Event Driven Automation Using StackStorm

Ansil | Lead SRE @ Cisco

About Me

What is event vs notification ?

An event is a state change in the system

A notification is sent when an event occurs

What is event driven automation?

Responding automatically to an event using a notification mechanism

The Kubernetes | Pod memory limit

Application is developed in Golang and included pprof package.

The application running in a Kubernetes system

The Pods have memory limit set

There is an alert configured to fire when Pod memory usage reaches 70% of the limit.

The oncall get the notification and engage application owner to investigate the issue.

Oops!

“Sorry! Pod restarted before collecting heap dump”

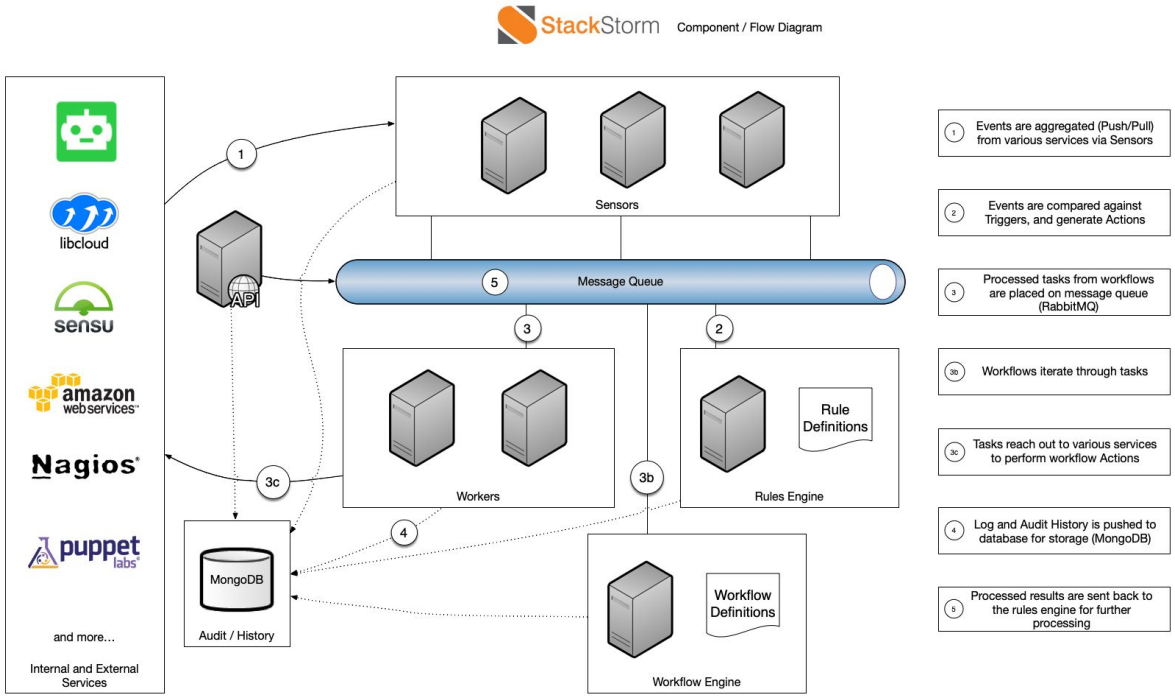
How to automate?

