Monitoring new customer logins to financial applications

A key measurement for improving bank customer experience is new user logins. This can help banks know what kind of experience new users are having, as well as any forced conscience denial to let the customer login. Analytics can improve customer experience.

Data required

Business service data for consumer financial applications

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.

• Some commands, parameters, and field names in the searches below may need to be adjusted to match your environment. In addition, to optimize the searches shown below, you should specify an index and a time range when appropriate.

► New account login denials

After registering for online banking access, users might be denied access for a variety of business reasons. You want to see when this occurs in your organization's software. Extract the fields that represent errors from your data, then run the following search.

|sourcetype=<consumer financial application data source> |eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S") |sort _time |where action="denied" |table _time, customer, action, sessionID, location

If a user was denied and then authorized, there might be an error in your software. You want to see if this happens in your system and, if so, how many times per day. Extract the fields that represent denial and authentication from your data, then run the following search.

|sourcetype=<consumer financial application data source> |eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S") |sort _time |stats first(action) AS first_action last(action) AS last_action last(_time) AS _time by customer,
New account login errors

After registering for a login, a customer receives an error upon first time logging in. You need a search that shows you when this happens so that you can look into the problem further. Extract the fields that represent errors from your data, then run the following search.

```
sourcetype=<consumer financial application data source>
|eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")
|sort _time
|where action="error"
|table _time, customer, action, sessionID, location, ResponseTime
```

New account login response times

After registering for access, a user might experience a longer than usual response time to log in. How many customers were effected by this bad user experience and should they be contacted? Extract the fields that represent customers and response times from your data, then run the following search.

```
sourcetype=<consumer financial application data source>
|eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")
|sort _time
|stats avg(ResponseTime) AS averageResp BY customer,location
|eventstats avg(averageResp) AS avg stdev(averageResp) AS stdev
|where averageResp>(avg+4*stdev)
```

Further, by comparing response times from different hours, it is possible to see if your application is behaving normally or abnormally. Extract the fields that represent response times from your data, then run the following search.

```
sourcetype=<consumer financial application data source>
|eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")
|sort _time
|timechart span=5m fixedrange=F count
timewrap 2h series=exact
```

New account action comparisons

Side-by-side comparisons provide useful information on trends. A trellis chart tells you how each action is performing over time with its own timechart. This is useful for side-by-side comparisons to chart customer experience. Extract the fields that represent actions such as authorized, denied, or error from your data, run the following search, and then view the results in a Trellis chart.

```
sourcetype=<consumer financial application data source>
|eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")
```

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
New account activity by location

A chart of new account login attempts over location by time can give you insight into how new account logins are performing with respect to location and time. Extract the fields that represent actions and locations from your data, then run the following search.

```
sourcetype=<consumer financial application data source>
eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")
sort _time
timechart span=15m fixedrange=F count(action) AS action BY location
```

You might also be interested in login actions by location. If some locations have fewer authorized actions than others, it may be time to investigate the customer experience.

```
sourcetype=<consumer financial application data source>
eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")
sort _time
chart count OVER location BY action
```

You can also use a timechart to specifically compare authorizations versus denials by location.

```
sourcetype=<consumer financial application data source>
eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")
sort _time
timechart span=15m fixedrange=F count(eval(action="authorized")) AS authorized
    count(eval(action="denied")) AS denied BY location
```

Finally, a timechart of different response times split by location provides insight into how new account logins are performing with respect to login response time. This can help you determine whether your services are functioning normally or out of the ordinary. For instance, if one location has an instant response time while another is taking several seconds, there might be a latency issue.

```
sourcetype=<consumer financial application data source>
eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")
sort _time
timechart span=15m fixedrange=F avg(ResponseTime) AS averageResponseTime BY location
```

Next steps

Errors and long response times can lead to a bad customers experience. Use the data from the searches in this use case to make decisions about what is normal for your application and what outcomes need troubleshooting. You might also want to consider what to do with customer who routinely have poor experiences with your application. Should these customers be tracked in other parts of the multi channel bank?
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 financial services:

- ATM usage statistics
- Retail banking transactions
- Credit card statistics

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

- .Conf Talk: 40 ways to use Splunk in financial services