Introduction

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

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

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.

History

Version	Date	Notes
1.0.1	08/2020	App Host support
1.0.0	12/2019	Initial release

License

Unless otherwise specified, contents of this repository are published under the MIT open-source LICENSE.

Installation

The integration package contains Python components that are called by the Resilient platform. These components run in the Resilient Circuits integration framework. The package also includes Resilient customizations that will be imported into the platform.

App Host Installation

With App Host, all the run-time components are pre-built. Perform the following steps to install and configure:

1. Within Resilient, navigate Administrative Settings and then Apps.
2. Click on the Install button and select the downloaded app-rc_data_feed_plugin_elasticfeed-x.x.x.zip file. This step will install the associated rules and message destination.
3. Once installed, navigate to the app's Configuration tab and edit the app.config file updating the [resilient] section as necessary and updating the [elastic_feed] section to reflect the location and authentication settings for your instance of Elasticsearch.

Integration Server Installation

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-plugin-elasticsearch-<version>.zip
[sudo] pip install --upgrade rc_data_feed-plugin-elasticsearch-<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-elasticsearch]
```

- Edit the resilient-circuits configuration file, as follows:
    - In the [resilient] section, ensure that you provide all the information required to connect to the Resilient platform.
    - In the [feeds] section, define the feed(s) you intend to use and create separate sections for each feed. For example: feed_names=elastic_feed
    - In the [elastic_feed] section, configure the settings for your elasticsearch environment.

```
[feeds]
feed_names=elastic_feed
reload=True
# feed_data is the default queue that will be listened to
queue=feed_data

[elastic_feed]
class=ElasticFeed
url=http://localhost
port=9200
# if using multiple organizations, consider indexes such as resilient_<org_ID>
# each document type will append to this index as elastic 6.0 onlyl supports one document
type per index
```

```
index_prefix=resilient_
#auth_user=
#auth_password=
cafile=false
```

ElasticFeed Class

This class allows you to write all incoming data to ElasticSearch. The data representation within Elastic is referenced by index, document type (incident, note, task, artifact, etc.) and document_id (incident_id, note_id, task_id, etc.). The following configuration items are supported:

Key	Values	Description
class	ElasticFeed	Indicates that the section is for an ElasticSearch.
url		Ex. https://eliastic.yourorg.com URL of Elastic server. Port is specified in it's own parameter.
port		Ex. 9200 Default is 9200
index		Ex. resilient if using multiple organizations, consider indexes such as resilient<org_ID>
auth_user		User and password to authenticate to ElasticSearch.
auth_password		User and password to authenticate to ElasticSearch.
cafile	True	False Specify 'false' to bypass certification authentication

Considerations

• ElasticSearch allows for the updating to and deleting of individual documents. No data duplication occurs. A recently deleted custom datatable column may also not update until circuits is re-run or until the datatable is edited in the UI. Consult section 7.2 of the rc-data-feed documentation for datatable limitations in general.