DB Connect Is Back

…and it is better than ever

Tyler Muth | Denis Vergnes

September 2017 | Washington, DC
Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.
Overview

What is this about again?
Splunk DB Connect

RDBMS and Splunk Bridge

- Performant
- Flexible
- Real-time
What Can You Do With It?
Use cases for structured data in Splunk

Import

Enrich

Export

Explore
What’s New?
DB Connect 3 content

Ease of use
WYSIWYG SQL and SPL editors, new UI, input bulk operations, input template

Performance
Performance boost up to 10x, vertical scalability

Flexibility
Stored procedures, 14 supported databases, Linux and Windows platform
Ease of Use
Ease of Use

- New UI to manage inputs, outputs, lookups
  - Wizard based
  - Type ahead dropdowns
  - Filterable tables
  - More .conf options: query time out, time range, application context
UI Improvements

▶ New UI
  - Wizard based
  - Type ahead dropdowns
  - Filterable tables
  - More conf options: query time out, time range, application context
Input Bulk Operations
One query to many inputs

▶ Time saver
  • Create or edit many similar inputs at the same time

▶ Flexible
  • Input can still be edited individually

1. Select Connections
2. Write query
3. Set properties
4. Save inputs
Input Templates

A better version of cookies mix

- Pre-made inputs
- 3 fields away to data collection
  - Connection
  - Input name
  - Index
Add-ons With Template
From an add-on to DB Connect

- Splunk Add-on for Oracle Database 3.7.0
  - Templates for metrics, auditing

- Splunk Add-on for Microsoft SQL Server 1.3.0
  - Templates for metrics, auditing, monitoring

- Splunk Add-on for McAfee 2.2.0
  - Template for EPO version 5

- Splunk Add-on for Nagios Core 1.1.0
  - Template for monitoring, configuration
Health checks

Is everything OK?

- Pre-built panels to monitor DB Connect
- Installation checks with Splunk Enterprise 6.5 and above
Performance
Under the hood

▶ Architecture change
  • Resource pooling is removed
  • Checkpoints are stored locally
  • Scheduled jobs: 1 JVM
  • Commands: 1 JVM per execution

▶ What does it mean?
  • SHC doesn’t run scheduled tasks (inputs, outputs)
  • No out-of-the-box solution for HA
  • No SQL connection pooling for commands
Performance – Queries

The improvement increases with dataset size, up to 4 times faster.
Performance – Outputs

Large datasets are output 2-9 times faster than version 2.4.x
Performance – Lookups

Large datasets are collected 1.5 times faster than version 2.4.x
Performance – Inputs

- Throughput of a single input remains the same as 2.3.x (about 2.5MB/s)
- Vertical Scalability:

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Concurrent inputs @60s interval</th>
<th>Overall throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 cores 16GB Linux VM</td>
<td>1600</td>
<td>20 MB/s</td>
</tr>
<tr>
<td>16 cores 16GB Linux VM</td>
<td>2000</td>
<td>25 MB/s</td>
</tr>
</tbody>
</table>
Demo

Show me!
Q&A

Don't forget to rate this session in the .conf2017 mobile app