This integration allows one to capture log entries from an integrations server for viewing and troubleshooting. This capability avoids the need to manually access and collect the logs.

Key Features

- filter logs by date (before, on or after a specified date and time)
- filter logs entries by number of log entries to return (ex. last 1000 lines)
- filter by minimum log level: DEBUG, INFO, WARNING and ERROR
- Retain log files as an attachment

fn-log-capture Functions for IBM Resilient

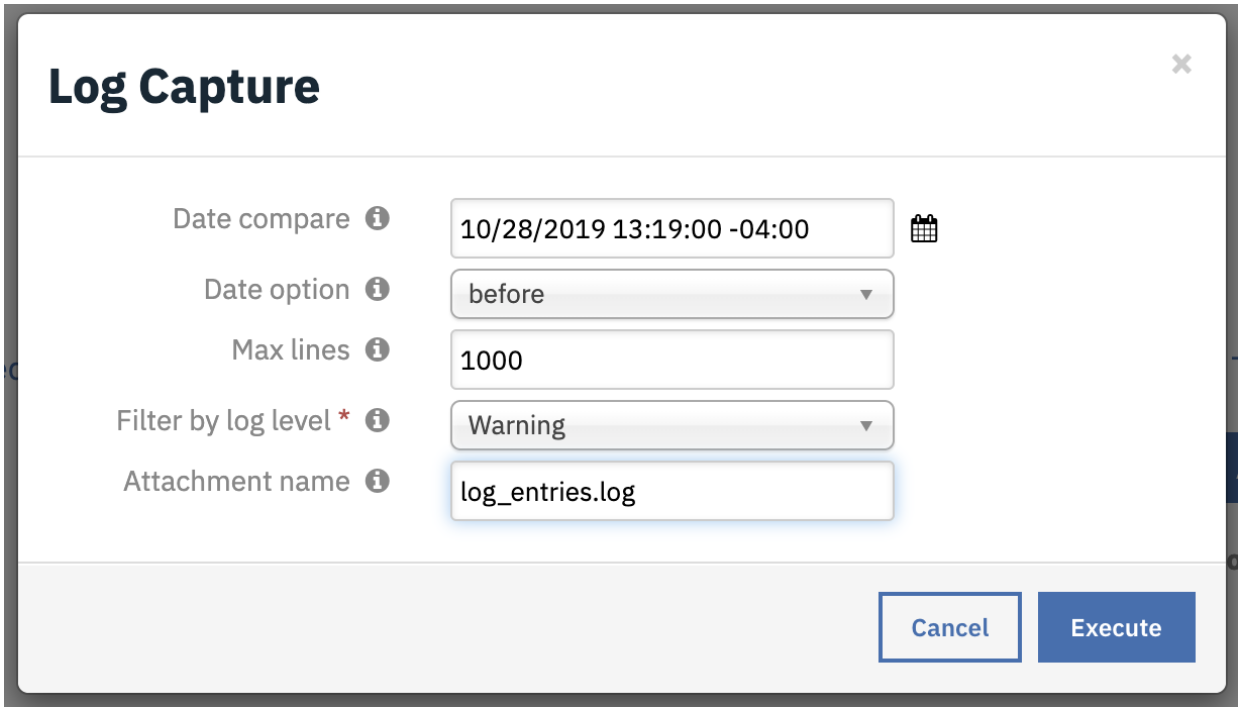
Release Notes

v1.0.0

- Initial Release

Overview

Resilient Circuits Components for 'fn_log_capture



Requirements

- Resilient platform >= `v32.0.4502`
- An Integration Server running `resilient_circuits>=30.0.0`
    - To set up an Integration Server see: ibm.biz/res-int-server-guide

Installation

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

```
$ unzip fn_log_capture-x.x.x.zip
```

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

```
$ cd fn_log_capture-x.x.x
```

- **Install** the package:

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

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

```
$ resilient-circuits customize -y -l fn-log-capture
```

- [Optional]: Run selftest to test the Integration you configured:

```
$ resilient-circuits selftest -l fn-log-capture
```

- **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-log-capture
```

Usage

- The Log Level represents the minimum value matched. For instance, DEBUG will also report INFO, WARNING and ERROR.
- All filter fields are additive. For instance, using an *after* compare date with maxlines will return the number of lines specified at the end of the log file (trimming the first set of lines).
- If the log file name is left blank, a system generated name is created in the format: <hostname>_resilient-circuits_<date_time>.log
- If you have more than one active Integration Server, this function cannot be installed on all. Presently there is no easy solution to allow mulitple installations of a function to target a specific integration server.

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.

No additional configuration required.

Support

Name	Version	Author	Support URL
fn_log_capture	1.0.0	IBM Resilient	support@resilientsystems.com