Splunk® DB Connect Deploy and Use
Splunk DB Connect 3.1.4

Generated: 5/22/2019 7:00 pm
Table of Contents

**Introduction** ........................................................................................................... 1
   - About Splunk DB Connect............................................................................ 1
   - What DB Connect can do......................................................................... 1
   - Who DB Connect is for.............................................................................. 1
   - Share data in Splunk DB Connect............................................................. 2
   - How Splunk DB Connect collects data...................................................... 2
   - Data Splunk DB Connect collects.................................................................. 2
   - Data DB Connect does not collect.............................................................. 12
   - How Splunk DB Connect works.................................................................... 13
   - How this add-on fits into the Splunk picture............................................... 18
   - How to get help and learn more about Splunk software............................. 18

**Before you deploy** .................................................................................................... 20
   - Prerequisites........................................................................................... 20
   - System requirements.................................................................................. 20
   - User permissions...................................................................................... 21
   - Java Runtime Environment (JRE) requirements........................................ 21
   - Database and JDBC database driver requirements.................................... 22
   - Architecture and performance considerations........................................... 22
   - Performance considerations in distributed environments........................ 23
   - General performance tuning considerations............................................. 25

**Install Splunk DB Connect** ..................................................................................... 28
   - Installation and setup overview................................................................. 28
   - Deploy DB Connect to Splunk Cloud......................................................... 28
   - Upgrade an existing DB Connect deployment............................................. 29
   - Migrate DB Connect deployment to DB Connect 3..................................... 29
   - Install database drivers......................................................................... 35
   - Install and configure Splunk DB Connect on a single instance Splunk
     platform deployment..................................................................................... 53
   - Install and configure Splunk DB Connect on a distributed Splunk
     platform deployment.................................................................................... 55
   - Check DB Connect installation health......................................................... 59

**Configure and manage Splunk DB Connect** ............................................................. 62
   - Configure Splunk DB Connect settings....................................................... 62
   - Configure Splunk DB Connect security and access controls....................... 64
   - Create and manage identities................................................................... 67
   - Create and manage database connections............................................... 69
# Table of Contents

## Configure and manage Splunk DB Connect
- Create and manage database inputs.................................................................73
- Create and manage bulk operations of the database inputs..............................81
- Create and manage database outputs...............................................................85
- Create and manage database lookups...............................................................90
- Use SQL explorer to make live reports...........................................................96
- Execute SQL statements and stored procedures with the dbxquery command.................................................................100
- Monitor Splunk DB Connect health.................................................................106

## Reference
- Configuration file reference............................................................................109
- app-migration.conf.spec................................................................................110
- db_connection_types.conf.spec.......................................................................111
- db_connections.conf.spec..............................................................................113
- db_inputs.conf.spec......................................................................................118
- db_outputs.conf.spec....................................................................................121
- db_lookups.conf.spec....................................................................................124
- identities.conf.spec......................................................................................127
- inputs.conf.spec............................................................................................127
- dbx_settings.conf.spec..................................................................................128
- Saved searches for Splunk DB Connect.........................................................129
- Data models for Splunk DB Connect..............................................................129

## Troubleshooting
- Troubleshoot Splunk DB Connect...................................................................131
- SQL tips and tricks..........................................................................................142

## Terminology
- Splunk DB Connect terminology....................................................................146
Introduction

About Splunk DB Connect

Splunk DB Connect 3 enables you to combine your structured data from databases with your unstructured machine data, and then use Splunk Enterprise to provide insights into all of that combined data.

When you use Splunk DB Connect, you are creating additional data inputs for Splunk Enterprise. That is, you're giving Splunk Enterprise more sources of data to consume. Splunk DB Connect is what connects your relational database data to Splunk Enterprise and makes that data consumable by Splunk Enterprise. In addition, Splunk DB Connect can do the reverse—write Splunk Enterprise data back to your relational database.

For more information about how DB Connect works, see How Splunk DB Connect works.

What DB Connect can do

Splunk DB Connect allows you to import tables, rows, and columns from a database directly into Splunk Enterprise, which indexes the data. You can then analyze and visualize that relational data from within Splunk Enterprise just as you would the rest of your Splunk Enterprise data.

DB Connect also enables you to output data from Splunk Enterprise back to your relational database. You map the Splunk Enterprise fields to the database tables you want to write to.

DB Connect also performs database lookups, which let you reference fields in an external database that match fields in your event data. Using these matches, you can add more meaningful information and searchable fields to enrich your event data.

Who DB Connect is for

Splunk DB Connect is great for users who:

- Want to quickly get data from a database into Splunk Enterprise.
• Want to perform on-the-fly lookups from data warehouses or state tables within Splunk Enterprise.
• Want to index structured data stored in databases in streams or batches using Splunk Enterprise.
• Want to write Splunk Enterprise data into databases in streams or batches.
• Want to preview data and validate settings such as locale and time zone, rising column and metadata choice, and so on before indexing begins, to prevent accidental duplication or other problems later on.
• Want to scale, distribute, and monitor database read-write jobs to prevent overload and be notified of failure.
• Want to know what databases are accessible to which Splunk Enterprise users, to prevent unauthorized access.

Share data in Splunk DB Connect

Splunk DB Connect includes the opt-in ability to send anonymized usage data to Splunk to help improve the add-on in future releases.

How Splunk DB Connect collects data

If you opt in, the add-on enables an internal library to track basic usage and crash information. The library uses browser cookies to track add-on user visitor uniqueness and sessions and sends events to Splunk using XMLHttpRequest (XHR) in JSON format.

Data Splunk DB Connect collects

If you opt in, Splunk DB Connect sends the following information to Splunk:

• The number of identities you defined on the Splunk platform instance.
• The number of connections you defined on the instance.
• The number of connections associated with each identity on the instance.
• Each connection's database type, whether SSL is enabled, and the connection's associated number of database inputs, outputs, and lookups.
• The number of databases inputs defined on the instance.
• Each input's type (batch mode or rising column).
• The number of database outputs you defined on the instance.
• The number of database lookups you defined on the instance.
• Whether you enabled search head clustering.
• Each search head's search head cluster mode.
The daily license usage for each source type that DB Connect defines. DB Connect uses to send daily license usage. You can disable the saved search without harming DB Connect operations.

- The Splunk Enterprise license size.
- The name and version number of every JDBC driver you installed.
- The server roles you defined (provided by the server-roles attribute of the /services/server/info endpoint).

<table>
<thead>
<tr>
<th>Event</th>
<th>Source Type</th>
<th>Description</th>
<th>Data sent includes common fields, plus</th>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session start</td>
<td>mint:ping</td>
<td>Each ping event indicates that a new session has started.</td>
<td>fsEncrypted</td>
<td>N/A</td>
<td>Not used, always “NA”</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>rooted</td>
<td>N/A</td>
<td>Not used, always false</td>
<td></td>
</tr>
<tr>
<td>Session end</td>
<td>mint:gnip</td>
<td>Each gnip event indicates that a session has ended.</td>
<td>ses_duration</td>
<td>int</td>
<td>How long the session lasted</td>
<td></td>
</tr>
<tr>
<td>Page views</td>
<td>mint:view</td>
<td>Triggered once per page view in the app.</td>
<td>current</td>
<td>string</td>
<td>The URL of the current web page, without the hostname.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>currentView</td>
<td>string</td>
<td>Not used. Hardcoded to 'examples'.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>domProcessingTime</td>
<td>int</td>
<td>Time spent to process the domain.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>domLookupTime</td>
<td>int</td>
<td>Time spent to look up the domain name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>elapsedTime</td>
<td>int</td>
<td>Time spent to render the page.</td>
<td></td>
</tr>
<tr>
<td>Event</td>
<td>Source Type</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App</td>
<td>mint:log</td>
<td>Usage and performance logs for the DB Connect that track dashboard memory</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>usage, dashboard loading times, the number of accounts, inputs, and regions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>API calls</td>
<td>mint:network</td>
<td>Configured API calls, usually HTTP API calls from the client side to the</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>app, and configuration (e.g., network (browser) to the Splunk server.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data sent includes common fields, plus</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>host</td>
</tr>
<tr>
<td>loadTime</td>
</tr>
<tr>
<td>previous</td>
</tr>
<tr>
<td>serverTime</td>
</tr>
<tr>
<td>level</td>
</tr>
<tr>
<td>log_name</td>
</tr>
<tr>
<td>failed</td>
</tr>
<tr>
<td>latency</td>
</tr>
<tr>
<td>protocol</td>
</tr>
<tr>
<td>requestLength</td>
</tr>
<tr>
<td>responseLength</td>
</tr>
</tbody>
</table>
Data sent includes common fields, plus

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
<th>Example value</th>
</tr>
</thead>
<tbody>
<tr>
<td>statusCode</td>
<td>string</td>
<td>HTTP response code.</td>
<td></td>
</tr>
<tr>
<td>url</td>
<td>string</td>
<td>The request URL, without the hostname.</td>
<td></td>
</tr>
</tbody>
</table>

**Common fields**

The data that the DB Connect sends to Splunk, if enabled, includes the following common fields. This set of fields includes several fields that are disabled or deliberately not used for the DB Connect for purposes of anonymization.

<table>
<thead>
<tr>
<th>Event</th>
<th>Source Type</th>
<th>Description</th>
<th>Example value</th>
</tr>
</thead>
<tbody>
<tr>
<td>apiKey</td>
<td>string</td>
<td>MINT API key for the DB Connect</td>
<td>4t2fk73n</td>
</tr>
<tr>
<td>appRunningState</td>
<td>Field is unused by the SDK. Shows a value of &quot;NA&quot; in all events.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>appVersionCode</td>
<td>Field is unused by the SDK. Shows a value of &quot;NA&quot; in all events.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>appVersionName</td>
<td>string</td>
<td>The version name of the app sending data.</td>
<td>4.1.0</td>
</tr>
<tr>
<td>browser</td>
<td>string</td>
<td>The browser name.</td>
<td>Chrome</td>
</tr>
<tr>
<td>browserVersion</td>
<td>string</td>
<td>The browser version.</td>
<td>47.0.2526.111</td>
</tr>
<tr>
<td>carrier</td>
<td>Field is unused by the SDK. Shows a value of &quot;NA&quot; in all events.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>connection</td>
<td>Field is unused by the SDK. Shows a value of &quot;NA&quot; in all events.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>device</td>
<td>string</td>
<td>The device making the request.</td>
<td>MacIntel</td>
</tr>
<tr>
<td>extraData</td>
<td>JSON object</td>
<td>This field stores custom information for the app.</td>
<td>6.3.1511</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This app uses extraData.splunk_version to store the version number of the Splunk platform instance.</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Type</td>
<td>Description</td>
<td>Example value</td>
</tr>
<tr>
<td>------------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>locale</td>
<td>string</td>
<td>The user locale set in the browser.</td>
<td>en-US</td>
</tr>
<tr>
<td>osVersion</td>
<td>string</td>
<td>The version code of the underlying operating system.</td>
<td>OS X 10.11.2</td>
</tr>
<tr>
<td>packageName</td>
<td>string</td>
<td>The package name of the DB Connect.</td>
<td>splunk_app_db_connect</td>
</tr>
<tr>
<td>platform</td>
<td></td>
<td>Not used for the DB Connect. Shows a value of &quot;web&quot; in all events.</td>
<td></td>
</tr>
<tr>
<td>remoteIP</td>
<td></td>
<td>Not used for the DB Connect. Shows a value of &quot;3.0.0.0&quot; in all events.</td>
<td></td>
</tr>
<tr>
<td>sdkVersion</td>
<td>string</td>
<td>The version of the SDK.</td>
<td>4.3</td>
</tr>
<tr>
<td>screenOrientation</td>
<td></td>
<td>Field is unused by the SDK. Shows a value of &quot;NA&quot; in all events.</td>
<td></td>
</tr>
<tr>
<td>session_id</td>
<td>string</td>
<td>A unique string to identify a session.</td>
<td>a5026251</td>
</tr>
<tr>
<td>state</td>
<td>string</td>
<td>Indicator of whether the browser is online or not. Can be either CONNECTED or DISCONNECTED.</td>
<td>CONNECTED</td>
</tr>
<tr>
<td>uuid</td>
<td>UUID</td>
<td>A random identifier to track the user's uniqueness</td>
<td>837227ea-4569-4675-9a17-ccb39ca6950a</td>
</tr>
</tbody>
</table>

### Example app performance and configuration events

DB Connect sends performance and configuration information using the `log_name` field in the `mint:log` source type. This `log_name` field contains two sub-fields, `name`, which indicates which type of logs are being transmitted, and `data`, the content of the tracking log.

There are three possible options for `name`:

- **track_performance**. When a user accesses a dashboard in the app, DB Connect sends performance logs for dashboard memory usage and loading times.
- **track_configuration**. When a Splunk admin visits the Configure page, DB Connect sends a log of the number of accounts, inputs, and regions configured in the app, and non-sensitive input configuration parameters.
- **track_usage**. When a Splunk admin visits the Configure page, DB Connect sends a log of the data volume that each input is responsible for.
The following examples demonstrate what data the DB Connect sends for each type of event.

<table>
<thead>
<tr>
<th>log_name.name</th>
<th>Example JSON object</th>
</tr>
</thead>
</table>
| track_performance | ```
{
    "memory":{
        "totalJSHeapSize":72200000,
        "usedJSHeapSize":39600000,
        "jsHeapSizeLimit":1620000000
    },
    "timing":{
        "navigationStart":1453273923766,
        "unloadEventStart":1453273923929,
        "unloadEventEnd":1453273923930,
        "redirectStart":0,
        "redirectEnd":0,
        "fetchStart":1453273923766,
        "domainLookupStart":1453273923766,
        "domainLookupEnd":1453273923766,
        "connectStart":1453273923766,
        "connectEnd":1453273923766,
        "secureConnectionStart":0,
        "requestStart":1453273923773,
        "responseStart":1453273923927,
        "responseEnd":1453273923929,
        "domLoading":1453273923939,
        "domInteractive":1453273923975,
        "domContentLoadedEventStart":1453273923975,
        "domContentLoadedEventEnd":1453273923975,
        "domComplete":1453273926985,
        "loadEventStart":1453273926985,
        "loadEventEnd":1453273926987
    }
}
``` |
| track_configuration | ```
{
    "identities": {
        "count": 7,
        "data": [
            
            "connections_count": 1
        ],
        "connections_count": 1
    },
    "connections_count": 0
}
``` |
<table>
<thead>
<tr>
<th>log_name.name</th>
<th>Example JSON object</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>log_name.name</td>
<td>Example JSON object</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>&quot;mssql_jtds_win_auth&quot;,</td>
<td>&quot;connection_type&quot;:</td>
</tr>
<tr>
<td></td>
<td>&quot;jdbcUseSSL&quot;: false,</td>
</tr>
<tr>
<td></td>
<td>&quot;inputs_count&quot;: 0,</td>
</tr>
<tr>
<td></td>
<td>&quot;outputs_count&quot;: 0,</td>
</tr>
<tr>
<td></td>
<td>&quot;lookups_count&quot;: 0</td>
</tr>
<tr>
<td>&quot;mysql&quot;,</td>
<td>&quot;connection_type&quot;:</td>
</tr>
<tr>
<td></td>
<td>&quot;jdbcUseSSL&quot;: false,</td>
</tr>
<tr>
<td></td>
<td>&quot;inputs_count&quot;: 4,</td>
</tr>
<tr>
<td></td>
<td>&quot;outputs_count&quot;: 2,</td>
</tr>
<tr>
<td></td>
<td>&quot;lookups_count&quot;: 3</td>
</tr>
<tr>
<td>&quot;mysql&quot;,</td>
<td>&quot;connection_type&quot;:</td>
</tr>
<tr>
<td></td>
<td>&quot;jdbcUseSSL&quot;: false,</td>
</tr>
<tr>
<td></td>
<td>&quot;inputs_count&quot;: 0,</td>
</tr>
<tr>
<td></td>
<td>&quot;outputs_count&quot;: 0,</td>
</tr>
<tr>
<td></td>
<td>&quot;lookups_count&quot;: 0</td>
</tr>
<tr>
<td>&quot;mysql&quot;,</td>
<td>&quot;connection_type&quot;:</td>
</tr>
<tr>
<td></td>
<td>&quot;jdbcUseSSL&quot;: false,</td>
</tr>
<tr>
<td></td>
<td>&quot;inputs_count&quot;: 0,</td>
</tr>
<tr>
<td></td>
<td>&quot;outputs_count&quot;: 0,</td>
</tr>
<tr>
<td></td>
<td>&quot;lookups_count&quot;: 0</td>
</tr>
<tr>
<td>&quot;mysql&quot;,</td>
<td>&quot;connection_type&quot;:</td>
</tr>
<tr>
<td></td>
<td>&quot;jdbcUseSSL&quot;: false,</td>
</tr>
<tr>
<td></td>
<td>&quot;inputs_count&quot;: 0,</td>
</tr>
<tr>
<td></td>
<td>&quot;outputs_count&quot;: 0,</td>
</tr>
<tr>
<td></td>
<td>&quot;lookups_count&quot;: 0</td>
</tr>
<tr>
<td>&quot;oracle&quot;,</td>
<td>&quot;connection_type&quot;:</td>
</tr>
<tr>
<td></td>
<td>&quot;jdbcUseSSL&quot;: false,</td>
</tr>
<tr>
<td></td>
<td>&quot;inputs_count&quot;: 0,</td>
</tr>
<tr>
<td></td>
<td>&quot;outputs_count&quot;: 1,</td>
</tr>
<tr>
<td></td>
<td>&quot;lookups_count&quot;: 1</td>
</tr>
<tr>
<td></td>
<td>&quot;connection_type&quot;:</td>
</tr>
<tr>
<td>log_name.name</td>
<td>Example JSON object</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>&quot;oracle&quot;,</td>
<td>&quot;jdbcUseSSL&quot;: true,</td>
</tr>
<tr>
<td></td>
<td>&quot;inputs_count&quot;: 0,</td>
</tr>
<tr>
<td></td>
<td>&quot;outputs_count&quot;: 0,</td>
</tr>
<tr>
<td></td>
<td>&quot;lookups_count&quot;: 0</td>
</tr>
<tr>
<td>&quot;postgres&quot;,</td>
<td>&quot;jdbcUseSSL&quot;: false,</td>
</tr>
<tr>
<td></td>
<td>&quot;inputs_count&quot;: 0,</td>
</tr>
<tr>
<td></td>
<td>&quot;outputs_count&quot;: 0,</td>
</tr>
<tr>
<td></td>
<td>&quot;lookups_count&quot;: 0</td>
</tr>
</tbody>
</table>


Example JSON object

```
"transactional": true,
"is_saved_search": false
```

```
"lookups": {
  "count": 4,
  "data": [
    "input_fields_count": 0,
    "output_fields_count": 0,
    "input_fields_count": 0,
    "output_fields_count": 0,
    "input_fields_count": 0,
    "output_fields_count": 0,
    "input_fields_count": 0,
    "output_fields_count": 0
  ]
},
"serverstatus": {
  "count": 1,
  "data": [
    "isSHCluster": false,
    "javaVersion": "1.8.0_92"
  ]
}
```

```
track_usage
{
  "usage": [
    {
      "time": "2017-06-21",
      "volumes": {
        "sakila_city_rising_input": "0"
      }
    },
    {
      "time": "2017-06-22",
      "volumes": {
```
<table>
<thead>
<tr>
<th>log_name.name</th>
<th>Example JSON object</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&quot;sakila_city_rising_input&quot;:</td>
</tr>
<tr>
<td></td>
<td>&quot;0&quot;</td>
</tr>
<tr>
<td></td>
<td>},</td>
</tr>
<tr>
<td></td>
<td>{</td>
</tr>
<tr>
<td></td>
<td>&quot;time&quot;: &quot;2017-06-23&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;volumes&quot;: {</td>
</tr>
<tr>
<td></td>
<td>&quot;sakila_city_rising_input&quot;:</td>
</tr>
<tr>
<td></td>
<td>&quot;0.001021385&quot;</td>
</tr>
<tr>
<td></td>
<td>},</td>
</tr>
<tr>
<td></td>
<td>{</td>
</tr>
<tr>
<td></td>
<td>&quot;time&quot;: &quot;2017-06-24&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;volumes&quot;: {</td>
</tr>
<tr>
<td></td>
<td>&quot;sakila_city_rising_input&quot;:</td>
</tr>
<tr>
<td></td>
<td>&quot;0&quot;</td>
</tr>
<tr>
<td></td>
<td>},</td>
</tr>
<tr>
<td></td>
<td>{</td>
</tr>
<tr>
<td></td>
<td>&quot;time&quot;: &quot;2017-06-25&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;volumes&quot;: {</td>
</tr>
<tr>
<td></td>
<td>&quot;sakila_city_rising_input&quot;:</td>
</tr>
<tr>
<td></td>
<td>&quot;0&quot;</td>
</tr>
<tr>
<td></td>
<td>},</td>
</tr>
<tr>
<td></td>
<td>{</td>
</tr>
<tr>
<td></td>
<td>&quot;time&quot;: &quot;2017-06-26&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;volumes&quot;: {</td>
</tr>
<tr>
<td></td>
<td>&quot;sakila_city_rising_input&quot;:</td>
</tr>
<tr>
<td></td>
<td>&quot;0&quot;</td>
</tr>
<tr>
<td></td>
<td>},</td>
</tr>
<tr>
<td></td>
<td>{</td>
</tr>
<tr>
<td></td>
<td>&quot;time&quot;: &quot;2017-06-27&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;volumes&quot;: {</td>
</tr>
<tr>
<td></td>
<td>&quot;sakila_city_rising_input&quot;:</td>
</tr>
<tr>
<td></td>
<td>&quot;0&quot;</td>
</tr>
<tr>
<td></td>
<td>]</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>

Data DB Connect does not collect

DB Connect does not collect or send the following kinds of data:

- Sensitive data such as usernames or passwords.
- Identifying information such as addresses, phone numbers, IP addresses, or hostnames.
• Indexed data that you ingest into your Splunk platform instance.

DB Connect does not collect any data that is not explicitly described in the Data Splunk DB Connect collects section above.

How to opt in or out

Splunk DB Connect presents an opt-in request the first time that you launch the app. You can also opt in at any time. In Settings, check the box under the Usage Collection tab.

To opt out, leave the box unchecked when the app presents the Help us improve Splunk products and services box. If you previously opted in but want to change your response, uncheck the box at the bottom of the Configure page, and then click Stop sending data. If you opt out after having previously opted in, the app immediately stops sending data to Splunk.

For more information about how Splunk collects and uses data, please refer to the Splunk Privacy Policy.

How Splunk DB Connect works

Splunk DB Connect is an add-on that bridges Splunk Enterprise with relational databases via Java Database Connectivity (JDBC). It enables Splunk Enterprise to connect to and exchange data with databases such as MySQL, Microsoft SQL Server, Informix, DB2, and many others, enriching your Splunk Enterprise data by combining it with data that was previously only available to you directly from those databases.

Use the add-on to configure database queries and lookups in minutes via the Splunk Enterprise interface. By installing Splunk DB Connect, you can broaden the range of data inputs available to Splunk Enterprise, because they can now include your relational databases. Splunk DB Connect can also do the reverse—send Splunk Enterprise data back for storage in your relational database tables. Splunk DB Connect enriches and combines unstructured data with structured data, which allows users to cross-reference, augment, and correlate between events in machine logs and external databases.

This topic provides an overview of how Splunk DB Connect works.
Setup

Before you can get started, you need to set up Splunk DB Connect. Download the Splunk DB Connect add-on, and then follow the instructions in either the single-server or distributed deployment installation topics. You can use Splunk DB Connect on a heavy forwarder to support continual data gathering or output. For more interactive use, including lookups, you should install the add-on on a search head.

All DB Connect instances require Java Runtime Environment (JRE) version 8 in order to enable JDBC. DB Connect uses a remote procedure call (RPC) server to manage communications with the Java subsystem. You must also install a Java Database Connectivity (JDBC) driver so that Splunk Enterprise can communicate with your databases. Review Install database drivers for more information and a listing of tested drivers.

A checklist of steps required for setting up Splunk DB Connect is available at Installation overview.

Identities

After installing prerequisites and Splunk DB Connect, you must create an identity. An identity is what defines the database user through which Splunk Enterprise will connect to your database(s). It is comprised of the username and password that you use to access your database(s). A single identity can be used by many connections, so that service accounts can be easily shared across multiple systems. This makes regular password changes easier to support.

Be aware that these are database credentials, and are not the same as your Splunk Enterprise credentials. When you configure an identity, you can specify the Splunk Enterprise roles that have read, read-write, or no access to the identity.
• Read access means that Splunk Enterprise roles will be able to use the identity.
• Read-write access means that Splunk Enterprise roles will be able to use and modify the identity.

By default, the Splunk Enterprise admin and db_connect_admin roles have read-write access to a new identity (sc_admin role for the cloud customer), the db_connect_user role has read access, and all other roles have no access.

For more information about setting up and using identities, see Create and manage identities.

Connections

Once you've created the necessary identities for your database environments, you'll need to create a connection. A connection is the information necessary to connect to a specific database. It is comprised of the address of your database (the host name), the database’s type, and the name of the database. When you configure a connection, you can specify which Splunk Enterprise roles have read, read-write, or no access to the connection. Read access means that Splunk Enterprise roles will be able to use the connection. Read-write access means that Splunk Enterprise roles will be able to use and modify the connection. By default, the Splunk Enterprise "admin" and "db_connect_admin" roles have read-write access to a new connection, the "db_connect_user" role has read access, and all other roles have no access.

It's important to remember that, while an identity can be used by several connections, each connection can only be assigned a single identity. When you create a new connection, you specify which identity you want to use with the connection. As you use Splunk DB Connect, you'll only need to specify the connection to use; it will use whatever identity you assigned it. This enables Splunk Enterprise users to work with database contents without knowledge of the database credentials stored in the identity.

For more information about setting up and using connections, see Create and manage database connections.
Database inputs

A **database input** enables you to retrieve and index data from a database using Splunk Enterprise. It's where you can start to narrow down the data you want to index by building a database query. You can either specify the catalog, schema, and table you want to access (in Automatic Query Mode), or enter a custom SQL query against the database (in Editor Query Mode). DB Connect also enables you to preview the results of your query, so that you know that your query is working the way you expect.

Several parameters also help Splunk Enterprise retrieve your data efficiently and in exactly the way you want. For instance, you can specify whether the input should be a batch input (everything dumped in at once), or whether the input has a rising column (a column that is continuously rising, such as an identifier number or timestamp). You can also specify whether to retrieve all rows or a certain number of rows, identify a timestamp format, and set how often to execute the query.