Event Driven Automation using StackStorm

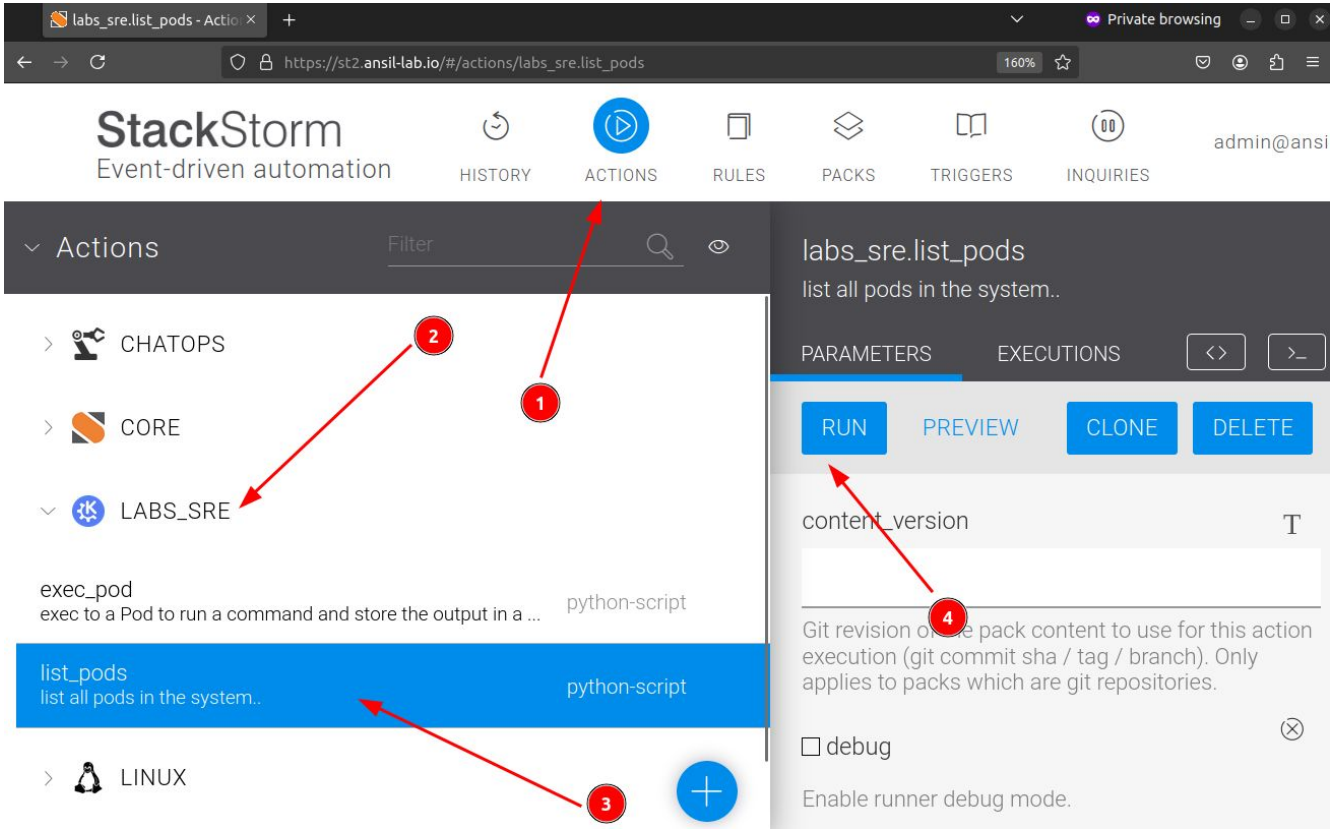
What is StackStorm?

StackStorm is a platform for integration and automation across services and tools. It ties together your existing infrastructure and application environment so you can more easily automate that environment. **It has a particular focus on taking actions in response to events.**

