

Alertmanager en mode cluster

Objectif

Avoir Alermanager en HA

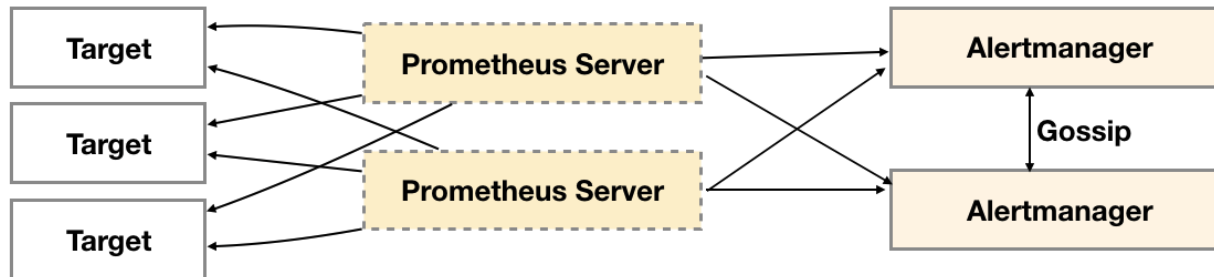
Fonctionnement Alertmanager en mode cluster

- Les alertes ne se propagent pas d'un membre à l'autre du cluster
- Les silences se propagent d'un membre à l'autre du cluster
- Les notifications sont envoyées en un seul exemplaire par un membre du cluster
- Les membres du cluster communiquent via le protocole Gossip en utilisant un port spécifique.

Synthèse principe de fonctionnement

- Il faut envoyer les alertes à tous les membres du cluster -> liaison Prometheus vers Alertmanager doublée
- Il suffit de poser un silence sur un seul membre pour qu'il soit propagé -> Kthxbye toujours connecté au service alertmanager
- Karma toujours connecté au service alertmanager.

Architecture



Architecture: ports différents pour les différents namespaces

Contexte

On a plusieurs clusters Alertmanager dans un cluster K8s (monitoring, monitoring-client, monitoring-app).

Problème

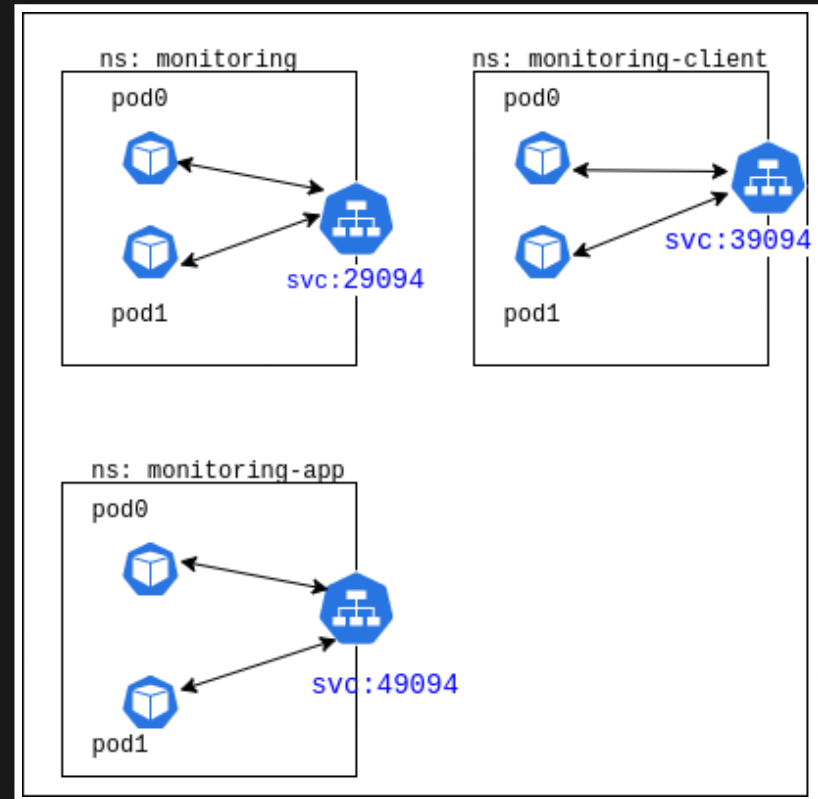
Dans certains cas les clusters Alertmanager peuvent former un seul gros cluster.

