

Introduction

This package contains the SplunkFeed Plugin to the Data Feed extension. This Data Feed extension allows one to maintain "replica" data for IBM SOAR incidents, artifacts, tasks, notes, etc. The updates are performed in near real-time.

This plugin allows this replica data to be maintained in Splunk.

Refer to the documentation on the Data Feed extension for uses cases support and configuration options. Also refer to the other Data Feed plugins which can be used in combination.

License

Unless otherwise specified, contents of this repository are published under the MIT open-source [LICENSE](#).

Release Notes

Version	Date	Notes
1.1.1	10/2022	Fix to handle rare corrupt event.message
1.1.0	5/2022	Replaced base component, adding attachment content, workspace separation, more control over auto data reload.
1.0.3	9/2020	App Host and Proxy Support

1.1.0 Changes

This release modified the base portion of the Data Feeder which is controlled by the `[feed]` section within the app.config file. New parameters have been added which you need to manually add if upgrading from a previous version:

Parameter	Value(s)	Capability
reload_types	incident,task,note,artifact,attachment,<data_table_api_name>	use reload_types to limit the types of objects when reload=true. Leave empty to include all data.

Parameter	Value(s)	Capability
workspaces	"Default Workspace": ["sqlserver_feed"], "workspace A": ["kafka_feed", "resilient_feed"]	This setting allows for the partitioning of Data Feeder execution among different workspaces. The format is to specify the workspace name with the data feeder components to associated with it: "workspace": ["app.config section_name"]. If unused, data from all workspaces is accessed.
include_attachment_data	true/false	set to true if attachment data should be part of the sent payload. When 'true', the attachment's byte data is saved in base64 format.

Compatibility

SOAR Compatibility: 30.0 or higher

CP4S Compatibility: 1.4 or higher

Installation

The data feeder app for Splunk contains Python components that are called by the IBM SOAR platform. It can either be installed directly in the app for management and execution through the App Host, or installed on your own Integration server, running our integration framework: resilient-circuits. It is preferred that an enterprise use App Host, as all the component installation and dependencies are already packaged.

App Host

Simply install the .zip file into the app. It includes:

- Rules to automatically share incident data with Splunk. Review the rules which start with 'Data Feeder:' if you wish to reduce the types of information shared. To share datatable data, create a new rule specifying the datatable and assign it to 'data_feed' destination. See the [app.config file](#) section for more information on how to configure your data feed environment.

Integration Server

Install the Python components

Complete the following steps to install the Python components:

- Ensure that the environment is up-to-date, as follows:

```
sudo pip install --upgrade pip
sudo pip install --upgrade setuptools
sudo pip install --upgrade resilient-circuits
```

- Run the following commands to install the package:

```
unzip rc_data_feed-<version>.zip (must be at least version 2.1.0)
[sudo] pip install --upgrade rc_data_feed-<version>.tar.gz
unzip rc_data_feed-plugin-splunkfeed-<version>.zip
[sudo] pip install --upgrade rc_data_feed-plugin-splunkfeed-
<version>.tar.gz
```

- Configure Resilient-circuits

The Resilient Circuits process runs as an unprivileged user, typically named integration. If you do not already have an integration user configured on your appliance, create it now. Complete the following steps to configure and run the integration:

- Using sudo, switch to the integration user, as follows:

```
sudo su - integration
```