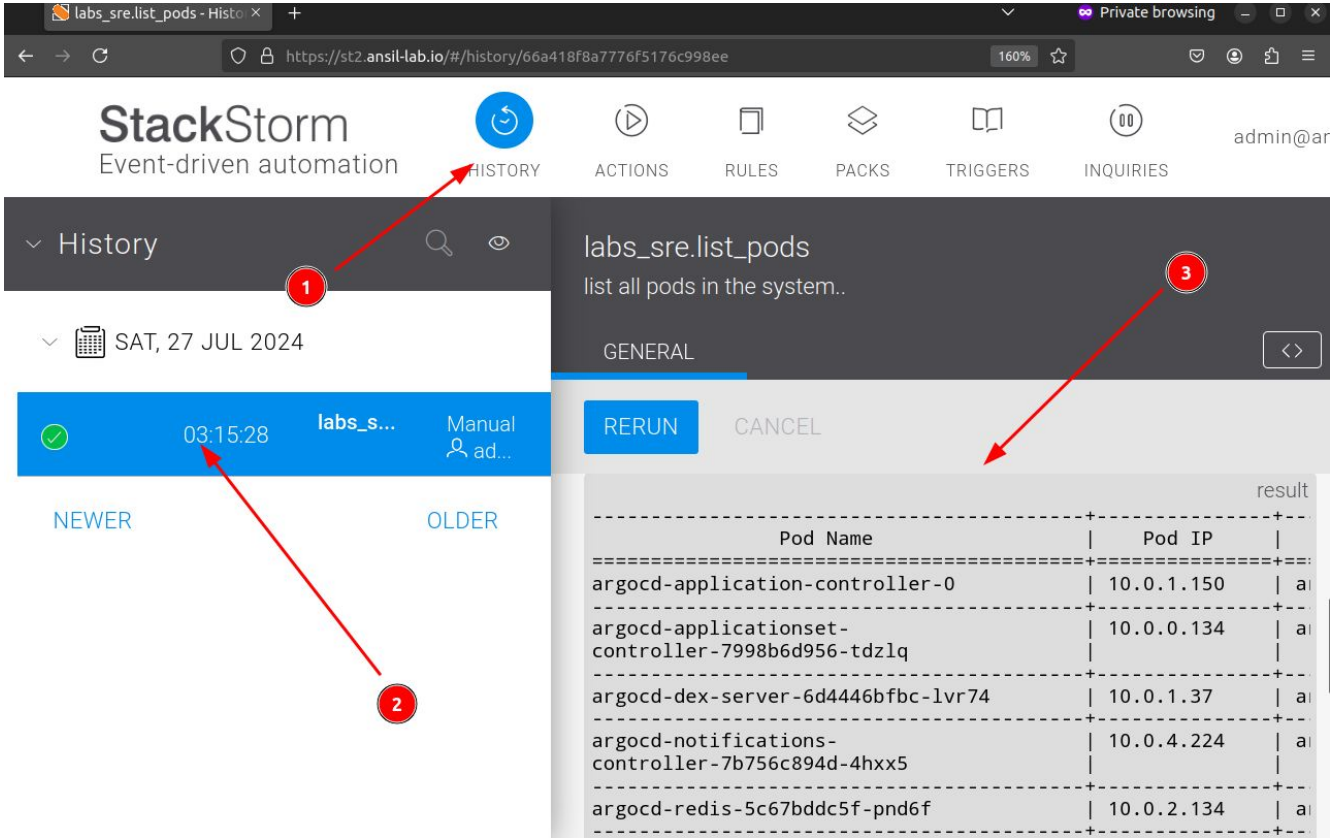
Architecture



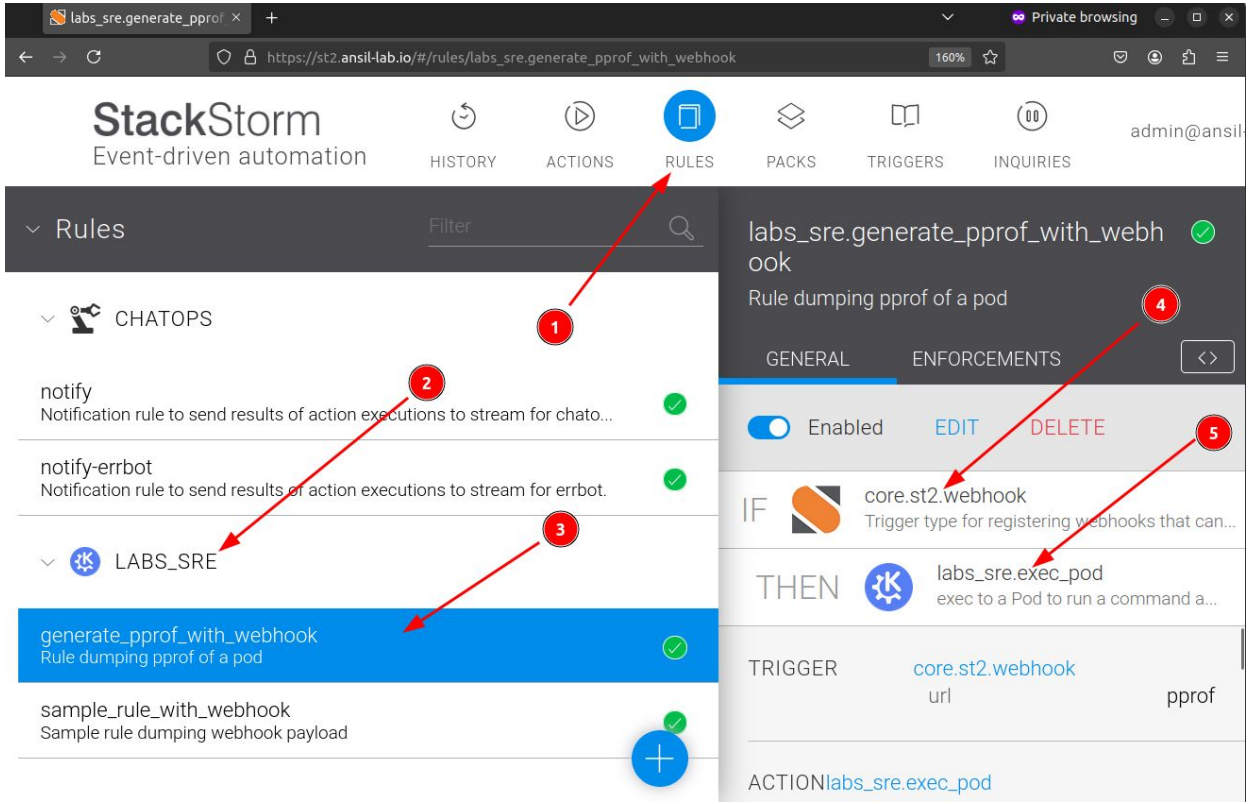
Actions


labs_sre.list_pods - Actio
Private browsing
https://st2.ansil-lab.io/#/actions/labs_sre.list_pods
160%
StackStorm
Event-driven automation
HISTORY
ACTIONS
RULES
PACKS
TRIGGERS
INQUIRIES
admin@ansi
Actions
Filter
CHATOPS
CORE
LABS_SRE
exec_pod
exec to a Pod to run a command and store the output in a ...
python-script
list_pods
list all pods in the system..
python-script
LINUX
labs_sre.list_pods
list all pods in the system..
PARAMETERS
EXECUTIONS
RUN
PREVIEW
CLONE
DELETE
content_version
Git revision of the pack content to use for this action execution (git commit sha / tag / branch). Only applies to packs which are git repositories.
debug
Enable runner debug mode.
1
2
3
4