Workaround

Utilisation d'un port différent pour chaque cluster Alertmanager.

Note: Tentative de connexion sur les autres membres des clusters Alertmanager mais ces connexions échoueront.

Architecture: ports différents pour les différents namespaces



Liste des alertes

Liste des alertes upstream spécifiques pour le mode cluster :

- `AlertmanagerClusterDown`
- `AlertmanagerClusterCrashlooping`
- `AlertmanagerClusterFailedToSendAlerts`
- `AlertmanagerConfigInconsistent`

Alerte upstream migrée dans nos rules custom :

- `AlertmanagerMembersInconsistent`

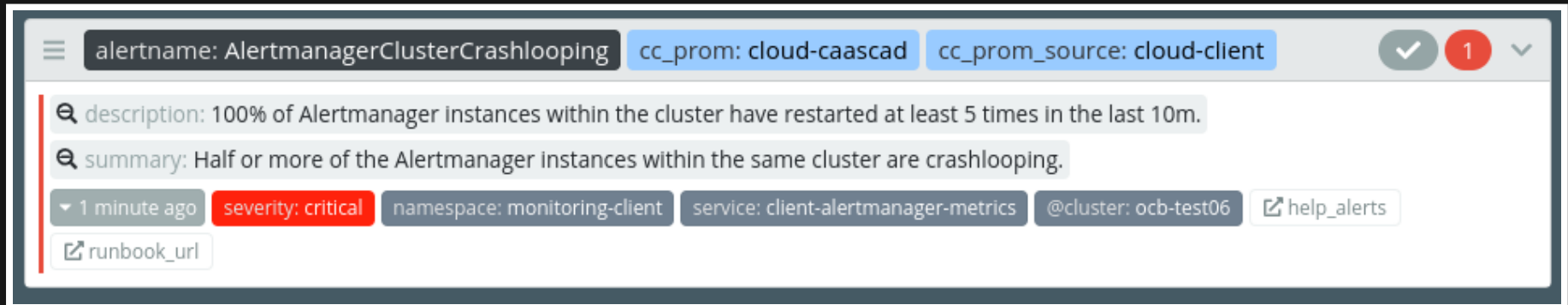
Alerte AlertmanagerClusterDown

- Description :
 - Au moins la moitié des membres du cluster est down
- Severity : critical
- Pannes :
 - Problème sur le noeud où il y'a le membre Alertmanager
 - Problème avec les membres Alertmanager
- Manifestation des pannes :
 - describe node
 - describe pod
 - logs d'erreur dans Alertmanager

The screenshot displays a web interface for a Kubernetes Alertmanager alert. At the top, a header bar contains the alert name 'alertname: AlertmanagerClusterDown' in a dark box, followed by two filter boxes: 'cc_prom: cloud-caascad' and 'cc_prom_source: cloud-client'. On the right of the header, there is a green checkmark icon, a red circle with the number '1', and a downward arrow. Below the header, the alert details are shown in a light gray box. It includes a 'description' field with the text '100% of Alertmanager instances within the cluster have been up for less than half of the last 5m.' and a 'summary' field with the text 'Half or more of the Alertmanager instances within the same cluster are down.' Below these fields, there is a row of metadata: '2 minutes ago' (with a dropdown arrow), 'severity: critical' (in a red box), 'namespace: monitoring-client', 'service: client-alertmanager-metrics', '@cluster: ocb-test02', and a 'help_alerts' button with an external link icon. At the bottom left, there is a 'runbook_url' button with an external link icon.

