

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?



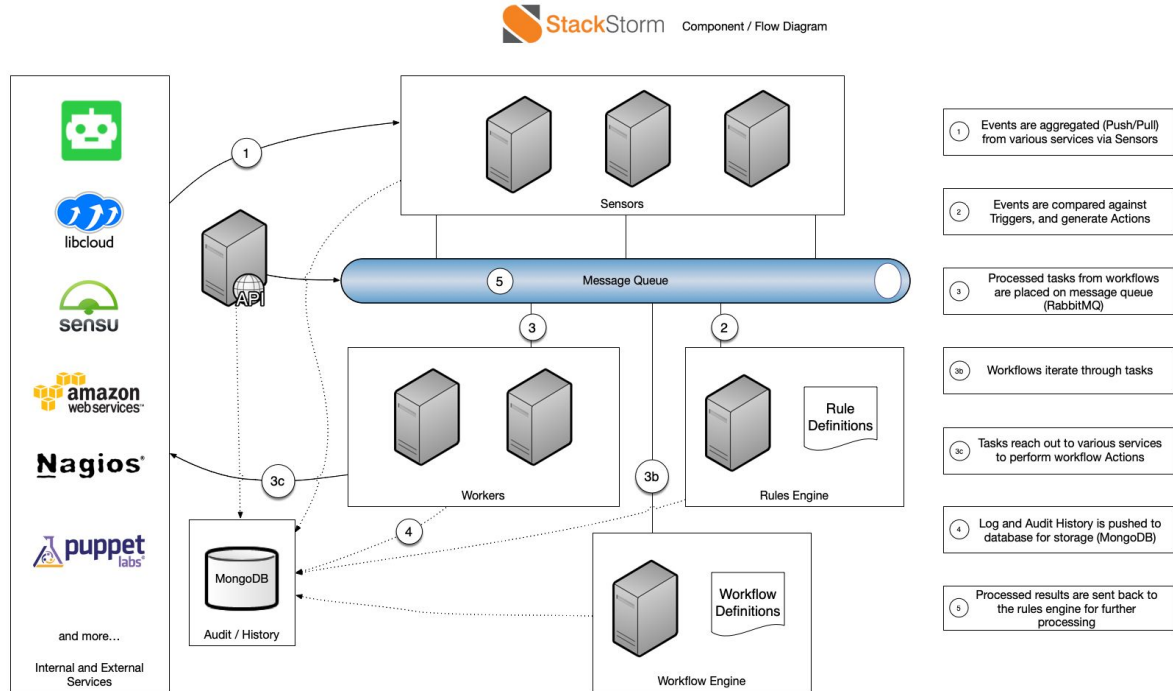
Event Driven Automation using StackStorm



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 - Action x +

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 T

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.

History

The screenshot displays the StackStorm web interface in a private browser window. The URL is `https://st2.ansil-lab.io/#/history/66a418f8a7776f5176c998ee`. The interface includes a navigation bar with tabs for HISTORY, ACTIONS, RULES, PACKS, TRIGGERS, and INQUIRIES. The 'History' tab is active, showing a list of workflow runs. A specific run is highlighted in blue, showing a successful status (green checkmark), the time '03:15:28', the workflow name 'labs_s...', and the trigger 'Manual'. Below the list are 'NEWER' and 'OLDER' links. To the right, a detailed view of the selected run is shown, including a 'GENERAL' tab, 'RERUN' and 'CANCEL' buttons, and a table of results.

StackStorm
Event-driven automation

admin@ar

History

SAT, 27 JUL 2024

03:15:28 labs_s... Manual ad...

NEWER OLDER

labs_sre.list_pods
list all pods in the system..

