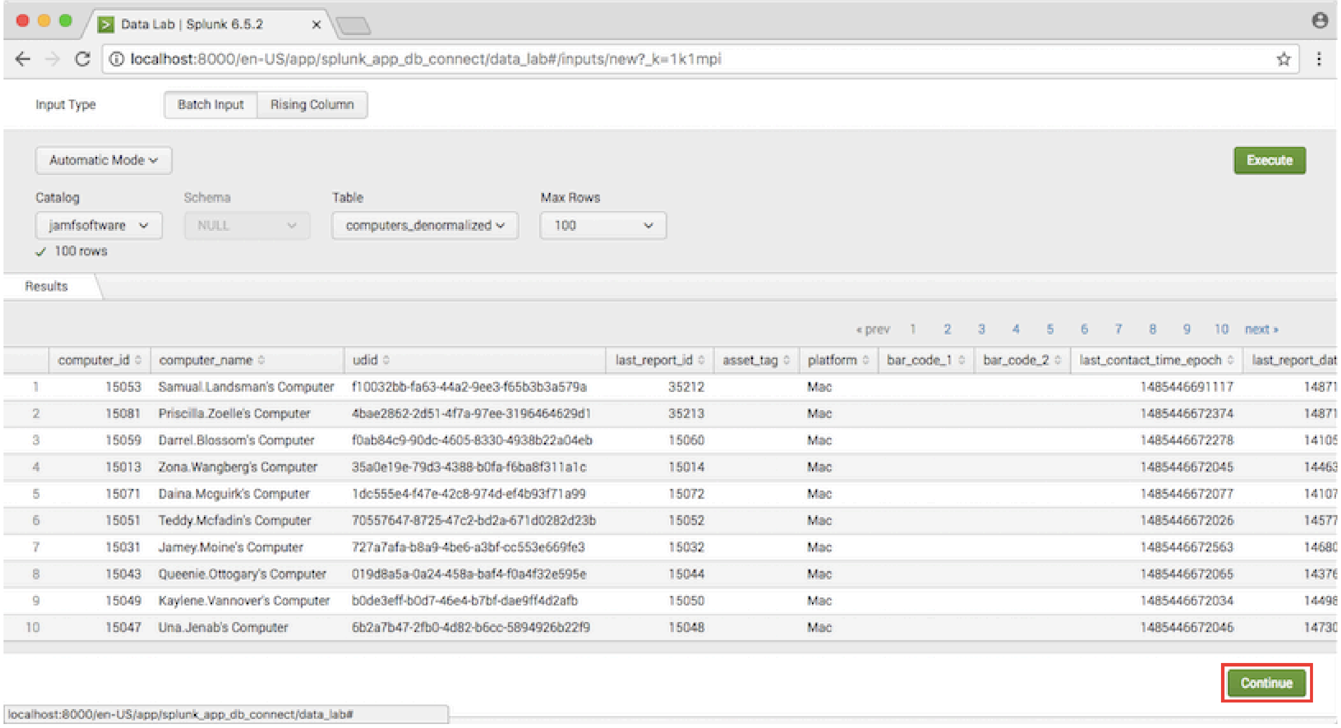
Description: Computer info from JSS MySQL db.

App: Splunk DB Connect

Connection: splunk_jss

Valid connection

In the second step, select which catalog (database) and table to use for the input feed. The lookup can be previewed before continuing.


Data Lab | Splunk 6.5.2
localhost:8000/en-US/app/splunk_app_db_connect/data_lab#/inputs/new?_k=1k1mpi
Execute
Results
« prev 1 2 3 4 5 6 7 8 9 10 next »
Continue
localhost:8000/en-US/app/splunk_app_db_connect/data_lab#