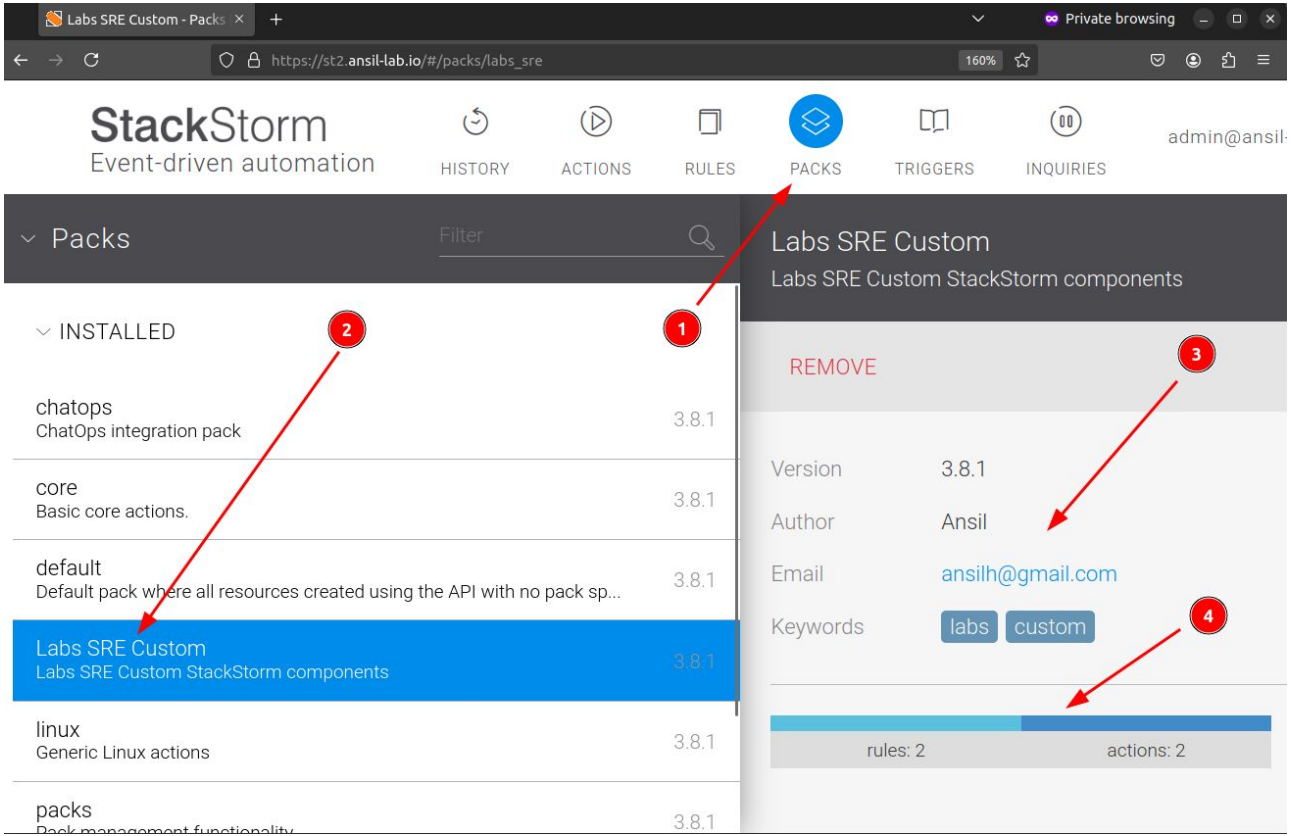
History


labs_sre.list_pods - Histo
Private browsing
https://st2.ansil-lab.io/#/history/66a418f8a7776f5176c998ee
160%
StackStorm
Event-driven automation
HISTORY
ACTIONS
RULES
PACKS
TRIGGERS
INQUIRIES
admin@ar
History
1
SAT, 27 JUL 2024
03:15:28
labs_s...
Manual
ad...
NEWER
OLDER
2
labs_sre.list_pods
list all pods in the system..
3
GENERAL
RERUN
CANCEL
result
Pod Name | Pod IP
argocd-application-controller-0 | 10.0.1.150
argocd-applicationset-controller-7998b6d956-tdzlq | 10.0.0.134
argocd-dex-server-6d4446bfbc-lvr74 | 10.0.1.37
argocd-notifications-controller-7b756c894d-4hxx5 | 10.0.4.224
argocd-redis-5c67bddc5f-pnd6f | 10.0.2.134

Rules


labs_sre.generate_pprof
Private browsing
https://st2.ansil-lab.io/#/rules/labs_sre.generate_pprof_with_webhook
160%
StackStorm
Event-driven automation
HISTORY
ACTIONS
RULES
PACKS
TRIGGERS
INQUIRIES
admin@ansil
Rules
Filter
CHATOPS
notify
Notification rule to send results of action executions to stream for chato...
notify-errbot
Notification rule to send results of action executions to stream for errbot.
LABS_SRE
generate_pprof_with_webhook
Rule dumping pprof of a pod
sample_rule_with_webhook
Sample rule dumping webhook payload
labs_sre.generate_pprof_with_webhook
Rule dumping pprof of a pod
GENERAL
ENFORCEMENTS
Enabled
EDIT
DELETE
IF
core.st2.webhook
Trigger type for registering webhooks that can...
THEN
labs_sre.exec_pod
exec to a Pod to run a command a...
TRIGGER
core.st2.webhook
url
pprof
ACTION
labs_sre.exec_pod
1
2
3
4
5