Once you create your database input, Splunk Enterprise uses DB Connect to query your database, and then indexes your data given the parameters you specified. Indexed data is available to searches, reports, and alerts.

For more information about setting up and using database inputs, see Create and manage database inputs.

Search

Once you've set up identities, connections, and database inputs, and Splunk Enterprise has indexed your data, you are ready to **search**. Indexed data obtained via Splunk DB Connect from relational databases is searchable just like the rest of your Splunk Enterprise data. To get started, see Searching and Reporting.

Some data is not suitable for indexing, but can be searched directly from Splunk Enterprise. DB Connect provides the **dbxquery** command for querying remote databases and generating events in Splunk Enterprise from the database query result set. The **dbxquery** command supports SQL queries and stored procedures that have been defined in your database. See dbxquery for command documentation.

For more information about searching in Splunk Enterprise, see the Search Manual.
Database outputs

Splunk DB Connect also enables you to write Splunk Enterprise data back to your relational database using **database outputs**. You can do this interactively from a search head or by setting up an automatic output from a heavy forwarder. Both cases assume that you are connecting to the database using an identity with sufficient write permissions.

DB Connect V3 provides a `dbxoutput` search command for running database outputs that you’ve defined in DB Connect. There is also a predefined **custom alert action** for using the `dbxoutput` command.

- For directions on how to create outputs in DB Connect, see Create and manage database outputs.
- To learn more about Alert Actions in Splunk Enterprise, see Custom alert actions overview.

Database lookups

Splunk DB Connect includes functionality for you to enrich and extend the usefulness of your Splunk Enterprise data through interactions with your external database. **Database lookups** give you real-time contextual information from a database during ad hoc explorations of data in Splunk.

An example of this functionality would be a lookup that takes a customer ID value in an event, matches that value with the corresponding customer name in your external database, and then adds the customer name to the event as the value of a new `customer_name` field. Therefore, if you have an event where `customer_id="24601"`, the lookup would add `customer_name="ValJean, Jean"` to that event.

DB Connect V3 provides the `dbxlookup` command for performing lookups by using remote database tables as lookup tables. Use `dbxlookup` to enrich your indexed events with the information stored in external databases.

- For detailed description on how to use the `dbxlookup` command, see `dbxlookup`
- For instructions on creating lookups in DB Connect, see Create and manage database lookups.
Health monitoring

Splunk DB Connect includes a health dashboard that allows you to monitor numerous aspects of your database connections and transactions with Splunk Enterprise.

For more information about using the health dashboard, see Monitor database connection health.

How this add-on fits into the Splunk picture

Splunk DB Connect is one of a variety of apps and add-ons available in the Splunk ecosystem. All Splunk apps and add-ons run on top of a Splunk Enterprise installation. You must first install Splunk Enterprise, then install the Splunk DB Connect add-on.

- For installation instructions, see Install Splunk DB Connect: Single server deployment or Distributed deployment.
- For details about Splunk apps and add-ons, refer to What are apps and add-ons? in the Splunk Admin Manual.
- To download Splunk Enterprise, visit the download page on splunk.com.
- To get more apps and add-ons, visit Splunk Apps.

How to get help and learn more about Splunk software

Splunk DB Connect is officially supported by Splunk.

How to get help

To get help with the Splunk DB Connect add-on, first consult the Troubleshooting section within this documentation.

You can also log a support case via the Splunk Support Portal.

If your deployment is large or complex, you can engage a member of the Splunk Professional Services team. They will assist you in deploying the Splunk DB Connect add-on.
Learn more about Splunk software

There are a variety of resources available to help you learn more about Splunk Enterprise and the Splunk DB Connect add-on, including:

- Splunk Enterprise documentation
- Splunk Answers
- The #splunk IRC channel on EFNET
Before you deploy

Prerequisites

Before you install this version of Splunk DB Connect, your environment must meet the requirements listed in this topic.

System requirements

- This version of Splunk DB Connect is compatible with Splunk Platform versions 6.6.0 and later.
- Splunk DB Connect is compatible with Splunk Cloud.
- Splunk DB Connect is not compatible with Splunk Light.
- Splunk DB Connect is not compatible with Splunk servers configured for FIPS compliance.

Operating systems and browsers

Splunk DB Connect runs Windows and *nix-based operating systems. For version details, see supported operating systems of Splunk Enterprise.

You can use the following browsers to use Splunk DB Connect on your Splunk platform:

- Apple Safari (latest)
- Google Chrome (latest)
- Microsoft Edge (latest)
- Microsoft Internet Explorer 11
- Mozilla Firefox (latest)

Splunk licenses and DB Connect

If you configure Splunk DB Connect to import data from a connected database into a Splunk Enterprise index, the amount of data Splunk Enterprise indexes counts towards your Splunk Enterprise license. Using the dbxquery, dbxlookup, and dbxoutput commands against a connected database in DB Connect does not count towards the license.

For more information about Splunk licenses, see How Splunk licensing works.
Splunk DB Connect Release Notes

For the latest known issues and fixed problems in Splunk DB Connect, see Release Notes.

User permissions

Before using DB Connect, a logged-in user must have the ability to write to the $SPLUNK_HOME/var directory (\%SPLUNK_HOME\%\var on Windows hosts) and to $SPLUNK_HOME/etc/apps/splunk_app_db_connect (\%SPLUNK_HOME\%\etc\apps\splunk_app_db_connect on Windows hosts) and its sub-directories. For more information, see Use access control to secure Splunk data.

Java Runtime Environment (JRE) requirements

Before deploying Splunk DB Connect, download and install one of the following compatible versions of the Java Runtime Environment:

Java Runtime Environment (JRE) version 8 from Oracle

1. Download and install the Server Java Runtime Environment version 8 from Oracle. Only use a supported JVM in server mode, not in client mode.
2. Once you have installed the JRE, write down the path to the JRE directory, or $JAVA_HOME. You need the filepath when you are configuring DB Connect. When DB Connect prompts you to input the JRE Installation path in Configuration > Settings, be sure to input the complete JRE filepath you wrote down.

OpenJDK 8 from the Open Java Development Kit project

1. Download and install the OpenJDK version 8 from the Open JDK project. Only use a supported JVM in server mode, not in client mode.
2. Once you have installed the JRE, write down the path to the JRE directory, or $JAVA_HOME. You need the filepath when you are configuring DB Connect. When DB Connect prompts you to input the JRE Installation path in Configuration > Settings, be sure to input the complete JRE filepath you wrote down.
If you are unsure whether you have the correct version of Java installed, access DB Connect setup. On the first screen of the DB Connect setup or at Configuration > Settings > General you can specify the path to your JRE. If there is a problem with the Java install or the system $JAVA_HOME variable is incorrect, DB Connect displays an error message. It is important that you resolve any JRE issues before proceeding as DB Connect uses Java Database Connectivity (JDBC) to communicate with your databases.

**Database and JDBC database driver requirements**

Splunk DB Connect supports connections to many databases. You must install a Java Database Connection (JDBC) driver before you can connect to databases with DB Connect.

For more information about the databases that Splunk DB Connect supports, see Supported databases.

For information about connecting to unsupported databases with Splunk DB Connect, see Other databases.

**Architecture and performance considerations**

When adding Splunk DB Connect to your deployment, there are several architecture and performance considerations to take into account. You can install and run Splunk DB Connect on Splunk Enterprise deployments ranging from a single host (indexer and Splunk Web both running on the same system) to a large distributed deployment (multiple search heads, search head clusters, indexers, load-balanced forwarders, and so on). This topic provides guidance for setting DB Connect up and running in these environments. It also describes the kind of performance you can expect based on your deployment and capacity requirements.

**Database performance considerations**

If Splunk DB Connect retrieves large amount of data from your database, it may affect your database performance, especially for the initial run. Subsequent runs of the same query may have less impact, as the database may cache results and only retrieve new data since the previous run of the query.
Performance considerations in distributed environments

To use Splunk DB Connect in a distributed search environment, including search head clusters, you must determine the planned use cases. For ad hoc, interactive usage of database connections by live users, install the app on search head(s). For scheduled indexing from databases and output of data to databases, install the app on heavy forwarder(s).

Note: DB Connect does not support running scheduled inputs and outputs on a search head cluster. Splunk recommends you run inputs and outputs from a heavy forwarder. Beginning with DB Connect 3, this recommendation is enforced. If you have been running scheduled inputs or outputs on a search head cluster using DB Connect 1 or DB Connect 2, you will need to move them onto a heavy forwarder before migrating to DB Connect 3.

When planning a large DB Connect deployment, the ideal configuration for your needs can depend on a number of factors, including:

- Total number of Forwarders in the deployment, and the hardware specifications of each.
- Total expected data volume to transfer.
- Number of database inputs per Forwarder.
- Dataset size, per input, per interval.
- **Execution Frequency**, the interval length between a database input's separate executions.
- **Fetch size** (note that not all JDBC drivers use this parameter for returning result sets).

Overloading the system can lead to data loss, so performance measurement and tuning can be critical. Use performance expectations as the reference to plan your deployment, and monitor expected data returns for loss conditions.

Performance expectations

This section provides measured throughput data achieved under certain operating conditions. Use the information here as a basis for estimating and optimizing the DB Connect throughput performance in your own production environment. As performance may vary based on user characteristics, application usage, server configurations, and other factors, specific performance results cannot be guaranteed.

The performance data in the following table were produced with the following test
bed and DB Connect configuration (note that increasing cores and/or RAM may improve scaling characteristics):

- Server: 8-core 2.60GHz CPU, 16GB RAM, 1Gb Ethernet NIC, 64bit Linux
- JVM config: MaxHeapSize = 4GB. (For more information about the JVM memory setting, see "Performance tuning advice").
- Data Source: Oracle 11g

### Inputs

- Number of inputs: 1600
- Data payload (per input execution) : 250KB
- Duration = 45 minutes
- Interval: 1 minute

total data volume = data payload * duration / interval * number of inputs = 17.5 GB

Data payload per input execution is the same for different input modes (rising column and batch)

### Queries

<table>
<thead>
<tr>
<th>Rows in data set</th>
<th>DB Connect 3</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1.2 seconds</td>
<td>1.3 seconds</td>
<td>1.6 seconds</td>
<td>4.1 seconds</td>
<td>22.9 seconds</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rows in data set</th>
<th>DB Connect 2</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1.4 seconds</td>
<td>1.5 seconds</td>
<td>2.4 seconds</td>
<td>11.4 seconds</td>
<td>103.5 seconds</td>
</tr>
</tbody>
</table>

### Lookups

<table>
<thead>
<tr>
<th>Rows in data set</th>
<th>DB Connect 3</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1.2 seconds</td>
<td>2.8 seconds</td>
<td>36.0 seconds</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.2 seconds</td>
<td>4.3 seconds</td>
<td>70.0 seconds</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Outputs

<table>
<thead>
<tr>
<th>Rows in data set</th>
<th>DB Connect 3</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2.1 seconds</td>
<td>1.9 seconds</td>
<td>3.0 seconds</td>
<td>9.1 seconds</td>
<td>67.2 seconds</td>
</tr>
</tbody>
</table>
General performance tuning considerations

While it's impossible to provide prescriptive advice for maximizing performance in every situation, the following observations and tips can help you tune and improve performance in your unique distributed deployment:

1. **Only select columns if you really need them.** A table can contain many types of columns. When ingesting data from a database into DB Connect, you likely don't need all of them. Therefore, instead of using a `SELECT * FROM ...` clause to fetch all the columns, select only what you need by using a `SELECT columnNeeded1, columnNeeded2, ... FROM ...` clause. More columns means more memory claimed by the task server; omit those unnecessary columns to make smarter use of your available memory. See SQL tips and tricks for more details.

2. **Avoid reaching the 5MB/10MB limit.** Very large column sizes can cause DB Connect to potentially run out of memory and behave erratically, so DB Connect has a column size limit of 10MB for data columns that hold two-byte data types and 5MB for one-byte data types. Columns with data exceeding these limits will have their data truncated. If possible, trim the amount of data stored per column so that you avoid the DB Connect hard caps.

3. **Adjust the fetch size based on your scenario.** The Fetch Size input parameter specifies the number of rows returned at a time from a database, which defaults to 300 rows. A higher fetch size means more records are received per database request, so fewer database requests are required to retrieve the same total number of records. This increases resource utilization on the database and in DB Connect, but can lead to performance improvements. Lowering the fetch size parameter can help prevent the Task Server from hitting its memory limit. If you receive out of memory errors when you increase the fetch size, you may need to increase the memory heap size from its default of 1/4 of system RAM.

4. **Reduce the total number of database inputs.** It can increase the amount of data that each input is taking in. This helps ensure that CPU cores have to handle fewer processes within a given window of time. Small datasets can be slower than large because of environment initialization.
5. **Reduce the concurrency of scheduled database tasks.** Shifting start times for scheduled tasks will reduce choke points during which inputs and outputs have to share resources. For more information, see "Set parameters" in Create and manage database inputs.

6. **Adjust batch_upload_size field.** The batch_upload_size field defines the number of events sent to splunkd through HEC per request, which defaults to 1,000 records. A higher batch upload size means more records are sent per HTTP post, so fewer server transactions are required to index the same total number of records. This increases resource utilization on the Forwarder, but can lead to performance improvements. You can increase the `batch_upload_size` field under `$SPLUNK_HOME/etc/apps/splunk_app_db_connect/local/db_inputs.conf` to have better performance.

7. **Specify sufficient hardware.** In general, Splunk recommends the same hardware specifications for DB Connect as it does for Splunk Enterprise. Increased hardware may be necessary for increased indexing loads.

8. **Configure Java for performance.** Current Java engines will automatically reserve 25% of the machine’s RAM on launch. If your JVM Options setting is specified as `-Xmx1024m` (which is the default value from DB Connect V2.0 to v2.2). You can remove it and use the default JVM setting. For more information about changing JVM options, see "JVM Options" in Configure DB Connect Settings.

9. **Configure Splunk for performance.** Increase Splunkd’s index queue size and number of Parallel Ingestion Pipelines to avoid concurrency limits.

10. **Configure DB Connect for performance** Set `SchedulerThreadPoolSize` to match the number of processor cores.

**Performance non-factors**

During testing, varying the following factors had a negligible effect on performance:

- There was no discernable performance difference between running in batch mode (all events processed) and running in rising column mode (just the new events processed) with the same dataset.
- The number of defined database connections does not limit performance. Note that the number of connections is different from the number of database inputs.
More performance help

If you are still experiencing performance issues, or want to receive feedback tailored to your setup, you have the following options:

• Post a request to the community on Splunk Answers.
• Contact Splunk Support.
Install Splunk DB Connect

Installation and setup overview

This topic provides an overview of how to install and set up Splunk DB Connect.

To deploy Splunk DB Connect on either a single instance of Splunk Enterprise or on a search head in a distributed deployment, you must have:

- Splunk Enterprise 6.6.0 or later, running on a supported operating system.
- One of the following supported Java environments:
  - Java Platform, Java Runtime Environment (JRE) 8 from Java Platform, Standard Edition.
  - Java Platform, Open Java Development Kit (OpenJDK) 8 from the OpenJava Project.
- A supported database running locally or elsewhere on your network.

Once the prerequisites are in place, you can start the DB Connect installation process:

1. Download and install the DB Connect add-on.
2. Install a JDBC driver for your database. See Install database drivers.
3. After installing DB Connect and restarting Splunk Enterprise, launch DB Connect.
4. Create a database identity and set up a database connection.
5. Create a new database input and use it as a data input in a Splunk Enterprise search.

For distributed deployments, there are further instructions for deploying the distributed deployment.

Deploy DB Connect to Splunk Cloud

If you want to deploy DB Connect to Splunk Cloud, contact Splunk Support for guidance and assistance. You cannot deploy DB Connect yourself because you cannot configure network access to databases on your Splunk Cloud instance. See Install an add-on in Splunk Cloud for details.
Upgrade an existing DB Connect deployment

Click the **Update** button and follow the wizard to upgrade your DB Connect using Splunk web, or you can download the package and **install the DB Connect**.

There are some known limitations on upgrading DB Connect on certain circumstances, please review the following list before upgrading.

1. If you are running DB Connect on Windows platform and want to upgrade to the higher version. You need to:
   1. On the Splunk Web home page, click **Apps > Manage Apps**.
   2. On the **Apps** page, navigate to Splunk DB Connect, and click **Disable**.
   3. Upgrade DB Connect and restart Splunk platform.
   4. On the Splunk Web home page, click **Apps > Manage Apps**.
   5. On the **Apps** page, navigate to Splunk DB Connect, and click **Enable**.

2. If you are using DB Connect (version prior to 3.0.0) and want to upgrade to DB Connect 3, see **Migrate DB Connect deployment to DB Connect 3**.

3. If you want to migrate DB Connect in Splunk Cloud, contact Splunk Support. Do not upgrade from previous versions yourself because you cannot migrate configuration files on your Splunk Cloud instance.

Migrate DB Connect deployment to DB Connect 3

DB Connect 3 rewrote the JDBC backend and data collection configuration files. You must migrate the environment, input, output, and lookup configurations you created in DB Connect 2 to DB Connect 3 (version 3.0.0 and later).

Since the deployment scenarios vary among different users, the script may fail to migrate your configurations. Therefore, you may require to redefine your configurations after DB Connect 3 installation.

Use the migration script `dbx_app_migration.py` located at `$SPLUNK_HOME/etc/apps/splunk_app_db_connect/bin` to migrate the following artifacts from DB Connect 2 to DB Connect 3:
• **JDBC Drivers** (If you use complex drivers such as Oracle, Spark SQL, or Teradata in your DB Connect 2 deployment, be sure to complete the extra step to manually migrate those drivers to DB Connect 3. Drivers that require many files and which have several dependencies do not automatically migrate.)

• **JVM Options**, such as JRE installation path, RPC server port, or memory configuration

• connections and identities

• database inputs

• database outputs

• database lookups

**User permissions**

Splunk recommends you to run the migration scripts using Splunk Python. Run the following script from a Linux Terminal or Windows Command Prompt:

```
$SPLUNK_HOME/bin/splunk cmd python
$SPLUNK_HOME/etc/apps/splunk_app_db_connect/bin/dbx_app_migration.py
```

Use `-h` to see all options for the `app_migration` command.

To migrate the DB Connect install, the user must have full read and write access to `$SPLUNK_HOME/var`, `$SPLUNK_HOME/etc/apps/splunk_app_db_connect`, and their subdirectories.

Depending on how you installed your instance of Splunk software, you may need to execute migration as a user with higher privileges than usual, such as root or LocalSystem, in order to have full access to files and processes the Splunk Enterprise service owns. See Use access control to secure Splunk data for details.

**Migration paths**

The following matrix summarizes your upgrade options from the version(s) of DB Connect you're running currently and the migration path to DB Connect 3.

<table>
<thead>
<tr>
<th>From</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB Connect 2.3.0</td>
<td>Use the migration scripts during the upgrade process.</td>
</tr>
<tr>
<td>DB Connect 2.3.1</td>
<td></td>
</tr>
<tr>
<td>DB Connect</td>
<td></td>
</tr>
<tr>
<td>From</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>2.4.0</td>
<td>1. Upgrade to DB Connect 2.4.0 first, no migration needed for this step. See single server deployment on how to install DB Connect.</td>
</tr>
<tr>
<td>DB Connect 2.x.x version prior to 2.3.0</td>
<td>2. Migrate to DB Connect 3 using migration scripts.</td>
</tr>
<tr>
<td>DBX 1.x.x</td>
<td>For DB Connect 1.x.x installation with few configurations, use Migrating from DB Connect 1.x.x to DB Connect 2.x.x and then follow Migrate to DB Connect 3 using migration scripts. There are known limitations to the DB Connect 2.1.x migration scripts, and a more complex environment may require a reinstallation of DB Connect 3 migrate manually.</td>
</tr>
</tbody>
</table>

If you have difficulties or errors when migrating DB Connect to the latest version, contact Splunk Support for migration support.

**Upgrade and migrate instructions**

The upgrade and migration processes are different for a single instance and for a distributed deployment. Follow the instructions below to upgrade and migrate DB Connect.

- Migrate DB Connect 2 to DB Connect 3 on a single instance.
- Migrate DB Connect 2 to DB Connect 3 on distributed deployment.

**Migrate DB Connect 2 to DB Connect 3 on a single instance**

1. You can upgrade to DB Connect version 3 from version 2.3.0 or later by clicking the Upgrade button in the Apps listing, or by downloading the latest installation package from https://splunkbase.splunk.com/app/2686/ and install DB Connect.
2. Restart your Splunk instance.
3. Run the migration script dbx_app_migration.py located at $SPLUNK_HOME/etc/apps/splunk_app_db_connect/bin

   dbx_app_migration.py [-h] [-scheme SCHEME] [-port PORT] [-verbose]

   - **-scheme**: Optional. URI scheme of Splunk platform, either http or https, the default is https.
   - **-port**: Optional. Port number of Splunk platform, the default is 8089.
   - **-verbose**: Whether to enable verbose logging, the default is False.
- **-help or -h**: Optional.

4. When prompted, enter the user name and password of the Splunk instance.

5. The migration scripts back up your existing drivers, connections, inputs, outputs, and lookups configuration in `$SPLUNK_HOME$/etc/apps/splunk_app_db_connect/migration_backups` and lists actions it performs.

6. View the actions the migration scripts list and choose whether to perform the migration based on your situation. To proceed, respond to the message with `Y`. Apply above actions, continue?[Y/n]Y

- If the migration succeeds, the status shows 100% done and the successful message appears.
- If there are errors during the migration, the errors appear during the migration, for example,

```
Performing action [3/29]:
|?????---------------------------------------------------------------| 10.3% Done!
failed to execute action 3, cause:HTTP 400 Bad Request -- Object
id=conn_mcafee_epo cannot be deleted in config=db_connections.
Y to skip failed action and continue, n to abort the migration?
```

You can decide whether to continue or abort the migration.

- If you choose to ignore the error and proceed, type `Y`.
- If you want to abort the migration, manually correct the error and migrate again. Copy the backup files under `$SPLUNK_HOME$/etc/apps/splunk_app_db_connect/migration_backups/splunk_app_db_connect` back to `$SPLUNK_HOME$/etc/apps/splunk_app_db_connect` before the next migration.

7. (Optional). When migrating from DB Connect 2 to DB Connect 3, you must move JDBC driver files to new locations. You cannot automatically migrate complex drivers that require many files and have many dependencies such as, Oracle, Spark SQL and Teradata. For those complex drivers, you must manually move the dependent JAR files in the `$SPLUNK_HOME/etc/apps/splunk_app_db_connect/drivers/<JDBC driver name>-libs` folder. See Install database drivers for more information.

8. Restart Splunk when the migration succeeds.

9. Once the migration scripts have completed, launch DB Connect 3. Click Datalab to view your transferred database inputs, outputs and lookups.

**Note**: If the task server cannot start after migration, you must kill the RPC server process manually and restart Splunk Enterprise again. This is a known issue when migrating on Ubuntu operating system.
Migrate DB Connect 2 to DB Connect 3 on a distributed deployment

Migrate DB Connect on the search head cluster

If you installed DB Connect on a search head cluster, use the cluster **deployer** to migrate from DB Connect 2 to DB Connect 3. If you are using scheduled inputs or outputs on the search head cluster, you must copy the configuration of a search head cluster node to a heavy forwarder, then migrate that forwarder to DB Connect 3. Because configuration replication between SHC nodes does not include the cluster deployer, you cannot migrate scheduled tasks to DB Connect 3 unless you copy the configuration files from an SHC node to a forwarder.

1. Scheduled inputs and outputs cannot run on a search head cluster in DB Connect 3. If you have scheduled inputs and outputs on DB Connect 2, you must copy the files under
   `$SPLUNK_HOME/etc/apps/splunk_app_db_connect` to a heavy forwarder before migrating.
2. Copy the JDBC driver from one of the cluster nodes to the subdirectories under
   `$SPLUNK_HOME/etc/shcluster/apps/splunk_app_db_connect/bin/lib` on the deployer.
3. To upgrade DB Connect on the deployer, download the latest version of DB Connect from https://splunkbase.splunk.com/app/2686 and untar the installation package to
   `$SPLUNK_HOME/etc/shcluster/apps/splunk_app_db_connect`. Note that you cannot use Splunk web to perform this step.
4. Run the
   ```bash
   splunk apply shcluster-bundle -target <URI>:<management_port>
   -auth <username>:<password>
   ```
   command on the deployer to distribute the upgrade bundle to search head cluster members.
5. To migrate the configurations on the deployer, see Migrate to DB Connect 3 using the migration scripts. Note that migration scripts can detect that you are migrating on the deployer and ask you to provide the API endpoint and credentials of one cluster node.
6. Run the
   ```bash
   splunk apply shcluster-bundle -target <URI>:<management_port>
   -auth <username>:<password>
   ```
   command to distribute the migration to search head cluster members and restart Splunk Enterprise when the migration succeeds.
Note the following:

- The `target` parameter specifies the URI and management port for any member of the cluster, for example, `https://10.0.1.14:8089`. You specify only one cluster member but the deployer pushes to all members. This parameter is required.
- The `auth` parameter specifies credentials for the deployer instance.

**Migrate DB Connect on heavy forwarder**

If you have schedule inputs and outputs on the search head cluster, back up your existing inputs and outputs on the heavy forwarder before migration. The migration procedure for a heavy forwarder is the same as migration on a single instance. See migrate DB Connect 2 to DB Connect 3 on a single instance.

**Migrate DB Connect resource pools**

Because of the increased vertical scale of DB Connect 3, resource pooling is not available. The tasks that you perform on the resource pool master do not distribute to other resource pool members after the migration. If you are using resource pool in DB Connect 2, see performance expectations to redesign your deployment. You can remove the other resource pool members to conserve resources or configure them as separate heavy forwarders to scale your deployment.

- **If you are running resource pool master and resource pool members all on heavy forwarders**: The migration procedure is the same as on a single instance. See migrate DB Connect 2 to DB Connect 3 on single instance for more details.
- **If you are running resource pool master on a search head cluster and resource pool members on heavy forwarders**: Back up your configurations to one of the resource pool members first, then migrate this pool member. The migration procedure is the same as the migration on a single instance. See migrate DB Connect 2 to DB Connect 3 on a single instance for details.

If you have difficulties or errors during the migration, see troubleshooting or contact Splunk Support.
Install database drivers

After you’ve downloaded and installed Splunk DB Connect, the first step in the DB Connect setup process is installing a Java Database Connectivity (JDBC) database driver.

After you add the database driver, continue with either the single server or distributed deployment instructions. You will be able to verify whether the database driver was installed successfully during DB Connect setup.

Supported databases

Splunk DB Connect supports the databases listed in the following matrix.