Input Type: Batch Input | Rising Column

Automatic Mode

Catalog: jamfsoftware

Schema: NULL

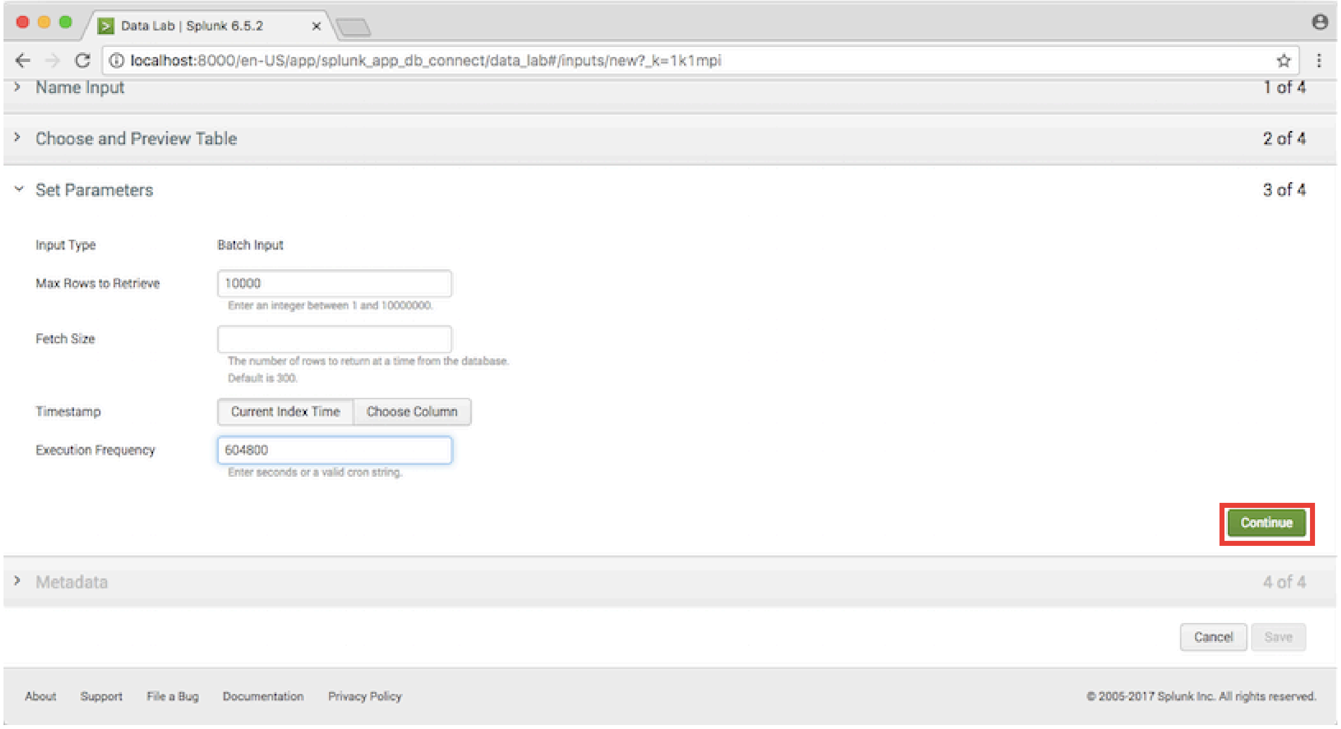
Table: computers_denormalized

Max Rows: 100

✓ 100 rows

	computer_id	computer_name	udid	last_report_id	asset_tag	platform	bar_code_1	bar_code_2	last_contact_time_epoch	last_report_dat
1	15053	Samual.Landsman's Computer	f10032bb-fa63-44a2-9ee3-f65b3b3a579a	35212		Mac			1485446691117	14871
2	15081	Priscilla.Zoelle's Computer	4bae2862-2d51-4f7a-97ee-3196464629d1	35213		Mac			1485446672374	14871
3	15059	Darrel.Blossom's Computer	f0ab84c9-90dc-4605-8330-4938b22a04eb	15060		Mac			1485446672278	14105
4	15013	Zona.Wangberg's Computer	35a0e19e-79d3-4388-b0fa-f6ba8f311a1c	15014		Mac			1485446672045	14463
5	15071	Daina.Mcguirk's Computer	1dc555e4-f47e-42c8-974d-ef4b93f71a99	15072		Mac			1485446672077	14107
6	15051	Teddy.Mcfadin's Computer	70557647-8725-47c2-bd2a-671d0282d23b	15052		Mac			1485446672026	14577
7	15031	Jamey.Moine's Computer	727a7afa-b8a9-4be6-a3bf-cc553e669fe3	15032		Mac			1485446672563	14680
8	15043	Queenie.Ottogary's Computer	019d8a5a-0a24-458a-baf4-f0a4f32e595e	15044		Mac			1485446672065	14376
9	15049	Kaylene.Vannover's Computer	b0de3eff-b0d7-46e4-b7bf-dae9ff4d2afb	15050		Mac			1485446672034	14498
10	15047	Una.Jenab's Computer	6b2a7b47-2fb0-4d82-b6cc-5894926b22f9	15048		Mac			1485446672046	14730

The third step configures some of the parameter data for the input. For example the maximum number of rows to pull at once and how often data is pulled from the database.



Input Type: Batch Input

Max Rows to Retrieve: 10000
Enter an integer between 1 and 10000000.

Fetch Size:
The number of rows to return at a time from the database. Default is 300.

Timestamp: Current Index Time | Choose Column

Execution Frequency: 604800
Enter seconds or a valid cron string.

