

fn-ansible-tower Functions for IBM Resilient

- [Release Notes](#)
 - [Overview](#)
 - [Requirements](#)
 - [Installation](#)
 - [Uninstall](#)
 - [Troubleshooting](#)
 - [Support](#)
-

Release Notes

Release	Date	Notes
v1.0.2	2/2021	Bug fix for paged results from templates, jobs, etc.
v1.0.1	12/2020	App Host support
v1.0.0	2/2020	Initial release

Overview

Resilient Circuits Components for 'fn-ansible-tower'

This integration provides the capability to execute jobs and return job results from Ansible Tower.

Specific features include:

- List Job Templates filtering by Project
- Execute Job Templates, specifying name/value pairs for job template substitution
- Execute ad-hoc Jobs, specifying name/value pairs for module parameters
- List Jobs run filtered by status or date
- Return Job run results

Search...

☒ Show Task Notes ☐ Oldest Notes First

Created By: 0 selected Date Created: All

Resilient Sysadmin added a note to the Incident 12/09/2019 23:06

Job Id: 144

Status: running

Template Name: panorama_add_malicious_ip

Finished: None

PLAY [add objects to groups] *****

TASK [Gathering Facts] *****

ok: [localhost]

TASK [paloaltonetworks.paloaltonetworks : Install pan-python required library] ***

ok: [localhost]

TASK [paloaltonetworks.paloaltonetworks : Install pandevice required library] ***

ok: [localhost]

TASK [paloaltonetworks.paloaltonetworks : Install xmlltodict required library] ***

ok: [localhost]

TASK [Create IP object from Resilient] *****

[DEPRECATION WARNING]: Classic provider params are deprecated; use "provider"

PLAY RECAP *****

localhost : ok=4 changed=0 unreachable=0 failed=1 skipped=0 rescued=0 ignored=0

be disabled by setting deprecation_warnings=False in ansible.cfg.

instead. This feature will be removed in version 2.12. Deprecation warnings can

Requirements

- Resilient platform >= v36.0
- An Integration Server running resilient_circuits>=30.0.0
 - To set up an Integration Server see: [ibm.biz/res-int-server-guide](#)

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_ansible_tower-x.x.x.zip.
- Go to the Configuration tab and edit the app.config file, editing the url, access credentials, etc.

Config	Required	Example	Description
username	Yes	``	User name for API access to Ansible Tower
password	Yes	``	Password for above user name
url	Yes	``	URL to Ansible Tower

Config	Required	Example	Description
cafile	Yes	False	<i>False for no SSL certificate verification or path to certificate file</i>

Integration Server

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

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

- **Install** the package:

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

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

```
$ resilient-circuits config -u
```

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

```
$ resilient-circuits customize -y -l fn-ansible-tower
```

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

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

Config	Required	Example	Description
username	Yes	``	<i>User name for API access to Ansible Tower</i>
password	Yes	``	<i>Password for above user name</i>
url	Yes	``	<i>URL to Ansible Tower</i>
cafile	Yes	False	<i>False for no SSL certificate verification or path to certificate file</i>

- **Save** and **Close** the app.config file.

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

```
$ resilient-circuits selftest -l fn-ansible-tower
```

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

```
$ resilient-circuits run
```

Custom Layouts

- Import the Data Tables like the screenshot below:

Tasks

Details

Breach

Notes

Members

News Feed

Attachments

Stats

Timeline

Artifacts

Email

Ansible Tower

Edit

Ansible Tower Job Templates

Search...

Print

Export

Reported On	Job Id	Project	Name	Description	Playbook	Last Run	
Wed Dec 18 16:19:47 UTC 2019	6	Group A	Scan Files	—	scan_files.yml	2019-12-02 16:04:23.489501Z	...
Wed Dec 18 16:19:47 UTC 2019	5	Group A	Review Host config files	—	config_files.yml	2019-12-18 16:24:55.288552Z	...
Wed Dec 18 16:19:47 UTC 2019	10	Group B	Find Files Artifact	—	find_files_artifact.yml	2019-11-25 19:32:34.411073Z	...
Wed Dec 18 16:19:47 UTC 2019	8	Group B	Scan Files	—	scan_files.yml	2019-11-15 22:05:13.826786Z	...
Wed Dec 18 16:19:47 UTC 2019	12	Group B	panorama_add_malicious_ip	—	panorama_add_malicious_ip.yml	2019-12-10 04:32:52.861234Z	...
Wed Dec 18 16:19:47 UTC 2019	11	Group B	scan and escalate	—	scan_and_esclate_files.yml	2019-11-25 01:08:13.289768Z	...

Displaying 1 - 6 of 6

Ansible Tower Launched Jobs

Search...

Print

Export

Reported On	Type	Launch Date	Completion Date	Status	Job Id	Name	Project	Run Tags	Skip Tags	Hosts	Arguments	Ignored Fields
Wed Dec 18 16:24:57 UTC 2019	template	2019-12-18 16:24:55.288552Z	2019-12-18 16:25:40.839231Z	success	149	Scan Files	Group A	—	—	—	—	u'extra_vars': u'msg': u'hello'

Displaying 1 - 1 of 1

Uninstall

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

```
$ pip uninstall fn-ansible-tower
```

- Open the config file, scroll to the [fn-ansible_tower] 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.

Configure Ansible Tower

No additional configuration is requirement for Ansible Tower.

Support

Name	Version	Author	Support Email
fn_ansible_tower	1.0.0	IBM Resilient	support@resilientsystems.com