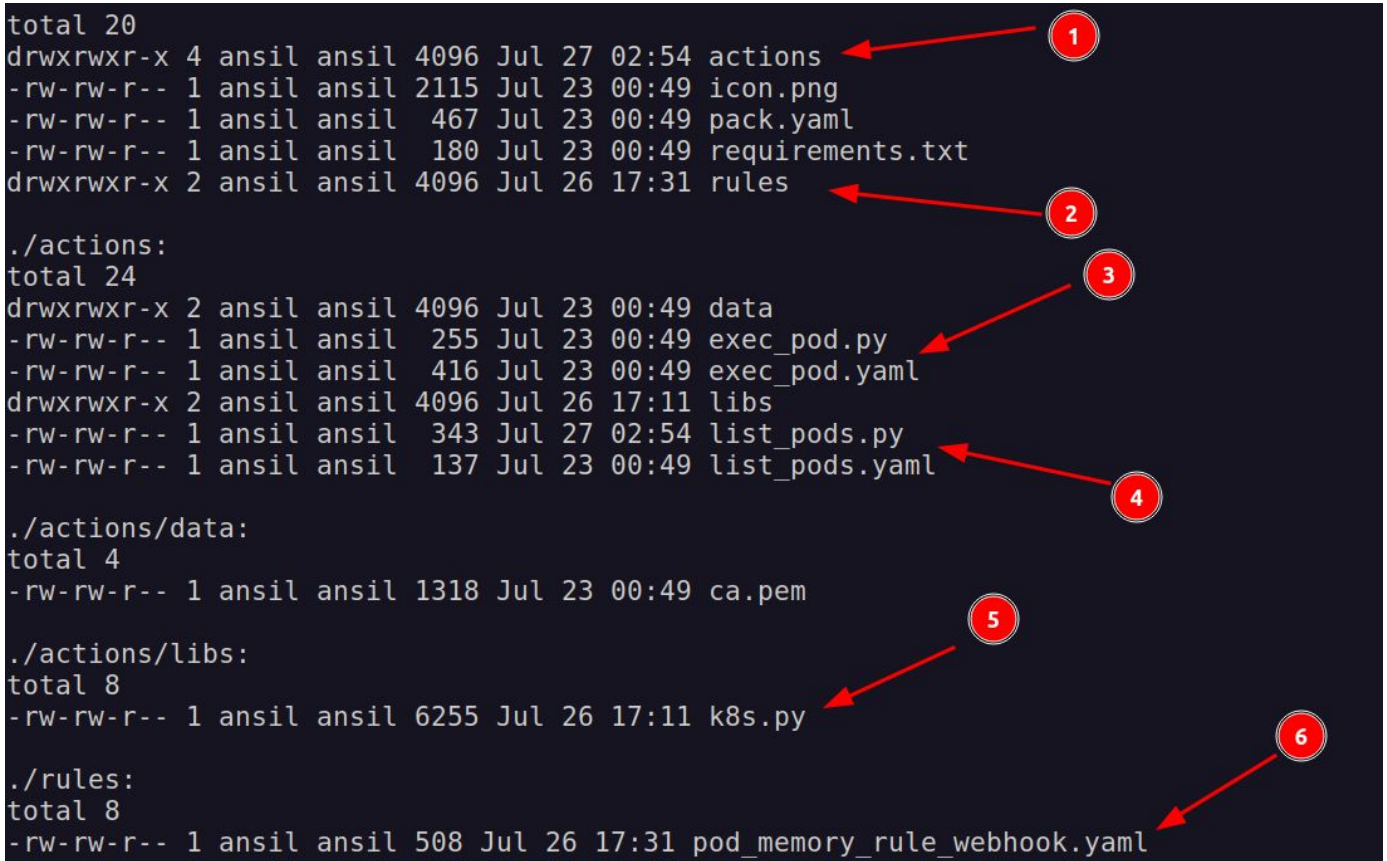
Packs


Labs SRE Custom - Packs
Private browsing
https://st2.ansil-lab.io/#/packs/labs_sre
160%
StackStorm
Event-driven automation
HISTORY
ACTIONS
RULES
PACKS
TRIGGERS
INQUIRIES
admin@ansil
Packs
Filter
INSTALLED
chatops
ChatOps integration pack
3.8.1
core
Basic core actions.
3.8.1
default
Default pack where all resources created using the API with no pack sp...
3.8.1
Labs SRE Custom
Labs SRE Custom StackStorm components
3.8.1
linux
Generic Linux actions
3.8.1
packs
3.8.1
Labs SRE Custom
Labs SRE Custom StackStorm components
REMOVE
Version
3.8.1
Author
Ansil
Email
ansilh@gmail.com
Keywords
labs
custom
rules: 2
actions: 2
1
2
3
4

Structure of a Pack

```
# contents of a pack folder
actions/                  #
rules/                    #
sensors/                  #
aliases/                  #
policies/                 #
tests/                    #
etc/                      # any additional things (e.g code generators, scripts...)
config.schema.yaml        # configuration schema
packname.yaml.example     # example of config, used in CI
pack.yaml                 # pack definition file
requirements.txt          # requirements for Python packs
requirements-tests.txt    # requirements for python tests
icon.png                  # 64x64 .png icon
```

