splunk>

FACT SHEET

Splunk® DB Connect

Reliable, Scalable, Real-Time Integration
with Relational Databases

HIGHLIGHTS

- Enrich Splunk search results with structured data from relational databases
- Explore and browse database schemas and tables
- Import and index data from relational databases for analysis and visualization in Splunk software
- Process machine data in Splunk Enterprise and export it to relational databases
- Connect new databases in minutes and scale to multiple concurrent databases

Integrate Splunk Enterprise to Relational Databases

Splunk DB Connect delivers reliable, scalable, real-time integration between Splunk Enterprise and traditional relational databases. Integrate structured data from relational databases with machine data in Splunk Enterprise to drive deeper levels of analysis and Operational Intelligence.

With Splunk DB Connect you can look up data in relational databases to enrich Splunk search results with business context. Or explore and browse database schemas and tables in relational databases before deciding to import data into Splunk for more comprehensive analysis. You can also process machine data in Splunk Enterprise and export it to relational databases.

Key Features and Benefits

Splunk DB Connect provides the following core features:

Database Lookup – Enrich machine-generated data by adding structured data from relational databases. By using Splunk Enterprise and Splunk DB Connect, key values contained in machine data can be used to reference related business data in relational databases, such as device addresses, product codes and media identifiers. For example, telecom providers can combine real-time service activation data with profile data from a customer master database to understand what types of customers are purchasing what types of plans—enabling in-depth real-time sales and customer analytics not possible before.

Explore Database Schemas – Browse and navigate database schemas and tables from the Splunk DB Connect user interface before deciding to import data into Splunk. View schemas, table names and user permissions, all from within the Splunk user interface. Splunk DB Connect supports stored procedures and any SQL 92 compliant query.

Import and Index Data from Relational Databases into Splunk Enterprise – Combine structured data from relational databases with machine data to drive end-to-end operational insights. The Splunk **Tail** command can be use to detect updated or new rows in the database by referencing time stamp values. Splunk DB Connect also enables you to import data via periodic snapshots of the database—where database tables are recorded from a single point in time. Grant user permissions to query only certain databases and restrict connections to read-only mode. Allow the input and output of data to be effectively unlimited to work with large data sets. Splunk DB Connect supports streaming and batch modes.

Process Data in Splunk Enterprise and Export It to Relational Databases – Leverage Splunk software as a key element of your data processing pipeline. Process machine data from multiple sources in Splunk Enterprise by combining and correlating it, and exporting it to relational databases for additional analysis. **Dboutput** is a Splunk search command that enables you to update existing records or add new records in a relational database.

Connection Pooling and Caching – For faster performance, Splunk DB Connect provides many performance-enhancing options, including the ability to execute multiple database commands that can run concurrently, run multiple active database connections, cache table metadata information, size the thread pool for database querying and cache the database lookup definitions.

Search Language Extensions – Splunk software lets users search and navigate their data from one place. Splunk DB Connect includes search language extensions that can be executed directly from the Splunk user interface. **Dbquery** and **Dbinfo** are Splunk search commands that enable you to execute database queries

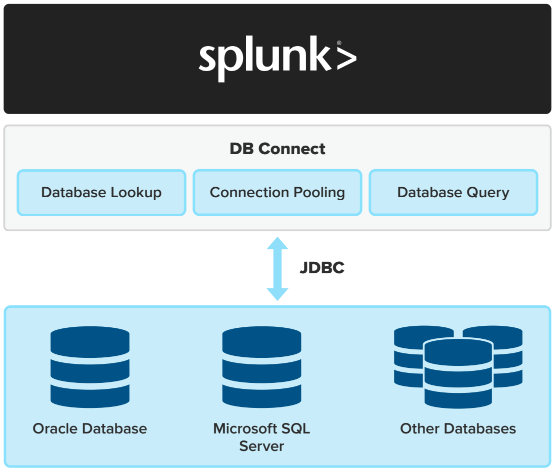

Figure 1: Integrate database information with the power of Splunk DB Connect's analytics and visualizations.

directly from the Splunk Enterprise user interface. **Dbinfo** fetches schema information from the database. **Dbquery** performs SQL queries and presents the results as Splunk visualizations. For example, dbquery database=ASSETDB “SELECT hostname, owner, department from host_information WHERE location LIKE ‘%NY%.’”

Splunk DB Connect in Action

Monitoring Critical Business Process to Optimize Revenue Cycle

A leading U.S.-based supplier of healthcare information technology solutions leverages Splunk DB Connect to gain real-time visibility into the patient eligibility process to improve its revenue cycle. Patient eligibility is a complex process that spans multiple systems—both within and outside an organization. Visibility into this process is important to ensure that patients get the right care at the right time, and that healthcare providers are reimbursed in a timely manner so they can continue to provide high-quality services.

With Splunk, the supplier has immediate visibility into this critical business process to improve patient and provider experience. The company can mitigate issues before they become critical, improve its processes, and also help clients improve their own business practices for best patient and provider experience.

Increasing Revenue by Understanding the Customer Journey

Trade Me is New Zealand’s leading online marketplace and classified advertising site. The company uses Splunk software for IT infrastructure monitoring and data analysis across its many websites, mobile apps and relational databases to gain insights into customer journeys, preferences and bidding actions. Insights are analyzed in real time to show the implications of new site features, photos, listings or marketing campaigns.

Splunk DB Connect helps Trade Me associate and integrate clickstream data, machine data from web logs, syslogs and access logs with structured data from the firm’s Microsoft SQL Server relational databases. Key values contained in Trade Me’s unstructured machine data are used to reference related business data contained in the SQL Server databases. All these mash-ups happen in real time, enabling a deeper understanding of customer behavior, bidding activities, popularity of listings and more. This provides business users with actionable insights to increase revenue and user engagement.

Improving Customer Experience Through Unified 360° View

Oscar Health uses technology to make health insurance simple, intuitive and human. Departments across Oscar Health leverage Splunk DB Connect to query and gain real-time insights from operational relational databases.

For example, the Finance Team leverages Splunk software and DB Connect to understand member demographics by age, plan type and gender. The Sales Team uses the software to gain visibility into effective policyholders at the beginning of every month. The Customer Service Organization—the largest user of Splunk software within Oscar—uses Splunk solutions to gain a unified view of Oscar members. Customer service representatives can deliver superior and personalized services, by reviewing member information in correlation with medical claims history, doctor visits, prescription data, web activity and prior customer service interaction. This visibility also enables Oscar Health to ensure appropriate resources are available to manage member queries and gain visibility into agent performance.

Product Requirements

Supported Databases

Splunk DB Connect is compatible with most relational databases including Teradata, IBM DB2, IBM Informix®, Oracle® Database, Microsoft® SQL Server, SAP Sybase®, PostgreSQL, MySQL™, SQLite, H2, HyperSQL, MemSQL and support for a generic ODBC driver. Refer to the Splunk DB Connect product documentation for the complete list of relational databases supported.

Splunk Requirements

All instances of Splunk Enterprise in a Splunk DB Connect deployment must run Splunk Enterprise 5.x and 6.x.

Free Download

Download Splunk and Splunk DB Connect for free. You’ll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual free license or purchase an Enterprise license by contacting sales@splunk.com.