Analyzing wire data from databases

Wire data is data contained within the headers and payloads of network packets as traffic moves from one node to another. The transaction payload is analyzed in real time and metadata is generated on those transactions. The metadata is a rich source of user and application information, and it can be used to troubleshoot performance issues, create activity baselines, and discover IT assets and their dependencies.

You want to extract this end-to-end visibility from the wire data related to database transactions at your organization in order to shorten mean time to repair (MTTR) and maintain full operational database availability.

You can use Splunk software to analyze key metrics related to database queries so that the queries can be optimized for the best possible performance and the effects of other systems on your database can be understood. These metrics include which are queries most common, most resource intensive, slowest to generate a response, and more.

Data required

Database data

The Splunk Stream app is the most common way to get wire data into Splunk, and it has source types included for popular databases (Oracle, MS-SQL, MySQL, and Postgres). Getting database data into Splunk from non-wire sources is done with log file ingestion and sometimes in combination with Splunk DB Connect with the associated technical add-on, such as the Splunk Add-on for Oracle Database or the Splunk Add-on for Microsoft SQL Server. Splunk DB Connect is used to query the database system tables to get information about the database.

How to use Splunk software for this use case

You can run many searches with Splunk software to analyze wire data from your databases. Depending on what information you have available, you might find it useful to identify some or all of the following:

- Top ten slowest database queries
- Trends in database query response times
- Trends in database query counts
- Top ten highest network utilization queries
- Top ten most common database queries

Next steps

To maximize their benefit, the how-to articles linked in the previous section likely need to tie into existing processes at
your organization or become new standard processes. These processes commonly impact success with this use case:

- Database administration tasks. will be guided with this data as it can correlate to external services that rely on the database. The wire data captured helps with end-to-end visibility between clients and database activity, augmenting native database monitoring features.
- Application development. Data from this use case allows you to visualize the impact of calls from the application made to the database.
- Middleware is frequently part of a database application. Profiling middleware would be beneficial as an important service to most applications.

Measuring impact and benefit is critical to assessing the value of IT operations. The following are example metrics that can be useful to monitor when implementing this use case:

- Mean time to resolution (MTTR): Databases are a key component to most applications, and being able to quickly identify problem areas and correct the causes will improve the quality of applications and service, as well as free up engineering time. Each ticket that is opened on a problem should be measured for time to resolve. These procedures and derivatives will enable staff to reduce mean time to resolution (MTTR).
- Number of database trouble tickets: Trending and prediction capabilities should allow for corrective action to be taken before a problem results in a trouble ticket. The number of tickets associated with databases and their dependencies should be reduced with the use of these procedures and derivative procedures. This should be measured at the ticketing system and grouped by application and tagged with Splunk, if you have these and similar procedures actively used. The grouping and tagging facilitate the measurement of the efficiency of Splunk.

This use case is also included in the IT Essentials Learn app, which provides more information about how to implement the use case successfully in your IT maturity journey. In addition, these Splunk resources might help you understand and implement this use case:

- Conf talk: [The path to operational enlightenment: an introduction to wire data](#)
- Conf talk: [Real-time Oracle monitoring with Splunk](#)
- Conf talk: [Service and Asset Discovery with Wire Data](#)