Reactionner - GLOBAL - Les logs généraux à tous les démons

Sommaire

Contexte

Pour stocker ses données, **Shinken Entreprise** utilise le système de base de données **MongoDB**.

- Cette page montre comment sécuriser les données de la base.
- Selon votre infrastructure, nous conseillons des stratégies de protection adaptée.

Une grande partie de la sécurisation de la base repose sur la limitation de l'écoute des requêtes sur la boucle locale (*localhost*).
Si la base n'écoute que sur la boucle locale, son accès automatiquement est limité et le chiffrement de ces connexions n'est plus utile (*on ne chiffre pas les données qui transitent sur la boucle locale*).

Infrastructure mono-serveur

Si vous n'avez qu'une seule machine pour votre installation de Shinken, la configuration par défaut de la base (*disponible dans le fichier /etc/mongod.conf*) lui permet seulement d'écouter les requêtes sur l'interface locale (*localhost*).

Extrait de /etc/mongod.conf

```
# Listen to local interface only. Comment out to listen on all interfaces.
bind_ip=127.0.0.1
```

Cela implique qu'aucun autre serveur ne pourra se connecter directement à la base MongoDB, seuls les démons de la machine pourrons interroger MongoDB sur la boucle locale (*localhost*).

C'est le moyen le plus simple de sécuriser l'accès à votre base.

Infrastructure multi-serveur avec une base MongoDB commune

Dans le cas où vous avez plusieurs machines sur votre infrastructure, nous préconisons de laisser la configuration par défaut de la base (*disponible dans le fichier /etc/mongod.conf*) qui limite l'écoute à l'interface locale (*localhost*).

Extrait de /etc/mongod.conf

```
# Listen to local interface only. Comment out to listen on all interfaces.
bind_ip=127.0.0.1
```

Pour que les démons, qui ne sont pas sur la machine qui héberge le **MongoDB**, puissent y accéder, nous recommandons d'utiliser des tunnels SSH.

- Ce système est intégré à Shinken et la mise en place des tunnels nécessite de simplement configurer les démons et modules qui se connectent à la base et de déployer la clé SSH de Shinken sur ces machines.

Cette approche à deux avantages :

- limite l'écoute de la base à l'interface locale,
- chiffre les connexions au serveur qui héberge la base MongoDB.

Infrastructure multi-serveur avec un cluster MongoDB

Ce chapitre suppose que vous soyez déjà familier avec les composants d'un cluster MongoDB (*voir la page Haute disponibilité de la base MongoDB (mise en place d'un cluster)*).

Protection entre Shinken et mongos

Vu qu'il faut un **mongos** sur chaque machine qui contient un démon ou un module de Shinken qui a besoin d'un accès au cluster MongoDB, il est possible de limiter l'écoute des mongos à l'interface locale (*localhost*).

Extrait de /etc/mongos.conf

```
# Listen to local interface only. Comment out to listen on all interfaces.
bind_ip=127.0.0.1
```

Dans ce cas, dans la configuration de Shinken, toutes les connexions à la base se feront sur l'adresse localhost.

Cette configuration va provoquer une erreur dans la validation de la configuration des modules de rétention.

Il faut autoriser "localhost" comme adresse valide avec l'option "mongodb_retention__database__bypass_banning_localhost_uri" de la configuration du module MongodbRetention (*voir la page Module MongodbRetention (Rétention en base de données centralisée par royaume)*).

Protection entre mongos et les mongod/mongo-configsrv

Cette protection est assurée par :

- La mise en place des règles de firewall qui permettront de limiter l'accès à la base (*voir la page Haute disponibilité de la base MongoDB (mise en place d'un cluster)*).
- La mise en place du chiffrement des connexions (*voir la page Activer le chiffrement (SSL) pour les communications d'un cluster MongoDB*).