GENERAL

RERUN CANCEL

		result
Pod Name	Pod IP	
argocd-application-controller-0	10.0.1.150	al
argocd-applicationset-controller-7998b6d956-tdzlq	10.0.0.134	al
argocd-dex-server-6d4446bfb-c-lvr74	10.0.1.37	al
argocd-notifications-controller-7b756c894d-4hxx5	10.0.4.224	al
argocd-redis-5c67bddc5f-pnd6f	10.0.2.134	al

Rules

The screenshot shows the StackStorm web interface for configuring rules. The main navigation bar includes 'HISTORY', 'ACTIONS', 'RULES' (selected), 'PACKS', 'TRIGGERS', and 'INQUIRIES'. The 'Rules' section is active, displaying a list of rules under two categories: 'CHATOPS' and 'LABS_SRE'. The rule 'generate_pprof_with_webhook' is highlighted in blue. A red arrow points from the 'RULES' tab to the list (1). Another red arrow points from the 'LABS_SRE' category header to the list (2). A third red arrow points from the 'generate_pprof_with_webhook' rule to the list (3). A fourth red arrow points from the rule name to the detailed view on the right (4). A fifth red arrow points from the 'DELETE' button to the detailed view (5).

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

Packs

The screenshot displays the StackStorm interface in a browser window. The top navigation bar includes icons for History, Actions, Rules, Packs, Triggers, and Inquiries. The main content area is divided into a left sidebar and a right pane.

Left Sidebar:

- 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 (highlighted)
- linux** (Generic Linux actions) 3.8.1
- packs** (Pack management functionality) 3.8.1

Right Pane:

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**

Red arrows and numbered circles (1-4) highlight specific elements:

- 1:** Points to the 'PACKS' icon in the top navigation bar.
- 2:** Points to the 'Labs SRE Custom' pack in the left sidebar.
- 3:** Points to the 'REMOVE' button in the right pane.
- 4:** Points to the 'actions: 2' bar in the right pane.

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
```

The diagram illustrates a directory tree structure for a custom pack. It shows the following hierarchy:

- Root directory (total 20):
 - actions (total 24):
 - data (total 4):
 - ca.pem
 - libs (total 8):
 - k8s.py
 - rules (total 8):
 - pod_memory_rule_webhook.yaml

Numbered red circles (1-6) and arrows indicate specific files or directories:

- 1: points to the `actions` directory.
- 2: points to the `rules` directory.
- 3: points to the `exec_pod.py` file.
- 4: points to the `list_pods.yaml` file.
- 5: points to the `k8s.py` file.
- 6: points to the `pod_memory_rule_webhook.yaml` file.

Action | 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()
```

