fn-joe-sandbox-analysis Functions for IBM Resilient

Release Notes

v1.0.4

- Apphost support

v1.0.3

- Bug fixes

v1.0.1

- Bug fixes & proxies

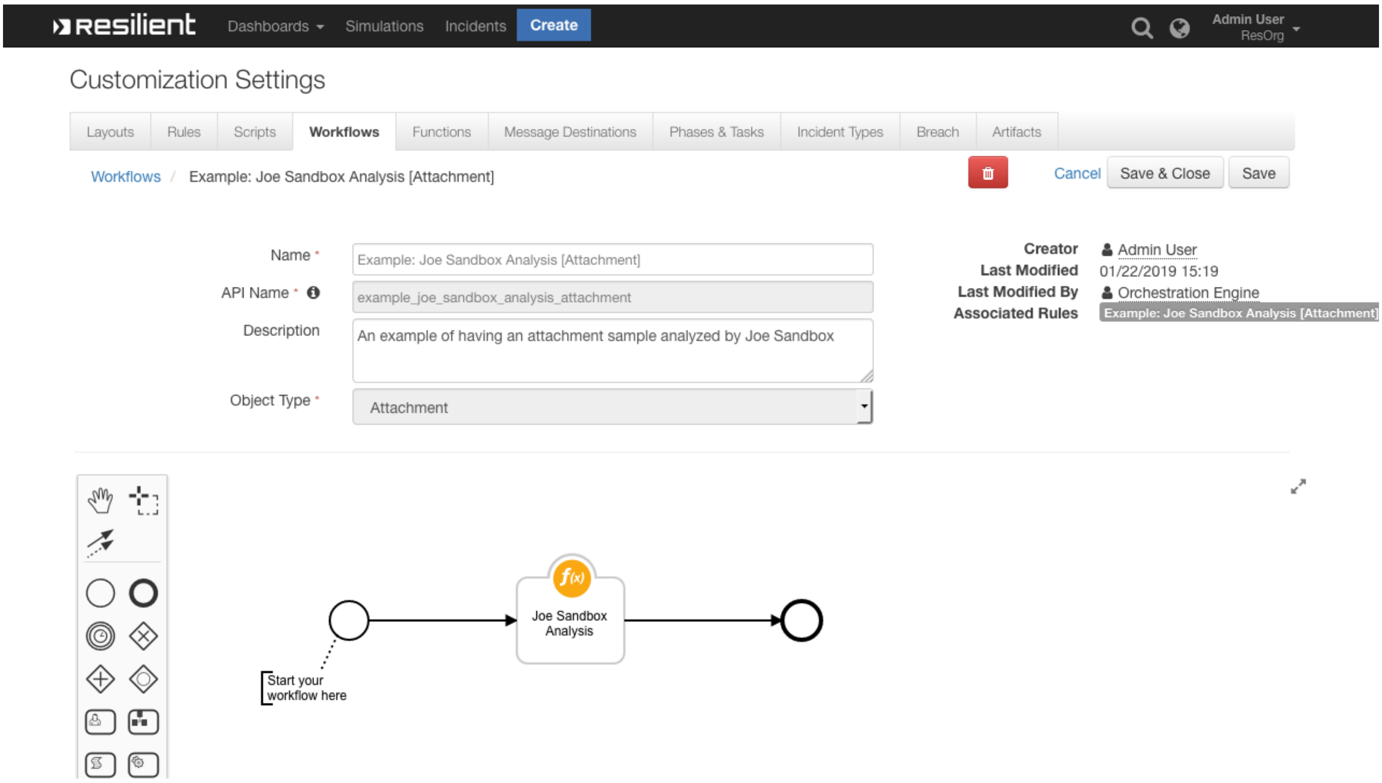
v1.0.0

- Initial Release

Overview

Resilient Circuits Joe Sandbox functions

This package contains a function that executes a Joe Sandbox Analysis of an Attachment or Artifact and returns the Analysis Report to IBM Resilient.