- The driver listed in the JDBC driver name/link column is the driver that Splunk has tested with Splunk DB Connect.
- DB Connect supports and has been tested with Java cryptography standard algorithm, if you need a stronger algorithm, you must install the "JCE Unlimited Strength Jurisdiction Policy Files." Legal restrictions may apply in your country. See Java Security Providers and JCE Download pages for details. Consult your database vendor's documentation for configuration instructions.

<table>
<thead>
<tr>
<th>Database</th>
<th>JDBC driver name</th>
<th>JDBC driver version tested</th>
<th>SSL support*</th>
<th>Cloud support**</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS RDS Aurora</td>
<td>MySQL Connector/J</td>
<td>5.1</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>AWS RedShift</td>
<td>RedshiftJDBC41-1.2.1.1001.jar</td>
<td>1.2</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Not compatible with RedshiftJDBC42-1.2.1.1001.jar.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM DB2 for Linux</td>
<td>DB2 JDBC Driver (JCC4)</td>
<td>4.16</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Informix</td>
<td>Informix JDBC Driver</td>
<td>3.0</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MemSQL</td>
<td>MySQL Connector/J</td>
<td>5.1</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>Microsoft JDBC Driver for SQL Server</td>
<td>4.2</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>jTDS JDBC Driver</td>
<td></td>
<td>1.3</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Database</td>
<td>JDBC driver name</td>
<td>JDBC driver version tested</td>
<td>SSL support*</td>
<td>Cloud support**</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>----------------------------</td>
<td>--------------</td>
<td>----------------</td>
</tr>
<tr>
<td>MySQL</td>
<td>MySQL Connector/J</td>
<td>5.1</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Oracle Database</td>
<td>Oracle JDBC driver</td>
<td>11.2</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>JDBC41 PostgreSQL Driver</td>
<td>42.2</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>When upgrading the Postgres database, you must also upgrade the Postgres driver</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAP SQL Anywhere (aka Sybase SA)</td>
<td>Sybase jConnect</td>
<td>7.0</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Spark SQL</td>
<td>Simba JDBC Driver</td>
<td>1.0.2.1004</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Sybase ASE</td>
<td>Sybase jConnect</td>
<td>7.0</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Sybase IQ</td>
<td>Sybase jConnect</td>
<td>7.0</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Teradata</td>
<td>Teradata JDBC Driver (terajdbc4.jar and tdgssconfig.jar)</td>
<td>15.0</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

* **SSL support**: This column specifies whether DB Connect tests and supports Secure Sockets Layer (SSL) connections to this database. Though other supported databases may support SSL connections, DB Connect support for SSL means that Splunk has tested SSL for that database type and supports connecting over SSL using DB Connect.

** **Cloud support**: This column specifies whether the database is supported for Splunk Cloud. You must enable SSL connection if you want to use DB Connect in a Splunk Cloud deployment.

**Other databases**

In addition to the supported databases that Splunk has tested and certified for use with DB Connect, you may also be able to use unsupported JDBC-compatible databases with Splunk DB Connect. You will need to provide the necessary JDBC drivers to add your own database types. For more information, see Install drivers for other databases.
Compatible database drivers

Click the link that corresponds to your database:

- AWS RDS Aurora
- AWS RedShift
- IBM DB2
- Informix
- MemSQL
- Microsoft SQL Server
- MySQL
- Oracle
- PostgreSQL
- SAP (previously Sybase) SQL Anywhere (SA)
- Spark SQL
- SAP/Sybase Adaptive Server Enterprise (ASE)
- SAP/Sybase IQ
- Teradata
- Install drivers for other databases.

Notes:

- In DB Connect 3.0.0, the main JDBC JAR file and the extended JAR files must be installed in different folders. The path for the extended JAR file is $SPLUNK_HOME/etc/apps/splunk_app_db_connect/drivers/<JDBC driver name>-libs. If you are using Spark SQL, or a Teradata or Oracle database, you must move dependent JAR files manually.
- Your database connection must be set up to return results encoded in UTF-8. Consult your database vendor’s documentation for instructions.
- DB Connect supports sending data that is in a multi-byte character set, such as Traditional Chinese, using a database output. Depending on your database, you may need to change certain settings on the database side to the database to properly receive and store the data. See Enable output to multi-byte character sets.

IBM DB2

IBM DB2 is supported when the database is running on Linux. Splunk doesn’t test or support DB2 on AS/400 or Windows.
**Note:** IBM DB2 is only supported when the database is running on Linux. Splunk doesn't test or support DB Connect with DB2 on AS/400 or on Windows.

If you want to use GSS API security mechanisms in IBM DB2, download **Java Cryptography Extension (JCE) Policy** to your `$JRE_Installation_Path/jre/lib/security` and set the encryptionAlgorithm parameter of JDBC URL as

```java
jdbcUrlFormat =
jdbc:db2://<host>:<port>/<database>:securityMechanism=9;encryptionAlgorithm=2;
```

Follow these instructions to install the DB2 JDBC Driver:

1. Go to DB2 JDBC Driver Versions and Downloads on the IBM website, and click the link for the latest **DB2 Version 10.5** driver.
2. Click the **Download** link for the **IBM Data Server Driver for JDBC and SQLJ** (JCC Driver).
3. Select the newest fix pack, and then click **Continue**. You will need to log in with your IBM ID, or create one if you don't already have one.
4. Click the **Download using your browser (HTTPS)** radio button, and then **Continue**.
5. Right-click the file name, and then save it to your hard disk.
6. Expand the downloaded file, and then expand the `db2_db2driver_for_jdbc_sqlj.zip` file.
7. Copy or move the `db2jcc4.jar` file to the `$SPLUNK_HOME/etc/apps/splunk_app_db_connect/drivers` directory.
8. **Reload** the driver under **Settings>Drivers**.

For additional information, see the Installing and Connecting to Clients documentation on the IBM website.

**AWS RDS Aurora, MemSQL, or MySQL**

Follow these instructions to install MySQL Connector/J for AWS RDS Aurora, MemSQL, or MySQL databases:

1. Download the MySQL Connector/J driver, version 5.1.24 or later (`mysql-connector-java-*--bin.jar`).
2. Download and uncompress either ZIP or TAR archive files. The uncompressed archive contains the JDBC driver (.jar).
3. Copy the `mysql-connector-java-version-bin.jar` file to the `$SPLUNK_HOME/etc/apps/splunk_app_db_connect/drivers` directory (`%SPLUNK_HOME%/etc/apps/splunk_app_db_connect/drivers` on Windows).
4. **Reload** the driver under **Settings>Drivers**

**Microsoft SQL Server**

You have several options for connecting to a Microsoft SQL Server. Start by determining:

- Which operating system (Windows or Linux) is running Splunk DB Connect.
- Which driver you want to use.
- How your database server authenticates your connection.

See **Legends** below the table for more detailed explanation.

Follow this table from left to right, choosing the options that correspond to your Microsoft SQL Server environment. For more information about the meaning of each column, see the legend that follows the table.

<table>
<thead>
<tr>
<th>Operating System*</th>
<th>Driver**</th>
<th>Authentication***</th>
<th>How to install driver</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>MS Generic</td>
<td>SQL Authentication</td>
<td>Install the SQL Server database driver using SQL server authentication</td>
</tr>
<tr>
<td></td>
<td>Windows Authentication</td>
<td>Install the SQL Server using MS Generic driver with Windows authentication</td>
<td></td>
</tr>
<tr>
<td>jTDS</td>
<td>SQL authentication</td>
<td>Install the SQL Server database driver using SQL server authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows authentication</td>
<td>Install the SQL Server using jTDS driver with Windows Authentication</td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td>MS Generic</td>
<td>SQL authentication</td>
<td>Install the SQL Server database driver using SQL server authentication</td>
</tr>
<tr>
<td></td>
<td>Kerberos authentication</td>
<td>Install the SQL Server database driver using the MS Generic driver with Kerberos authentication</td>
<td></td>
</tr>
</tbody>
</table>
**Operating System**: The operating system on which DB Connect is running. DB Connect is supported on both Linux and Windows Server.

**Driver**: The JDBC driver that DB Connect will use to connect to your database:

- **MS Generic**: Microsoft JDBC Driver for SQL Server (the "generic Microsoft driver")
- **jTDS**: Open source jTDS driver

**Authentication**: The type of service account that DB Connect will use to connect to your database:

- **SQL Authentication**: Log into SQL Server as a SQL Server user. This option assumes you will create an identity that uses a username and password that is defined on the database.
- **Windows Authentication**: Log into SQL Server as a Microsoft Integrated Windows Authentication user ("domain user"). This assumes that you are creating an identity that uses a domain, user name, and password to connect to the database, and that the user you assign to the identity is part of an Active Directory user group that has been set up to log into your SQL Server.
- **Kerberos Authentication**: DB Connect uses a Kerberos client (Linux) to negotiate an authentication ticket with the Active Directory environment directly. This assumes that the user you assign to the identity is part of an Active Directory user group that has been set up to log into your SQL Server.

### Install the SQL Server database driver using a SQL server authentication

If you will log onto your SQL Server database using a SQL Server user name and password (non-domain attached), follow these instructions:

<table>
<thead>
<tr>
<th>Operating System*</th>
<th>Driver**</th>
<th>Authentication***</th>
<th>How to install driver</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>jTDS</td>
<td>SQL authentication</td>
<td>Install the SQL Server database driver using SQL server authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows authentication</td>
<td>Install the SQL Server using jTDS driver with Windows Authentication</td>
</tr>
</tbody>
</table>
Install the SQL server database driver

1. Download the appropriate JDBC driver for SQL Server:
   - For the Microsoft JDBC Driver for SQL Server (the "MS Generic Driver"), go to the Microsoft JDBC Drivers for SQL Server download page and click **Download**. On the Choose the download you want page, select the checkboxes next to the appropriate download: `sqljdbc_4.2.8112.100_enu.tar.gz` for Linux; `sqljdbc_4.2.8112.100_enu.exe` for Windows. Be sure to download version 4.2 of the driver, and then click **Next**. Expand the downloaded file.
   - For the open source jTDS driver, download the driver from the jTDS Project.

2. Move the driver file to the correct location:
   - For the MS Generic Driver, from inside the `sqljdbc_4.2` directory, copy or move the `sqljdbc42.jar` file to the `$SPLUNK_HOME/etc/apps/splunk_app_db_connect/drivers` directory ($%SPLUNK_HOME%\etc\apps\splunk_app_db_connect\drivers on Windows hosts).
   - If you will need to use a database service account on Windows with the Generic driver, you will also need to install the JDBC Auth library:
     1. From the Microsoft JDBC Driver 4.2 for SQL Server download, locate the `sqljdbc_auth.dll` file. This file is at the following path, where `<region_code>` is the three-letter region code (for example, `enu` for U.S. English), and `<architecture>` is the processor type (`x86` or `x64`): `Microsoft JDBC Driver 4.2 for SQL Server\sqljdbc_4.2<region_code>\auth\<architecture>\sqljdbc_auth.dll`
     2. Copy the `sqljdbc_auth.dll` file to `C:\Windows\System32` on your Splunk Enterprise server.
     3. From the Windows Control Panel, go to **Services**, and then get properties on **Splunk Service**.
     4. Click the **Log On** tab, and then change the **Log on as** setting from the Local System account to that of the logged on domain user.

       **Note:** The domain user should have sufficient privileges to access the SQL Server instance.

     5. Save your changes, and then restart the Splunk Enterprise server for the changes to take effect.
   - For the jTDS driver, copy the .jar file you downloaded to the `$SPLUNK_HOME/etc/apps/splunk_app_db_connect/drivers` directory.
When you create a connection to this database in DB Connect, be sure to choose either MS-SQL Server Using MS Generic Driver or MS-SQL Server Using jTDS Driver, depending on your driver, from the Connection Types popup menu.

**Install the SQL Server using jTDS driver with Windows Authentication**

If you will log onto your SQL Server database as a Microsoft Integrated Windows Authentication user ("domain user"), follow these instructions. These instructions assume that you are creating an identity that uses a domain, user name, and password to connect to the database, and that the user you assign to the identity is part of an Active Directory user group that has been set up to log into your SQL Server.

**Note:** These instructions apply whether DB Connect is running on Linux or Windows.

1. See the instructions on how to Install the appropriate JDBC driver for SQL Server and move the driver to the correct location
2. When you set up a new identity for this database, be sure to select the checkbox labeled Use Windows Authentication Domain? Then, in the Windows Authentication Domain that appears, type the name of your domain.
3. When you create a connection to this database, be sure to choose MS-SQL Server Using jTDS Driver With Windows Authentication from the Connection Types popup menu.

**Install the SQL Server using MS Generic driver with Windows authentication**

If you’re running DB Connect on Windows, you can connect to a Microsoft SQL Server with a Windows domain and user name by using the Microsoft generic driver and enabling the Splunk Enterprise service to run as the logged on domain user:

1. See the instructions on how to Install the appropriate JDBC driver for SQL Server and move the driver to the correct location
2. From the Windows Control Panel, go to Services, and then get properties on Splunk Service.
3. Click the **Log On** tab, and then change the **Log on as** setting from the Local System account to that of the logged on domain user.

**Note:** The domain user should have sufficient privileges to access the SQL Server instance.

4. Save your changes, and then restart the Windows machine running DB Connect for the changes to take effect.

5. When you **set up a new identity** for this database, be sure to select the checkbox labeled **Use Windows Authentication Domain?** Then, in the **Windows Authentication Domain** that appears, type the name of your domain.

6. When you **create a connection** to this database, be sure to choose either **MS-SQL Server Using MS Generic Driver With Windows Authentication** from the **Connection Types** popup menu.

**Install the SQL Server database driver using the MS Generic driver with Kerberos authentication**

If you're running DB Connect on Linux, you can connect to a Microsoft SQL Server using a Windows domain and user name by enabling Kerberos authentication.

Before starting the following procedure:

1. See the instructions on how to **Install the appropriate JDBC driver for SQL Server and move the driver to the correct location**
2. Enable Kerberos on the Microsoft SQL Server.

Now complete the following steps to enable DB Connect to use Kerberos authentication to connect to your SQL Server database:

1. First, get the domain name:
   1. Log onto the Windows server that is running your SQL Server database.
   2. At the command line, run `systeminfo`, and then copy down the domain name (next to the **Domain:** label).
2. Next, get the Kerberos Distribution Center (KDC) information:
   1. From the command line, run the following, replacing `<domain>` with the domain name you copied in the previous step: `nltest /DSGETDC:<domain>`
   2. Copy down the name of the domain controller, which is next to the **DC:** label. This is the KDC host name.
3. Back on the machine running DB Connect, use the `kinit` command to generate a `krb5.conf` file, which Kerberos will use to authenticate with the SQL Server for DB Connect.

1. First, install `kinit` by entering the following at the command line:
   ```
   apt-get install krb5-user
   ```
   If you are prompted to enter a realm, enter the domain name you obtained in Step 1, but in all upper-case letters. For example, if your domain is `abc.dbx`, you'd enter `ABC.DBX`.

2. Next, use `kinit` to initialize the Kerberos ticket cache. Enter the following at the command line, replacing `<username>` with the appropriate user name (such as `Administrator`) and `<DOMAIN>` with the domain name, in upper-case letters:
   ```
   kinit <username>@<DOMAIN>
   ```

   The `krb5.conf` has been generated in the `/etc` directory.

   **Note:** If the `krb5.conf` file is not in the `/etc` directory, set the following option in JVM Options under the Settings tab:
   ```
   -Djava.security.krb5.conf=/path/to/krb5.conf
   ```

4. Create an identity in DB Connect.

1. Select **New Identity** under **Explorer > Identities**.
2. Enter **Identity Name**, **Username**, **Password**, and then click **save**.
   - **Username**: Enter the username of your Kerberos account. If you don't select **Use Windows Authentication Domain?**, you have to append `@<DOMAIN>` at the end of the username, e.g. `Administrator@<DOMAIN>`
   - **Password** and **Confirm Password**: Enter the password of your Kerberos account.
   - **Use Windows Authentication Domain?**: If you select it, you have to enter the `<DOMAIN>` in **Windows Authentication Domain** field, then you don't have to append `@<DOMAIN>` at the end of the **Username**.

   **Note:** You can add multiple identities if you need to use the different users to do the Kerberos authentication.

5. Finally, create a new connection in DB Connect as you normally would, keeping in mind the following:
   - **Database Types**: Be sure to choose **MS-SQL Server Using MS Generic Driver with Kerberos Authentication** from the popup menu.
JDBC URL Format: Once you've entered all the necessary connection information, add the following to the JDBC URL string to enable DB Connect to use the Kerberos authentication you just set up:

- integratedSecurity=true
- authenticationScheme=javaKerberos

After you’re finished, the field should contain the following:

jdbc:sqlserver://<host>:<port>;databaseName=<database>;selectMethod=cursor;integratedSecurity=true;authenticationScheme=javaKerberos

Note: To debug Kerberos authentication, set the following option in JVM Options under the Settings tab:
-Dsun.security.krb5.debug=true

Multiple SQL Server instances

If you have multiple instances of Microsoft SQL Server installed on your server, you will need to edit the JDBC connection string to add a parameter that explicitly references the instance you want to contact.

1. Follow the instructions in "Override db_connection_types.conf" to make a copy of the db_connection_types.conf file in the local directory and copy the stanza for the Microsoft SQL Server driver you’re using into the file.
2. Edit the jdbcUrlFormat or jdbcUrlSSLFormat (if you're connecting using SSL) setting by appending it with the following: ;instanceName=
3. Set the instanceName parameter to the name of the instance you want to connect to. For example:
   jdbc:sqlserver://dbx-sqlserver.mydomain.com:1433;databaseName=master;instanceName=test
4. Save and close the file, and then Reload the driver under Settings>Drivers

After you add the database driver, continue with either the single server or distributed deployment instructions. You will be able to verify whether the database driver was installed successfully during DB Connect setup. If you've already set up DB Connect and are adding a new database, click Settings in the top navigation bar and then the Driver tab to view the driver status. If you have trouble, see "Troubleshoot driver connections."

Sybase ASE, SAP/Sybase SA, and SAP/Sybase IQ

Follow these instructions to download and install the jConnect for JDBC driver for Sybase Adaptive Server Enterprise (ASE), SAP/Sybase SQL Anywhere, and
SAP/Sybase IQ:

1. Go to the SAP software downloads page and log in.
2. Search for and download the jConnect package.
3. Expand the file you just downloaded and locate the `jconn4.jar` file inside the `classes` directory.
4. Copy or move the `jconn4.jar` file to the
   `$SPLUNK_HOME/etc/apps/splunk_app_db_connect/drivers` directory
   (`%SPLUNK_HOME%\etc\apps\splunk_app_db_connect\drivers` on Windows hosts).
5. **Reload** the driver under **Settings>Drivers**.

Though you can also install the open source jTDS driver to connect to Sybase Adaptive Server Enterprise (ASE), the jTDS driver should not be used in production deployments of DB Connect.

**Spark SQL**

Your Spark instance must be running the Thrift JDBC/ODBC service before Splunk will be able to connect to it. Follow these instructions to install the Simba Spark JDBC driver:

**Note:** SparkSQL support requires Thrift server setup for JDBC
http://spark.apache.org/docs/latest/sql-programming-guide.html#running-the-thrift-jdbcodbc-server

1. Go to the Spark JDBC Driver page on the Simba website.
2. Click and download the ZIP file for the latest version of the driver. You can download for 30 days free trial or purchase it.
3. Expand the `Simba_Spark_JDBC_Desktop.zip` file you just downloaded.
   There are two zip file in the `Simba_Spark_JDBC_Desktop.zip` folder, expand `SimbaRTU_SparkJDBC41_Client_1.0.2.1004.zip`.
4. Copy all the `SparkJDBC41.jar` file to
   `$SPLUNK_HOME/etc/apps/splunk_app_db_connect/drivers` and the other .jar files under
   `$SPLUNK_HOME/etc/apps/splunk_app_db_connect/drivers/SparkJDBC41-libs`.
5. Copy your Spark JDBC driver license file to the
   `$SPLUNK_HOME/etc/apps/splunk_app_db_connect/drivers` directory.
6. **Save and restart RPC server** under **Settings > General Settings**.

**Teradata**

Follow these instructions to install the Teradata JDBC Driver:
1. Go to the Teradata JDBC Driver page on the Teradata website.
2. Click the link to download the ZIP or TAR file for the latest version of the driver. You need to log in with your Teradata user account.
3. Expand the file you just downloaded.
4. From inside the TeraJDBC_... directory, copy or move the two .JAR files (terajdbc4.jar to the
   $SPLUNK_HOME/etc/apps/splunk_app_db_connect/drivers and
tdgssconfig.jar to the
   $SPLUNK_HOME/etc/apps/splunk_app_db_connect/drivers/terajdbc4-libs)
directory.
5. **Reload** the driver under **Settings>Drivers**.

For more information, including how to use the tdgssconfig.jar file, see the readme.txt file inside the TeraJDBC_... directory, or the Teradata JDBC Driver Reference.

**Oracle**

Follow these instructions to install the Oracle JDBC Driver:

1. Go to the Oracle JDBC Driver Downloads page.
2. After you have downloaded the correct driver for your database, copy the .JAR driver file to the
   $SPLUNK_HOME/etc/apps/splunk_app_db_connect/drivers directory
   (%SPLUNK_HOME%/etc/apps/splunk_app_db_connect/drivers on Windows hosts). If you want to use ojdbc7 to parse XML data type, add
   xmlparserv2.jar as a dependency
3. **Reload** the driver under **Settings>Drivers**.

For users of Oracle 11g, the SSL_DH_anon_WITH_3DES_EDE_CBC_SHA,
SSL_DH_anon_WITH_RC4_128_MD5, and SSL_DH_anon_WITH_DES_CBC_SHA cipher
suites are disabled by default in Java 8. To allow these cipher suites, see the
Test or Revert changes to Oracle's JDK and JRE Cryptographic Algorithms
section of the Java documentation.

**Connect to Oracle using SSL**

You can connect to an Oracle database using Secure Sockets Layer (SSL) 3.0 (TLS) in three ways:

- Without using SSL authentication: Neither client (DB Connect) nor server verifies each other’s certificate authority (CA).
- Using one-way SSL authentication: The client verifies the server’s CA.
• Using two-way SSL authentication: Both client and server verify each
other's CA.

If you are using one-way or two-way authentication, you will need to have set up an Oracle wallet on the server. Oracle wallets store credentials for connecting to Oracle databases. An Oracle wallet is not required on the client if you're not using SSL authentication.

The basic steps for setting up one of these SSL connections are:

1. **Configure Oracle wallets:**
   1. Create and configure a server wallet.
   2. Create and configure a client wallet.
   3. Enable the auto-login feature.

2. **Enable SSL and configure settings on the Oracle database server:**
   1. Set the server's auto-login Oracle wallet location in the `sqlnet.ora` and `listener.ora` files.

3. **Configure DB Connect:**
   1. Copy JDBC drivers to the appropriate DB Connect directory.
   2. Create a database connection using the correct JDBC URL.
   3. Specify the wallet location in your connection's stanza within the `db_connections.conf` file.

**Configure Oracle wallets**

First, create and configure standard wallets for both the server and client using Oracle Wallet Manager, and enable the auto-login feature. Do one of the following:

- Follow the instructions in 9.3 How to Create a Complete Wallet: Process Overview, within Chapter 9, Using Oracle Wallet Manager, in the *Oracle Database Advanced Security Administrator’s Guide*.
- To use the Wallet Manager's `orapki` command-line utility instead of the Wallet Manager UI, see Appendix F, "orapki Utility."

Make a note of the location of your Oracle wallets, particularly if you changed the default location.

After following the appropriate set of Oracle instructions, you will have created your Oracle wallets, imported the appropriate certificates into your wallets, and set the auto-login feature for your wallets. Be sure that, if you are setting up either one-way or two-way authentication, you have a wallet on both the DB Connect machine and the Oracle server. The DB Connect machine's wallet
should contain the server wallet’s CA.

Enable SSL and configure settings on the Oracle database server

Next, enable and configure SSL on the Oracle database server by adding the path to your server wallet to the sqlnet.ora and listener.ora files:

1. On your Oracle database server, navigate to the .../network/admin directory. For example:
   
   `/u01/app/oracle/product/11.2.0/dbhome_1/network/admin`

2. Edit the sqlnet.ora file and add the following, changing the DIRECTORY path to the path to the server wallet:
   
   ```
   WALLET_LOCATION=(SOURCE=(METHOD=FILE)(METHOD_DATA=(DIRECTORY=/server/wallet/path/)))
   ```

3. In the same file, set SSL_CLIENT_AUTHENTICATION to FALSE if you’re either connecting with no SSL authentication or with one-way SSL authentication. Set SSL_CLIENT_AUTHENTICATION to TRUE if you’re connecting with two-way SSL authentication. For more information, see Configuring Secure Sockets Layer Authentication in the Oracle Database Advanced Security Administrator’s Guide.

4. In the same directory, edit the listener.ora file. Add the same wallet location and set SSL_CLIENT_AUTHENTICATION in the same way.

5. Save and close both files.

Set up the SSL connection using a cipher suite:

- For no SSL authentication, use an anonymous Diffie-Hellman key exchange.
- For one-way or two-way SSL authentication, use a cipher suite like RSA or standard DH.

Configure DB Connect and enable an SSL connection on the client

Now, configure DB Connect. Start by copying the JDBC drivers to the appropriate DB Connect directory:

1. On the Oracle server, navigate to $ORACLE_HOME/jlib.
2. Using your network or removable media, copy ojdbc6.jar file to the $SPLUNK_HOME/etc/apps/splunk_app_db_connect/drivers directory ($%SPLUNK_HOME%\etc\apps\splunk_app_db_connect\drivers on Windows hosts) on the machine running DB Connect, and then copy the following .jar files under $SPLUNK_HOME/etc/apps/splunk_app_db_connect/drivers/ojdbc6-libs directory
Next, set up a new identity, and then a new connection:

1. Follow the instructions in Create and manage database connections to set up a new connection.
2. Use your server information to set up the connection, and be sure to select the Enable SSL checkbox.
3. When you get to the JDBC URL Format field, click the "Click here" link beneath the field to edit the JDBC URL.
4. In the JDBC URL Format field, paste the following:
   
   ```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=servername)(PORT=2484))(CONNECT_DATA=(SERVICE_NAME=servicename)))
   ```

5. Save the connection.
6. Go to $SPLUNK_HOME/etc/apps/splunk_app_db_connect/local, and edit the db_connections.conf file.
7. Find the connection stanza with the name you gave it, and edit the connection_properties argument. Here is an example:
   ```
   connection_properties =
   {
   "oracle.net.authentication_services": "(TCPS)",
   "oracle.net.ssl_cipher_suites": "SS",
   ...
   }
   ```
   Connection_properties is in JSON format, it represents JDBC connection properties. The properties you defined here need to be consistent with what you configured in Database. See JDBC with Oracle 12c Database for more information.
8. Save and close the db_connections.conf file.