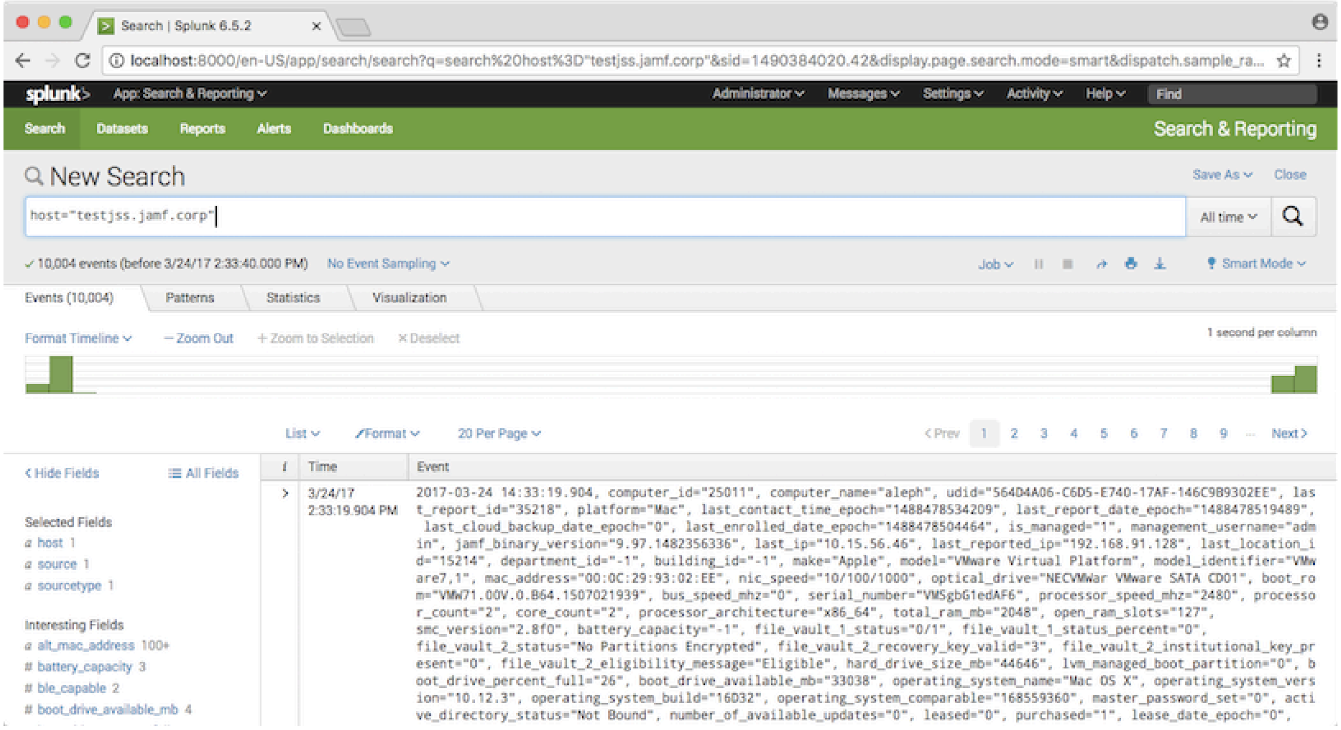
In the fourth step the host, source, sourcetype, and index can be specified. Each of these values help organize data coming in to Splunk and is used in searches. See the Spunk documentation for more detailed descriptions.

Splunk Documentation : Managing database inputs

Search Splunk Data

The database input will pull data from the Jamf Pro MySQL database on the interval used. This data can be searched and used in any way Splunk can use data.

For example, searching by the data 'host'.



```
host="testjss.jamf.corp"
```

✓ 10,004 events (before 3/24/17 2:33:40.000 PM)   No Event Sampling

i	Time	Event
>	3/24/17 2:33:19.904 PM	2017-03-24 14:33:19.904, computer_id="25011", computer_name="aleph", udid="564D4A06-C6D5-E740-17AF-146C9B9302EE", last_report_id="35218", platform="Mac", last_contact_time_epoch="1488478534209", last_report_date_epoch="1488478519489", last_cloud_backup_date_epoch="0", last_enrolled_date_epoch="1488478504464", is_managed="1", management_username="admin", jamf_binary_version="9.97.1482356336", last_ip="10.15.56.46", last_reported_ip="192.168.91.128", last_location_id="15214", department_id="-1", building_id="-1", make="Apple", model="VMware Virtual Platform", model_identifier="VMware7,1", mac_address="00:0C:29:93:02:EE", nic_speed="10/100/1000", optical_drive="NECVMWar VMware SATA CD01", boot_rom="VMW71.00V.0.B64.1507021939", bus_speed_mhz="0", serial_number="VMSgbG1edAF6", processor_speed_mhz="2480", processor_count="2", core_count="2", processor_architecture="x86_64", total_ram_mb="2048", open_ram_slots="127", smc_version="2.8f0", battery_capacity="-1", file_vault_1_status="0/1", file_vault_1_status_percent="0", file_vault_2_status="No Partitions Encrypted", file_vault_2_recovery_key_valid="3", file_vault_2_institutional_key_present="0", file_vault_2_eligibility_message="Eligible", hard_drive_size_mb="44646", lvm_managed_boot_partition="0", boot_drive_percent_full="26", boot_drive_available_mb="33038", operating_system_name="Mac OS X", operating_system_version="10.12.3", operating_system_build="16D32", operating_system_comparable="168559360", master_password_set="0", active_directory_status="Not Bound", number_of_available_updates="0", leased="0", purchased="1", lease_date_epoch="0",