Customization Settings

Workflows / Example: Joe Sandbox Analysis [Attachment]

Name * Example: Joe Sandbox Analysis [Attachment]

API Name * example_joe_sandbox_analysis_attachment

Description An example of having an attachment sample analyzed by Joe Sandbox

Object Type * Attachment

Creator Admin User

Last Modified 01/22/2019 15:19

Last Modified By Orchestration Engine

Associated Rules Example: Joe Sandbox Analysis [Attachment]

Requirements

- Resilient platform >= `v38.2.3`
- An Integration Server running `resilient_circuits>=32.0.0`
  - To set up an Integration Server see: ibm.biz/res-int-server-guide
  - If using API Keys, minimum required permissions are:
    - Org Data: Read, Edit
    - Function: Read

Installation

App Host

All the components for running this integration in a container already exist when using the App Host app.

To install,

Navigate to Administrative Settings and then the Apps tab.

Click the Install button and select the downloaded file: `app-joe_sandbox_analysis-1.0.4.zip`.

Go to the Configuration tab and edit the app.config file, editing the API key for fn_joe_sandbox_analysis qand making any additional setting changes.

Integration Server

- Download the `fn_joe_sandbox_analysis.zip`.
- Copy the `.zip` to your Integration Server and SSH into it.
- **Unzip** the package:

```
$ unzip fn_joe_sandbox_analysis-x.x.x.zip
```

- **Change Directory** into the unzipped directory:

```
$ cd fn_joe_sandbox_analysis-x.x.x
```

- **Install** the package:

```
$ pip install fn_joe_sandbox_analysis-x.x.x.tar.gz
```

- Import the **configurations** into your app.config file:

```
$ resilient-circuits config -u -l fn-joe-sandbox-analysis
```

- Import the fn_joe_sandbox_analysis **customizations** into the Resilient platform:

```
$ resilient-circuits customize -y -l fn-joe-sandbox-analysis
```

- Open the config file, scroll to the bottom and edit your fn_joe_sandbox_analysis configurations:

```
$ nano ~/.resilient/app.config
```

Config	Required	Example	Description
jsb_accept_tac	Yes	`True`	*Enter a description of the config here*
jsb_api_key	Yes	``	*Enter a description of the config here*
jsb_analysis_url	Yes	`https://jbxcloud.joesecurity.org/v2/analysis`	*Enter a description of the config here*
jsb_analysis_report_ping_delay	Yes	`120`	*Enter a description of the config here*
jsb_analysis_report_request_timeout	Yes	`1800`	*Enter a description of the config here*

- **Save** and **Close** the app.config file.
- [Optional]: Run selftest to test the Integration you configured:

```
$ resilient-circuits selftest -l fn-joe-sandbox-analysis
```

- **Run** resilient-circuits or restart the Service on Windows/Linux:

```
$ resilient-circuits run
```

Uninstall

- SSH into your Integration Server.
- **Uninstall** the package:

```
$ pip uninstall fn-joe-sandbox-analysis
```

- Open the config file, scroll to the [fn_joe_sandbox_analysis] section and remove the section or prefix `#` to comment out the section.
- **Save** and **Close** the app.config file.

Troubleshooting

There are several ways to verify the successful operation of a function.

Resilient Action Status

- When viewing an incident, use the Actions menu to view **Action Status**.
- By default, pending and errors are displayed.
- Modify the filter for actions to also show Completed actions.
- Clicking on an action displays additional information on the progress made or what error occurred.

Resilient Scripting Log

- A separate log file is available to review scripting errors.
- This is useful when issues occur in the pre-processing or post-processing scripts.
- The default location for this log file is: `/var/log/resilient-scripting/resilient-scripting.log`.

Resilient Logs

- By default, Resilient logs are retained at `/usr/share/co3/logs`.
- The `client.log` may contain additional information regarding the execution of functions.

Resilient-Circuits

- The log is controlled in the `.resilient/app.config` file under the section [resilient] and the property `logdir`.
- The default file name is `app.log`.
- Each function will create progress information.
- Failures will show up as errors and may contain python trace statements.

Support

Name	Version	Author	Support URL
fn_joe_sandbox_analysis	1.0.4	IBM Resilient	http://ibm.biz/resilientcommunity