AWS RedShift, Informix, and PostgreSQL

For all other supported databases, follow these instructions:

1. Download your JDBC database driver:
   - If you don’t already have a JDBC driver for your database, see the supported database matrix and click the link for your database. Download the JAR driver file for your database.
   - If you already have a JDBC driver for your database, or you are using a different driver from what is listed in the supported database matrix, locate the .JAR driver file.
2. After you have downloaded the correct driver for your database, copy the .JAR driver file to the

\$SPLUNK_HOME/etc/apps/splunk_app_db_connect/drivers directory

(\$SPLUNK_HOME%/etc\apps\splunk_app_db_connect\drivers on Windows hosts).

3. **Reload** the driver under **Settings>Drivers**.

**Install drivers for other databases**

You can add custom support to Splunk DB Connect for any database that has a JDBC driver, even if it doesn't appear in the supported database matrix.

**Notes:**

- Connecting to a database that is not listed in the supported database matrix is not supported by Splunk Support.
- At a minimum, Splunk DB Connect supports querying custom database connections. For some custom database connections, certain query-related features may not work.

Installing a custom database is a multi-step process:

1. **Download and install the JDBC driver file.**
2. **Add the custom database to db_connection_types.conf.**
3. **Troubleshoot or disable connection validation, if necessary.**

**Download and install the JDBC driver file**

Download the JDBC driver for the database you want to add, and copy the .JAR file to the \$SPLUNK_HOME/etc/apps/splunk_app_db_connect/drivers directory

(\$SPLUNK_HOME%/etc\apps\splunk_app_db_connect\drivers on Windows hosts).

**Add the custom database to db_connection_types.conf**

When you add a custom database connection that Splunk DB Connect does not support by default, you must create a stanza to define the database connection in a copy of db_connection_types.conf under

\$SPLUNK_HOME/etc/apps/splunk_app_db_connect/local

(\$SPLUNK_HOME%/etc\apps\splunk_app_db_connect\local on Windows hosts), for example

```
displayName = $your database name$
```

51
serviceClass = com.splunk.dbx2.DefaultDBX2JDBC
jdbcDriverClass = $JDBC driver class$
jdbcUrlFormat = $JDBC URI Format$
ui_default_catalog = $database$

For more information, see Configuration file reference.

Database connection validation

Each time DB Connect uses a database connection, it tries to validate that the database connection is actually working. If validation fails, you might see an error message, such as "ValidateObject failed".

DB Connect uses these two methods to validate a connection:

1. If a testQuery is specified in db_connection_types.conf, DB Connect executes that query, and receives a response that validates that the connection is working.
2. If testQuery is not specified, DB Connect uses the Java method connection.isValid(), and relies on the JDBC driver to answer. Some JDBC drivers do not implement this API call. (For instance, Apache Derby was built against Java 1.5, where JDBC doesn't have the method isValid.) The workaround is to specify a manual testQuery, such as SELECT 1.

After you add the custom database driver, continue with either the single server or distributed deployment instructions.

Enable SSL for your database connection

DB Connect has built-in support for connecting via SSL to several supported databases. Though other supported databases may support SSL connections, DB Connect support for SSL means that Splunk has tested SSL for that database type and supports connecting over SSL using DB Connect.

If you want to deploy DB Connect in Splunk Cloud. You must enable SSL connection for your database. See supported database matrix for the database supported for cloud deployment.

DB Connect will detect whether it supports SSL for your database type,

- If DB Connect supports SSL connections for your database type, enabling an SSL connection is easy. When you create a new database connection, select the Enable SSL checkbox.
- If DB Connect does not natively support SSL for your database type, you
cannot select the Enable SSL checkbox in connection settings, it is grey out. However, you can add in SSL support by selecting Edit JDBC URL and editing the URL. Be aware that Splunk cannot certify that databases for which DB Connect does not have native support for SSL will connect via SSL correctly. Splunk Support will not help you troubleshoot such connections.

Use a different default driver for your database

You can change the driver that DB Connect uses for your database type. This can be useful if you want to use a custom driver to connect to your database. To change the driver, you edit the db_connection_types.conf file.

First, get the JDBC driver vendor’s Java driver class name. For example, the class name of the Microsoft JDBC Driver for SQL Server is com.microsoft.sqlserver.jdbc.SQLServerDriver. Once you've found the correct Java class name, do the following:

1. Using a text editor, open the db_connection_types.conf from within $SPLUNK_HOME/etc/apps/splunk_app_db_connect/default/ (%SPLUNK_HOME%/etc\apps\splunk_app_db_connect\default on Windows hosts).
2. Find the stanza for the database type for which you want to configure a custom driver, select it, and then type Ctrl-C or Command-C to copy it.
3. Create a new db_connection_types.conf file (if one doesn't already exist) in $SPLUNK_HOME/etc/apps/splunk_app_db_connect/local/ (%SPLUNK_HOME%/etc\apps\splunk_app_db_connect\local on Windows hosts). If the file is a new file, open it and type [local] and then two new lines.
4. Paste in the database stanza you copied from the default db_connection_types.conf file.
5. Change the entry next to jdbcDriverClass to match the Java class name for your custom driver.
6. If you want to retain the ability to choose the original database driver, change the name of the stanza and update the displayName attribute to differentiate it from the original driver.
7. Restart Splunk Enterprise.

Install and configure Splunk DB Connect on a single instance Splunk platform deployment
This topic shows you how to install and configure Splunk® DB Connect on a single instance (the indexer and Splunk Web both running on the same system). Ensure you meet all prerequisites before installing.

Install the Splunk DB Connect

To install Splunk DB Connect, use Splunk Web:

1. Log in to Splunk Web and go to Apps > Find More Apps.
2. Use the search box to find db connect.
3. Click the green Install button next to Splunk DB Connect.
4. Click Restart Splunk.

You can also download the app package from Splunkbase and then install it offline:

1. Download Splunk DB Connect and save it to a temporary location that you can access from your Splunk Enterprise instance.
2. Log in to Splunk Web, go to Apps > Manage Apps, then click Install app from file.
3. Navigate to the package that you downloaded—splunk_app_db_connect-<version>.tgz—and click Upload.
4. Click Restart Splunk.

You can also install DB Connect by copying its directory into your Splunk Enterprise apps directory:

1. Download Splunk DB Connect and save it to a temporary location that you can access from your Splunk Enterprise instance.
2. Un-tar the download.
3. Move the splunk_app_db_connect directory into $SPLUNK_HOME/etc/apps.
4. Restart Splunk Enterprise.

Install database drivers

Before setting up Splunk DB Connect, install a JDBC driver for your database. See Install database drivers. You can proceed without having first installed database drivers, but you need to do so before you can use DB Connect to connect to your database.
Set up Splunk DB Connect

Before you can start using Splunk DB Connect, you need to set it up.

When you open Splunk DB Connect for the first time, you see the following screen:

Click Setup to access the general settings page. See General Settings for more detailed instruction on how to configure the settings of this page.

**Note:** When you install Splunk DB Connect and enable SSL for the RPC server, DB Connect generates an RPC server SSL certificate with a validity period of two years at $SPLUNK_HOME/etc/apps/splunk_app_db_connect/certs/default.jks. Periodically check the validity of the certificate by running the following command: $JRE_Installation_Path/bin/keytool -list -v -keystore $SPLUNK_HOME/etc/apps/splunk_app_db_connect/certs/default.jks

To renew the certificate, delete the default.jks file just before or after it is set to expire. DB Connect regenerates the certificate.

Install and configure Splunk DB Connect on a distributed Splunk platform deployment

To use Splunk DB Connect in a distributed search environment, including search head clusters, you must install the app on search heads and heavy forwarders.

- DB Connect does not allow you to run scheduled inputs and outputs on a search head cluster from DB Connect 3.x.x. If you want to perform the scheduled tasks, you must run them on a heavy forwarder.
- In a distributed environment, the heavy forwarder will need to be able to search your deployment’s indexers in order to output to the DB. See Deploy a distributed search environment in the Distributed Search manual.
to learn how to set up distributed search on your deployment's heavy forwarders.
• DB Connect 3.x.x does not support resource pooling. See migrate DB Connect 2.x.x to DB Connect 3.x.x on distributed deployment.
• DB Connect is incompatible with deployment server. Do not attempt to distribute DB Connect using deployment server.
• DB Connect is incompatible with search head pooling, which was deprecated with Splunk Enterprise 6.2.0.

Deployment topologies

Design your deployment based on architecture and performance considerations. The list below specifies the typical deployment topologies in which you can install Splunk DB Connect. In all cases, you should install DB Connect on a dedicated search head.

• Single search head, multiple indexers, load-balanced forwarders
• Multiple search heads, multiple indexers, load-balanced forwarders
• Indexer cluster, single search head
• Search head cluster, multiple independent indexers, load-balanced forwarders

For general information about configuring the topology components described in this section, see Distributed Splunk Enterprise overview, or any of the following topics:

• Single search head: Deploy a distributed search environment, Add search peers to the search head
• Search head clusters: About search head clustering, Search head clustering architecture
• Multiple indexers: Indexers in a distributed deployment
• Indexer clusters: About indexer clusters and index replication, The basics of indexer cluster architecture
• Load-balanced forwarders: About forwarding and receiving, Set up load balancing

 Deploy DB Connect on search head clusters

You can deploy Splunk DB Connect in a search head clustering environment. To install, use the deployer to distribute DB Connect to all of the search head cluster members. Be aware that you must use the cluster deployer, not Deployment Server, to distribute DB Connect to search head cluster members.

For more information about configuring search head clusters, see Configure the
If you have not already done so, deploy and configure a search head cluster.

1. Install the database driver(s) for the database(s) you want to connect to with DB Connect. Access the instructions on the Install database drivers for details.

2. Install DB Connect on the deployer. Access the instructions on the Single server deployment for details.

3. Set up identities and connections for your database(s).

4. Copy the `splunk_app_db_connect` directory from `$SPLUNK_HOME/etc/apps/` to the `$SPLUNK_HOME/etc/shcluster/apps/` directory on the deployer. Note that this includes all custom configuration files as well as JDBC drivers. Note that `kerberos_client.conf`, `identity.dat` cannot be replicated to other SHC nodes after it's been modified. You need to copy the files manually to other SHC nodes.

