MLTK SETUP GUIDE

- ## INSTALLATION

    1. Download “Splunk Machine Learning Toolkit” of version 4.5.0 or above from splunkbase - https://splunkbase.splunk.com/app/2890/
    2. This app can be installed either through UI from "Manage Apps" or by extracting the compressed file into **`$SPLUNK_HOME$/etc/apps`** folder.
    3. Restart Splunk

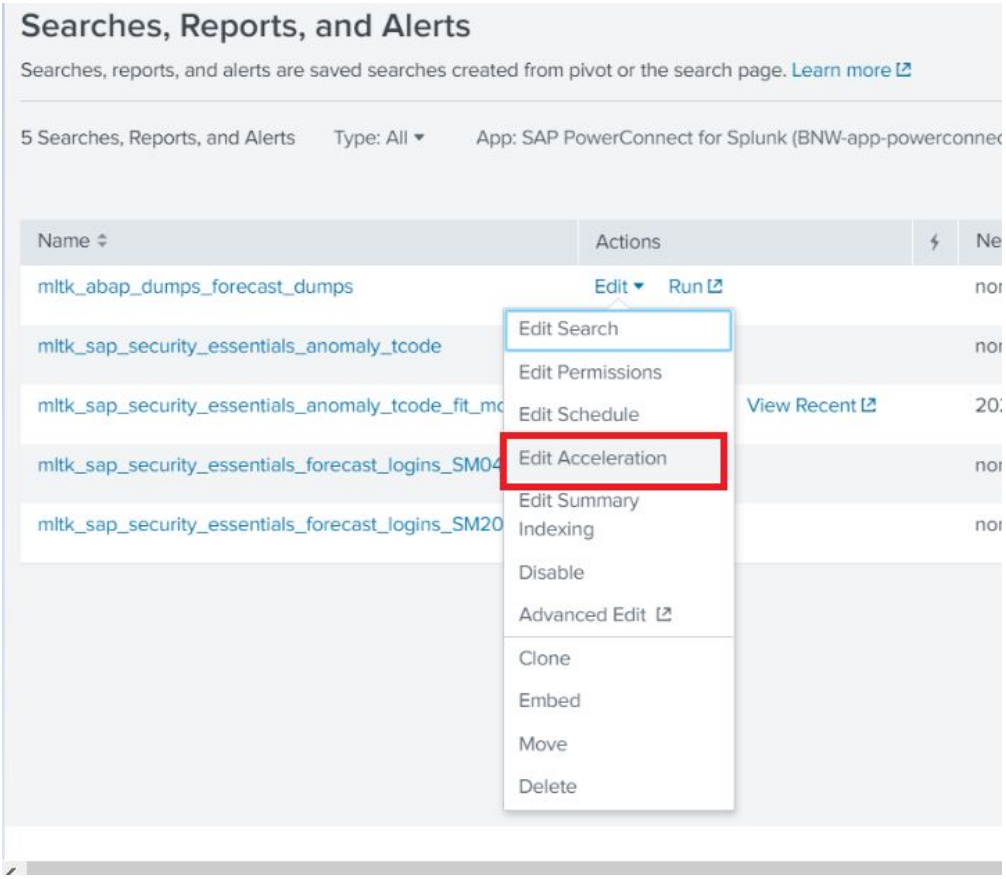
- ## SAVEDSEARCHES

    The following saved searches are used to improve the search performance for the MLTK panels by acceleration. By default this feature is disabled. Users need to manually enable the acceleration

    1. "mltk_sap_security_essentials_anomaly_tcode" - For the "Anomaly Detection: T-Code Executions" panel present in SAP Security Essentials dashboard.
    2. "mltk_sap_security_essentials_forecast_logins" - For the "Forecasting: User Logins" panel present in SAP Security Essentials dashboard.
    3. "mltk_abap_dumps_forecast_dumps" - For the "Forecasting: ABAP dumps" panel present in ABAP Dumps dashboard.

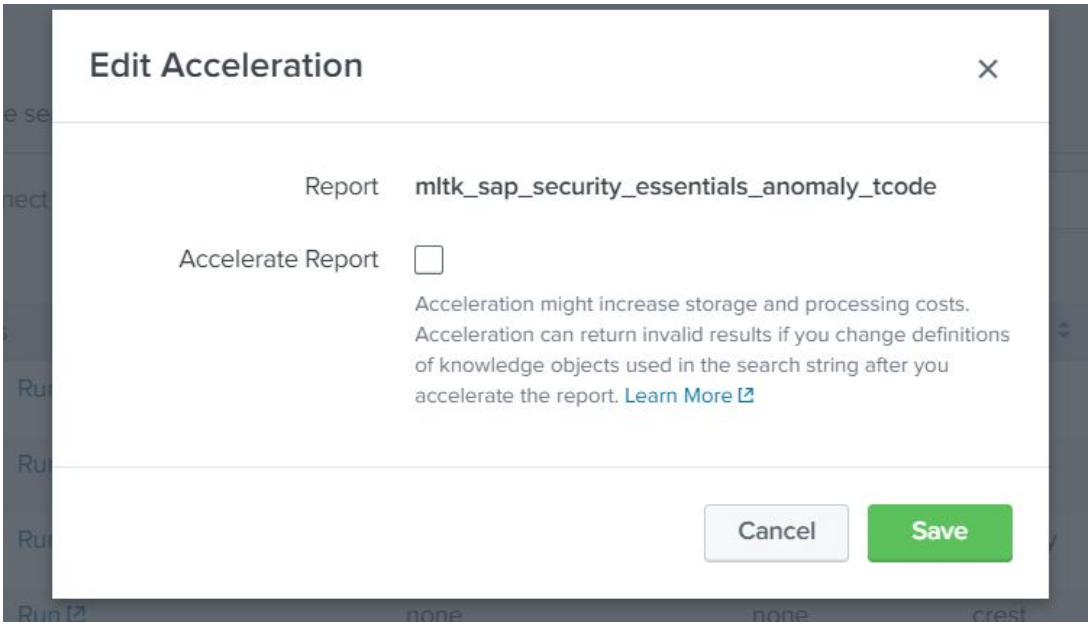
    The steps to change the acceleration are:-

    1. On Splunk's menu bar, Click on Settings -> Searches, reports, and alerts.
    2. Select SAP Powerconnect for Splunk (BNW-app-powerconnect) in App.
    3. Click on "Edit" dropdown under "Actions" and click on "Edit Acceleration" for the savedsearch you want to enable acceleration for.



I. Under the Acceleration label, you will find "Accelerate this search" check box.

II. By making a check / uncheck "Accelerate Report" check box, the acceleration option of savedsearch will be enabled/disabled.



III. Click on "Save".