Gestion des logs avec grafana

—

Par Votre nom

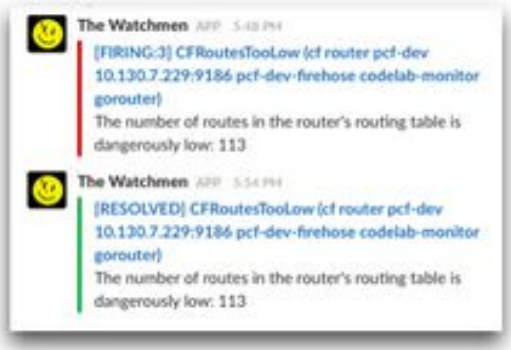
Cette presentation nous permettra de connaitre comment gérer les logs avec grafana et quels sont les outils utilisés pour cela.

En production, l'arrêt d’une application pour une raison ou une autre cause beaucoup de perte... Ainsi, la surveillance des logs afin de prévoir d’une certaine manière les possibles pannes ou dysfonctionnement est un art d’une grande importance.

Le système que nous allons utiliser pour la gestion des logs dans cette presentation tire son origine d'une plateforme tres utilise : Prometheus.
Prometheus est une solution qui utilise la labellisation et qui consomme peut de ressource pour son utilisation. Il est utilisé pour le monitoring de systèmes, de serveurs, d'applications... mais n'offre pas la même aisance en ce qui concerne la gestion des logs. L'utilisateur doit s'adapter pour pouvoir gérer ses logs. En règle générale c'est elasticsearch qui est appelé à la rescousse....

Problème

1. Alert



2. Dashboard

3. Adhoc Query

4. Log Aggregation

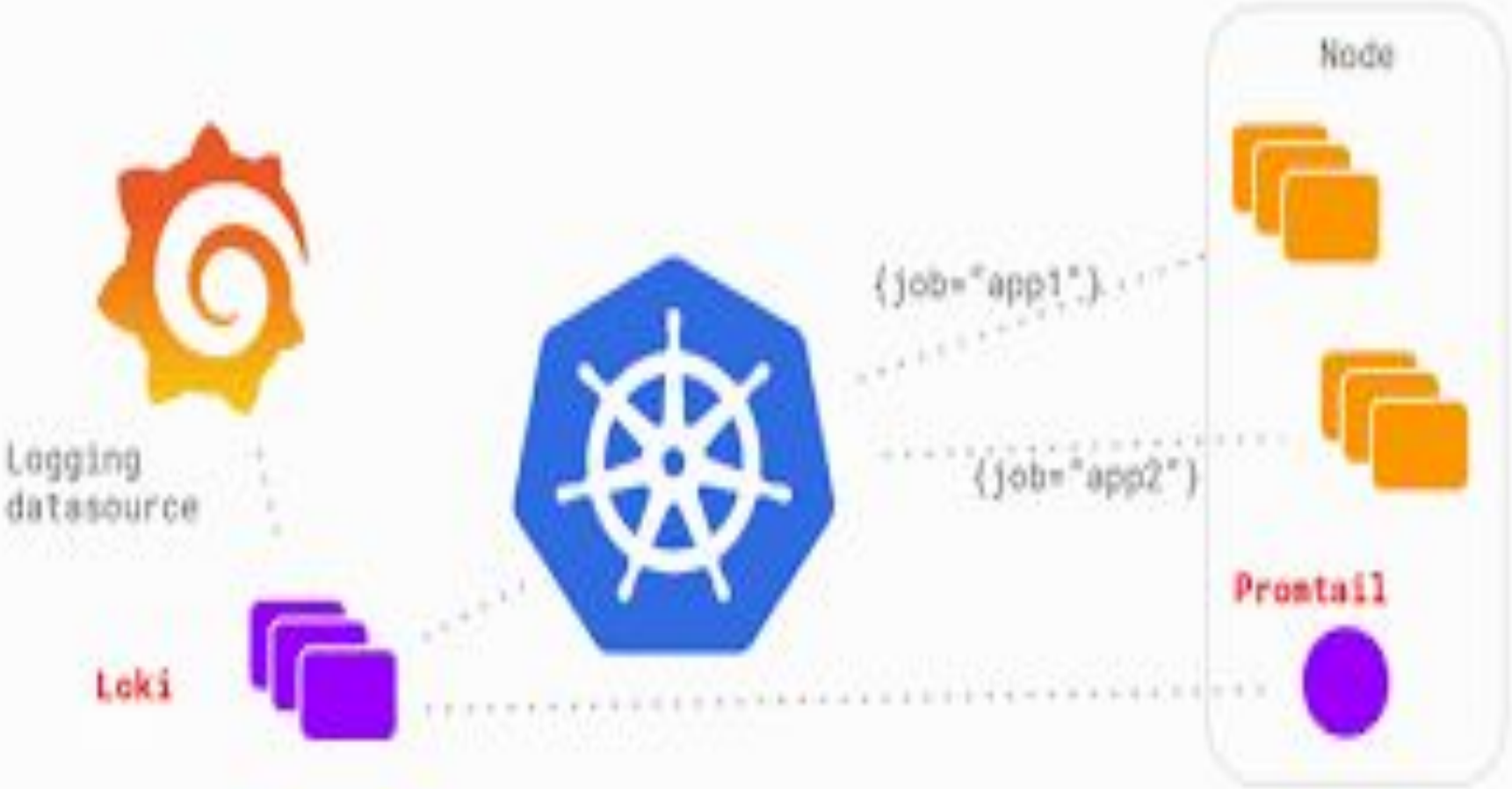
5. Distributed Tracing

Fix!

Résolution

Loki a justement été conçu dans le but de simplifier cette mise en place en répondant aux critères suivants :

- être un produit simple à démarrer ;
- consommer peu de ressources ;
- fonctionner tout seul sans intervention de maintenance particulière ;
- servir de support à l'investigation en complément de Prometheus en cas de pépin.


Node
{job="app1"}
{job="app2"}
Logging
datasource
Promtail
Loki

L'expérience

Matériel

- Une machine ubuntu
- Promtail
- Loki
- Grafana

Procédure

1. La première étape consiste à installer grafana (presentation de grafana...)

2. Ensuite, nous devons installer Loki et le definir comme etant un service

3. Pour terminer, nous devons installer Promtail et le définir comme un service également

Procédure

4. Créer un utilisateur pour la gestion du service Promtail et l'ajouter au groupe des administrateurs afin qu'il puisse afficher certains logs

5. Demarrer les services a savoir, grafana, Loki et Promtail, puis faire passer les logs a Promtail avec la commande journalctl

Conclusion

Pour la gestion des logs, c'est la suite Grafana, Loki, Promtail qui est utilisée en générale. Cependant, Grafana peut être utilisé avec ElasticSearch ou Kibana pour cela.

Un bon concurrent de Promtail est Fluentd. Cependant, pour pouvoir l'utiliser avec Grafana, il faut passer par des outils comme Zabbix, SPlunk...