5. Deploy the configuration bundle by running the `splunk apply` command on the deployer:

   ```bash
   splunk apply shcluster-bundle -target <URI>:<management_port> -auth <username>:<password>
   ``

   ◊ The `-target` parameter specifies the URI and management port for any member of the cluster, for example, `https://10.0.1.14:8089`. You specify only one cluster member but the deployer pushes to all members. This parameter is required.

   ◊ The `-auth` parameter specifies credentials for the deployer instance.

6. The deployer displays a message that asks you to acknowledge that the cluster members may restart. Click Y to acknowledge.

   For more information about deploying a configuration bundle, see Deploy a configuration bundle.

   For full instructions about how to use the deployer to distribute apps, add-ons, and their configuration bundles, see Use the deployer to distribute apps and configuration updates.

   When you use DB Connect in a search head clustering (SHC) environment, use the deployer to push configuration changes to SHC members. If you prefer to use the DB Connect UI or modify .conf files and then replicate configuration to SHC members, restart Splunk Enterprise on SHC members after you have updated
them with the new configuration. There are three reasons why you must restart SHC members after updating their configuration:

- When you make a configuration change on a search head, such as a change to the RPC server port, Splunk Enterprise replicates changes to the SHC members automatically. However, the SHC members may still use the old configuration until you restart them.
- Splunk Enterprise automatically replicates SHC for changes you make to most of the DB Connect-specific settings and objects through the REST API. Splunk Enterprise does not automatically replicate changes you make by editing .conf files on a search head. To ensure that Splunk Enterprise replicates all your changes, and to replicate any changes you made by editing .conf files, you must restart the search head on which you made the change.
- Splunk Enterprise does not automatically replicate changes you make by editing kerberos_client.conf and identity.dat files. You need to manually replicate the files to other SHC node.

A note about indexes

When you create a database input, you must select the index you want to index the data your database receives. When you choose an index, by default you must choose one of the indexes on that instance of Splunk Enterprise. This means that you cannot choose an index that you have configured on a search peer but not distributed to the rest of the deployment.

To select an index that you have not configured on, for instance, a forwarder or search head that is running DB Connect, you can create or edit an indexes.conf file, and then distribute it using Deployment Server. Although you cannot distribute DB Connect configuration using a Deployment Server, you can distribute indexes.conf files.

To configure peer indexes in a distributed deployment, follow the instructions in Configure the peer indexes in an indexer cluster. First, you edit the indexes.conf file, and then you distribute it to peers. This practice ensures that you configure search heads and forwarders to send all logs to the indexer tier, which prevents this distribution of indexes.conf from causing Splunk Enterprise to create local indexes on search heads and forwarders.

Once you have distributed the configuration, applications like DB Connect know which indexes exist to validate configuration.
Check DB Connect installation health

Beginning with version 3.1.0, DB Connect provides health checks for the Splunk Access and customize health check to help you diagnose common issues.

Note:

♦ The Monitoring Console is only visible to users with the Splunk Enterprise admin role.
♦ The health check feature is available with Splunk version 6.5 and above.

To use the health check, go to Settings of your Splunk instance and click Monitoring console. On the monitoring console page, click Health Check tab. There are seven preconfigured health check items provided by DB Connect. You can check the health of these items by selecting DB Connect and clicking Start, or leave the filters blank to run all available health checks.

The Splunk DB Connect health check items are:

- **DB Connect connection configuration.**
  Checks that database connection configurations (identities and connections) are syntactically correct and that all dependencies between stanzas can be resolved.

- **Data lab configuration.**
  Checks that data access configurations (inputs, outputs, lookups) are syntactically correct and that all dependencies between stanzas can be resolved.

Note:

◊ Configuration entries with incorrect syntax will not appear in the user interface, and must be corrected via configuration files.
• **JDBC driver installation.**
  Checks that connections configured in DB Connect have the corresponding JDBC driver and version installed correctly.

• **DB Connect file permission.**
  Checks the existence and permission settings of the folders that the DB Connect processes will need to read and write: DB Connect application folder, checkpoint folder and log folder.

• **JVM installation.**
  Checks the existence and version of the JVM that DB Connect is configured to use to run individual commands and the Task Server.

• **Java server configuration.**
  Checks the JVM bootstrap conditions of the DB Connect Task Server.

• **Kerberos environment configuration.**
  Checks the configuration file for Kerberos is correctly configured to support Microsoft Active Directory authentication. Note that this item is only performed on Linux servers when at least one database connection uses Kerberos.

After the health check process is done, the result summary (how many succeeds, how many errors or warning messages) will be listed on the page. You can expand each health check item to see the detailed result.

**Example 1:** After checking all the health check items, all the health check items are succeeded.

**Example 2:** After checking all the DB Connect health check items, there are some issues in Data lab configuration and JDBC driver installation. You can expand the health check item JDBC driver installation, it shows the error messages and suggested action provided by Splunk. You can also view the details of the issue in the Result table.
Besides installation health check, DB Connect also provides pre-built panels for you to monitor DB Connect input health, input performance and the connection health with database. See Monitor database connection health for details.
Configure and manage Splunk DB Connect

Configure Splunk DB Connect settings

This topic explains how to setup DB Connect before you use it to access databases.

General tab

1. Access Configuration > Settings.
2. The General Settings tab contains settings related to your Java Runtime Environment (JRE) and Task Server. Change any settings you wish. When DB Connect 3.x prompts you to input the JRE Installation path, be sure to input the complete JRE filepath. Refer to Prerequisites for further details.
3. Click Save to restart the Task Server's Java process. You do not need to restart Splunk Enterprise for changes on this page to take effect.

JRE Installation Path (JAVA_HOME)

DB Connect attempts to detect the JAVA_HOME environment variables as the JRE installation path if possible. You can change it to the Java home path you want to use for DB Connect.

JVM Options

This field lists Java Virtual Machine parameters. For more information about available JVM parameters, access Oracle's JVM documentation.

DB Connect saves the options in this field in $SPLUNK_HOME/etc/apps/splunk_app_db_connect/jars/server.vmopts.
Task Server Port

This field contains the port number of the task server. DB Connect uses an RPC server to manage communications with the Java subsystem. The default port is 9998, but you can use any unassigned, unused port on your system.

Drivers tab

This tab contains a list of supported database connection types, along with install status and version number information.

If there is no JDBC driver for a connection type, the Installed column shows an X icon and the word "No". By default, there are no drivers.

1. To install a JDBC driver, follow the instructions in "Install database drivers."
2. Once you have moved the appropriate JAR file to the $SPLUNK_HOME/etc/apps/splunk_app_db_connect/drivers directory, click the Reload button.

If you have installed a JDBC driver and it still does not register:

- Verify that you have installed the driver properly by repeating the steps in "Install database drivers."
- Access the "Supported databases matrix" to verify that DB Connect supports the driver and its version. If necessary, download a newer version of the driver.
- Follow the applicable steps in "Troubleshoot driver connections."

When DB Connect detects a driver, it displays a green checkmark icon and the word "Yes" next to the database, as shown in the screen shot below. It also displays the version information of the driver.
Logging levels

Versions 3.0.x and above of Splunk DB Connect provides graphical configurations of the logging levels of DB Connect. DB Connect logs activity to files in $SPLUNK_HOME/var/log/splunk and automatically indexes to _internal. The relevant log files for DB Connect are:

- splunk_app_db_connect_server.log
- splunk_app_db_connect_job_metrics.log
- splunk_app_db_connect_dbx.log
- splunk_app_db_connect_audit_server.log

By default, DB Connect logs all SQL queries it executes at the INFO level. You can enable other logging levels using the UI below, or by adjusting the dbx_settings.conf file at splunk/etc/apps/splunk_app_db_connect/default/dbx_settings.conf.

Usage Collection tab

This tab contains an option to grant permission for Splunk to collect statistics about how you use DB Connect. See sending usage data to Splunk DB Connect to learn more about the data that DB Connect sends to Splunk.

Configure Splunk DB Connect security and access controls

The role-based user access controls in Splunk Enterprise enable you to set up access permissions for identity and connection objects, as well as capabilities for inputs, outputs, and lookups in Splunk DB Connect. You can grant a user global access to all DB Connect features and available database connections, or limit a
user's access to only specific database connections or capabilities.

Before using DB Connect, the logged-in user must have the ability to write to the
$SPLUNK_HOME/var directory (%SPLUNK_HOME%\var on Windows hosts) and to
$SPLUNK_HOME/etc/apps/splunk_app_db_connect
($SPLUNK_HOME/etc/apps/splunk_app_db_connect on Windows hosts) and its
sub-directories. For more information, see Use access control to secure Splunk
data.

Roles

When thinking about permissions in DB Connect, familiarize yourself with the
Splunk Enterprise role-based user access system. You can create Splunk
Enterprise users with passwords and assign them to roles. Roles determine the
access and permissions of any user you assign to that role, including whether a
user can access DB Connect. Roles determine users’ capabilities for many
Splunk Enterprise tasks, including DB Connect tasks.

When you install DB Connect, it adds two new roles to Splunk Enterprise:
db_connect_admin and db_connect_user. In addition, Splunk Enterprise gives
DB Connect capabilities to its admin role.

- The db_connect_user role has 11 capabilities and inherits from the user
  role. Its capabilities involve reading DB Connect objects.
- The db_connect_admin role has 31 capabilities and inherits from the
db_connect_user role. Its capabilities involve reading and writing DB
  Connect objects, plus actions involving the task server.
- The existing Splunk Enterprise admin role automatically gets all DB
  Connect-specific capabilities when you install DB Connect.

To set or view the capabilities of a specific role from within Splunk Enterprise, go
to Settings > Access controls > Roles. From here you can also create new
roles with specific capabilities.

Permissions

You set permissions when you define the DB Connect identities and
connections. An identity object contains encrypted database credentials. A
connection object contains the necessary information for connecting to a remote
database.

Use the Permissions table on the New Identity and New Connection setup
pages to specify the Splunk Enterprise roles that have access to the identity or
connection.

- **Read access** to an object means that Splunk Enterprise roles will be able to use the object.
- **Write access** to an object means that Splunk Enterprise roles will be able to use and modify the object.

By default, the Splunk Enterprise "admin" and "db_connect_admin" roles have read-write access to objects such as identities or connections, the "db_connect_user" role has read access. All other roles have no access.

The permissions you set when you create a new identity or a new connection are related to Splunk Enterprise roles, and are not related to database permissions. Because identities store encrypted database credentials, the level of database access that an identity has is directly related to the user account that you store in the identity. When you use an identity to connect to your database, your access to that database is limited to the database access level of the user you have stored in that identity.

For example, if you added the credentials of user1 to identity1, and user1 only has access to table abc on the database and not to table xyz, a connection that uses identity1 only has access to table abc, and not xyz, on the database. That means that any database input, output, or lookup using that connection also only has access to just table abc on that database.

Therefore, you must consider which database credentials to store within a DB Connect identity. You may wish to create DB Connect-specific users on the database who have access to only the database tables you want to access with Splunk Enterprise, and then assign those users to your identities.

**Capabilities**

Every role in Splunk Enterprise has capabilities. In DB Connect, permissions define access for identities and connections, but capabilities define access for DB Connect-specific modular inputs, which include inputs, outputs, and lookups.

By defining the capabilities a role has, you define what that role can do with the inputs, outputs, and lookups you have created. For instance, the **db_connect_user** role can use inputs, outputs, and lookups, but the **db_connect_admin** role includes the additional capabilities that enable it to edit inputs, outputs, and lookups (specifically, "edit_modinput_mi_input," "edit_modinput_mi_output," and "edit_modinput_mi_lookup").
Read-only connections

Splunk DB Connect supports the **readonly** JDBC attribute which can restrict connections to read-only mode. This setting alone does not guarantee that users connecting via DB Connect will not be able to write to the database.

When you create a new connection, select the **readonly** checkbox to restrict users to using `SELECT` statements with the database. The **readonly** checkbox cannot always guarantee read-only access; the database driver ultimately allows or prevents changes.

If you use the read-only option, ensure that, on the database itself, you limit the user to read-only access. To determine if you database supports read-only access, read Supported databases or check your database vendor's documentation.

Create and manage identities

An **identity** object contains database credentials. It comprises the username and password that Splunk DB Connect uses to access your database.

Note that your database credentials and are not the same as your Splunk Enterprise credentials. When you configure a DB Connect identity, you use the Splunk Enterprise role-based access control system to define access to the identity.

Create an identity

1. From within Splunk DB Connect, access the **Configuration > Databases > Identities** tab and click **New Identity**.
2. Complete the following fields:
   - **Identity Name**
   - **Username**: Enter the name of the database user you want to connect as.
Note: Ensure that the database user has sufficient access to the data you want to search. For example, you might create a database user account whose access is limited to the data you want Splunk Enterprise to consume.

- **Username**: Enter the password for the user you entered in the Username field.

- **Password**: Enter the password for the user you entered in the Username field.

Note: Your password is encrypted. DB Connect requires this field to connect to your database.

- **Use Windows Authentication Domain**: This setting is for identities that connect to Microsoft SQL Server databases. Enable this setting if you need to specify a Windows Authentication Domain.

- **Windows Authentication Domain**: If you selected the Use Windows Authentication Domain checkbox, enter the domain in this field. For more information about connecting to Microsoft SQL Server databases using Windows Authentication, see "Microsoft SQL Server."

3. In the Permissions tab, update the Splunk Enterprise permissions for this identity. For more information, see Permissions.

4. Click Save.

**Edit Identities**

To see a list of the defined identities, go to Configuration > Databases > Identities. To see a list of identities, reference the the table below.

To edit an identity, click its name. You can edit the following attributes of an identity, except where noted:

- **Status**: Disable an identity by clicking Disable. You cannot disable an identity if any connections are using it. In that case, DB Connect displays an error message that reads *Can not disable this identity!*

- **Identity Name**: Not editable. To change the name of an identity, clone it, give the clone the name you want, and then delete the original identity.

- **Username, Password, Use Windows Authentication Domain? checkbox and Windows Authentication Domain**: If you selected the Use Windows Authentication Domain checkbox, enter the domain in this field. For more information about connecting to Microsoft SQL Server databases using Windows Authentication, see "Microsoft SQL Server."

- **Permission**: The Permissions table is where you specify the Splunk Enterprise roles that have read, write, or no permissions to the identity. By default, the Splunk Enterprise admin and db_connect_admin roles have read-write access to a new identity, the db_connect_user role has read...
access, and all other roles have no access.
♦ Read access means that Splunk Enterprise roles are able to use the identity.
♦ Write access means that Splunk Enterprise roles are able to use and modify the identity.

Create and manage database connections

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

Create a database connection

To create a new connection:

1. From within Splunk DB Connect, click the Configuration > Databases > Connections tab.
2. Click New Connection.

   **Note:** If you have not yet created an identity, the New Identity window appears. Create a new identity, and then you can create a new connection.

3. On the New Connection page, complete the following fields:
   ♦ **Connection name**
   ♦ **Identity**: Choose the identity you want to use with this connection.
   ♦ **Connection Type**: A list of supported databases. Choose the type of database to which you’re connecting.

   **Note:** This list contains all supported databases, regardless of whether you installed their drivers. You must first install the database driver for the database type you want to use. Choosing a database from this list without installing the corresponding driver will not work. For information about the Microsoft SQL Server
options listed here, see "Microsoft SQL Server."

♦ **Timezone**: If you want to convert data of date and time types read from the database into the Splunk server’s local time zone, specify the source database time zone for the conversion. When the time zone is set, you have two time zone conversion options depending on the **localTimezoneConversionEnabled** setting in `db_connections.conf`:

◊ When **localTimezoneConversionEnabled** is undefined or set to false, the system will only convert index time values read from table columns in the source database into the local time zone. This conversion option only applies to inputs.

◊ When **localTimezoneConversionEnabled** is set to true, the system will convert all date and time data type (datetime, time, date, timestamp) values into the local time zone except source datetime values that already include time zone information (e.g., `TIMESTAMP WITH TIMEZONE`). This conversion option applies to inputs, dbxqueries, and dblookups.

If you leave the **Timezone** field blank, the system will assume that the source database time zone and Splunk server’s local time zone are the same and will read and index the date and time data as is.

**Example**

<table>
<thead>
<tr>
<th>Timestamp in database</th>
<th>Database timezone</th>
<th>Splunk Server (JVM) timezone</th>
<th>Indexed timestamp value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Without timezone conversion</strong></td>
<td>2006-02-15 04:34:33</td>
<td>UTC</td>
<td>Asia/Shanghai (GMT+8)</td>
</tr>
<tr>
<td><strong>With timezone conversion</strong></td>
<td>2006-02-15 04:34:33</td>
<td>UTC</td>
<td>Asia/Shanghai (GMT+8)</td>
</tr>
</tbody>
</table>

**Note:**

- Note that if the column in your database contains timezone information (e.g. column with a `TIMESTAMP WITH TIMEZONE` type), the timezone you set here will be ignored.
- The timezone setting defaults to JVM time zone. If there is no JVM time zone settings, the
time zone of your operating system will be used.

- For MySQL database driver, you need to set useLegacyDatETIMECode setting to false in the JDBC URL if you want to use the timezone setting.

**JDBC URL Settings**

- **Host**: Enter the address, or host, of the database.
- **Port**: (Optional.) Enter the port number of the database. You don’t need to enter a port number here if your database is using its default port.
- **Default Database**: Enter the default database or catalog name for the database type you chose. The usage and meaning of this parameter varies between database vendors, so check your database vendor's documentation. For more information, see supported databases matrix.
- **Enable SSL**: Select this checkbox to enable Secure Sockets Layer (SSL) encryption for the connection. SSL support is not available for all connection types. For further information, see supported databases matrix and Enable SSL for your database connection. To find out how to connect to Oracle using SSL for encryption, see Connect to Oracle using SSL (for encryption only).
- **JDBC URL Preview**: A Java Database Connectivity (JDBC) Uniform Resource Locator (URL) is a URL that encodes all the necessary information for connecting to your database. The JDBC URL Preview field is not editable by default, but will populate, using placeholder values, with the correct URL format according to the database type you have chosen.
- **You can manually edit the URL format by selecting Edit JDBC URL.** When you select this field, the JDBC URL Preview will become editable. This is useful if you need to add customized JDBC URL parameters to the JDBC URL, but is not recommended unless you already know what customizations you want to add. Connection parameters vary among JDBC drivers. Consult your database vendor's documentation for a list of supported parameters and values.

**Note:** DB Connect supports LDAP connection, you need to specify the LDAP URL in JDBC URL field. Consult your database vendor’s documentation on how to generate LDAP URL.
Advanced Settings

♦ Fetch Size: (Optional.) Enter the number of rows to return at a time from the database. If you leave this field blank, it defaults to 300.
♦ Readonly: Select this checkbox to indicate your intention for users to only use `SELECT` statements with the database. Be aware that this cannot always guarantee read-only access. DB Connect will do its best to ensure that no changes are made, but it is the database driver that ultimately allows or prevents changes. If you intend to use the read-only option, ensure that, on the database itself, the user you're connecting as is limited to read-only access. See Read only connections for more details.

4. In the Permissions table, update the Splunk Enterprise permissions for this database connection. For more information, see Permissions.
5. Click Save to save the connection.

Note: If the connection you create is valid, you can save the connection successfully. Otherwise the error message will prompt up, you need to check the configuration of the connection and save again.

Edit connections

Go to Configuration > Databases > Connections to see a list of the defined database connections.
Note: The list of connections that you can see is defined by the permissions that have been set on each connection. For more information, see Permissions.

Connection actions

You can make changes to a connection using the following buttons on the connection page under the Edit tab:

- **Disable/Enable**: Disable/Enable a connection by clicking Disable/Enable here. You cannot disable a connection if any inputs, outputs, or lookups are using it. In that case, this button is greyed out.
- **Edit**: Edit the connection by clicking its name or edit button.
- **Clone**: Creates a copy of the connection. You must give the copy a new name.
- **Delete**: Deletes the connection. You cannot delete a connection if any inputs, outputs, or lookups are using it. In that case, this button is greyed out.
You can also edit the attributes of a connection listed in Create a database connection, except its name. To change the name of a connection, clone it, give the clone the name you want, and then delete the original connection.

Permissions

The Permissions table is where you specify the Splunk Enterprise roles that have read, read-write, or no access to the connection.

- Read access means that Splunk Enterprise roles will be able to use the connection.
- Write access means that Splunk Enterprise roles will be able to use and modify the connection.

By default, the Splunk Enterprise "admin" and "db_connect_admin" roles have write access to a new connection, the "db_connect_user" role has read access, and all other roles have no access.

Override db_connection_types.conf

For fine-grained control over your database connections, you can override the JDBC connection strings for your database driver. The db_connection_types.conf file lists the supported database types, driver parameters, and test queries. To override it, copy the db_connection_types.conf file under $SPLUNK_HOME/etc/apps/splunk_app_db_connect/default to $SPLUNK_HOME/etc/apps/splunk_app_db_connect/local.

You can now fine-tune your database connection by editing its JDBC parameters. If the stanza name in the db_connection_types.conf in local is identical to the name in the same file in default, it will override its connection settings. Consult your JDBC driver vendor’s documentation for exact parameter syntax. The db_connection_types.conf.spec file will also help you understand the individual settings. When you’re done, restart Splunk Enterprise.

Create and manage database inputs

A database input object lets you fetch and index data from a database. Database inputs are what enable Splunk Enterprise to query your database, identify the data to consume, and then tag and index the data. Once you have set up a database input, you can use that in the same way that you use other data input you have defined in Splunk Enterprise.
Splunk DB Connect 3.1.x supports creating inputs using the templates created in Splunk Add-ons. You'll be saved the work of repeatedly recreating basic content of inputs. The templates of the add-on will be listed in the template field of DB Connect. These add-ons include:

- Splunk Add-on for Microsoft SQL Server
- Splunk Add-on for Oracle Database
- Splunk Add-on for McAfee
- Splunk Add-on for Nagios Core

**Create a database input**

You can create a new input from scratch. Additionally, if the add-on is a Splunk Supported Add-on, you can create your new input using a template.

Complete the following instructions to create a database input in DB Connect:

**Note:**

- If you have not yet created an identity or a connection, you must do so before you can create a database input.
- If you create the input by using a template, then to make the supported add-on appear in the **Templates** drop-down in the DB Connect UI, you first need to copy `db_input_templates.conf` from your add-on's default directory to your `splunk_db_connect/local` directory.
- If you create the input by using a template, all the settings from the template will be set for the new input. You can change them based on your needs, but be aware that the changes will be saved to the input you create but not to the template.
- Inputs only support SQL queries such as "select...from...where", not DDL such as "create table..."

To create a new input, click **Data Lab > Inputs** and then **New Input**.

1. On the **Set SQL Query** page, complete the following steps and then click **Next** to go to the **Set Properties** page.
   1. **Choose table.** Choose the database table you want to use with this input.
   2. **Specify SQL query.** Specify a query to run to fetch data from your database.
3. Choose input type. Specify the input type and related settings of this input.

2. On the Set Properties page, complete the following steps and then click Finish.
   1. Basic information. Specify the name, description and the application of this input.
   2. Parameter settings. Configure the fetch size, execution frequency and max row to retrieve of this input.
   3. Metadata. Specify the metadata of this input, the value will be used by Splunk to index your data events.

Choose Table

1. Choose a connection that you want to use for this input from the drop-down list under the Connection field. The drop-down list lists all the connections you have configured in DB Connect, you can also enter the connection name to search the connection you want to use. Once you have select the connection, Splunk DB Connect will try to validate the connection, and will display an error message if it is not able to do so. You cannot continue the new input setup process unless a valid connection is specified.
2. From the corresponding dialog menus, choose the Catalog, Schema, and Table that contain the data you want to pull into Splunk platform.

Specify SQL query

After you choose the table, the corresponding SQL query will be displayed in SQL Editor, you can preview the result of the query. If you need further edit or write your own SQL query, you can write it directly in SQL Editor and click Execute SQL to preview the result. You can make complex SQL statements easier to read by clicking Format SQL.

Note: If you want to use SQL query from template, select the template from the drop-down menu. Be aware that using a template will overwrite the previous SQL you specified.

Note: Inputs only support SQL queries such as "select...from...where", not DDL such as "create table..."

Choose input type

Specify an input type for your query, either Batch or Rising. Then configure the related fields for the input type.
• **Batch.** A batch input invokes the same database query each time the input is run and returns all results.
• **Rising.** A rising input has a column that DB Connect uses to keep track of what rows are new from one input execution to the next.

**Batch input**

A batch input invokes the same database query each time the input is run and returns all results. It does not keep track of whether rows have been added since the last time the input was run. Batch input mode is ideal for unchanging historical data that will be indexed into Splunk once. It can also be useful for re-indexing data that updates through time, such as personnel records or state tables, though this has license impact; lookups may be a better choice.

To create a batch input type,

1. Select **Batch** under **Input Type** field.
2. Choose the **Timestamp** column.

Specify which column contains the timestamp that will be used to order this data in the Splunk index. This value will be used to populate the `_time` variable and is required for indexing time-series data.

• **Current Index Time:** Assigns indexed data a timestamp value that is equal to index time. Specify this option if your data has no timestamp.
• **Choose Column:** Select the column that contains the timestamp value.

If this column is in a format which cannot be parsed as a timestamp by DB Connect, you will be shown a field where a Java SimpleDateTimeFormat compatible parser can be entered so that Splunk can understand the timestamp value.

• **Column:** This option only appears if you selected **Choose Column** in the previous option. Choose the column that contains the timestamps you want to use.
• **Query timeout:** Enter the number of seconds to wait for the query to complete. The default is 30 if you leave it blank.

**Rising input**

A rising input has a column that DB Connect uses to keep track of what rows are new from one input execution to the next. When you create a rising input type, you must specify the rising column. You can specify rising column as any column whose value increases or decreases over time, such as a timestamp or sequential ID. For example, you can use columns such as row_id, transaction_id,
employee_id, customer_id, last_updated, and so on.

Note that timestamps are not ideal for rising columns, though they often are the best available choice. Using a timestamp for rising column can produce the following problem conditions:

- A high rate of event generation can cause data duplication or loss, because checkpointing in a stream of timestamp-distinguished records assumes there is never more than one row created in a given time. If you set the time to a one second level of resolution and get five records per second, you lose or duplicate four records from every run.
- Clock skew, NTP skew corrections, physical moves between timezones, and daylight savings events can cause data mis-ordering, duplication, or loss. If the skew is towards the future, then the resulting checkpoint value may temporarily or permanently stop data collection.
- Non-numeric datetime values cannot be evaluated numerically, and lexical sorting can produce unpredictable results. If time series data is ordered lexically, then the resulting checkpoint value may temporarily or permanently stop data collection.

To create a rising input, select Rising and configure the following fields:

- **Rising column**: The rising column is the column from which DB Connect will update the checkpoint value each time the input is run.
- **Checkpoint value**: The checkpoint value is how DB Connect determines what rows are new from one input execution to the next. The first time the input is run, DB Connect will only select those rows that contain the value higher or lower than the value you specified in this column. Each time the input is finished running, DB Connect updates the input’s checkpoint value with the value in the last row of the checkpoint column.
- **Update the SQL query that includes a ? symbol and order by clause for the checkpoint value. The question mark (?) as the checkpoint placeholder and an order by clause. Every time the input is run, DB Connect replaces the question mark with the latest checkpoint value.**

Note:

- From DB Connect 3 and later, the rising column checkpoints of the input are stored in `$SPLUNK_HOME/var/lib/splunk/modinputs/server/splunk_app_db_connect`. For each input, it creates a separate checkpoint file.
- To see what column types (varchar, number, timestamp, and so on) are supported as rising column value types in DB
Connect-supported databases, see supported rising column types by database.

With a rising column mode input, you could:

- Effectively create a "descending column," or a column wherein the checkpoint decreases every time the input runs.
  
  ```sql
  SELECT abc, xyz FROM table WHERE abc < ? ORDER BY abc DSC
  ```

- Customize the comparison operation to determine the checkpoint value by evaluating a SQL function result, while simultaneously avoiding using query wrapping.
  
  ```sql
  SELECT CONCAT(last_name, first_name) as NAME, ACTOR_ID, FIRST_NAME, LAST_NAME FROM actor WHERE CONCAT(last_name, first_name) > ? ORDER BY CONCAT(last_name, first_name)
  ```

- Customize the WHERE clause to add additional conditions other than the comparison expression that is specified in rising column inputs.
  
  ```sql
  SELECT * FROM (SELECT * FROM ACTOR WHERE ACTOR_ID > ?) ACTOR JOIN FILM_ACTOR ON actor.ACTOR_ID = FILM_ACTOR.ACTOR_ID JOIN FILM ON FILM_ACTOR.FILM_ID = FILM.FILM_ID ORDER BY ACTOR.ACTOR_ID
  ```

- Use other advanced SQL features in the WHERE clause—for example a CASE statement.

After the input type is specified, click Next to go to the Set Properties page.

**Basic information**

Configure the following fields,

- **Name**: Specify the name of the input. Be aware the input name cannot contain space or special characters.
- **Description**: Optional. The description of the input.
- **Application**: The name of the Splunk Enterprise app where this input object will be saved. By default, the pop-up menu is set to Splunk DB Connect. This menu enables other apps to use DB Connect inputs, outputs, and lookups within their own context.

**Parameter settings**

Complete the following fields,
• **Max Rows to Retrieve**: Optional. The maximum number of rows to retrieve with each query. If you set this to 0 or leave it blank, it will be unlimited.

• **Fetch size**: Optional. The number of rows to return at a time from the database. The default is 300 if you leave it blank.

• **Execution Frequency**: The number of seconds or a valid cron expression i.e. 0 18 * * * (every day at 6PM).

**Metadata**

The metadata fields are used by Splunk to index your data events. As you search the indexed data using Splunk Enterprise, data from the query can be identified by fields value you enter here.

• **Host**: Optional. The host defined on the connection will be used if you leave it blank.

• **Source**: Optional. The input name will be used if you leave it blank.

• **Source type**: Enter a sourcetype field value for Splunk Enterprise to assign to queried data as it is indexed. Click the field and enter a value, or choose an existing value from the menu that appears.

• **Index**: Enter an index value for the index in which you want Splunk Enterprise to store indexed data. You can enter the index name or choose it from the typeahead menu.

**Note**: If you want to use the customized index, you have to make sure the index exists in Splunk platform. Otherwise you have to create the index in Splunk Enterprise first to prevent data loss.

**Edit database inputs**

To see a list of the defined database inputs, first click the Data Lab>Inputs tab. You will see a list of your database inputs.

To edit a database input, click its name. You can make changes to a database input using the following buttons on the input page:

• **Enable/Disable**: Disable an input by clicking Enable/Disable here.

• **Edit**: Edit the input by clicking the name or the Edit button.

• **Clone**: Creates a copy of the input. You must give the copy a new name.

• **Delete**: Deletes the input.

You can also edit any of the attributes of a database input listed in Create a database input, except its name. To change the name of an input, clone it, give
the clone the name you want, and then delete the original input.

**Supported rising column types by database**

The following matrix summarizes what column types (varchar, number, timestamp, and so on) are supported as rising column value types in DB Connect-supported databases.

<table>
<thead>
<tr>
<th>Database</th>
<th>varchar</th>
<th>int, float, real, bigint</th>
<th>timestamp</th>
<th>datetime</th>
<th>date</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS RDS Aurora</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>AWS RedShift</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DB2/Linux</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>MemSQL</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>MySQL</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Oracle</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAP SQL Anywhere</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sybase ASE</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sybase IQ</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Teradata</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The column marked x means this column is supported.
* Information for Informix databases is not currently available.

**Use database inputs**

Once you've configured a database input and your data has been indexed by Splunk Enterprise, you can use that input just as you do any other data input you've defined in Splunk Enterprise. Use the Search Processing Language (SPL) to write a series of commands and arguments.
For a quick view of what an input returns to Splunk Enterprise, go to the database inputs page by clicking **Data Lab>Inputs** in the top navigation bar, click the name of the input to view, and then click the **Find Events** button on the right side of the screen. The search app opens with a pre-populated search that searches on your input.

You can search for keywords and use Boolean operators such as **AND**, **OR**, and **NOT**, plus wildcard characters ("*"):

manufacturing (widgets AND gadgets OR gewgaw*)

Fields in Splunk Enterprise correspond to columns in your database. Search for fields using the syntax: `fieldname="field value"

source="db2input"

Chain search commands and arguments together using the pipe ("|") character. For example, the following search retrieves indexed events from the database input `db2input` that contain the term "manufacturing" and, for those events, reports the most common **LOCATION** values:

manufacturing source="db2input" | top LOCATION

To refine your search further, show only the fields you want using the fields keyword. The following search only shows the five fields listed after fields, plus a timestamp, for each event retrieved:

source="db2input" | fields ADMRDEPT DEPTNAME DEPTNO LOCATION MGRNO

Of course, you can do much more with search in Splunk Enterprise. To learn more:

- Read the Search Tutorial. Since you've already gotten your data into Splunk Enterprise, start with Part 4, Using Splunk Search.
- See Search and reporting in the *Splunk Enterprise Overview* manual for a guide to documentation that is based on your level of familiarity with Splunk Enterprise and on what you want to do with your data.
- For information specific to SQL users, see *SQL tips and tricks* in this manual, and Splunk SPL for SQL users in the *Splunk Enterprise Search Reference* manual.

### Create and manage bulk operations of the database inputs

At some point, you may need to create, change or delete multiple inputs from different connections at the same time. From Splunk DB Connect 3.1.0, you can...
do this by performing a bulk operation. The bulk operation includes:

- Bulk creation
- Bulk edit (including enable and disable)
- Bulk delete

Create multiple inputs

The bulk creation allows you to create multiple inputs using different connections at the same time. To perform a bulk creation, go to Data lab > Input and choose Create under the drop-down list of Bulk Actions. Complete the following procedures to bulk create multiple inputs and then click Finish.

1. Select Connections
2. Input Settings and preview the result
3. Confirmation

Select Connections

Select the connections which will be used by the new inputs you create. If you want to select all connections, check the checkbox in the table header. Once you have selected the connections, Splunk DB Connect will try to validate them and displays the status of the connections at the right side of the page. If you have a connection which is not valid, you can edit it on the create and manage database connection page and validate it again by clicking Revalidate all.

Note: Be aware that you can continue to the next step even there are invalid connections, but the invalid connection(s) may impact the data you want to fetch from the database and the input will not be created successfully. Splunk recommends you to make sure all the connections you select are valid before going to the next step.

Input settings

Configure the following settings and then preview the result of one connection before clicking Next.

Note: The meaning and verification of bulk input settings is the same as single input. If you need more information, see create a database input for details.
• **Template**: Choose the template you want to use for the inputs. If you do not want to use the template, leave this field blank. If you create inputs by using a template, all the settings from the template will be set for the inputs. You can change them based on your needs, be aware that the changes will be saved to the input you create but not to the template.

• **Input Type**: Choose the input type for the inputs, either **Batch** or **Rising**.

• **SQL Query**: Specify the SQL query that you want to use.

• **Timestamp**: Specify the timestamp column you want to use. You can use **Current Index Time** or choose the timestamp column by selecting **Choose Column**.

• **Query Timeout**: Optional. The number of seconds to wait for the query to complete. The default is 30 if you leave it blank.

• **Name Prefix**: Specify the prefix for the inputs you create. All the inputs you create in one bulk creation operation will have the same prefix.

• **Description**: Optional. The description of the inputs.

• **Application**: The name of the Splunk Enterprise app where this input object will be saved. By default, the pop-up menu is set to Splunk DB Connect.

• **Max row to retrieve**: Optional. The maximum number of rows to retrieve with each query. If you set this to 0 or leave it blank, it will be unlimited.

• **Fetch size**: Optional. The number of rows to return at a time from the database. The default is 300 if you leave it blank.

• **Execution Frequency**: The number of seconds or a valid cron expression e.g. 0 18 * * * (every day at 6PM).

• **Host Value**: Optional. The host defined on the connection will be used if you leave it blank.

• **Source**: Optional. The source field value for Splunk Enterprise to assign to queried data as it is indexed.

• **Source Type**: The sourcetype field value for Splunk Enterprise to assign to queried data as it is indexed.

• **Index**: The index in which you want Splunk Enterprise to store indexed data. You can enter the index name or choose it from the typeahead menu.

After configuring the input settings, you can choose one connection to preview the result. Choose one connection from the drop-down list and click **Execute SQL**. The result of this connection will be displayed on the preview page. If you are satisfied with the result, click **Next**. Otherwise, go back and edit the input settings until you get expected result.

On the confirmation page, review the inputs settings and then click **Finish**.
Edit multiple inputs

This bulk operation allows you to edit multiple inputs at the same time. The bulk edit operations available depend on the inputs selected and the nature of the field(s) you want to change.

To perform a bulk editing, go to Data lab -> Input and choose Edit under the drop-down list of Bulk Actions.

Then complete the following steps,

- **Select Inputs.** Select the inputs you’d like to perform the bulk operation on, and click Next.
- **Edit Inputs.** Select the field(s) which you want to edit by checking the field's name and enter the value of the field. Once you have modified the value of the field, it will be set to all inputs you selected. For the detailed description about each field, see input settings.

**Note:** To make the inputs consistent, there are some constraints and dependency on editing the inputs fields.

- If you want to edit the input type, configure the following dependent fields based on the input type you choose.
  - Batch input type: SQL Query field, timestamp field.
  - Rising input type: SQL Query field, Rising Column field (checkpoint value) and timestamp field.
- If you want to edit the SQL Query field, the following dependent field needs to be updated.
  - Batch input type: timestamp field.
  - Rising input type: Rising Column field (checkpoint value) and timestamp field.

The dependent fields will be greyed out in Splunk UI before you specifying the Input Type or SQL Query field if they have different values.

- Select an input to preview the result and then click Next.
- On the confirmation page, review the settings you edit for the selected inputs and then click Finish.

Delete multiple inputs

The bulk operation allows you to delete multiple inputs at the same time. To perform a bulk deletion, go to Data lab -> Input and choose Delete under the drop-down list of Bulk Actions.

On the Delete inputs page, select the inputs names you want to delete and click
Next. A confirmation dialog box pops up and lists all the inputs you want to delete. If you are OK to delete all the inputs, click Yes, delete all or otherwise Cancel.

Create and manage database outputs

A database output object lets you define how to send data from Splunk Enterprise to a database on a recurring basis. Defining database outputs is useful if you want to store your indexed Splunk Enterprise data in a relational database.

Create a database output

From within Splunk DB Connect, click the Data Lab > Outputs tab and click New Output.

Complete the following steps to create a database output.

1. **Set up search.** Perform a SPL or a saved search to search the event data in Splunk platform.
2. **Choose table.** Choose the table from database which Splunk event data will be exported to.
3. **Fields mapping.** Map the Splunk Enterprise fields you selected to columns in your database.
4. **Set properties.** Configure the basic settings and parameters of the output.

Set up search

In this step, you define the Splunk Enterprise fields that you want to output to the database table as columns:

1. Perform a search of your Splunk Enterprise data. You can either enter a search using the Search Processing Language (SPL), or you can run a saved search.
2. To select a saved search, click Saved Search and then choose the one you want to use from the drop-down list. Splunk Enterprise performs the search and displays the results in a table. Each column corresponds to a Splunk Enterprise field.
3. Specify the time range you want to run the search. Be aware that you cannot choose real-time time range since it will keep running the search all the time. It is a known issue in DB Connect 3.1.0.
Tips:

◊ You can fine-tune the format of your output directly from this search field by using standard search commands. For example, if you want Splunk Enterprise to display and use output to send data to your database as key-value pairs, use the `eval` search command here. If you want to change the quoting pattern, use `rex`.

◊ If you want Splunk Enterprise to send a specific number of rows each time the output runs, use the `head` search command. For example, to specify that the output should send no more than 1000 rows each time it runs, define your search as follows:

```
index=main sourcetype=foo status=ERROR | head 1000
```

◊ If you want to use the Saved Search, set the permission of the saved search to This app only (`splunk_app_db_connect`) or All apps.

4. Run the search and if you are ok with the result, click Next.

Choose table

In this step, you choose the table from database which Splunk event data will be exported to.

1. **Connection**: Choose the database connection you want to use with this output. DB Connect validates the connection and displays an error message if it is not able to do so. You cannot continue the new output setup process unless you have specified at least one valid connection the Connection dialog.

2. From the corresponding dialog menus, choose the **Catalog**, **Schema**, and **Table** that contain the columns you want to map the Splunk event data to.

3. Once you have chosen the table, you can preview the data on the Table Schema Preview page. It lists the column name, data type, column size and related fields of the table.

4. Click Next.

Fields mapping

In this step, you map Splunk data field(s) to the database column(s).
• **Fields Mapping.** Click **Add Search Field** and choose the field name of Splunk data you want to output. Then select the column name in the **Table Column** field. The data of the selected field will be exported to the column in your database table. You can add multiple Splunk fields/table columns pairs if you need to.

• **UPSERT Configuration.** UPSERT allows either insert a row, or on the basis of the data of the column already existing, UPDATE that existing row instead. If you choose to **Enable UPSERT**, then specify the **Key** column in your table.

**UPSERT Example:** UPSERT is enabled and the **id** column is set as the key column.

<table>
<thead>
<tr>
<th>id</th>
<th>name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001</td>
<td>Jack</td>
</tr>
<tr>
<td>1002</td>
<td>Michael</td>
</tr>
</tbody>
</table>

If there are two data events to be exported to this table, one is 'id=1001, name=Dianel', the other is 'id=1003, name=Leo', then the updated table is

<table>
<thead>
<tr>
<th>id</th>
<th>name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001</td>
<td>Dianel</td>
</tr>
<tr>
<td>1002</td>
<td>Michael</td>
</tr>
<tr>
<td>1003</td>
<td>Leo</td>
</tr>
</tbody>
</table>

**Set properties**

**Basic information**

• **Name:** The output name cannot contain any spaces. Do not use special characters in the output name.

• **Description:** Optional. The short description of this output.

• **Application:** The name of the Splunk Enterprise app in which DB Connect saves this output object. By default, the pop-up menu selects **Splunk DB Connect**. This menu enables other apps to use DB Connect inputs, outputs, and lookups within their own context.

**Parameter Settings**

• **Query Timeout:** Enter the number of seconds for a single query to wait to complete. The default is 30 if you leave it blank.

• **Scheduling:** Configure **Execution Frequency** if you want to schedule this
output, you can enter the number of seconds or a valid cron expression
e.g. 0 18 * * * (every day at 6PM).

Edit database outputs

To see a list of the database outputs you defined, navigate to the Configuration
> Outputs tab.

To edit a database output, click its name. You can make changes to a database
output using the following buttons on the output page:

- **Enable/Disable**: Enable or disable an output.
- **Edit**: Edit an output by clicking its name or the Edit button.
- **Clone**: Create a copy of the output. You must give the copy a unique
  name.
- **Delete**: Delete the output.

You can also edit any of the attributes of a database output listed in Create a
database output, except its name. To change the name of an output, clone it,
give the clone the name you want, and then delete the original output.

Enable output to multi-byte character sets

DB Connect can send data that is in a multi-byte character set, such as
Traditional Chinese, using a database output. Depending on your database, you
may need to change certain settings to the database to properly receive and
store the data.

- **MySQL**: When creating a connection to a MySQL database, customize the
  JDBC URL by adding some additional query parameters. For more
  information, access MySQL documentation for Inserting unicode UTF-8
  characters into MySQL.
- **PostgreSQL**: By default, this database supports multi-byte character sets.
  You do not need to take additional steps.
- **Microsoft SQL Server**: Ensure your database columns’ data types are
  N-variant types, such as NVARCHAR versus VARCHAR).
- **Oracle**: Change your database character set to AL32UTF8. For more
  information, access Oracle’s documentation for Supporting Multilingual
  Databases with Unicode.
- **Other databases**: Consult your database's documentation for more
  information about enabling multi-byte character sets.
Use database outputs

Database outputs run automatically at the frequency you set during the "scheduling" step of the setup process. To verify that database outputs are working properly, query your database after a few executions of the output operation to ensure that DB Connect is sending your Splunk Enterprise data properly.

♦ DB Connect 3 does not support running scheduled task (input or output) on the search head in the Search head cluster deployment. You must run the scheduled task on a heavy forwarder.
♦ In a distributed environment, the heavy forwarder will need to be able to search the Indexers in order to output to the DB. See Deploy a distributed search environment in the "Distributed Search" manual to learn how to set up distributed search on your deployment’s heavy forwarders.

Use modular alert to run database output

DB Connect provides a modular alert which allows users to actively respond to events and send alerts. You can configure the DBX output alert action on the Alert Actions Manager page. See alert action manager.

To use the DB Connect modular alert:

1. Navigate to the Search page in DB Connect.
2. Create a search, then select Save as > Alert.
3. Enter the title and optional description.
4. In the Trigger Actions field, select DBX output alert action.
5. Enter the Output Name. The output name must exist in DB Connect.

For details about custom alert, see Create custom alert.

Use dbxoutput command to run database output

dbxoutput is a search command you can use to run database outputs that you have defined in DB Connect.
**Syntax**

dbxoutput output=<string>

**Required Arguments**

output

Syntax: output=<string>

Description: Name of a configured database output object.

**Example**

The following example uses the output `dbx_output` to send the results of a search query to a database.