- Use one of the following commands to create or update the resilient-circuits configuration file. Use -c for new environments or -u for existing environments.

```
resilient-circuits config -c
or
resilient-circuits config -u [-l rc-data-feed-plugin-splunkfeed]
```

app.config file

- Edit the app.config configuration file, as follows:
 - In the [resilient] section, ensure that you provide all the information required to connect to the IBM SOAR platform.
 - In the [splunk_hec_feed] section, configure the settings for your splunkfeed environment.
 - In the [feeds] section, define the feed(s) you intend to use and create separate sections for each feed. For example:

```
[feeds]
# comma separated section names. ex. sqlserver_feed,file_feed
feed_names=splunk_hec_feed
reload=False
# use reload_types to limit the types of objects when reload=true.
# Ex: incident,task,note,artifact,attachment,<data_table_api_name>
```

```
reload_types=  
# set to true if Elasticsearch errors occur during reload=true  
reload_query_api_method=false  
  
# feed_data is the default message destination that will be listened to  
queue=feed_data  
  
# set to true if attachment data should be part of payload send to plugins  
include_attachment_data=false  
# if necessary, specify the supported workspace (by label, case sensitive)  
and the list of feeds associated with it  
# ex: 'Default Workspace': ['sqlserver_feed'], 'workspace A':  
['kafka_feed', 'resilient_feed']  
workspaces=
```

SplunkHECFeed Class

The SplunkHECFeed class utilizes the Splunk HTTP Event Collector for data import. This is convenient as the data from IBM SOAR is readily converted to JSON which can be natively consumed by Splunk.

Key	Values	Description
class	SplunkHECFeed	Indicates that the section is for Splunk ES.
token	Ex. 81e2d4bb-c008-49ac-a7a7-c0bf408c999	API token defined for the HEC data input.
host	Ex. splunk.yourorg.com	
port	Ex. 8088	The default is 8088
index	Ex data_feeder	The name of the index already defined.
event_host	Ex. myorg.com	Optional host name to record as the source of the events.
event_source	Ex. resilient	Optional source name of the events. Specifying a value improves searching
event_source_type		Optional source_type if one value is used for all events. If unspecified, each object type (incident, task, note, etc.) is used as the source_type
use_ssl	True	False

Considerations

- Enable the HTTP Event Collector within Splunk ES before using this data feed.
- Splunk events are immutable. IBM SOAR object changes are represented as new events. No event deletion is possible.

- Be aware that when using `reload=True`, all IBM SOAR records will be duplicated in Splunk each time resilient-circuits is re-started. Use the app.config setting `reload_types` to specify the data sent if you want to either limit the object types or to also include datatables.

Splunk Configuration

Follow these steps to create an HTTP Event Collector:

1. Go to Settings and select Indexes.
2. Create an index for data feeder. Your requirements will guide you to the correct settings. We have tested with Index Data Type **Events** and App **Search and Reporting**.

New Index [X]

General Settings

Index Name:
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type: ☒ Events ☐ Metrics
The type of data to store (event-based or metrics).

Home Path:
Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).

Cold Path:
Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path:
Thawed/resurrected db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check: ☒ Enable ☐ Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index:
Maximum target size of entire index.

3. Go to Settings and select Data Inputs.
4. For HTTP Event Collector, click the **Add new** Action.
5. Enter information about your collector, specifically, the index(es) to enable and the Default Index. No other settings are necessary (such as Source Type) but can be added for further identification.

Edit Token: Data Feeder

Description

optional

Source

optional

Set Source Type

Entered sourcetype ▾

Source Type

▾

Select Allowed Indexes (optional)

Available indexes

add all >

audit_summary

cim_modactions

data_feeder

endpoint_summary

history

Selected indexes

< remove all

data_feeder

resilient

Select indexes that clients will be able to select from.

Default Index

data_feeder ▾

Output Group (optional)

None ▾

Enable indexer acknowledgement

☐

Cancel

Save

6. Once created, copy the Token Value for use in the app.config token setting.

HTTP Event Collector

Global SettingsNew Token

Data Inputs > HTTP Event Collector

5 TokensApp: Allfilter20 per page ▾

Name	Actions	Token Value	Source Type	Index	Status
Data Feeder	EditDisableDelete	8dda4b40-acfb-4b81-8d72-		data_feeder	Enabled

Additional Data Feed Documentation

For more information on the setup and use of the data feeder, including the use of the Data Sync Incident function, refer to the [Data Feeder Documentation](#).