

PrometheusRules & Alertes via Grafana

Présentation 08/11/22

Contexte

La solution a été mise en place pour la plateforme BETA.

- permet d'utiliser l'API de Prometheus pour :
 - visualiser les PrometheusRules définies dans Prometheus ,
- permet d'utiliser l'API d'Alertmanager pour :
 - visualiser les alertes, silences ,
 - faire des queries sur les alertes, silences ,
 - créer des tableaux de bord dans Grafana.

PrometheusRules (datasource Thanos)

Deux façons de voir les PrometheusRules :

- par état des alertes (firing, pending etc.) ;
- par groupe .

Possibilité de filtrer les rules avec plusieurs options disponibles :

- `status` ,
- `labels`.

Alertes dans Grafana

Deux façons de voir les alertes :

- avec `unified alerting` ;
- avec le plugin `camptocamp-prometheus-alertmanager-datasource`.

Unified Alerting : ConfigMap

```
1  apiVersion: v1
2  data:
3    datasource_alertmanager.yaml: |
4      apiVersion: 1
5      datasources:
6      - name: "Alertmanager-cloud-client"
7        type: "alertmanager"
8        access: proxy
9        orgId: 1
10       url: "http://client-alertmanager.monitoring-client.svc.cluster
11       jsonData:
12         implementation: "prometheus"
13  kind: ConfigMap
14  ...
```

Unified Alerting : Utilisation

The screenshot displays the 'Alerting' configuration page in a dark-themed UI. The page title is 'Alerting' with the subtitle 'Alert rules and notifications'. A navigation bar at the top contains four items: 'Alert rules', 'Contact points', 'Notification policies', 'Silences', and 'Alert groups'. The 'Contact points' item is highlighted with a red box. Below the navigation bar, there is a section titled 'Choose Alertmanager' with a dropdown menu showing 'Alertmanager'. The main section is titled 'Contact points' and includes a description: 'Define where the notifications will be sent to, for example email or Slack.' Below this is a table with three columns: 'Contact point name', 'Type', and 'Actions'. The table contains two rows: one for 'rocketchat' with type 'Webhook' and an edit icon, and one for 'null' with an edit icon. At the bottom, there is a blue box with an information icon and the title 'Global config for contact points'. The text inside says: 'For each external Alertmanager you can define global settings, like server addresses, usernames and password, for all the supported contact points.' Below this text is a button labeled 'View global config'.

Alerting
Alert rules and notifications

Alert rules **Contact points** Notification policies Silences Alert groups

Choose Alertmanager
Alertmanager

Contact points
Define where the notifications will be sent to, for example email or Slack.

Contact point name	Type	Actions
rocketchat	Webhook	
null		

Global config for contact points
For each external Alertmanager you can define global settings, like server addresses, usernames and password, for all the supported contact points.

[View global config](#)

Unified Alerting : Démo

Lien : [Grafana unified alerting](#)

- visualisation des receivers ;
- visualisation des alertes ;
- création d'un silence ;
- suppression d'un silence ;
- ajout d'un receiver.

Unified Alerting :

Comparaison Karma / Grafana

	Installation actuelle de Karma	Grafana
Possibilité de faire des groupes custom selon les labels	−	+
Le créateur du silence est l'utilisateur avec lequel on s'authentifie	−	+
Un seul outil à maintenir	−	+
Possibilité d'ignorer certains receivers	+	−
Visualisation des alertes affectées lors de la création de silences	+	−
Auto-complétion pour le filtrage avec des labels	+	−
Compatibilité Alertmanager	+	−

Plugin : Visualisation Alertes

- plugin type datasource : `camptocamp-prometheus-alertmanager-datasource` ;

Plugin : Déploiement

- installation plugin : `default.yaml` ;

```
grafana:
  plugins:
    - "camptocamp-prometheus-alertmanager-datasource"
```

- définition configmap pour utiliser la datasource :

```
apiVersion: v1
kind: ConfigMap
  name: grafana-datasource-alertmanagerplugin
data:
  alertmanager_plugin.yaml: |
    datasources:
      - name: "Prometheus AlertManager"
        type: "camptocamp-prometheus-alertmanager-datasource"
        url: "http://alertmanager:9093"
```

Plugin : Dashboard

Alertmanager Alerts

- le dashboard **upstream** ne fonctionnait pas (juin 2022) à cause des filtres ;
- construction d'un nouveau dashboard qui contient 3 panels :
 - alertes actives ,
 - alertes silencées ,
 - alertes prometheus (construite avec la métrique **ALERT_FOR_STATE** provenant de la datasource Thanos).