```
<search query> | dbxoutput output="dbx_output"
```

**Create and manage database lookups**

A database lookup object enables you to enrich and extend the usefulness of your Splunk Enterprise data through interactions with your external database.

For example, a database lookup is a lookup that takes a customer ID value in an event, matches that value with the corresponding customer name in your external database, and then adds the customer name to the event as the value of a new `customer_name` field. Therefore, if you have an event where `customer_id="24601"`, the lookup adds `customer_name="Valjean, Jean"` to the event.

You can run lookups against your database by specifying the `dbxlookup` command in your search query.

The database data DB Connect transfers when it performs lookups does not count toward your daily Splunk Enterprise indexing quota.

**Select between database lookups and Splunk lookups**

Splunk provides lookups by default which enable high-speed lookup functionality by holding the desired data in memory or the KV store. CSV lookups are cached in memory for high speed access. This is ideal behavior for data sets that are infrequently changed, smaller than available RAM, or both. KV Store lookups are not fully cached in memory, but they do consume resources. In either case, these
lookups can be created and updated from an external database using the dbxquery command in a scheduled search. For instance, the following search could be used to maintain a CSV lookup of IDs and names:

```
| dbxquery query="SELECT actor_id,first_name,last_name FROM "sakila"."dbo"."actor"" connection="ms-sql"
| inputlookup append=true actor-lookup.csv
| dedup actor_id
| outputlookup actor-lookup.csv
```

A database lookup is different from a Splunk lookup because each execution will contact the database for the current state of the rows in question. This is ideal behavior for data sets that are rapidly changing, very large, or both, because the user receives the freshest data possible.

**Create a database lookup**

From within Splunk DB Connect, navigate to the Data Lab > Lookups tab and click New Lookup. You have to Create a new identity and create a new connection, before you can create a new database lookup.

Complete the following steps to create a database lookup.

- **Set Reference Search.** Perform a Splunk Enterprise search to select the fields on which to base the lookup.
- **Set Lookup SQL.** Specify a reference search to fetch data from your database.
- **Field Mapping.** Map your selected database table column, plus any new column you want to add, to Splunk Enterprise fields.
- **Set Properties.** Configure the basic settings and parameters of the lookup.

**Set Reference Search**

In this step, you perform a search or use the saved search of you Splunk indexed data.

1. Perform a search of your Splunk Enterprise data. You can either enter a search using the Search Processing Language (SPL), or you can run a report (saved search).
2. To select a saved search, click Saved Search and then choose the one you want to use from the drop-down list. Splunk Enterprise performs the search and displays the results in a table. Each column corresponds to a Splunk Enterprise field.
   If you want to use the Saved Search, set the permission of the saved
search to **This app only (splunk_app_db_connect)** or **All apps**.
3. Click **Next**.

**Set Lookup SQL**

In this step, you specify a search to fetch data from your database.

1. Choose a connection that you want to use for this lookup from the **Connection** field. The drop-down list lists all the connections you have configured in DB Connect, you can also enter the connection name to search the connection you want to use. Once you have select the connection, Splunk DB Connect will try to validate the connection, and will display an error message if it is not able to do so. You cannot continue the new lookup setup process unless a valid connection is specified.
2. From the corresponding dialog menus, choose the **Catalog**, **Schema**, and **Table** that contain the columns you want to base for this lookup.
3. After you choose the table, the corresponding SQL query will be displayed in **SQL Editor**, you can preview the result of the query. If you need further edit or write your own SQL query, you can write it directly in SQL Editor and click **Execute SQL** to preview the result. You can make complex SQL statements easier to read by clicking **Format SQL**. This is a one-way operation.
   The reference search fields of Splunk data will be listed at the right side of the page. You can use it as a reference to specify your SQL query.
4. Click **Next**.

**Field Mapping**

In this step, you map the selected Splunk fields with the database table column(s), then you can add the table columns as new Splunk data fields to enrich you Splunk data.

1. **Search fields mapping.** Click **Add Search Field** and choose the field name you want to match to the database table column. Then select the column name in the **Table Column** field. You can add multiple pairs of fields and columns if you need to.
2. **Add table column(s) as new Splunk fields.** Click **Add Column** and choose the column name on the drop-down list, the column you select will be added as new fields in Splunk data.
3. **Set alias name to the table columns.** (Optional) To make the name of the database column easy to understand, You can rename the database column by entering a new name in **Aliases** field. The name must be
unique, and must not overlap with the field name. When you choose a
database column in the first part of this step, do not then choose the same
database column in the second part of this step.
4. The corresponding search will be displayed in Preview Results field. You
can run the search to preview the data by clicking Open in Search.

**Set properties**

Configure the following fields:

- **Name**: The output name cannot contain any spaces. Do no use special
characters.
- **Description**: The description of the lookup
- **Application**: The name of the Splunk Enterprise app in which DB Connect
saves this lookup object. By default, the DB Connect selects Splunk DB
Connect. This menu enables other apps to use DB Connect inputs,
outputs, and lookups within their own context.

You can use the generated dbxlookup command in the summary page to
enrich your Splunk data. See more on Use dbxlookup to perform lookups in DB
Connect.

**Edit database lookups**

To see a list of the defined database lookups, first click the Data Lab>Lookup
tab. To edit a database lookup, click its name. You can make changes to a
database lookup using the following buttons on the lookup page:

- **Enable/Disable**: Enable/Disable a lookup by clicking Disable here.
- **Edit**: Edit a lookup by clicking its name or the Edit button.
- **Clone**: Creates a copy of the lookup. You must give the copy a new
name.
- **Delete**: Delete the lookup.

You can also edit any of the attributes of a database lookup listed in Create a
database lookup, except its name. To change the name of a lookup, clone it, give
the clone the name you want, and then delete the original lookup.

**Use dbxlookup to perform lookups in DB Connect**
**Description**

dbxlookup is a search command for performing lookups by using remote database tables as lookup tables. Use dbxlookup to enrich your indexed events with the information you have stored in external databases. If you are not using Verbose search mode, you must explicitly reference input fields in the search.

**Syntax**

There are two ways to use `dbxlookup` command.

```
dbxlookup chunksize=<integer> lookup=<lookup_name>
```

The argument `<lookup_table_name>` refers to the lookup you defined in DB Connect UI. From DB Connect 3.1.0, dbxlookup command allows users to declare Splunk fields/table column mapping directly in the options. The syntax is similar as `lookup`. Users do not have to create a lookup in UI before using it in `dbxlookup` command.

```
dbxlookup connection=<connection name> query=<SQL query> chunksize=<integer> <database_key_column> AS <splunk_key_field> OUTPUT <column_destname> AS <field_destname>
```

**Argument**

If you want to use the lookup defined in DB Connect, use the following

lookups

**Syntax:** lookup=<lookup_name>

**Description:** Required. It refers to the lookup name you defined in UI.

chunksize

**Syntax:** <integer>

**Description:** Optional. Specifies the number of events will be used to look up the database of each query.

**Default:** 1000.

If you want to define the connection, SQL query and mappings directly in `dbxlookup` command, use the following

connection

**Syntax:** connection=<connection name>
**Description:** Required. Specifies the connection name you want to use for the lookup.

**query**

**Syntax:** query=<SQL query>

**Description:** Required. Specifies the SQL query to search the data in your database.

**chunks**

**Syntax:** <integer>

**Description:** Optional. Specifies the number of events will be used to look up the database of each query.

**Default:** 1000.

**<database_key_column>**

**Syntax:** <string>

**Description:** Refers to a table column in the database table to match the key value against the field in Splunk. You can specify multiple <database_key_column> values separated.

**<splunk_key_field>**

**Syntax:** <string>

**Description:** Refers to a Splunk field which to acquire the value to match in the database table. You can specify multiple <splunk_key_field> values.

**<column_destname>**

**Syntax:** <string>

**Description:** Refers to a table column in the database table to be copied into the Splunk field. You can specify multiple <column_destname> values separated by commas.

**<field_destname>**

**Syntax:** <string>

**Description:** The alias name of <column_destname> in Splunk. You can specify multiple <field_destname> values separated by commas.

**Default:** The value of the <field_destname> argument.

When using the dbxlookup command, if an OUTPUT clause is not specified, all the table columns that are not the key field are used as output fields. If the OUTPUT clause is specified, the output lookup fields overwrite existing fields.
Examples

Example 1: This example uses the lookup "GTS_Product_Lookup" to enrich the results of a Splunk Enterprise search query.

```
sourcetype=GTS_Sessions | dbxlookup lookup="GTS_Product_Lookup" | stats sum(product_price) as "spend" by uid
```

Example 2: If you are not using Verbose search mode, you must explicitly reference input fields in the search:

```
sourcetype=GTS_Sessions | fields pid, uid | dbxlookup lookup="GTS_Product_Lookup" | stats sum(product_price) as "spend" by uid
```

Example 3: This example defines the connection, SQL query, mappings and alias name directly in `dbxlookup` command.

```
sourcetype=GTS_Sessions | dbxlookup connection="sh-oracle" query="SELECT * FROM "TEST"."DBX" ID AS customer_id OUTPUT data AS customer_data, name AS customer_name
```

Example 4: If there is no alias name, the table column name will be set as the corresponding Splunk field name.

```
sourcetype=GTS_Sessions | dbxlookup connection="sh-oracle" query="SELECT * FROM "TEST"."DBX" ID OUTPUT data, name AS "Last Name"
```

Use SQL explorer to make live reports

DB Connect 3.x.x provides a SQL Explorer interface to help you use `dbxquery` to query your database in real time. You can browse the database connections, catalogs, and schema, write and test SQL commands, and modify results with Splunk’s SPL commands. You can use the resulting command in Splunk Enterprise searches to create reports, alerts, and dashboard panels.

Use SQL Explorer to build queries

You can reproduce the examples on this page in your test environment using a free tool such as MySQL Sakila sample database.
1. Navigate to Data Lab > SQL Explorer in DB Connect.
2. Select a Connection that you defined in create and manage database connections.
3. Browse to the desired Catalog, Schema, and Table from the type-ahead lists on the left. Refer to the a basic query of the table you selected in the SQL Editor window.
4. Replace or customize the query by writing SQL in SQL Editor. Click Format SQL to make complex SQL statements easier to read. This is a one-way operation.
5. DB Connect generates the dbxquery command and displays it in the SPL Editor. If you want to further customize the command, write SPL in this window, then click Run to see the results.
6. Click Open in Search to copy the final dbxquery command to Splunk Search in a new Tab. Add visualizations, look for patterns, or save the query as a dashboard panel, alert, saved search, or report. Each use of these new elements generates a live query to the database. Review access controls and performance considerations before you deploy in production.

Use variables in dbxquery to build dashboard panels

DB Connect allows users to use variables in dbxquery to interactively query databases and create dashboards. You can use variables to enter an input, select multiple time pickers, or dynamically drill down. In the example below, create a dashboard form in which the user enters a first name into a DB Connect search from the sakila sample database.

1. Create a SQL statement by choosing Connection, Catalog, Schema or Table under Data Lab > SQL Explorer.

   SELECT * FROM `sakila`.`actor` WHERE first_name='PENELOPE'
2. DB Connect generates the `dbxquery` command and presents it in the SPL Editor. Edit the SPL if you wish, then click Open In Search.

```sql
| dbxquery query="SELECT * FROM `sakila`.`actor` where first_name='PENELOPE'" connection="sh-mysql"
```

3. DB Connect generates the SPL and presents it in the Searching and Reporting app, where you can further edit the SPL or use visualizations.

4. Click Save As > Dashboard Panel > New Dashboard to create a dashboard. If you are not familiar with how to create and edit dashboards, see create dashboards for details.

5. Add a form element for the user to use. Click Edit > Add Input > Text to edit the Token. Set the input field name to First Name and the token to `first_name` in this form, then click Apply. See token usage in dashboards for further details.

6. Click Edit Search to edit the SPL, and replace where `first_name='PENELOPE'` with where `first_name='$first_name$'`. This variable name is the token name from your input form, bracketed with dollar signs. Click Apply to continue.
7. Test the form by entering 'RICHARD' in the **First Name** input field. The dashboard updates with the value you entered in this field.

**Use dynamic variables in dashboard panels**

Now, replace the **First Name** form with a drop down that allows the user to select from existing names in the table.

1. Return to SQL Explorer and edit the SQL statement to select a distinct list of first names from the actors table.

   ```sql
   SELECT DISTINCT first_name FROM `sakila`.`dbo`.`actor`
   ```

   Test the result, then Open in Search to copy the resulting `dbxquery` command.

2. Edit the dashboard again, then edit the input form element. Change the type from **Text** to **Dropdown**. Under **Dynamic Options**, set the "Search String" field to the `dbxquery` command for selecting a distinct list of names:

   ```sql
   | dbxquery query="SELECT DISTINCT first_name FROM `sakila`.`dbo`.`actor`" connection="sh-mysql". Set the "Field For Label" field to first_name, and set the "Field for Value" field to first_name. Click **Apply**. See token usage in dashboards for further details.
   ```

3. Test the form by selecting 'ANGELINA' from the dropdown input field. The dashboard updates with the value you entered in this field.
Limitations of time-based inputs

Splunk Enterprise dashboards and Splunk DB Connect support many types of variables in a dashboard, including string, numeric, and time values. The native Splunk Enterprise dashboard time selector is not always a good choice for dashboards that use DB Connect to perform time-based queries. The time selector allows users to select exact time representations (for instance, `earliest=%m/%d/%Y:%H:%M:%S`) and relative time representations (for instance, `[+|-]<time_integer><time_unit>`) in the same form. These two types of WHERE conditions use different SQL which can cause SQL errors. To avoid errors, customize the form to limit available time input formats. See date and time format variables for details.

Execute SQL statements and stored procedures with the dbxquery command

Splunk DB Connect has the `dbxquery` command for executing SQL statements and stored procedures within Splunk Enterprise searches and dashboards. Use SQL explorer to edit your query or write the `dbxquery` based on the syntax below.

Description

dbxquery is a custom search command for querying remote databases and generating events in Splunk Enterprise from the database query result set.
Syntax

```
-dbxquery connection=<string> [fetchsize=<int>] [maxrows=<int>]
[timeout=<int>] [shortnames=<bool>] query=<string> OR procedure=<string>
[params=<string1,string2>]
```

Required Arguments

**connection**

Syntax:  `connection=<string>`
Description: Name of a configured database connection object.

**query** or **procedure**

**query**

Syntax:  `query=<string>`
Description: A SQL query. You can also use a URL-encoded SQL query, but you must percent-encode all spaces (%20).

**procedure**

DB Connect supports stored procedures in databases beginning with version 3.0.0. A stored procedure is a set of Structured Query Language (SQL) statements with an assigned name. It is stored in the database in compiled form so that several programs can share it. You can call the stored procedures of your database by using a procedure argument instead of a query argument. Many stored procedures expect variables in the form of an ordered list of arguments. You can pass these variables from Splunk to the stored procedure using the params argument. Note that the dbxquery command is a generating command and needs to be the first command in a search. See Cross-database queries on this page for examples of the syntax needed to pass parameters to dbxquery.

Syntax:  `procedure=<string>`
Description: A stored procedure invocation.

This table lists procedure syntax formats for different type of databases.

<table>
<thead>
<tr>
<th>Supported databases</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS RDS Aurora</td>
<td>dbxquery procedure=&quot;{call &lt;procedure-name&gt;}&quot;</td>
</tr>
<tr>
<td>Informix</td>
<td></td>
</tr>
<tr>
<td>MemSQL</td>
<td></td>
</tr>
</tbody>
</table>
Supported databases | Syntax
--- | ---
Microsoft SQL Server, MySQL, SAP SQL Anywhere, Sybase ASE, Sybase IQ, IBM DB2 for Linux, Teradata |  
Oracle | dbxquery procedure="{call <procedure-name>(?)}"  
Postgres, AWS RedShift | dbxquery procedure="{?=call <procedure-name>}"

Important notes on stored procedure support in DB Connect:

♦ dbxquery only supports stored procedures which return a single result set.

IBM DB2 examples

♦ If you use an IBM DB2 for Linux or Teradata database, you must return the result as Cursor type and open it within the stored procedure. See the IBM DB2 for Linux stored procedure example below for details.

Stored procedure example (IBM DB2 for Linux)

```
CREATE OR REPLACE PROCEDURE TEST_IBMSP (IN actor_id varchar(30))
  DYNAMIC RESULT SETS 1
  LANGUAGE SQL
BEGIN
  DECLARE result_set CURSOR WITH RETURN TO CLIENT FOR
  SELECT * FROM ACT WHERE ACTNO <= actor_id;
  OPEN result_set;
END;
```

Oracle examples

♦ If you use an Oracle database, you must store the result in the first parameter and set it as OUT SYS_REFCURSOR. See the Oracle Stored procedure example below for details.
Stored procedure examples (Oracle)

Create stored procedure 1:

```sql
CREATE OR REPLACE PROCEDURE test_orasp_1(
    p_ref_cursor OUT SYS_REFCURSOR,
    p_var_in IN VARCHAR
) AS
BEGIN
    OPEN p_ref_cursor FOR
    SELECT 'you passed-in: ' || p_var_in out_var FROM dual;
END test_orasp_1;
```

Use stored procedure 1:

```plaintext
| dbxquery connection=splunk_test procedure="{call test_orasp_1(?,?) }" params="foo"
```

Create stored procedure 2:

```sql
CREATE OR REPLACE PROCEDURE TEST_ORASP_2(
    ref_cursor OUT SYS_REFCURSOR,
    id IN VARCHAR
) AS
BEGIN
    OPEN ref_cursor FOR
    SELECT * FROM soe.customers WHERE customer_id = id;
END TEST_ORASP_2;
```

Use stored procedure 2:

```plaintext
| dbxquery connection=splunk_test procedure="{call test_orasp_2(?,?) }" params="50865"
| makeresults count=1
| eval cust_id="50865"
| map search="| dbxquery connection=splunk_test procedure="{call test_orasp_2(?,?) }" params="$cust_id$" "
```

Optional Arguments

fetchsize

**Syntax:** fetchsize=<int>
The number of rows to return at a time from the database. To avoid running out of memory, the query result set is divided into multiple pieces and returned to DB Connect one piece at a time. This argument specifies how many rows are in each of those pieces. Depending on the RPC server’s maximum heap size and whether the target database table contains any unusually large columns, you may want to specify a smaller value for this argument. The maximum value for this option is 10,000.

**Default:** varies per database type

### maxrows

**Syntax:** maxrows=<int>

**Description:** The maximum number of rows to return. If you do not specify a value for `maxrows`, `dbxquery` returns 100,000 rows at most. There is no maximum value for this argument, but retrieving a very large number of records may result in performance issues or out-of-memory messages. In this case, you should experiment with setting `maxrows` to a lower number that is manageable by your Splunk Enterprise server hardware.

**Default:** `maxrows=100000`

### params

**Syntax:** params="string1,string2"

**Description:** The value(s) of the variable(s) you defined in `query` or `procedure`. The value of the `params` is in CSV format.

**Note:** The value of `params="BOB"` is different from `params="  BOB"`. The space character is not skipped inside the quotation marks.

**Example:** The values of `actor_id` and `actor_name` are defined in `params="3,BOB"`, which is 3 and BOB respectively.

```
 dbxquery query="select * from actor where actor_id > ? and actor_name = ?" connection="mysql" params="3,BOB"
```

Another example for using stored procedure, 150 and BOB are the values for the variables in the procedure `sakila.test_procedure`.

```
 dbxquery procedure="{call sakila.test_procedure(?, ?)}" connection="mysql" params="150,BOB"
```

### shortnames

**Syntax:** shortnames=<bool>

104
Description: By default, the returned fields will be in the form
Default: shortnames=true
Note: To emulate the output format of the dbquery command from DB
Connect 1.x.x, set the output to csv and shortnames to true.

timeout

Syntax: timeout=<int>
Description: Specifies the timeout of your query in seconds. Set to zero
to allow unlimited execution. Typically the value should be less than query
job lifetime, which defaults to 10 minutes (600 seconds). For more
information, see
http://docs.oracle.com/javase/7/docs/api/java/sql/Statement.html#setQueryTimeout(int).
Default: timeout=600

Examples

| dbxquery query="SELECT actor_id, first_name as fname, last_name as lname, last_update FROM actor" connection="mySQL"
| dbxquery query="SELECT actor_id, first_name as fname, last_name as lname, last_update FROM actor" connection="mySQL" maxrows=100

Cross-database queries

DB Connect 2.2.0 and later includes improved support for using the dbxquery
command in complex Search Processing Language (SPL) statements. You can
now use dbxquery with subsearches, so that you can effectively perform
cross-database queries—enriching or filtering data on the fly.

Using a command such as append with dbxquery, you can run a separate
database search and add the output to the first search. For example, the
following search query appends results obtained from a SQL Server database
connection object to results obtained from a MySQL database connection object:

| dbxquery connection=mysql query="SELECT * FROM sakila.city" | append
[dbxquery connection="sql_server" query="SELECT * FROM sakila.actor"]

You can use any of the following search commands to produce cross-database
query results:

- append: Appends the results of a subsearch to the current results.
- appendcols: Appends the columns of the subsearch results with the
  input search results.
• **join**: Combines the results of a subsearch with the results of a main search. One or more of the columns must be common to each result set.
• **map**: Runs a search repeatedly for each input record or result. You can run the `map` command on a saved search, a current search, or a subsearch.

For more information about subsearches:

• Read About subsearches in the *Splunk Enterprise Search Manual*.
• Read How to use the search command in the *Splunk Enterprise Search Manual*.

**Deprecated Arguments**

The following `dbxquery` arguments are not functional. They do not produce errors if you leave them in the command line.

- `wrap`
- `output`

**Monitor Splunk DB Connect health**

Splunk DB Connect provides pre-configured health dashboards that allow you to monitor and troubleshoot several aspects of your database connections and inputs from inside Splunk Enterprise. Using numerous pre-built Splunk visualization panels, you can monitor DB Health and Input Metrics.

Data model acceleration for DB Connect dashboards is disabled by default. If your DB Connect dashboards are slow, enable data model acceleration.

**Permissions**

A logged-on user must be assigned a role that has access to both the `_internal` index and "dbx_health" source type in order to see the health dashboards. If none of the user’s roles has permission to either search `_internal` or view data with `sourcetype="dbx_health"`, DB Connect displays a "Permission denied" error message.
DB Connect input health

This dashboard provides pre-built panels to give you insights about your input operation health.

To use the health log dashboard, go to Splunk DB Connect, then click the **Health > DB Connect Input Health** tab.

The pop-up menus along the top of the window are controls you can use to refine the data in the dashboard. By default, they show all available data from the last 24 hours.

- **Total Errors**: The total number of errors for all the inputs.
- **%Error**: The percentage of the errors among all input jobs.
- **Number of Input Jobs over Time**: The number of input Jobs over the time you choose.
- **Input Jobs Errors over Time**: The total errors of input jobs over the time you choose.

DB Connect Input Performance

This dashboard gives you insights about the inputs performance.

To use the input performance dashboard, go to Splunk DB Connect, then click the **Health > DB Connect Input Performance** tab.

- **Input Jobs Median Duration**: The median duration of input jobs over the time you choose.
- **Input Jobs Median Time Distribution**: The median distribution time for each input.
- **HEC Median Duration**: The median duration of HEC.
- **HEC Median Throughput**: The median throughput of HEC
- **HEC Connection Status**: HEC connection status over the time you choose.
- **HEC Upload Time**: HEC upload time over the time you choose.
- **HEC Median Upload Time(ms) by Input Name**: HEC median upload time for each input.
- **HEC Median Throughput(MB) by Input Name**: HEC median throughput for each input.
DB Connect Connection Health

This dashboard gives you insights about the connection health.

To use the input performance dashboard, go to Splunk DB Connect, then click the **Health > DB Connect Connection Health** tab.

- **Total Errors**: The total number of errors of the connection you choose.
- **%Error**: The percentage of the errors among all input jobs.
- **Number of Each Connection over Time**: The number of connections per each connection over the time period you select.
- **Connections Errors over Time**: The number of errors per each connection over the time period you select.
- **Number of Each Operation over Time**: The number of operations (dbxinput, dbxoutput and dbxlookup) over the time period you select.
- **Operations Errors over Time**: The errors of each operation over the time period you select.

Connection Pool Health (scheduled inputs/outputs)

- **Active Connections**: The number of active connections of each connection pool over the time period you select.
- **Idle Connections**: The number of idle connections of each connection pool over the time period you select.
- **Pending Connections**: The number of pending connections of each connection pool over the time period you select.
- **Total Connections Pool**: The total number of connections (including active, pending and idle connections) of each connection pool over the time you select.
- **Connections Wait Time**: The waiting time for each connection pool.
- **Connections Usage Time**: The usage time for each connection pool.
- **Connections Wait Median Duration**: The median waiting duration for each connection pool.
- **Connections Usage Median Duration**: The median duration usage of each connection pool.
Reference

Configuration file reference

Splunk DB Connect includes the following custom configuration spec files:

- app-migration.conf.spec
- db_connection_types.conf.spec
- db_connections.conf.spec
- db_inputs|db_inputs.conf.spec
- db_outputs|db_inputs.conf.spec
- db_lookups.conf.spec
- identities.conf.spec
- inputs.conf.spec
- dbx_settings.conf.spec

The most current versions of these spec files exist in the $SPLUNK_HOME/etc/apps/splunk_app_db_connect/README/ folder, %SPLUNK_HOME%\etc\apps\splunk_app_db_connect\README\ directory on Windows.

Configuration files for version upgrades

Configuration files for Splunk DB Connect have changed in DB Connect version 3. DB Connect does not transfer your configuration files to the new version automatically. See Migrate DB Connect deployment to DB Connect 3.0.0

The following sections describe the .conf files where settings existed in previous versions of DB Connect, and where they exist in DB Connect version 3.

DB Connect version 2 configuration files

- **app-migration.conf**: Specifies options for migrating from DB Connect 1.x.x to DB Connect 2.x.x.
- **db_connection_types.conf**: Lists the database types, driver parameters, and test queries DB Connect supports.
- **db_connections.conf**: Stores all configuration necessary for connecting to a specific database, unless overridden by parameters from identities.conf.
- **healthlog.conf**: Manages the behavior of the self-monitoring health dashboard in DB Connect.
identities.conf: Stores credentials that DB Connect uses to connect to databases in the standard Splunk Enterprise credential store.
inputs.conf: Configures database indexing, lookup, and output behavior using modular inputs. Also includes per-input Java options.

**DB Connect version 3 configuration files**

- app-migration.conf: Specifies options for migrating from DB Connect 2.x.x to DB Connect 3.x.x.
- db_connection_types.conf: Lists the database types, driver parameters, and test queries that DB Connect supports.
- db_connections.conf: Stores all configuration necessary for connecting to a specific database, unless overridden by parameters from identities.conf.
- db_inputs.conf: Configures database indexing behavior using modular inputs.
- db_lookups.conf: Configures database lookup behavior using modular inputs.
- db_outputs.conf: Configures database output behavior using modular inputs.
- inputs.conf: Keeps the Task Server running using modular inputs.
- identities.conf: Stores credentials DB Connect uses to connect to databases in the standard Splunk Enterprise credential store. (The credentials are obfuscated hash text.)

For more information about configuration files, see About configuration files in the Splunk Enterprise Admin Manual. For more information about how Splunk Enterprise determines which configuration files take precedence, see Configuration file precedence in the Splunk Enterprise Admin Manual.

**app-migration.conf.spec**

The app-migration.conf file specifies options for migrating from DB Connect v1 to DB Connect v2 using the migration scripts.