Custom Pack


total 20
drwxrwxr-x 4 ansil ansil 4096 Jul 27 02:54 actions
-rw-rw-r-- 1 ansil ansil 2115 Jul 23 00:49 icon.png
-rw-rw-r-- 1 ansil ansil 467 Jul 23 00:49 pack.yaml
-rw-rw-r-- 1 ansil ansil 180 Jul 23 00:49 requirements.txt
drwxrwxr-x 2 ansil ansil 4096 Jul 26 17:31 rules
./actions:
total 24
drwxrwxr-x 2 ansil ansil 4096 Jul 23 00:49 data
-rw-rw-r-- 1 ansil ansil 255 Jul 23 00:49 exec_pod.py
-rw-rw-r-- 1 ansil ansil 416 Jul 23 00:49 exec_pod.yaml
drwxrwxr-x 2 ansil ansil 4096 Jul 26 17:11 libs
-rw-rw-r-- 1 ansil ansil 343 Jul 27 02:54 list_pods.py
-rw-rw-r-- 1 ansil ansil 137 Jul 23 00:49 list_pods.yaml
./actions/data:
total 4
-rw-rw-r-- 1 ansil ansil 1318 Jul 23 00:49 ca.pem
./actions/libs:
total 8
-rw-rw-r-- 1 ansil ansil 6255 Jul 26 17:11 k8s.py
./rules:
total 8
-rw-rw-r-- 1 ansil ansil 508 Jul 26 17:31 pod_memory_rule_webhook.yaml
1
2
3
4
5
6

Action | YAML

```yaml
---
name: "list_pods"
runner_type: "python-script"
description: "list all pods in the system.."
enabled: true
entry_point: "list_pods.py"
```

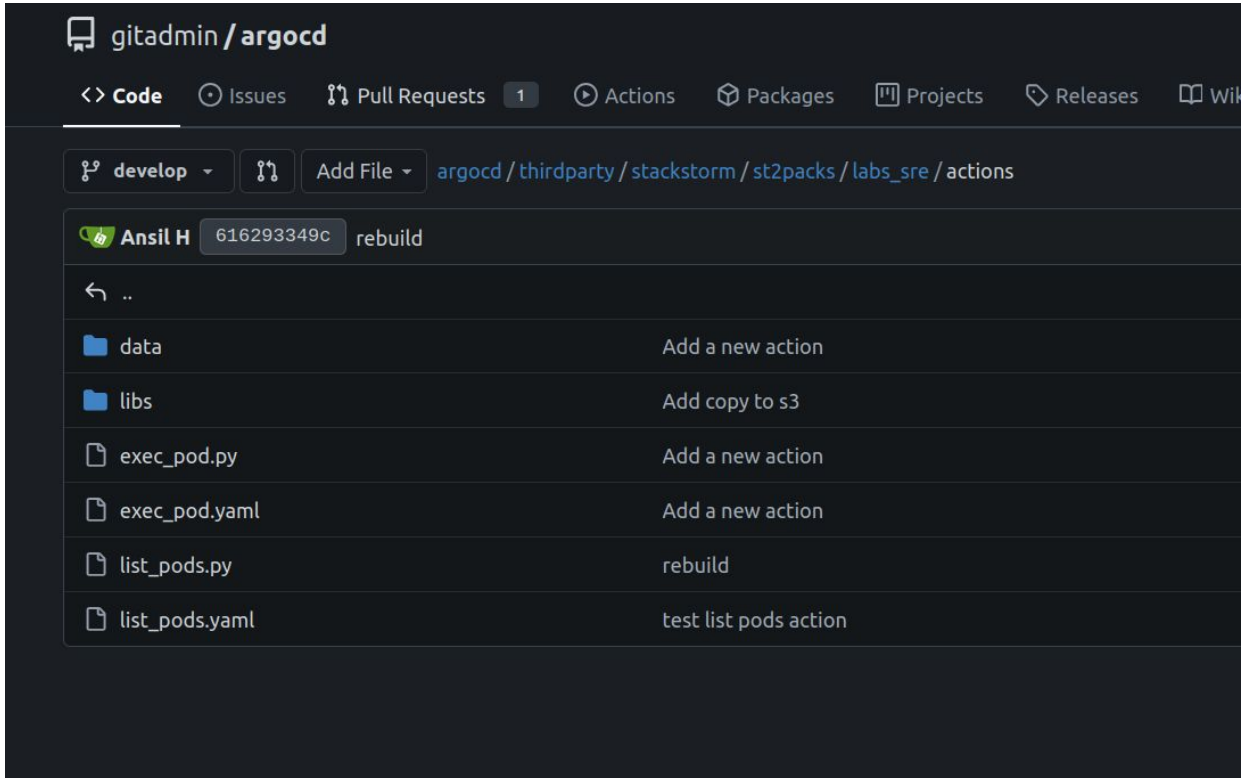
Action | Python

```
import sys
import libs.k8s
from texttable import Texttable
from typing import Dict, List, Tuple
from st2common.runners.base_action import Action


class listPodsAction(Action):
    def run(self) -> Tuple[bool, str]:
        ret, pods = libs.k8s.listPods()
        data = Texttable()
        data.add_rows(pods)
        return ret, data.draw()
```

