fn-whois-rdap Functions for IBM Resilient

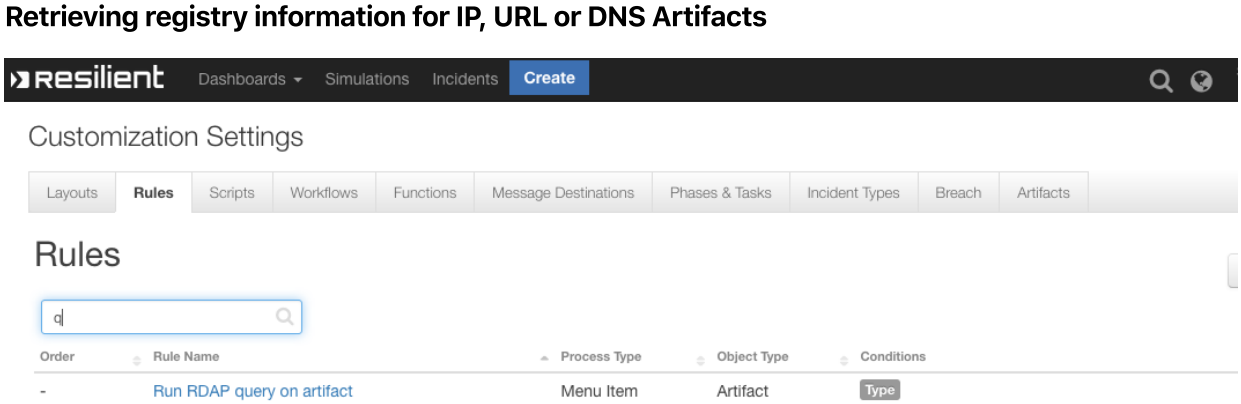
Release Notes

History

Version	Comment
1.0.2	Updated examples
1.0.1	Support for App Host
1.0.0	Initial release

Overview

Retrieving registry information for IP, URL or DNS Artifacts



This integration retrieves registry information (via legacy WHOIS or new RDAP protocol) for IP, URL or DNS Artifacts that provides enrichment and threat intelligence on suspicious address. The information is added directly to artifact description and can include dns-zone, asn and asn description & other useful metadata.

Requirements

- IBM Resilient >= v35.0.5468
- An Integration Server running resilient_circuits>=32.0.0

- To setup an Integration Server see the Integration Server setup documentation

App Host Installation

All the components for running Whois in a container already exist when using the App Host app.
Once installed, review the app.config file in the Customizations tab.

```
[fn_whois_rdap]
# uncomment to include proxy support
#proxy_https=https://some_proxy.com
#proxy_http=http://some_proxy.com
```

Integration Server Installation

- Download the app-fn_whois_rdap-x.x.x.zip.
- Copy the .zip to your Integration Server and SSH into it.
- **Unzip** the package:

  ```
  $ unzip app-fn_whois_rdap-x.x.x.zip
  ```

- **Install** the package:

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

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

  ```
  $ resilient-circuits customize -y -l fn-whois-rdap
  ```

- **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-whois-rdap
  ```

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

View the community forums for help with this app.