Migration MMapV1 vers Wired Tiger

Sommaire

Concept

L'authentification par mot de passe à MongoDB garantit que seul l'utilisateur Shinken peut accéder aux données dans la base.

Activer l'authentification par mot de passe dans MongoDB

Pour activer l'authentification dans MongoDB, il rajoute le champ suivant dans le fichier de configuration /etc/mongod.conf

```
security:
 authorization: enabled
```

Exemple de fichier de configuration :

```
# for documentation of all options, see:
#   http://docs.mongodb.org/manual/reference/configuration-options/

# where to write logging data.
systemLog:
  destination: file
  logAppend: true
  path: /var/log/mongodb/mongod.log

# Where and how to store data.
storage:
  dbPath: /var/lib/mongo
  journal:
    enabled: true


# how the process runs
processManagement:
  fork: true  # fork and run in background
  pidFilePath: /var/run/mongodb/mongod.pid


# network interfaces
# NOTE: when go as a replicat member (cluster), change the 27017 to 27018 according to configuration
#       and comment the bindIp parameter
net:
  port: 27017
  unixDomainSocket:
    enabled: false
  bindIp: 127.0.0.1  # Listen to local interface only, comment to listen on all interfaces.




storage:
    engine: wiredTiger


security:
 authorization: enabled
```

Pour prendre en compte l'activation de l'authentification, il faut redémarrer le démon de la base de données :

```
systemctl restart mongod
```

Tant qu'aucun utilisateur n'a été crée, la base dispose d'une exception de connexion en localhost pour créer un utilisateur ayant mes privilèges de créer d'autres utilisateurs

Créer l'utilisateur Shinken

Il faut se connecter au shell MongoDB sur le serveur où se trouve la base (il faut être en localhost lors de cette connexion)

Lancer le shell MongoDB

```
mongo
```

Depuis le shell MongoDB lancer les commandes suivantes :

```
use admin
```

```
db.createUser(
 { user : 'YOUR_USER',
   pwd : 'YOUR_PASSWORD',
   roles : [ { role : 'root', db : 'admin' } ]
 }
)
```

Adapter la commande au nom de votre utilisateur et à votre mot de passe.

Il ne faut pas changer le champ role et db. En effet pour que Shinken fonctionne correctement, il a besoin de privilèg avancé sur l'ensemble des bases.

A partir de maintenant, seul l'utilisateur qui vient d'être crée peut se connecter à la base.

Déclarer l'utilisateur et le mot de passe dans Shinken

Dans les fichiers de configuration

Il faut désormais déclarer l'utilisateur et le mot de passe dans Shinken.

L'ensemble des composants de Shinken qui se connectent à MongoDB et qui doivent avoir leur configuration modifiée sur le serveur de l'Arbiter :

- Le démon Synchronizer : (*voir la page* Paramètres globaux (synchronizer.cfg))
- Le module event-manager-reader : (*voir la page* Module event-manager-reader)
- Le module event-manager-writer : (*voir la page* *FOR_MERGE - 005.0 - SEF-11716 - Module event-manager-writer*)
- Le module Graphite-Perfdata : (*voir la page* Module Graphite-Perfdata)
- Le module MongoDB : (*voir la page* Module MongoDB)
- Le module MongodbRetention : (*voir la page* Module MongodbRetention (Rétention en base de données centralisée par royaume))
- Le module SLA : (*voir la page* Module SLA)
- Le module livedata-module-sla-provider (*voir la page* Le livedata-module-sla-provider)
- Le collecteur de type discovery-import (*voir la page* Collecteur de type discovery-import (Scan NMAP))
- Dans le cas de l'utilisation de l'outil tier Grafana, il faut aussi modifier le fichier de configuration **/opt/graphite/conf/mongodb.conf** (*voir la page* Grafana - v8.3.2)

Dans les commandes

Une fois que l'authentification par mot de passe est activée dans la base, il faut passer les identifiants aux commandes qui se connectent à la base. Pour vérifier si une commande nécessite de s'authentifier à MongoDB, faire --help. Les paramètres à utiliser sont --mongo-username et --mongo–password. Les commandes qui doivent se connecter à MongoDB commencent qu'elles onts les privlièges suffisant pour fonctionner avant de commencer leur action pour s'assurer de ne pas créer d'inconsistance dans Shinken.

Si l'option **--mongo-password** est utilisée, le mot de passe risque d'être visible dans l'historique des commandes (*via la commande* ***history***).

Pour éviter d'exposer le mot de passe, il est possible d'utiliser cette commande uniquement avec l'option **--mongo-username**. Un prompt interactif apparaîtra alors pour demander le mot de passe.

Pour automatiser les commandes dans un script, il est possible de rediriger le contenu d'un fichier contenant le mot de passe (*en utilisant* ***cat*** *par exemple*) : --mongo-password $(cat my_file).