```
[<migrationId>]
# stanzas are identified by their migrationId
# a migrationId is used to decide which migration business logic to load and apply

STATE = <string>
# JSON encoded state store for all migrations of type <migrationId>
```
DEST_CONF = <string>
# by default the DEST_CONF will be <migrationId>. Use if we need to override,
# for example mi_input://, mi_output://, and mi_lookup:// are all in inputs.conf but
# require different business logic for migration.

db_connection_types.conf.spec

The db_connection_types.conf file lists the supported database types, driver parameters, and test queries.

Compared to version 2.x, in DB Connect 3, the fields

- cwallet_location and oracle_cipherSuites have been merged into connection_properties.
- sslConnectionType has been removed.

# @copyright@
# The file contains the specification for database connection types

[<name>]

serviceClass = <string>
# required
# Splunk Java class that provides JDBC support for this database connection type.

supportedVersions = <string>
# optional
# list (comma separated) supported versions(majorVersion.minorVersion) of JDBC driver implemented by serviceClass
# installed driver major version must == MajorVersion and minor version >= MinorVersion for a driver to be considered supported

jdbcUrlFormat = <string>
# required
# JDBC Connection URL used for this database connection type. Supported variables: host, port, database, informixserver.

jdbcUrlSSLFormat = <string>
# optional
# JDBC Connection URL used for this database connection type if
jdbcUseSSL is enabled. Supported variables: host, port, database, informixserver.

jdbcUseSSL = [true | false]
# optional
# default is false, whether this type of connection will use SSL connection.

djdbcDriverClass = <string>
# optional
# Driver vendor Java class that provides JDBC support for this database connection type.

testQuery = <string>
# optional
# simple SQL to test validation for this database type.
# JDBC 4 compliant drivers do not need this parameter.

displayName = <string>
# optional
# Describe the database connection type for end users.

database = <string>
# required if used in jdbcUrlFormat or jdbcUrlSSLFormat.
# JDBC URL variable for the default database or schema used for this database connection type.

port = <integer>
# required if used in jdbcUrlFormat or jdbcUrlSSLFormat.
# JDBC URL variable for the network port used for this database connection type.

useConnectionPool = [true | false]
# optional, default is true.
# The connection pooling is based on Hikari, refer to https://github.com/brettwooldridge/HikariCP

ui_default_catalog = <string>
# optional
# ignored since 3.0

ui_default_schema = <string>
# optional
# ignored since 3.0

maxConnLifetimeMillis = <integer>
# optional, default is 120000 = 120 seconds
# valid when useConnectionPool = true
# The maximum lifetime in milliseconds of a connection in the connection
# pool. An in-use connection will never be retired, only when it is closed
# will it then be removed.
# A value of zero means the connection has an infinite lifetime.

maxWaitMillis = <integer>
# optional, default is 30000 = 30 seconds
# valid when useConnectionPool = true
# The maximum number of milliseconds that the pool will wait (when there
# are no
# available connections) for a connection to be returned before throwing
# an exception.
# [250, 300000] milliseconds is a reasonable value to wait to establish
# a connection.
# The max wait time is 300000 milliseconds (300 seconds).

maxTotalConn = <integer>
# optional, default is 8 connections
# valid when useConnectionPool = true
# The maximum number of active connections that can be allocated from
# this pool at the same time, or negative for no limit.

collection_properties = <string>
# optional
# Set JDBC variables for this database connection type.
# For example: {"useLegacyDatetimneCode": false}

db_connections.conf.spec

The db_connections.conf file stores all configuration necessary for connecting
to a specific database, unless overridden by parameters from identities.conf.

Compared to DB Connect 2, in DB Connect 3, the fields

- **username** and **password** have been removed.
- **cwallet_location**, **sslConnectionType** and **oracle_cipher_suites** have
  been removed, configure these fields in **connection_properties**.
# The file contains the specification for database connections

[<name>]

serviceClass = <string>
# optional
# inherits from db_connection_types.conf if not configured
# java class that serves the jdbc service for this type.

customizedJdbcUrl = <string>
# optional
# the user customized jdbc url used to connect to database, empty or
# missing means use template to generate jdbc url.
# see jdbcUrlFormat and jdbcUrlSSLFormat defined in db_connection_types.conf.spec

jdbcUseSSL = [true | false]
# optional
# inherits from db_connection_types.conf if not configured
# default is false, whether this type of connection will support SSL connection.

jdbcDriverClass = <string>
# optional
# inherits from db_connection_types.conf if not configured
# java jdbc vendor driver class.

testQuery = <string>
# optional
# inherits from db_connection_types.conf if not configured, if still
# not provided, JDBC isValid API will be used.
# simple SQL to test validation for this database type.

database = <string>
# required only when other parameters refer to.
# inherits from db_connection_types.conf if not configured
# The default database that the connection will use

connection_type = <string>
# required
# The type of connection configured in db_connection_types.conf that
# the connection refer to

identity = <string>
# required
# The database identity that the connection will use when connecting to
# the database
# an identity provides username and password for database connection.

isolation_level = <string>
# optional
# The transaction isolation level that the connection should use
# valid values are: TRANSACTION_NONE, TRANSACTION_READ_COMMITTED,
# TRANSACTION_READ_UNCOMMITTED, TRANSACTION_REPEATABLE_READ,
# TRANSACTION_SERIALIZABLE and DATABASE_DEFAULT_SETTING
# default: DATABASE_DEFAULT_SETTING.

readonly = true|false
# optional
# default to false
# Whether the database connection is read-only. If it is readonly, any
# modifying SQL statement will be blocked

host = <string>
# required only when other parameters refer to.
# The host name or IP of the database server for the connection
# Possible variable from jdbcUrlFormat.

port = <integer>
# required only when other parameters refer to.
# inherits from db_connection_types.conf if not configured
# The TCP port number that the host database server is listening to for
# connections
# Possible variable from jdbcUrlFormat.

informixserver = <string>
# optional
# Required option for informix server to compose proper jdbc connection
# url.
# This attribute is used for informix server connection setup only.
useConnectionPool = true|false
# optional
# boolean to make connection use a connection pool
# defaults to true

collection_properties = <string>
# optional, differs via different databases.

fetch_size = <integer>
# optional, default is 100, the number of rows retrieved with each trip to the database.

maxConnLifetimeMillis = <value>
# optional, default is 120000 = 120 seconds
# valid when useConnectionPool = true
# The maximum lifetime in milliseconds of a connection. After this time is exceeded the connection will fail the next activation, passivation or validation test.
# A value of zero or less means the connection has an infinite lifetime.

maxWaitMillis = <value>
# optional, default is 30000 = 30 seconds
# valid when useConnectionPool = true
# The maximum number of milliseconds that the pool will wait (when there are no available connections) for a connection to be returned before throwing an exception.
# [250, 300000] milliseconds is a reasonable value to wait to establish a connection. The max wait time is 300000 milliseconds (300 seconds).

idleTimeout = <integer>
# optional, default is 600000 = 10 minutes
# The maximum amount of time that a connection is allowed to sit idle in the pool in milliseconds.
# valid when useConnectionPool = true and when minIdle is defined to be less than maxTotalConn.
# Whether a connection is retired as idle or not is subject to a maximum variation of +30 seconds, and average variation of +15 seconds.
# A connection will never be retired as idle before this timeout.
# Once the pool reaches minIdle connections, connections will no longer be retired, even if idle.
# A value of 0 means that idle connections are never removed from the pool.
# The minimum allowed value is 10000ms (10 seconds).
maxTotalConn = <value>
# optional, default is 8 connections
# valid when useConnectionPool = true
# The maximum number of active connections that can be allocated from
# this pool at the same time, or negative for no limit.

timezone = <time zone identifier>
# optional, default uses JVM time zone
# The identifier could be:
# an offset from UTC/Greenwich, that uses the same offset regardless
given date-time e.g. +08:00
# an area where a specific set of rules for finding the offset from
UTC/Greenwich apply e.g. Europe/Paris.

localTimezoneConversionEnabled = [true | false]
# optional, default is false
# valid when a time zone is set
# When turned on, time-related fields are read from the DB using the
configured time zone and then translated to the JVM time zone.
# For example, with a DB using UTC and the JVM using GMT+8, the datetime
field defined in the DB
# 2017-07-21 08:00:00 will be displayed 2017-07-21 16:00:00

Example:

[oracle_example]
connection_type = oracle
database = orcl
disabled = 0
host = oracle.host.com
identity = oracle_identity
jdbcUseSSL = true
port = 2484
readonly = false
customizedJdbcUrl =
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=oracle.host.com)(PORT=2484))(CONNECT_DATA=(SERVICE_NAME=orcl)))
connection_properties = {
"oracle.net.authentication_services":
"(TCPS)",
"oracle.net.ssl_cipher_suites":
"(SSL_DH_anon_WITH_3DES_EDE_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA)",
"javax.net.ssl.trustStore": "/opt/splunk/cwallet/cwallet.sso",
"javax.net.ssl.trustStoreType": "SSO",
"javax.net.ssl.keyStore": "/opt/splunk/cwallet/cwallet.sso",
"javax.net.ssl.keyStoreType": "SSO"}

[informix_example]
connection_type = informix
database = test
disabled = 0
host = informix-demo.host.com
identity = informix_win
informixserver = demo_on
jdbcUseSSL = false
port = 9088
readonly = false
customizedJdbcUrl =
jdbc:informix-sqli://informix-demo.host.com:9876/test:informixserver=demo_on;DELIMITER=Y

**db_inputs.conf.spec**

```plaintext
[<name>]
description = <string>
# optional
# Description for this input

interval = <integer|string>
# required
# interval to fetch data from DB and index them in Splunk
# It could be a number of seconds or a cron expression

index = <string>
# optional
# index to store events imported in Splunk
# If not specified default index is used
# default to 'default'

source = <string>
# optional
# source associated to events indexed
# By default, the stanza name will be used

sourcetype = <string>
# required
# source type associated to events indexed

host = <string>
# optional
# host associated to events indexed

mode = [batch|rising|advanced]
# required
# Operational mode.
# advanced is deprecated since DBX v3.1, use rising instead.

connection = <string>
# required
# Indicates the database connection to work on.

query = <string>
```
# required
# SQL statement to retrieve data from remote database connection.

query_timeout = <integer>
# optional
# the max execution time of a SQL, the default is 30 seconds.

max_rows = <integer>
# optional
# the max rows of data retrieval. the default is 0, which means unlimited.

fetch_size = <integer>
# optional
# The number of rows to return at a time from the database. The default is 300.

batch_upload_size = <integer>
# optional
# Number of rows to be uploaded to HEC in one batch. Default is 1000.

tail_rising_column_name = <string>
# deprecated since DBX v3.1.0, using tail_rising_column_number instead.
# optional if batch mode
# at tail mode, the rising column is the column which is always rising
# as the checkpoint of the tail loading.

tail_rising_column_fullname = <string>
# deprecated since DBX v3.1.0, using tail_rising_column_number instead.
# optional if batch mode
# fullname of input tail rising column, currently this value is used by
# front end only.

tail_rising_column_number = <integer>
# required for advanced mode
# 1-based position of rising column in the data loading.

input_timestamp_column_name = <string>
# deprecated since DBX v3.1.0, using input_timestamp_column_number
# instead
# optional
# the input timestamp column name, the data of this column will be the
# event time. If not set, dbinput will use the current timestamp as the
# event time.

input_timestamp_column_fullname = <string>
# deprecated since DBX v3.1.0, using input_timestamp_column_number
# instead
# optional
# full name of input timestamp column, currently this value is used by front end only.

input_timestamp_column_number = <integer>
# optional
# 1-based column number of input timestamp.

input_timestamp_format = <string>
# optional
# Specifies the format of input timestamp column, in JavaSimpleDateString format.
# with index_time_mode as dbColumn, if this property is provided then DBX will use ResultSet#getString to get the value
# and try to parse the timestamp with given format, else if this property is not present DBX will try to use ResultSet#getTimestamp
# to get the timestamp.

index_time_mode = [current|dbColumn]
# required
# Specifies how to set the index time.
# current: use current time as index time
# dbColumn: use a DB column as index time.

max_single_checkpoint_file_size = <integer>
# optional
# Max checkpoint file size before archiving checkpoint file in bytes.
# Default is 10MB, max is 100MB.

ui_query_mode = [simple|advanced]
# deprecated since DBX v3.1.0, it is ignored by the UI
# optional
# Specifies whether the UI should use simple mode or advanced mode for SQL queries.

ui_query_catalog = <string>
# deprecated since DBX v3.1.0, it is ignored by the UI
# optional
# in simple mode, this value will be pre-populated into the catalog dropdown

ui_query_schema = <string>
# deprecated since DBX v3.1.0, it is ignored by the UI
# optional
# in simple mode, this value will be pre-populated into the schema dropdown

ui_query_table = <string>
# deprecated since DBX v3.1.0, it is ignored by the UI
# optional
# in simple mode, this value will be pre-populated into the query dropdown

template_name = <string>
# optional
# if provided and the value is not empty it means this input is created based on a template and the
# value is the name of the template.

Example

[test_input]
interval = 3600
index = main
sourcetype = dummy_type
mode = batch
connection = test_connection
query = SELECT * FROM `sakila`.`actor`
max_rows = 100
ui_query_catalog = sakila
ui_query_mode = simple
ui_query_schema = NULL
ui_query_table = actor

[test_advanced_input]
interval = 3600
index = main
sourcetype = dummy_type
mode = advanced
connection = test_connection
query = SELECT * FROM `sakila`.`actor` where actor_id >= ? order by actor_id
max_rows = 100
ui_query_catalog = sakila
ui_query_mode = advanced
ui_query_schema = NULL
ui_query_table = actor
tail_rising_column_name = actor_id

db_outputs.conf.spec

[<name>]
description = <value>
# optional
# Description for this output
interval = <string>
  # required
  # Specifies the interval to fetch data from Splunk and export to a
database
  # Valid only if scheduled is enabled
  # It could be a number of seconds or cron expression

connection = <string>
  # required
  # Specifies the database connection to persist splunk data.

table_name = <string>
  # required
  # Specifies the table name used to export data.

using_upsert = [true|false]
  # optional
  # Specifies if upsert is used when exporting data to the table

unique_key = <string>
  # required if upsert is enabled
  # Specifies the column used as key to verify if the row needs to be
inserted or updated.

query_timeout = <integer>
  # optional
  # Specifies the timeout (in seconds) for the SQL statement while
exporting data.
  # If the database supports batch operations, the timeout may apply to
the whole
  # batch or to each single statement. This behavior depends on the JDBC
driver.
  # For more information please consult the documentation of the driver
about the
  # following API Statement#setQueryTimeout.
  # Default to 30 seconds.
  # 0 means unlimited.

time_out = <integer>
  # deprecated since DBX v3.1, use search_time_out and query_timeout
instead.

search_timeout = <integer>
  # optional
  # Specifies the max time (in seconds) for a search job to run, if the
search
  # takes longer than this limit the job will be finalized then only part
of the
  # data will be exported.
  # default is 0, which means unlimited.

search = <string>
# required
# Specifies the splunk search to pull data for output.
# If is_saved_search is enabled then this value specifies the saved search name.

query_earliest_time = <string>
# optional
# Specifies the earliest time applied to the search.
# The format is defined by Splunk time modifiers.
# default to null, which means no lower bound limit.

query_latest_time = <string>
# optional
# Specifies the latest time applied to the search.
# The format is defined by Splunk time modifiers.
# default to null, which means no upper bound limit.

is_saved_search = [true | false]
# optional
# specify the max time (in seconds) a search job can run, if time exceeded then search job will be finalized then partial events will be outputted.
# default is 0, which means unlimited.

customized_mappings = <string>
# required
# Specifies the output data name (fieldx) and database column number (1...n) mappings.
# The expected format is:
#   field1:column1:type1,field2:column2:type2,?,fieldN:columnN:typeN
# For compatibility reason the following format is also supported but is deprecated:
#   field1:column1,field2:column2,?,fieldN:columnN

scheduled = [true|false]
# required
# Specifies wether the output is scheduled.
# An unscheduled output is typically used in dbxoutput command context.

ui_mappings = <string>
# deprecated since DBX v3.1.0, it is ignored by the UI
# optional
# JSON mappings, purely for storage purposes

ui_selected_fields = <string>
# deprecated since DBX v3.1.0, it is ignored by the UI
# optional
# JSON array of selected fields, purely for storage purposes

ui_saved_search_str = <string>
# deprecated since DBX v3.1.0, it is ignored by the UI
# optional
# saved search string of the current saved search

ui_query_sql = <string>
# deprecated since DBX v3.1.0, it is ignored by the UI
# optional

ui_query_mode = [simple|advanced]
# deprecated since DBX v3.1.0, it is ignored by the UI
# optional

ui_query_catalog = <string>
# optional
# Specifies the table used to initialize the UI editor

ui_query_schema = <string>
# optional
# Specifies the schema used to initialize the UI editor

ui_query_table = <string>
# optional
# Specifies the table used to initialize the UI editor

Example

[test_output]
description = this is a test output
interval = 40 * * * *
connection = test_connection
table_name = `test_table`
using_upsert = 0
search = index=main | stats count(*) by test_column
is_saved_search = 0
time_out = 6000
customized_mappings = test_column:varchar_col:12
ui_mappings =
[["inputField":"test_column","outputField":"test_output_column","valType":"VARCHAR","sqlType":12]]
ui_selected_fields = [{"value":"skip","label":"Skip this Column"},{"value":"test_column","label":"test_column"}]
ui_query_catalog = test_catalog
ui_query_schema = NULL
ui_query_table = output_test

db_lookups.conf.spec

[<name>]
description = <string>
# optional

124
# Description for this lookup

lookupSQL = <string>
# required
# Specifies the SQL query for lookups.

collection = <string>
# required
# Specifies the database connection to use.

output_column_map = <string>
# required
# Key/value pairs of database column to search result column in JSON format.

input_column_map = <string>
# required
# Key/value pairs of search result column to database column in JSON format.

ui_input_spl_search = <string>
# optional
# the splunk spl search which will be used for choosing lookup

ui_input_saved_search = <string>
# optional
# the splunk saved search which will be used for choosing lookup

ui_use_saved_search = [true|false]
# optional
# if true, then ui will use ui_input_saved_search
# if false, then ui will use ui_input_spl_search

input_fields = <string>
# deprecated since DBX v3.1.0, it is replaced by input_column_map
# Specifies the input fields for lookups.

output_fields = <string>
# deprecated since DBX v3.1.0, it is replaced by output_column_map
# Specifies the output fields after lookups.

ui_query_mode = [simple|advanced]
# deprecated since DBX v3.1.0, it is ignored by the UI
# optional
# specify whether the ui should use simple mode or advanced mode for SQL queries

ui_query_catalog = <string>
# deprecated since DBX v3.1.0, it is ignored by the UI
# optional
# in simple mode, this value will be pre-populated into the catalog dropdown

ui_query_schema = <string>
# deprecated since DBX v3.1.0, it is ignored by the UI
# optional
# in simple mode, this value will be pre-populated into the schema dropdown

ui_query_table = <string>
# deprecated since DBX v3.1.0, it is ignored by the UI
# optional
# in simple mode, this value will be pre-populated into the query dropdown

ui_column_output_map = <string>
# deprecated since DBX v3.1.0, it is ignored by the UI
# optional
# JSON mapping from db result column to field name

ui_field_column_map = <value>
# deprecated since DBX v3.1.0, it is ignored by the UI
# optional
# JSON mapping from search result field to db column

ui_query_result_columns = <value>
# deprecated since DBX v3.1.0, it is ignored by the UI
# optional
# JSON encoded array of query result columns
# stores the columns from the associated lookupSQL

Example:

[test_lookup]
lookupSQL = SELECT * FROM `sakila`.`actor`
connection = test_connection
input_fields = test_input_field
output_fields = actor_id
ui_query_mode = simple
ui_query_catalog = sakila
ui_query_table = actor
ui_input_spl_search = index=main | stats count(*) by test_input_field
ui_use_saved_search = 0
ui_query_result_columns =
  [{"name":"actor_id"},{"name":"first_name"},{"name":"test_input_field"},{"name":"last_update"}]
ui_column_output_map =
  [{"removable":false,"label":"actor_id","value":"actor_id","name":"actor_id","alias":"output_actor_id"}]
ui_field_column_map =
  [{"name":"test_input_field","selected":true,"removable":true,"label":"test_input_field"}]

126
identities.conf.spec

The identities.conf file stores credentials used to connect to databases in standard Splunk credential store (obfuscated hash text).

# @copyright@
# The file contains the specification for database identities
(username/password)

[[<name>]]

username = <string>
# required
# the username for this database connection identity

password = <string>
# required
# The encrypted value of the password for this database connection identity.

domain_name = <string>
# optional
# Specifies the windows domain name which the username belongs to

use_win_auth = [true|false]
# optional
# Specifies wether the Windows Authentication Domain is used

Example

[[mysql_local]]
username = admin
password = UdxEsEmBjVU/1cINqMVGAQgBKT4DLlX/2c9Ka+3oUOVy=
use_win_auth = false

inputs.conf.spec

Instead of configuring inputs, outputs and lookups in one inputs.conf file, in DB Connect 3, inputs, outputs and lookups are configured in discrete files db_inputs.conf, db_outputs.conf and db_lookups.conf. This increases configurability and performance.
Note: Modifying inputs.conf file stanzas outside of the DB Connect app, such as in the search app or manager context, is not supported.

# @copyright#
# The file contains the specification for all db connect modular inputs
# # server - the modular input that runs java server

[server://<name>]
config_file = <string>
# required
# If the value is an absolute path, taskserver will treat it as the config_file path.
# If the value is a relative path, taskserver will prepend SPLUNK_HOME and generate the actual config_file path.
# On UNIX systems, a path is absolute if its prefix is "/".
# On Microsoft Windows systems, a path is absolute if its prefix is a drive specifier followed by "\", or if its prefix is "\\\".

keystore_password = <string>
# required
# Specifies the java keystore password
# The keystore contains the certificate to set up the HTTPS connection to the
# task server.

interval = <integer>
# required
# Specifies the interval used by Splunkd to monitor Java server. If Java process
# is stopped, Splunkd will spawn a new Java process.

**dbx_settings.conf.spec**

The dbx_settings.conf file contains DB Connect settings such as the $JAVA_HOME path, the JVM Options string, and Splunk usage collection. These settings can also be configured in DB Connect on the Settings page.

# @copyright#

[java]
javaHome = <string>
# optional
# Specifies the path to Java home. The path defined will be used to resolve the
# java command location. Typically, the /bin/java or \bin\java.exe will
be
# appended to this path to resolve the command location on *nix and
windows
# respectively.
# If not specified the JAVA_HOME environment variable is used.
# If JAVA_HOME is also undefined, java command is directly used. In that
# case,
# java command must be defined in the PATH environment variable.

jvm_options = <string>
# optional
# JVM options to be applied to DBX task server.

**Saved searches for Splunk DB Connect**

Splunk DB Connect includes the following saved searches.

To enable or disable a saved search:

1. From the **Settings** menu, choose **Searches, reports, and alerts**.
2. Under the **Action** column of the saved search, choose **Edit > Enable/Disable** to enable or disable it.

<table>
<thead>
<tr>
<th>Name</th>
<th>Purpose</th>
<th>Action required</th>
</tr>
</thead>
<tbody>
<tr>
<td>splunk_app_db_connect.apimetricscollector: calculate indexed data volume</td>
<td>Calculates the amount of data indexed in your Splunk platform by sourcetype.</td>
<td>Automatically enabled. No action required. Scheduled to run once daily at twenty minutes past midnight.</td>
</tr>
</tbody>
</table>

**Data models for Splunk DB Connect**

Splunk DB Connect includes four data models to support health and performance dashboards.

<table>
<thead>
<tr>
<th>Name</th>
<th>Purpose</th>
<th>Accelerated</th>
<th>Action required</th>
</tr>
</thead>
<tbody>
<tr>
<td>DBX_Job_Metrics</td>
<td>Supports the DB Connect Input Performance</td>
<td>No</td>
<td>None</td>
</tr>
<tr>
<td>Name</td>
<td>Purpose</td>
<td>Accelerated</td>
<td>Action required</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>DBX_Health_Metrics</td>
<td>Supports Task server health providing JVM heap size, REST API metrics, etc</td>
<td>No</td>
<td>None</td>
</tr>
<tr>
<td>DB_Connection_Metrics</td>
<td>Supports the DB Connect Connection Health dashboard.</td>
<td>No</td>
<td>None</td>
</tr>
<tr>
<td>DB_Health_Audit</td>
<td>Supports the DB Connect Connection Health dashboard.</td>
<td>No</td>
<td>None</td>
</tr>
</tbody>
</table>
Troubleshooting

Troubleshoot Splunk DB Connect

This topic describes how to troubleshoot common Splunk® DB Connect issues.

Answers

Have questions? In addition to these troubleshooting tips, visit Questions related to Splunk DB Connect on Splunk Answers to see what questions and answers the Splunk community has about using Splunk DB Connect.

Health dashboard

When you're trying to figure out the cause of degraded performance or figure out how failure rates correspond to transaction type or database user, the place to start is the health dashboard in Splunk DB Connect.

The health dashboard is a pre-configured dashboard that allows you to monitor and troubleshoot several aspects of your database connections from inside Splunk Enterprise. For more information about the health dashboard, see Monitor database connection health.

You can also see whether DB Connect is generating any internal errors, using a search with the following parameters:

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

Health dashboard shows "Permission denied" error message

If the health dashboard displays a "Permission denied" error message instead of any data, the problem is likely a permissions issue with the logged-on user.

A logged-on user must be assigned a role that has access to both the _internal index and "dbx_health" source type in order to see the health dashboard. If none of the roles a user is assigned has permission to either search _internal or view data with sourcetype="dbx_health", the dashboard will display the "Permission denied" error.
DB Connect logging

Splunk DB Connect has extensive logging options, which can be configured in Settings. Before contacting Splunk support, you might want to enable debug logging, in case you need to provide Splunk support with DB Connect debug logs. Splunk DB Connect activity is logged to files in $SPLUNK_HOME/var/log/splunk and automatically indexed to _internal. The relevant log files for DB Connect are

- splunk_app_db_connect_server.log
- splunk_app_db_connect_server_access.log
- splunk_app_db_connect_job_metrics.log
- splunk_app_db_connect_health_metrics.log
- splunk_app_db_connect_dbx.log
- splunk_app_db_connect_audit_server.log
- splunk_app_db_connect_audit_command.*.log

To view DB Connect logging activity, use a search command such as the following:

