Syncsort Ironstream® Dataset Analyzer

Introduction

The Ironstream® Dataset Analyzer app has been supplied for you to add to your Splunk® installation. This app includes dashboards intended to give a flavor of what is possible with Ironstream and the data feed from your z/OS™ platform.

Note: These instructions are based on the latest (6.2+) versions of Splunk. Steps may vary depending upon the version you are using and different setup may be required to achieve a successful deployment.

App Installation and Setup

Before beginning you should have installed a copy of Ironstream. If this is not the case, contact your Syncsort representative. You can obtain further information from:

http://www.syncsort.com/en/Products/Mainframe/Ironstream

Install the App

Sign in to Splunk as an administrative user and follow these steps to install the app:

On the Splunk home page, click the **Manage Apps** cogwheel (top left, above the list of current apps):

1. On the **Apps** page, click **Install app from file**.
2. Click **Browse** or **Choose File** on the **Upload app** dialog and locate the downloaded **Syncsort_Ironstream_Dataset_Analyzer.spl** file. Select it and click **Open**.
3. Leave the **upgrade app** option unchecked.
4. Click **Upload**. The app and its associated components will be installed into Splunk.
5. The installation file will be processed and you may prompted for a Splunk restart.

Populate an Ironstream Index

The Dataset Analyzer app processes several types of SMF data. A Splunk index containing the following SMF types is required:

SMF 14	INPUT or RDBACK dataset activity
SMF 15	OUTPUT, UPDAT, INOUT, or OUTIN dataset activity
SMF 17	Scratch dataset activity
SMF 30	Common Address Space activity
SMF 80	RACF (security) activity

Please refer to the **Ironstream Configuration** section below or the Ironstream documentation for configuration steps to allow the index to be populated with at least the above data types.

Critical Datasets Dashboard Lookup File

The app allows customization of the datasets monitored by the "Critical Dataset Tracking" dashboard. An external lookup CSV file is supplied for you to alter according to your own requirements. It can be found in the following directory of your Splunk installation:

.\etc\apps\Syncsort_Ironstream_Dataset_Analyzer\lookups\CriticalDatasets.csv

Please **DO NOT** alter the first line of this file. It is used to identify the data in the file. Append the datasets you wish to monitor below the first line; each dataset name on a new, separate line.

Customize the App

The app is just an example of what can be achieved with Ironstream and Splunk. You are free to change any aspect of the app to suit your own requirements.

You can add, remove or modify the dashboard panels and charts as follows:

1. Sign in to Splunk as an administrative user.
2. Select a dashboard within the app.
3. Click **Edit** to reveal the menu below and choose **Edit Panels**
4. You can now interact with the dashboard panels and charts:
   a. Change their titles, size, location etc.
   b. Make search and timescale changes.
   c. Alter chart types and options.
5. Click **Done** to commit any changes.

Alternatively, you can modify the source XML of the dashboard. This is achieved as follows:

1. Sign in to Splunk as an administrative user. You should see an **Edit** button top, right of the dashboard.
2. Click **Edit** to reveal the menu below and choose **Edit Source XML**
3. The dashboard XML source is displayed.

> You are advised to take a copy of the XML source before making any changes

4. Make your changes and click **Save**.

App Compatibility

The app was created and tested with Splunk version 6.2+. It may not be 100% compatible with earlier Splunk versions.

If you are running a version of Splunk prior to 6.2 you may wish to unzip the package file (Syncsort_Ironstream_Dataset_Analyzer.spl) and extract the XML from the following view to check for compatibility:

.\etc\apps\Syncsort_Ironstream_Dataset_Analyzer\default\data\ui\views\syncsort_ironstream_Dataset_Analyzer_monitor.xml

Ironstream Configuration

Ironstream forwards selected z/OS messages and information for Splunk apps to process and use for reporting purposes. Ironstream is delivered with appropriate messages filters in place but we recommend the ASMFILTR job be run with the following messages specified for filtering in the SSDFFSMF step:

```
//SSDFFSMF EXEC ASMSSDF
//ASM.SYSIN DD *
SSDFFSMF TITLE '- IRONSTREAM MESSAGE SELECTION TABLE'
*---------------------------------------------------------
* THIS SAMPLE TURNS ON ALL SMF RECORD TYPES SUPPORTED IN
* IRONSTREAM VERSION 1.2
*---------------------------------------------------------
        SSDFFSMF 00, 14, 15, 17, 19, 30, 42, 60, 61, 62, 64, 65,
                 66, 70, 71, 72, 73, 75, 76, 77, 80, 100, 101,
                 102, 110, 113, 117, 118, 119, 120, 208
        END
//*---------------------------------------------------------
```

SMF types 14, 14, 17, 30 and 80 are required for the Dataset Analyzer app to function.

Feedback, Questions, Problems

We welcome your questions, comments and feedback. Please do not hesitate to contact your Syncsort representative.