Reporting on key trade statistics in a brokerage

Employees at your brokerage need to know the status of their trades within their process and their flow. You want to use your Splunk deployment to store all process events in one location to be searched with common IDs and to present key statistics for the trades.

Data required

Business service data for trades

Procedures

- Splunk recommends that customers look into using data models, report acceleration, or summary indexing when searching across hundreds of GBs of events in a single search. The searches provided here are a good starting point, but depending on your data, search time range, and other factors, more can be done to ensure that they scale appropriately.
- To optimize the search shown below, you should specify a time range. You may also need to adjust field names (such as trade ID) to match what is available in your application logs and lookup files.

Top customers trading

By knowing who are your top customers trading, you can separate them out in your data to make offers and treat them with a certain status. Extract the fields that represent customer or account ID from your data, then run the following search.

```
|sourcetype=<trade logs>
|top customer limit=10
|sort - count
|fields - percent
```

Status of a trade in application logs

Knowing the status of trades is important for optimizing trade flows and troubleshooting as trades travel from front office to back office (application to application) and for reporting. By tracing a trade through time through your trade logs, you can find out where it went during each step and at which step it might have gotten stuck. Extract the fields that represent the trade ID, then run the following search.

If the field names are different across your application logs, you can use the coalesce command shown in the following sample search to collapse them into one name. Otherwise, that line of the search is not necessary.
Pricing statistics for bought and sold symbols

Statistics on buy and sell orders such as min, max, mean, and standard deviation of price can help analysts make decisions in near-real time using machine data rather than relying on a hourly report. This search provides an indicator of how the market is moving for any time slice. Extract the fields that represent symbols and price from your data, then run the following search, changing the action to “sell” when needed.

```
| sourcetype=<trade logs>  
| sort - _time  
| eval tradeID=coalesce(tradeID, tradeIDReceived, tradeIDSent)  
| stats list(_raw) BY tradeID  
```

Total trading volume for bought and sold symbols

Knowing the highest quantity bought or sold by symbol provides insights into market trends. This quantity and symbol list changes hour to hour and day to day, so this search provides an indicator of how the market is moving for any time slice. Extract the fields that represent symbols and quantity from your data, then run the following search, changing the action to "sell" when needed.

```
| sourcetype=<trade logs>  
| sort - _time  
| where action="buy"  
| stats min(price) as min_price max(price) AS max_price stdev(price) AS stdev_price mean(price) AS mean_price BY symbol  
| eval min_price=tostring(round(min_price, 2),"commas"), max_price=tostring(round(max_price, 2),"commas"), stdev_price=tostring(round(stdev_price, 2),"commas"), mean_price=tostring(round(mean_price, 2),"commas")  
```

Next steps

The Splunk Essentials for the Financial Services Industry app helps you automate the searches provided in this article. The app also provides more insight on how they can be applied in your environment, how they work, the difficulty level, and what data can be valuable to run them successfully. In addition, the Splunk Essentials for the Financial Services Industry app provides a number of other monitoring and reporting solutions for brokerage services, such as complying with MFID.

Finally, these additional Splunk resources might help you understand and implement this use case:

- [Conf Talk: 40 ways to use Splunk in financial services](#)