Plugin : Utilisation #1 - menu *Explore*

Explore Prometheus AlertManager

Split Add to dashboard Last 1 hour Run query

A (Prometheus AlertManager)

Receiver Filters (comma separated key=value) alertname="HighDiskUsage /var", monitor="3333" Active Silenced Inhibited

+ Add query Query history Inspector

Time	SeverityValue	description	help_alerts	summary	alertname	dc	device	environment	fstype
2022-11-03 18:49:42	2	Disk Usage above 9...	https://github.com/...	High Disk Usage de...	HighDiskUsage /var	CAV	dm-1	Preproduction	ext4

Plugin : Utilisation #2 - Dashboard *Alertmanager* *Alerts*

General / Alertmanager Alerts ☆

Alert: All State: firing Environment: All Service: All Instance: All Alerts annotations: ☐

Alertmanager Active Alerts

SeverityValue	description	help_alerts	runbook_url	summary	alertname	cpu	host	instance	monitor	prometheus	service	seve
2	Disk Usage above 90% detected for instance . http://intranet.rah.orange-business.com/detail.php	https://github.com/influxdata/telegraf/tree/release-1.22/plugins/inputs/disk		High Disk Usage detected for instance.	HighDiskUsage /		tstsqd001		3333	monitoring-obs-ucc2/ucc2-prometheus	OS_disk	v
2	High CPU Usage detected for instance FWSADC002.	https://github.com/influxdata/telegraf/tree/release-1.22/plugins/inputs/cpu	https://www.site24x7.com/learn/linux/cpu-utilization.html	High CPU Usage detected for instance.	HighCpuUsage	cpu-total	FWSADC002	FWSADC002	3333	monitoring-obs-ucc2/ucc2-prometheus		v

Alertmanager Silenced Alerts

SeverityValue	description	help_alerts	runbook_url	summary	alertname	cpu	host	instance	monitor	prometheus	service	seve
2	Disk Usage above 90% detected for instance . http://intranet.rah.orange-business.com/detail.php	https://github.com/influxdata/telegraf/tree/release-1.22/plugins/inputs/disk		High Disk Usage detected for instance.	HighDiskUsage /		tstsqd001		3333	monitoring-obs-ucc2/ucc2-prometheus	OS_disk	v
2	High CPU Usage detected for instance FWSADC002.	https://github.com/influxdata/telegraf/tree/release-1.22/plugins/inputs/cpu	https://www.site24x7.com/learn/linux/cpu-utilization.html	High CPU Usage detected for instance.	HighCpuUsage	cpu-total	FWSADC002	FWSADC002	3333	monitoring-obs-ucc2/ucc2-prometheus		v
2	{{ printf "%.4g" \$value }}% of the {{ \$labels.job }}/{{ \$labels.service }} targets	https://runbooks.prometheus-		One or more Prometheus	TargetDown				3333	monitoring-obs-	caascad-kube-	v

Prometheus Alerts

alertname	environment	instance	service	severity	Timestamp
HighDiskUsage /	Staging	{{ \$labels.instance }}	OS_disk	warning	2022-10-12 15:44:45
HighDiskUsage /	Staging	collab-sao	OS_disk	warning	2022-10-12 15:44:45

Plugin : Démo

- Grafana :
 - Menu *Explore*
 - Dashboard *Alertmanager Alerts*

Plugin : Observations

- l'avantage principal de cette solution est d'avoir une seule interface pour la supervision des plateformes ;
- dans le menu *Explore* il n'y a pas d'autocomplétion ;
- dans dashboard labels `alertstatus` et `alertstatus_code` ne fonctionnent pas à cause d'une modification `upstream` ;
- repo maintenu :
 - trois releases en 2022 (bug fixes et quelques features en plus) ,
 - mise à jour récente : dernier commit 7 juin.

Questions
