Heya

## Overview

## Phase 1 - Configuration

Using **Splunk Python** a script should be able to do the following:

Using a Sumo access/key id:

* Create a HTTPS hosted collector in the customer instance

## Phase 2 - Collection

Get the following files and send them to the above Sumo HTTPS endpoint

|  |  |  |
| --- | --- | --- |
| File Path | Type | Description |
| $SPLUNK\_HOME/etc/apps/\*/\*/data/ui/views/\*.xml | Dashboards (App) |  |
| $SPLUNK\_HOME/etc/users/\*/\*/local/data/ui/views/\*.xml | Dashboards (User) |  |
| $SPLUNK\_HOME/etc/apps/\*/\*/\*.conf | Config (App) |  |
| $SPLUNK\_HOME/etc/users/\*/\*/\*/\*.conf | Config (User) |  |
| $SPLUNK\_HOME/etc/system/\*/\*.conf | Config (System) |  |
| $SPLUNK\_HOME/search\_pool/etc/apps/\*/\*.conf | Config (Pool - App) |  |
| $SPLUNK\_HOME/search\_pool/etc/users/\*/\*.conf | Config (Pool - User) |  |
| $SPLUNK\_HOME/etc/slave-apps/\*/\*.conf | Config (Cluster - Apps) |  |
| $SPLUNK\_HOME/etc/apps/\*/metadata/\*.meta | Permissions |  |
| $SPLUNK\_HOME/etc/licenses/enterprise/\*.lic\* | Licensing |  |
| $SPLUNK\_HOME/etc/passwd | Accounts (Local) |  |
| $SPLUNK\_HOME/search\_pool/pooling/pooling.ini | Config (Pool) |  |
| $SPLUNK\_HOME/etc/splunk.version | Version |  |
| $SPLUNK\_HOME/log/web\_access.\* | Usage (Web) |  |
| $SPLUNK\_HOME/log/splunkd\_access.\* | Usage (API) |  |
| $SPLUNK\_HOME/log/audit.\* | Usage (Audit) |  |
| $SPLUNK\_HOME/etc/users/\*/\*/history/\*.csv | Usage (User) |  |
| $SPLUNK\_HOME/search\_pool/etc/users/\*/\*/history/\*.csv | Usage (Pool - User) |  |
| $SPLUNK\_HOME/log/license\_usage.\* | Usage (License) |  |

We have historically asked users to manually run these in their own Splunk environment, however these would be better suited to a local authenticated REST API call.

|  |  |  |
| --- | --- | --- |
| Query | Type | Description |
| index=\_internal source=\*license\_usage.log\* type=Usage  | eval gb=b/1024/1024/1024  | bin \_time span=1d  | stats sum(gb) AS daily\_gb BY \_time  | stats avg(daily\_gb) AS average\_daily\_ingest\_gb | Usage (License) |  |

## Phase 3 - Reporting

> Comparative performance