Syncsort Ironstream® SYSLOG Dashboard

Introduction

The Ironstream® SYSLOG dashboard has been supplied for you to add to your Splunk® installation. This dashboard includes some panels 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 steps may be required to achieve a successful deployment.

Dashboard Installation

Before beginning you should have downloaded a copy of the Ironstream demonstration to a locally accessible location. A free trial is available at:

> http://www.syncsort.com/en/TestDrive/TestDriveIronstream

Install the Dashboard

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

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_Syslog.spl** file. Select it and click **Open**.
3. Leave the **upgrade app** option unchecked.
4. Click **Upload**. The dashboard and its associated components will be installed into Splunk.
5. The installation file will be processed and you may prompted for a Splunk restart.

Create the Ironstream Index

A new Splunk index is required. By default this is called **Ironstream**. This is the storage location for the SYSLOG data sent from z/OS™ by Ironstream.

1. Sign in to Splunk as an administrative user and click **Settings** | **Indexes** to view the list of existing index definitions.
2. Click **New** to display the **Add new** dialog.
3. Enter **Ironstream** into the Index name field. Complete the other fields according to your requirements.
4. Click **Save** to create the index.

Note: If you use another name for the index the dashboard will not work without modification. See below for details on how to modify the dashboard.

Add a Port Monitor

You will need to create a Splunk port monitor to allow data to flow from Ironstream on z/OS™ to the target index:

1. Sign in to Splunk as an administrative user and click **Settings** | **monitor** to start the **Add Data** set up process.
2. Click the **TCP / UDP** entry.
3. **Select Source:**
    i. Ensure TCP is chosen on the page that appears and enter the port number you have designated for incoming z/OS™ data.

> The port number **MUST** match the number in the settings for Ironstream on z/OS™

4. Click **Next**.
5. **Input Settings**:
    i. Choose **Select** for the **Sourcetype** and **Structured** | **_json**.
    ii. **App context**: Select **Syncsort Ironstream® SYSLOG** (name of the app - see above).
    iii. **Host: IP | DNS | Custom** selection will depend upon your own network.
    iv. **Index:** Select the **Ironstream** index (you may need to click **Refresh**).
6. Click **Review**.
7. If you are happy with the settings, click **Submit** to create the port monitor.

The port monitor will not direct inbound Ironstream data to the target index.

Restart Splunk

If something is not working correctly restart your Splunk instance to ensure the dashboard and associated components are fully available.

Modifying the Dashboard

The dashboard is just a basic sample of what can be achieved with Ironstream and Splunk. You are free to change any aspect of the dashboard 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. You should see an **Edit** button top, right of the dashboard.
2. Click **Edit** to reveal the menu below and choose **Edit Panels**
3. 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.
4. 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**.

Examples of what you can change:

- You can alter the embedded searches to return different z/OS™ SYSLOG data.
- Use an alternative index name instead of **Ironstream**. If you do this, you will also need to:
    - Alter the Ironstream settings in z/OS™ to ensure the correct Splunk index is receiving data.
    - Ensure the Splunk port monitor is referencing the correct index.
    - Update the dashboard XML to use the alternate index name.
        - Change all references from:

          index=ironstream to index=<name of your choice>
- Add, remove or alter the panels displayed on the dashboard.
- Alter the frequency the dashboard panels are updated.

Dashboard Compatibility

The dashboard was created and tested with Splunk version 6.2.3. 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_Syslog.spl) and extract the XML from the following view:

.\etc\apps\Syncsort_Ironstream_Syslog\default\data\ui\views\syncsort_ironstream_syslog.xml

Ironstream Compatibility

The dashboard requires Ironstream to forward certain syslog messages in order for them to be processed and reported correctly. 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 SSDFFLOG step:

```
//SSDFFLOG EXEC ASMSSDF
//ASM.SYSIN DD *
SSDFFLOG TITLE '- SYSLOG SAMPLE MESSAGE SELECTION TABLE'
SSDFFLOG SELECT=(ACF2,CICS,DB2,DB2L,IEF,IMS,RACF,TOPS,USS, +
WAS,WEBS), +
CHAR3=(CSV), +
CHAR4=($HAS)
END
//*-----------------------------------------------------------
```

Feedback

We welcome your comments and feedback. If you have any comments or questions please do not hesitate to contact your Syncsort representative.