fn-pa-panorama Functions for IBM Resilient

- Release Notes
- Overview
- Requirements
- Installation
- Uninstall
- Troubleshooting
- Support

Release Notes

v1.0.1

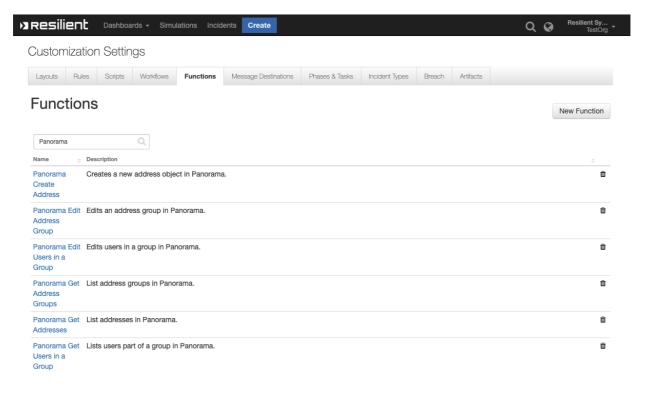
· App Host support

v1.0.0

Initial Release

Overview

Resilient Circuits Components to Integrate with the Panorama Platform



Contains Functions to get and edit addresses groups, get and create addresses, and get and edit users in a group within Panorama.

Requirements

- IBM Resilient >= v35.2
- An App Host paired with Resilient or an Integration Server running resilient_circuits>=30.0.0
 - To setup and pair an App Host with Resilient, visit the IBM Knowledge Center
 - To setup an Integration Server see: ibm.biz/res-int-server-guide
- resilient-lib>32.0.140
- Panorama 9.0

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-fn_pa_panorama-x.x.x.zip.
- Go to the Configuration tab and edit the app.config file, editing the API key for Panorama and making any additional setting changes.

Config	Required	Example	Description
panorama_host	Yes	https://0.0.0.0	The location where your Panorama software is running.
api_key	Yes	<panorama_api_key></panorama_api_key>	API key generated in the step above
cert	Yes	[True/False]	True or False
http_proxy	No	http://0.0.0.0:3128	Optional http proxy
https_proxy	No	http://0.0.0.0:3128	Optional https proxy

Integration Sever

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

\$ unzip fn_pa_panorama-x.x.x.zip

• Change Directory into the unzipped Directory:

\$ cd fn_pa_panorama-x.x.x

• Install the package:

\$ pip install fn_pa_panorama-x.x.x.tar.gz

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

\$ resilient-circuits config -u

• Import the fn_pa_panorama customizations into the Resilient platform:

\$ resilient-circuits customize -y -l fn-pa-panorama

• Generate the API key for Panorama:

curl -X GET 'https://<server_ip>/api/?type=keygen&user=<your_username>&password= <your_password>' -k

• Open the config file, scroll to the bottom and edit your fn_pa_panorama **configurations**:

\$ nano ~/.resilient/app.config

Config	Required	Example	Description
panorama_host	Yes	https://0.0.0.0	The location where your Panorama software is running.
api_key	Yes	<panorama_api_key></panorama_api_key>	API key generated in the step above
cert	Yes	[True/False]	True or False
http_proxy	No	http://0.0.0.0:3128	Optional http proxy
https_proxy	No	http://0.0.0.0:3128	Optional https proxy

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

\$ resilient-circuits selftest -l fn-pa-panorama

• 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-pa-panorama

- Open the config file, scroll to the [fn_pa_panorama] 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_pa_panorama	1.0.1	IBM Resilient	http://ibm.biz/resilientcommunity