Database data

Databases are the fundamental elements of information collection, storage and analysis of digital information. Databases are categorized as either relational, in which data is organized in spreadsheet-like tables of columns and rows, or NoSQL (nonrelational), where information is organized purely by columns (column store) as key-value pairs, by unstructured documents or interconnected graphs linking related data elements.

Structured Query Language (SQL) statements are the main interface in relational databases. SQL statements are used to create, read, update, and delete data in the database. Visibility into this activity enables you to do all of the following and more:

- Detect and identify long running queries as candidates for optimization
- Detect and identify slow queries as candidates for optimization
- Monitor trends in query behavior for capacity and planning
- Detect unauthorized data access
- Attest to compliance with data governance controls and rules

In the Common Information Model, database query data is typically mapped to the Databases data model.

Application

When your Splunk deployment is ingesting database data, you can use it to accomplish security and compliance, IT Ops, and application delivery use cases.

- Analyzing wire data from databases
- Identifying database performance issues
- Monitoring AWS Relational Database Services (RDS) with Splunk Infrastructure Monitoring

Source types

Guidance for onboarding data can be found in the Splunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud). In addition, these Splunk Add-Ons and Apps are helpful for working with antivirus data.

- Splunk Add-on for Oracle Database
- Splunk DB Connect
- Splunk Add-on for MySQL
- Splunk Add-on for Microsoft SQL Server