Alerte AlertmanagerClusterCrashlooping

- Description :
 - Au moins la moitié des membres du cluster est en crashloopbackoff
- Severity : critical
- Pannes :
 - Problème avec les membres Alertmanager
- Manifestation des pannes :
 - describe pod
 - logs d'erreur dans Alertmanager



Alerte AlertmanagerClusterFailedToSendAlerts

- Description :
 - Tous les membres du cluster Alertmanager échouent à envoyer des notifications à un type de receiver
- Severity : critical
- Pannes :
 - problème sur le receiver
 - problème de configuration Alertmanager
- Manifestation des pannes :
 - logs d'erreur dans Alertmanager
 - configuration Alertmanager



alertname: AlertmanagerClusterFailedToSendAlerts

cc_prom: cloud-caascad



1



cc_prom_source: cloud-caascad

🔍 description: The minimum notification failure rate to email sent from any instance in the cluster is NaN%.

🔍 summary: All Alertmanager instances in a cluster failed to send notifications to a critical integration.

▼ 5 minutes ago

severity: critical

namespace: monitoring

integration: email

service: caascad-alertmanager-metrics

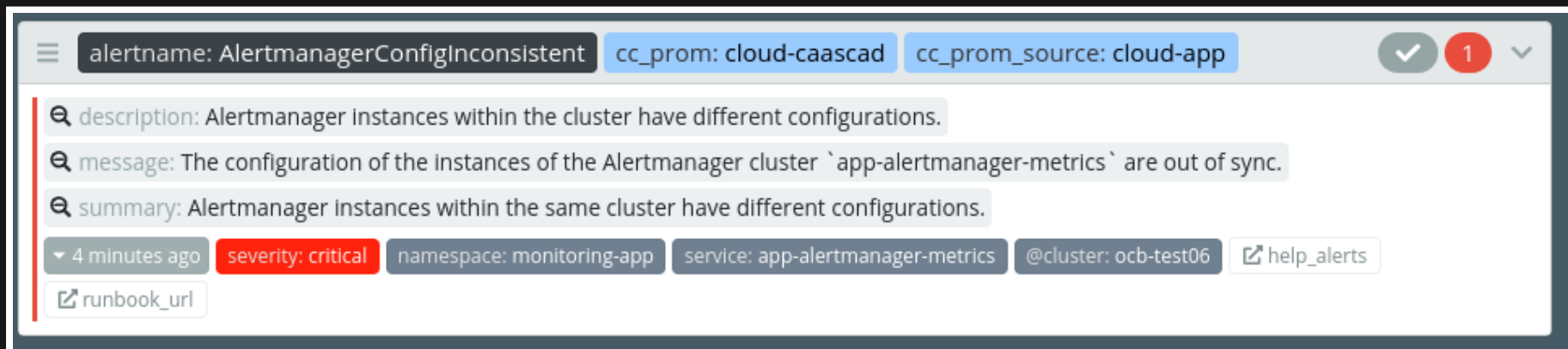
@cluster: ocb-test06

🔗 help_alerts

🔗 runbook_url

Alerte AlertmanagerConfigInconsistent

- Description :
 - Des membres du cluster Alertmanager n'ont pas la même configuration
- Severity : critical
- Pannes :
 - Problème de rechargement de configuration pour un des membres Alertmanager
- Manifestation des pannes :
 - configuration différente pour les membres



Alerte AlertmanagerMembersInconsistent

- Description :
 - Au moins un des membres du cluster Alertmanager ne peut pas être trouvé
 - Trop de membres sont dans le cluster Alertmanager
- Severity : critical
- Pannes :
 - Inconsistences sur les adresses IPs dans les endpoints Alertmanager
 - Problème de cache pour les IPs
- Manifestation des pannes :
 - describe endpoints
 - logs de debug dans Alertmanager

Alerte AlertmanagerMembersInconsistent

 alertname: AlertmanagerMembersInconsistent cc_prom: cloud-caascad cc_prom_source: cloud-client  2 

 message: Alertmanager monitoring-client/client-alertmanager-0 has found 2 members of the client-alertmanager cluster
▼ 12 minutes ago instance: 172.16.0.93:9093 pod: client-alertmanager-0

 message: Alertmanager monitoring-client/client-alertmanager-1 has found 2 members of the client-alertmanager cluster
▼ 12 minutes ago instance: 172.16.0.195:9093 pod: client-alertmanager-1

severity: critical namespace: monitoring-client container: alertmanager endpoint: metrics job: client-alertmanager
service: client-alertmanager-metrics @cluster: ocb-test05  help_alerts

Questions