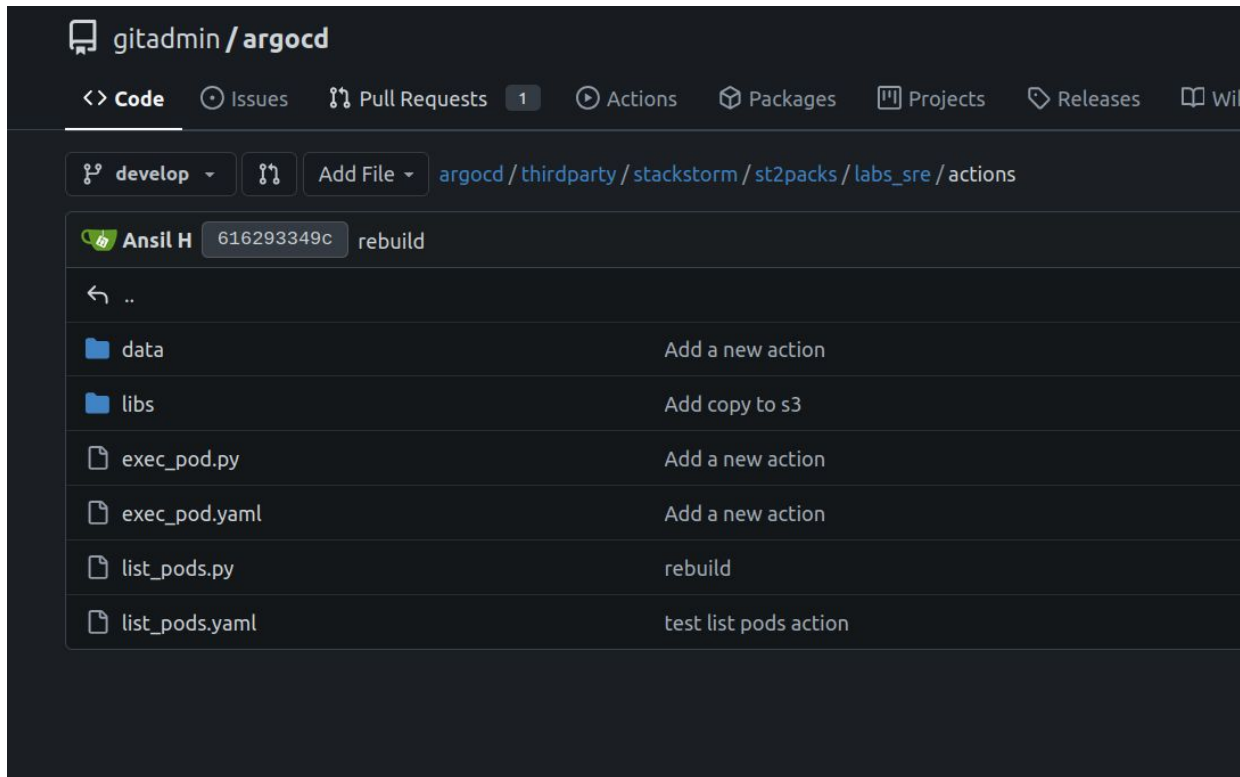
Rules

```
---
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

Dashboard > StackStorm Image Build > ST2-add-pack >

Status

✓ ST2-add-pack

</> Changes

Full project name: StackStorm Image Build/ST2-add-pack

► Build Now

⚙ View Configuration

🔍 Full Stage View

★ Favorite

📅 Job Config History

🌊 Open Blue Ocean

🔗 Gitea

🔍 Pipeline Syntax

Stage View

	Declarative: Checkout SCM	Repo checkout	Build and Push st2pack Image	Build and Push st2actionrunner Image	Build and Push st2web Image	Build and Push st2auth Image	Tag Images
Average stage times: (Average full run time: ~2min 20s)	13s	5s	1min 29s	0ms	0ms	0ms	2s
#14 Jul 27 02:56 2 commits	19s	5s	2min 5s				2s
#13 Jul 26 17:31 2 commits	13s	5s	1min 20s				2s
#12							

☀ Build History

trend ▼

ArgoCD App Sync

The screenshot displays the ArgoCD web interface for an application named 'stackstorm'. The interface is divided into several sections:

- Header:** Shows the application name 'stackstorm' and a search bar.
- Navigation Bar:** Includes buttons for 'DETAILS', 'DIFF', 'SYNC', 'SYNC STATUS', 'HISTORY AND ROLLBACK', 'DELETE', and 'REFRESH'.
- App Health:** Displays 'Healthy' with a green heart icon.
- Sync Status:** Shows 'Synced to develop (eee41bb)' with a green checkmark. Below this, it states 'Auto sync is not enabled.' and provides author and comment information for the sync operation.
- Last Sync:** Shows 'Sync OK to eee41bb' with a green checkmark. It indicates the sync succeeded an hour ago (Sat Jul 27 2024 03:15:09 GMT+0530) and provides author and comment information.
- Pod Details:** Three panels show pod status for different nodes (192.168.56.65, 192.168.56.66, and 192.168.56.67). Each panel includes a 'CPU MEM' bar chart, a 'PODS' status bar with green checkmarks, and a 'node' label. Below the status bar, it shows 'Kernel Version: 6.5.0-44-generic' and 'OS/Arch: linux/amd64'.