```
index=_internal sourcetype=dbx*
```

You can control access to logged events by limiting access to the _internal index using Splunk Enterprise roles. For example, by default non-administrators can't access _internal. Database and Splunk Enterprise administrators should work together to determine the optimal logging setup for their environment and decide how to handle special scenarios like troubleshooting. For more information about what Splunk Enterprise logs about itself, see "What Splunk logs about itself" in the Splunk Enterprise Troubleshooting Manual.

By default, DB Connect logs all executed SQL queries at INFO level. Logged along with each SQL query is the user that ran the query, the parameters, the number of results returned, and the name of the input, output, or lookup that was run.

Troubleshoot driver connections

If you're having trouble connecting to your database using Splunk DB Connect or loading your database's JDBC driver, please perform the following checks before contacting Splunk support:

- Is DB Connect running in Splunk Enterprise?
- Is Splunk Enterprise working correctly?
• Is the database working correctly?
  • Verify you've installed the driver properly by repeating the steps in "Install database drivers."
  • Verify that the driver and the driver version are supported by looking for them in Supported databases. If necessary, download a newer version of the driver.
  • Is the right JDBC driver being loaded? To find out, in DB Connect, click Configuration in the top navigation bar, Settings, and Drivers to view the driver status screen. You can also search the _internal index for your specific driver's .JAR file. For example: index=_internal sourcetype=dbx_server mysql-*.jar
  • Can you access the database with your browser or database client?
    ♦ To test the connection to an Oracle database, use the Toad Java viewer.
    ♦ To talk to a Postgres database, use the Postgres tool.
    ♦ To talk to other types of databases, try DBVisualizer.

Use one of these tools to connect to the database and ensure that connectivity is good, host and port are correct, and that your credentials work. Then, copy those settings to DB Connect and try again.

**RPC server certificate expiration**

When you install Splunk DB Connect and the RPC server is set to use SSL, DB Connect generates an RPC server SSL certificate with a validity period of two years at $SPLUNK_HOME/etc/apps/splunk_app_db_connect/certs/default.jks. It's a good idea to periodically check the validity of the certificate by running the following command:

```
$JRE_Installation_Path$/bin/keytool -list -v -keystore $SPLUNK_HOME/etc/apps/splunk_app_db_connect/certs/default.jks
```

To renew the certificate, delete the default.jks file just before or after it is set to expire, and it will be regenerated.

**Issues with bad line breaking/line merging**

The problem is caused by Splunk line-break heuristics. Typically, log file data includes event timestamps, which Splunk understands. If you have timestamps in your database rows, you'll avoid line-break issues. Be sure to set output timestamp and specify that the timestamp column is the actual timestamp column.
If you don't have timestamps in your database rows

If you don’t have timestamps in your database rows, you have to set the timestamp option to **Current Index Time** when creating an input.

If your timestamp is not of type datetime/timestamp

Splunk DB Connect expects the timestamp column in your database to be of type **datetime/timestamp**. If it is not (for example, it is in format `char/varchar/etc.`), you can first try to convert the SQL statement into the correct type using the `CAST` or `CONVERT` functions. If this method doesn’t work, you can use the following workaround:

In the Set timestamp step when creating or editing an input, next to **Timestamp**, choose the **Choose Column** setting. Then, select the column from the drop down menu. Next, click the **Datetime Format** option, and then specify the timestamp using a Java **DateTimeFormatter** pattern so DB Connect can obey the timestamp output format setting. For example, if the database column `EVENT_TIME` which is the 5th columns from the result contains strings, such as `CHAR, VARCHAR, or VARCHAR2`, with values like `01/26/2013 03:03:25.255`, you must specify the parse format in the appropriate copy of `db_inputs.conf`.

```plaintext
index_time_mode = dbColumn
input_timestamp_column_number = 5
input_timestamp_format = MM/dd/yyyy HH:mm:ss.SSS
```

Unexpected session key expiration

A system clock change or suspend/resume cycle can cause unexpected session key expiration. To remedy the problem, restart the Splunk Enterprise system using DB Connect.

Cannot connect to IBM DB2

IBM DB2 is supported only when the database is running on Linux. Splunk doesn’t test or support DB Connect with DB2 on AS/400 or on Microsoft Windows.

Cannot connect to Microsoft SQL server

If you cannot connect to a Microsoft SQL server, ensure you’ve correctly followed the steps listed in **Microsoft SQL Server**. Specifically, verify that you are using the
correct driver, host, and port:

- **Driver:** You can use either the Microsoft JDBC Driver for SQL Server or the jTDS driver. Be aware that, in contrast to the Microsoft driver, the jTDS driver does not support connecting over Secure Sockets Layer (SSL).

- **Host:** To specify a host for Microsoft SQL, use a fully qualified domain name, a short name, or an IP address. Do not use the Microsoft SQL convention of `<SERVERNAME\DATABASE>` for the host field.

- **Port:** Many Microsoft SQL Servers use dynamic ports instead of TCP/1433. Work with your database administrator to identify the correct port, or see "Verifying the port configuration of an instance of SQL Server" on the Microsoft website.

For more information about using Windows authentication with DB Connect and Microsoft SQL Server, see "Connecting to SQL Server" in the Install database drivers topic.

**Cannot connect to Oracle SQL Server**

If you cannot connect to a Oracle database, first ensure you've correctly followed the steps listed in Oracle database.

**Connect to Oracle using SSL (for encryption only)**

If you're having trouble connecting to Oracle using SSL for encryption:

1. First verify whether the connection works using an external tool that uses JDBC to connect to Oracle, such as DBVisualizer, with the following JDBC URL. Replace the `<host>`, `<port>`, and `<database>` placeholders with their actual values in your setup.

   ```
   jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=<host>)(PORT=<port>))(CONNECT_DATA=(SERVICE_NAME=<database>)))
   ```

   If the connection does not work, work with your database admin to correctly configure SSL for encryption.

2. If the connection works, click **Edit JDBC URL** button and enter the JDBC URL in the **JDBC URL** field. See more details about the JDBC URL settings, see create a database connection.

3. Restart Splunk Enterprise.
**Oracle Error Codes**

If you receive an error attempting to connect to an Oracle database, try the following. The most common error codes are:

**ORA-12504: TNS:listener was not given the SID in CONNECT_DATA**

This error means that the SID was missing from the CONNECT_DATA configuration. To troubleshoot, check that the connect descriptor corresponding to the service name in **TNSNAMES.ORA** also has an SID component in the CONNECT_DATA stanza.

**ORA-12505: TNS:listener does not currently know of SID given in connect descriptor**

You are receiving this error because the listener received a request to establish a connection to the Oracle database, but the SID for the instance either has not yet dynamically registered with the listener or has not been statically configured for the listener. Typically, this is a temporary condition that occurs after the listener has started, but before the database instance has registered with the listener.

To troubleshoot, try waiting a few moments and try the connection again. You should also check which instances are currently known by the listener by executing: `lsnrctl services <listener name>`

**ORA-12514: TNS:listener does not currently know of service requested in connect descriptor**

This error occurs because the listener received a request to establish a connection to the database. The connection descriptor received by the listener specified a service name for a service that either has not yet dynamically registered with the listener or has not been statically configured for the listener.

To troubleshoot, try waiting a few moments and try the connection again. You should also check which instances are currently known by the listener by executing: `lsnrctl services <listener name>`

**Explanation of Oracle TNS Listener and Service Names**

TNS is a proprietary protocol developed by Oracle. It provides a common interface for all industry-standard protocols and enables peer-to-peer application connectivity without the need for any intermediary devices.

DB Connect uses Java (through JDBC driver) to connect Splunk Enterprise to a TNS Listener, which in turn connects to the Oracle Database. You can configure
DB Connect to connect via the Service Name or the Oracle SID. Typically, most connectivity issues with DB Connect and Oracle Databases are caused by misconfiguration of the TNS Listener.

**Settings in local .conf files are not being honored**

If you notice that the custom settings you've specified in .conf files in your DB Connect /local directory are not being honored, here are a few things to try:

- First, be aware that settings specified within a stanza in a .conf file that resides in the /local DB Connect directory will take precedence over the corresponding entry in the same .conf file in the /default DB Connect directory. For more information, see Configuration file precedence.
- Stanza names and .conf file names must match exactly in both the /default and /local directories. The most common cause of this problem is misspellings in stanza names.

**Missing instances of Microsoft SQL Server**

If you have multiple instances of Microsoft SQL Server installed on your server, edit the JDBC connection string to add a parameter that explicitly references the instance you want to contact.

1. Follow the instructions in "Override db_connection_types.conf" to make a copy of the db_connection_types.conf file in the local directory and copy the stanza for the Microsoft SQL Server driver you're using into the file.
2. Edit the jdbcUrlFormat or, if you're connecting using SSL, jdbcUrlSSLFormat setting by appending it with the following:
   
   ;instanceName=

3. Set the instanceName parameter to the name of the instance you want to connect to. For example:
   
   jdbc:sqlserver://dbx-sqlserver.mydomain.com:1433;databaseName=master;instanceName=test

4. Save and close the file, and then restart Splunk Enterprise.

**Incomplete field values are extracted when the value contains double quotes**

When DB Connect encounters a column value during search-time field extraction that contains double quotation marks, it extracts the value, but stops extracting at the first quote. For example, consider this value named string:
string="This is "an extraordinary" event, not to be missed."

DB Connect extracts this as follows:

string="This is "

The rest of the value is ignored.

This occurs because auto-kv extraction will not handle quotation marks inside fields. If you have quotation marks inside fields, you will need to create field extractions for the datasource. For more information about search-time field extractions, see Create and maintain search-time field extractions through configuration files.

**Rows with invalid timestamp value are skipped during indexing**

You may encounter two scenarios in which the input will fail because of invalid timestamp values:

- The data type of the timestamp column is DATE, TIME or TIMESTAMP and it contains NULL.
- The data type of the timestamp column is not DATE, TIME or TIMESTAMP, and it returns invalid value after you convert it to Java date format.

The following screen shot is of the Configure Timestamp Column window from the third step of database input setup. The data format of the highlighted last_update column is VARCHAR. You need to set the data format in [Datetime format](#) under the table.
Unicode decode errors

If while using Splunk DB Connect you see Unicode decoding errors, your database might not be set up to return results encoded in UTF-8. For example, you might see errors in Splunk Enterprise that include the following line if your database is returning results that are not UTF-8-encoded:

```
UnicodeDecodeError: 'utf8' codec can't decode byte 0xe4 in position 30: invalid continuation byte
```

Splunk DB Connect requires that your database connection be set up to return results encoded in UTF-8. Consult your database vendor's documentation for instructions about how to do this.

DB Connect shows a task server communication error

When you launch DB Connect, the RPC service attempts to bind to port 9998 by default. If port 9998 is already in use by another service, you will see an error to load your configurations.

To work around this, you can change the port number to which the RPC service binds. To do this:

1. Go to the settings page from the configuration menu item
2. Edit the Task server port field to set an available port
3. Save your settings
4. The server will restart using this new port setting
Web interface timeouts

If you are experiencing timeouts while using the Splunk DB Connect interface, and hardware and network performance are not an issue, consider increasing the user session timeout values as described in Configure user session timeouts in the *Splunk Enterprise Admin Manual*.

DB Connect opens a lot of DB connections

Scheduled jobs such as inputs and outputs will use and re-use connections from a connection pool (this pool size is 8 by default, see `maxTotalConn` and `useConnectionPool` in `db_connections.conf` to change connection pooling behavior for scheduled jobs). Interactive DBX search commands (`dbxquery`, `dbxlookup`, `dbxoutput`) do not use the connection pool mechanism. Instead, each command execution establishes a new connection to the database server. If this behavior causes performance degradation, you can limit access to the affected connections or configure the database to limit the number of connections allowed for the Splunk DB Connect service account. Please refer to the documentation of your database engine provider to configure this setting.

Debug HTTP Event Collector port issues

In DB Connect 3.0.0, the architecture changed so that the JDBC driver returns the results to a Java thread. The Java thread calls the HTTP Event Collector (HEC) which then sends the results to `splunkd` and populates the indexers.

As a result of this change, you may find that the HEC is not working because of port issues. The following are examples of indicators that HEC is not working:

- **Normal Query** (in the Data Lab > SQL Explorer menu) returns results, but the DB Input does not populate the indexer.
- In the Health > DB Input menu, you see an error.

To validate and resolve the HEC port issues:

1. Navigate to your Splunk search bar and enter `index=*_internal* 8088`, replacing 8088 which whatever your HEC port is.

2. The search returns one of these two messages:

   ◊ FATAL HTTPServer -Could not bind to port 8088 This error comes from splunkd.log
3. To fix HEC port issues, go to Settings > Data Input > HEC > Global Settings and change the port.

4. Restart your instance of Splunk Enterprise.

The performance is slow when output data events from DB Connect to MySQL database

If you encounter issues on poor performance when exporting data events to MySQL database, you need to check your network status. If the issue is due to network latency, you can workaround this by setting rewriteBatchedStatements=true when you edit JDBC URL. See more details about this workaround on JDBC batch insert performance. Note that using this workaround may have some potential issues, see more on MySQL Configuration Properties for Connector

Oracle driver delaying database connection in Linux environments

When deployed in Linux environments, the Oracle driver sometimes causes connection delays. Program your Java Virtual Machine (JVM) to use /dev/urandom instead of /dev/random using one of the following options:

Option 1

1. On your JVM, navigate to Configuration > Settings.
2. Edit the JVM options to override the securerandom.source setting in your Java environment with /dev/urandom:
   -Djava.security.egd=file:/dev/./urandom
3. Navigate to $SPLUNK_HOME/etc/apps/splunk_app_db_connect/local/.
4. Open commands.conf and add an additional argument to dbxquery, dbxlookup, dbxoutput commands. For example:

   [dbxquery]
   command.arg.1 =
   -Dlogback.configurationFile=../config/command_logback.xml
   command.arg.2 = -Djava.security.egd=file:/dev/.urandom
   command.arg.3 = -DDBX_COMMAND_LOG_LEVEL=INFO
   command.arg.4 = -cp
   command.arg.5 = ../jars/command.jar
command.arg.6 = com.splunk.dbx.command.DbxQueryCommand

[dbxoutput]
command.arg.1 =
-Dlogback.configurationFile=../config/command_logback.xml
command.arg.2 = -Djava.security.egd=file:/dev/./urandom
command.arg.3 = -DDBX_COMMAND_LOG_LEVEL=INFO
command.arg.4 = -cp
command.arg.5 = ../jars/command.jar
command.arg.6 = com.splunk.dbx.command.DbxOutputCommand

[dbxlookup]
command.arg.1 =
-Dlogback.configurationFile=../config/command_logback.xml
command.arg.2 = -Djava.security.egd=file:/dev/./urandom
command.arg.3 = -DDBX_COMMAND_LOG_LEVEL=INFO
command.arg.4 = -cp
command.arg.5 = ../jars/command.jar
command.arg.6 = com.splunk.dbx.command.DbxLookupCommand

5. Save your changes.

Option 2

1. Navigate to $JAVA_HOME/jre/lib/security/, and open the java.security file in a text editor.
2. Add the following line: securerandom.source=file:/dev/./urandom
3. Save your changes.

SQL tips and tricks

If you are having trouble configuring Splunk DB Connect database inputs, or if you have written overly complex Splunk Processing Language (SPL) queries to use with your DB Connect inputs, consider instead refining your SQL queries.

• Use the dbxquery search command to write SQL queries directly in the Splunk Enterprise Search & Reporting app.
• When you set up a new database input, use Advanced Query Mode to enter your custom SQL query. In step 2 of the input creation process, you specify a query to run to fetch data from your database. Instead of the default Simple Query Mode, which limits you to simply choosing catalog, schema, and table, choose Advanced Query Mode, then enter your SQL query into the field. You can preview your query results before saving the input.
About NULL values

Splunk does not distinguish NULL and empty values. In other words, for Splunk a NULL value is equivalent to an empty string. If you want to replace NULL value by a well identified value you can use fillnull or eval commands. NULL values can also been replaced when writing your query by using COALESCE function. You can consult your database's documentation about this function for details.

It is also important to note that DB Connect cannot accept NULL values for a rising column or a column used as index time in inputs definition. Such values will cause input jobs to fail.

Use CAST or CONVERT to handle certain column types

Splunk Enterprise supports ASCII text, and cannot directly index binary fields like Binary Large Object (BLOB) and Character Large Object (CLOB). If Splunk Enterprise does not support a column type in your database, or you want to change a column type to a specific type before sending the data to Splunk Enterprise, use the CAST or CONVERT SQL functions to change the type of the column.

The CAST and CONVERT functions convert a value from one data type to another. CONVERT provides additional style functionality and more complex conversions, but Oracle discourage its use in current Oracle database releases.

Use CAST or CONVERT to improve date and time handling

Splunk Enterprise assigns timestamps to indexed event data at index time. You can also specify a column for time stamp extraction when you configure an input. If the column is DATETIME, no additional configuration is required.

If they are not in DATETIME columns, you need to help Splunk recognize the timestamps in your database. If the column is a VARCHAR or string, then you can pre-process the data using Java DateTimeFormatter. Alternatively, you can convert the timestamp to the correct datatype using a custom SQL statement with CAST, CONVERT, or TO_TIMESTAMP functions. Use SQL to change your string column type into a DATETIME column to set the index time value.

Many data sources may contain multiple date or time columns that you do not need to set the index time value, but which you do need to be present the data in readable, friendly formats. In this scenario, use a custom SQL statement with CAST or CONVERT functions to turn epoch values into a locale-oriented date and
time, shift a local time to UTC, or trim a detailed timestamp to a broader date value.

**Use REPLACE or SUBSTRING to modify value quoting**

If you have problems involving quotation mark processing during search-time field extraction or indexing (such as the "Incomplete field values are extracted when the value contains double quotes" troubleshooting issue), modify your quotation marks. Modify quotation marks, or any punctuation mark, in event data before Splunk Enterprise processes the events by using either the REPLACE or SUBSTR SQL functions.

Use the REPLACE function to replace every occurrence of a quotation mark (" or other character with another character or string. Use the SUBSTR function to return a portion of the string, beginning at a position in the string that you specify.

Be aware that these SQL functions are not equivalent to the replace($X,Y,Z$) and substr($X,Y,Z$) evaluation functions that you can use in Splunk Enterprise with the eval, fieldformat, and where search commands. The REPLACE or SUBSTR SQL functions execute before Splunk Enterprise receives data, while the replace($X,Y,Z$) or substr($X,Y,Z$) evaluation functions execute at search time in Splunk Enterprise. Use the former to ensure that Splunk Enterprise properly indexes values with spaces or other delimiter characters.

**Use AS to change column names**

To change the names of columns before either indexing or running lookups, you can use the AS keyword to create an alias. You can use aliases to create a temporary name for columns, making the column headings easier to read when you are retrieving results.

The basic syntax to alias a column in SQL is as follows:

<column_name> AS <alias_name>

In this example, <column_name> is the name of the column that you want to alias, and <alias_name> is the alias you want to assign to the column.

In the following example, you rename the MIN(price) field as cheapest. Therefore, cheapest is the name of the second column that Splunk Enterprise returns to DB Connect in the result set.
SELECT category, MIN(price) AS cheapest
FROM items
GROUP BY category

**Use CASE, COALESCE, or CONCAT to compare and combine two fields**

You have several options to compare and combine two fields in your SQL data. The following examples describe situations in which you can use CASE, COALESCE(), or CONCAT() to compare and combine two column values. Use either query wrapping (inline views) or an advanced mode database input to use the resulting columns as a rising column. Inline views are enabled by default. For more information, see Use inline views (query wrapping) and Use an advanced mode database input, in this topic.

**CASE**

Use the CASE expression to take actions based on the result of a conditional expression. For example, use a SQL statement like the following if you have two fields that you want to conditionally merge into one.

```sql
CASE WHEN first_name IS NOT NULL THEN last_name AS full_name
```

**COALESCE()**

The COALESCE() function is shorthand for the CASE expression, and returns the first non-null expression that it finds within its arguments. For example, use a SQL statement like the following if you have several fields that you want to conditionally merge into one. This returns the first existing field.

```sql
COALESCE(first_name,middle_name,last_name) AS full_name
```

**CONCAT()**

Use the CONCAT() function to concatenate, or combine, fields. It is equivalent to the || operator. For example, use a SQL statement like the following if you have two fields that have values that you want to merge into one:

```sql
CONCAT(first_name,last_name) AS full_name
```

The following example is only possible with an advanced mode database input, which replaces the question mark (?) character with a checkpoint value. For more information about advanced mode, see Advanced in the Create and manage database inputs topic.

```sql
SELECT CONCAT(last_name, first_name) as NAME, ACTOR_ID, FIRST_NAME, LAST_NAME FROM actor WHERE CONCAT(last_name, first_name) > ? ORDER BY CONCAT(last_name, first_name))
```
Terminology

Splunk DB Connect terminology

access controls

Also known as role-based access controls (RBAC), access controls comprise a system for defining access policy based on the system rather than the user. Splunk DB Connect uses the RBAC system in Splunk Enterprise, in which you define roles and assign users to them. Users can belong to multiple roles. A user's access to a given resource or action reflects what's specified in the permissive role to which that user belongs. For more information, see Configure security and access controls.

batch input

In batch input mode, the app invokes the same query each time and returns all results. Batch input mode is ideal for use with historical data that will not change and will be consumed and indexed once. For more information, see Create and manage database inputs.

connection

A database connection object contains the necessary information for connecting to a remote database. For more information about connection objects, see Create and manage database connections.

database input

A database input object lets you fetch and index data from a database. Database inputs are what enable Splunk Enterprise to query your database, identify the data to consume, and then tag and index the data. Once you've set up a database input, you can use that input just as you do any other data input you have defined in Splunk Enterprise. For more information, see Create and manage database inputs.

database lookup

A database lookup object enables you to enrich and extend the usefulness of your Splunk Enterprise data by fetching additional data from your external
database. For more information, see Create and manage database lookups.

**database output**

A **database output** object lets you define how to send data from Splunk Enterprise to a database on a recurring basis. Define database outputs to store your indexed Splunk Enterprise data in a relational database. For more information, see Create and manage database outputs.

**identity**

An **identity** object contains database credentials. It comprises the username and obfuscated password that DB Connect uses to access your database. For more information about identity objects, see Create and manage identities.

**permissions**

Permissions indicate the level of access you assigned to a role. The access specifies how a user with that role can interact with knowledge objects such as identities and connections in Splunk Enterprise. **Read access** to an object means that Splunk Enterprise roles are able to use the object. **Read-write access** to an object means that Splunk Enterprise roles are able to use and modify the object. For more information, see Configure security and access controls.

**rising column**

A **rising column** input finds the new records you want and returns only those records with each query. When you create a rising column input type, you must specify the rising column. You can specify as rising column any column whose value increases over time, such as a timestamp or sequential ID. The rising column is how DB Connect keeps track of which records are new. For more information, see Create a database input.

**role**

A **role** is a collection of permissions and capabilities. You assign roles to users in Splunk Enterprise. The roles a user belongs to determine which identity, connection, input, output, and lookup objects that user is able to see and interact with in Splunk DB Connect. For more information, see Configure security and access controls.
task server

A task server enables Splunk DB Connect to send and receive data via JDBC. The task server is an instance of a web server that listens on a dedicated port (9998 by default) for instructions to connect to a database.

table

A database table is collection of data organized by intersecting vertical columns and horizontal rows. Rows and columns intersect in cells.