

Grafana

Introduction

Grafana est une plateforme permettant de créer des tableaux de bord de visualisation pour les métriques. Grafana permet la création de différents types de widget et de met à disposition de nombreuses options pour la visualisation des métriques.

Plus de détails sont disponibles sur le site officiel: <https://grafana.com/>

Installation

L'installation de Grafana sous CentOS se fait via un RPM. La version de Grafana testée avec Shinken Entreprise est la v5.1.3.

Pour l'installer, utiliser la commande suivante:

```
yum install https://s3-us-west-2.amazonaws.com/grafana-releases/release/grafana-5.1.3-1.x86_64.rpm
```

Une fois l'installation terminée, le lancement de Grafana dépend de la version de CentOS utilisée.

- Sous CentOS 6

```
service grafana-server start
```

- Sous CentOS 7

```
systemctl start grafana-server
```

Accès à Grafana une fois installé:

1. port = 3000
2. identifiants : admin/admin

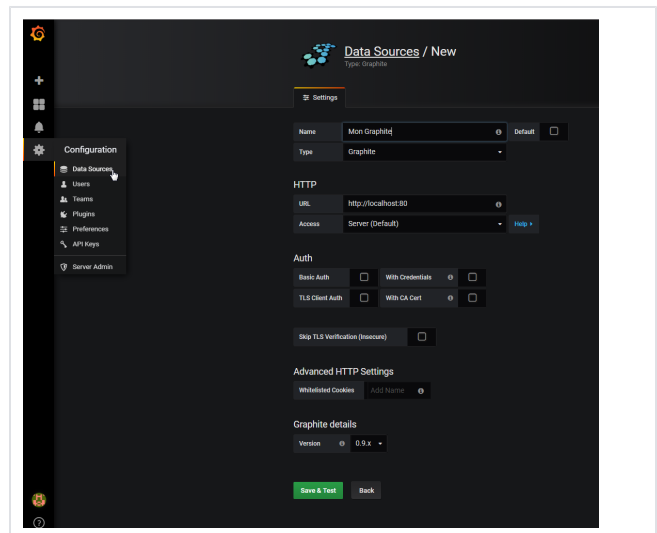
Connexion avec Graphite

Pour pouvoir récupérer les métriques générées par Shinken et enregistrées dans Graphite, Grafana doit avoir accès à Graphite. Pour cela, il faut ajouter dans Grafana une source de données Graphite.

Dans l'interface, aller dans la catégorie Data Sources , puis ajouter une nouvelle source de type Graphite, qui sera paramétrée comme suivant:

- **URL:** adresse du serveur hébergeant Graphite, sur le port 80. Par exemple:

```
http://adresse_serveur:80
```



Si Grafana est installé sur un serveur différent du serveur Graphite, il faudra effectuer une étape de configuration supplémentaire. Par défaut, Graphite autorise seulement les connexion locales. Pour permettre à des serveurs distants d'accéder à ses données, il faut:

- Changer la ligne suivante dans le fichier de configuration Apache de Graphite:

```
/etc/httpd/conf.d/graphite.conf
```

```
<VirtualHost 0.0.0.0:80>
```

Cette ligne permet de spécifier les interfaces réseau de la machine sur lesquelles effectuer l'écoute. Spécifier 0.0.0.0 ou * permet d'écouter sur toutes les interfaces réseau. On peut mettre une seule interface à la place en spécifiant l'IP de l'interface réseau concernée.

- Redémarrer Apache pour prendre en compte les modifications
Sur CentOS 6:

```
service http restart
```

Sur CentOS 7:

```
systemctl restart httpd
```

L'installation et la connexion de Grafana avec Graphite est maintenant terminée.

Vous pouvez maintenant créer des tableaux de bords, ajouter des utilisateurs et permettre la visualisation des métriques de Shinken.

Intégration dans Shinken

Pour centraliser la visualisation des éléments supervisés par Shinken, il est possible d'intégrer les dashboards Grafana dans un tableau de bord Shinken en utilisant la [Widget Page web](#).



Astuce

L'ajout de "&kiosk=true" dans l'URL du dashboard Grafana permet de cacher les barres de navigation de Grafana pour n'afficher que les éléments visualisés

Par exemple:



Lien vers la mapping nomuuid nécessaire pour grafana, et suivi des requêtes

Lors de l'utilisation de grafana, les requêtes vont arriver dans le serveur apache du serveur graphite avec des noms et non pas des uuids comme dans l'interface de visualisation qui elle fonctionne avec des uuids.

Pour cela il faut que le serveur apache ait accès à un mapping entre les noms et les uuids. Il faut le lier à la base SLA qui a en son sein ce mapping.

Cette configuration se fait au sein du fichier `/opt/graphite/conf/mongodb.conf` via le champ `URI`.

`/opt/graphite/conf/mongodb.conf`

```
URI=mongodb://localhost/?w=1&fsync=false
```

Les logs de cette connexion se font au sein du fichier `/var/log/graphite/info.log`

Les logs de mise à jour du cache seront activés. Si vous souhaitez suivre la mise à jour du mapping nom `uuid` et les requêtes pour un hôte particulier, vous pouvez saisir le nom de l'hôte dans le fichier `/opt/graphite/storage/whisper/apache_graphite_host_filter_log`. Vous verrez sa mise à jour dans le mapping, ainsi que les requêtes de recherches de métriques le concernant.

Sécurisation de la connexion graphite MongoDB

Comme toutes les connexions vers MongoDB il est possible, et même recommandé, de sécuriser la communication via un tunnel chiffré SSH. Ceci se définit dans le fichier `/opt/graphite/conf/mongodb.conf` avec les paramètres:

Nom du paramètre	Valeur par défaut	Utilité
<code>USE_SSH_TUNNEL</code>	0	Si 1, la connexion sera protégées par un tunnel SSH
<code>SSH_USER</code>	shinken	Nom distant de l'utilisateur de connexion
<code>SSH_KEYFILE</code>	<code>/opt/graphite/conf/id_rsa</code>	Chemin vers la clé SSH privée utilisée
<code>SSH_TUNNEL_TIMEOUT</code>	5	Durée du timeout au bout duquel on recommande l'établissement du tunnel s'il a échoué

La gestion de la clé SSH privée dans le cas de cette connexion est expliquée dans la page [Création automatique et gestion de la clé SSH de l'utilisateur shinken](#) car il faut copier la clé SSH de l'utilisateur shiken dans un répertoire accessible à apache qui héberge Graphite:

```
cp /var/lib/shinken/.ssh/id_rsa /opt/graphite/conf/id_rsa
chown apache:apache /opt/graphite/conf/id_rsa
```