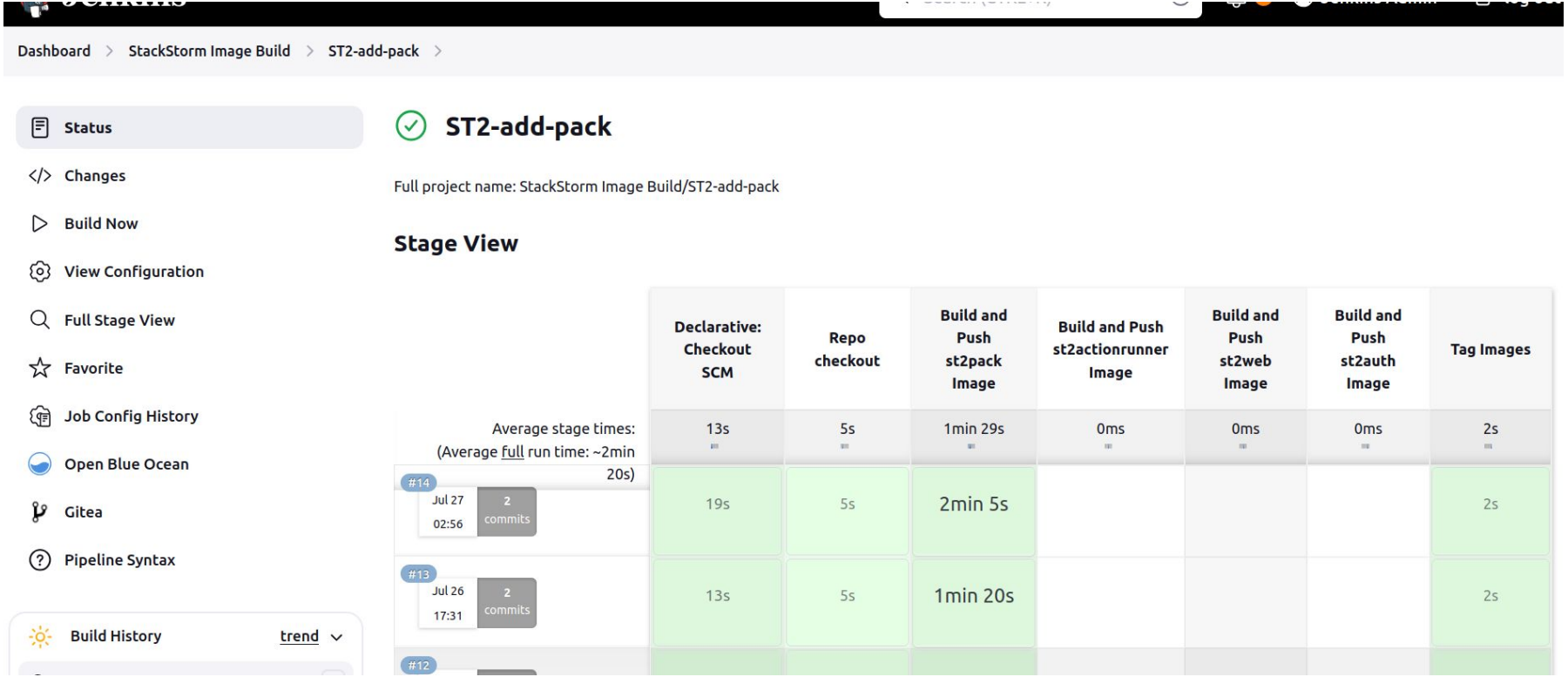
Rules

```
---
name: "generate_pprof_with_webhook"
pack: "labs_sre"
description: "Rule dumping pprof of a pod"
enabled: true

trigger:
    type: "core.st2.webhook"
    parameters:
        url: "pprof" # URL : https://st2.ansil-lab.io/st2api/v1/webhooks/pprof
criteria:
  trigger.body.alerts[0].labels.alertname:
    type: "startswith"
    pattern : "Pod Memory Limit"

action:
    ref: "labs_sre.exec_pod"
    parameters:
        pod: "{{trigger.body.alerts[0].labels.pod}}"
        namespace: "dm-demo-app"
```

Pack Development



Jenkins job to build custom pack



ArgoCD App Sync