Salesforce

Salesforce data is a type of CRM, ERP, and other business application data that provides insight into the usage and adoption of the Salesforce platform. The data can also be used for security and troubleshooting purposes. The data is gathered by Splunk via modular inputs that poll the Salesforce APIs at a configurable interval.

Salesforce data can be used to search and report on user activity such as logon analytics, review browsing history by user to tell which features are being adopted. For security monitoring, you can also track behaviors for unauthorized access and for data loss prevention.

Configuration

Guidance for onboarding data can be found in the Splunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud). Refer to the documentation, and note the following:

- Recommended index: sfdc
- Source type: sfdc*
- Input type: Modular inputs
- Add-on or app: Splunk Add-on for Salesforce
- Sizing estimate: The best way to estimate sizing is to send the data to Splunk and use the monitoring console to get ingest sizing by index or sourcetype. Data ingest will vary widely, but an estimated baseline is 100/MB per day per item.

Validation

The first step in validating the logs is to run a search and confirm that the index is getting data in the proper time frame and that the source types and sources are as expected. Further validation is done by inspecting the events and making sure the needed fields are seen. A search similar to the following is a good starting point.

```
| tstats values(sourcetype) WHERE index=sfdc group by index
```

Application

When your Splunk deployment is ingesting Salesforce data, you can use the data to achieve the following:

- Protecting a Salesforce cloud deployment