Mécanismes de sécurisation du chiffrement

Sommaire

Concepts

Pour limiter les risques de perte de données, nous avons mis en place un certain nombre de protections :

- Avertissements en cas d'oubli de sauvegarde de la clé (shinken-healthcheck et commandes d'administration)
  - Utilisez la commande shinken-protected-fields-keyfile-export qui informe Shinken Entreprise que la clé a été exportée.
- Vérification de la cohérence entre la configuration décrite dans les fichiers et la base de données du Synchronizer.
  - L'encadré ci-contre vous explique de quoi il s'agit
  - La section ci-dessous **Vérification de la cohérence de la configuration** détaille les différents cas.
- Solution de secours en cas de perte de la clé
  - Si vous égarez votre clé veuillez vous référer à la documentation de shinken-protected-fields-keyfile-rescue-from-backup.
- **En cas d'incohérences et de risques de pertes de données, le Synchronizer refusera de démarrer et les outils de mener à bien leurs actions. Ils afficheront également les détails de ces incohérences.**

shinken-healthcheck

```
[ synchronizers ]
   [synchronizer: synchronizer-master]
       AT RISK: synchronizer-master is defined with the localhost address. It is a problem in distributed mode. Please configure it with the LAN IP/FQDN address instea
       OK:      Mongodb server is available at: mongodb://localhost/?safe=false
       OK:      Auth_secret is a custom variable
       OK:      Connection to daemon is OK at port 7765
       OK:      Connection to Synchronizer UI is OK at port 7766
       OK:      Daemon version is: v02.08.01-release.fr
       [Encryption status]
           ERROR:   The key has never been exported. Run shinken-protected-fields-keyfile-export and follow instructions
           OK:      Encryption ENABLED with key named : kn
```

Incohérence des données

Lorsque le Synchronizer démarre, il lit la configuration dans des fichiers et l'applique.

La configuration appliquée est sauvegardée dans la base de données.

Lorsque la configuration est modifiée par les commandes d'administration des données sensibles ou par d'autres biais, ces fichiers de configuration sont mis à jour, mais tant que le Synchronizer n'est pas redémarré, celui-ci ne prend pas en compte la nouvelle configuration.

C'est alors qu'il peut y avoir une incohérence, qui pourrait mettre en péril vos données si le Synchronizer démarrait et appliquait la configuration des fichiers sans vérification.

Vérification de la cohérence de la configuration

Le Synchronizer et les outils d'administration des champs protégés vérifient la cohérence entre les fichiers de configuration et la base de données.

Les points suivants sont vérifiés

- Le chiffrement est-il activé ?
- Nom de la clé
- la clé a-t-elle changé entre le fichier de configuration et celle utilisée pour le chiffrement de la base ?

En fonction du risque de perte de données, cette vérification donnera lieu à une erreur ou pas.

Ce tableau décrit les différents cas.

Chiffrement activé dans la base	Chiffrement activé dans la configuration	Incohérence	Conséquences
✗	✓	Clé différente	**Lors du redémarrage du Synchronizer, la base sera chiffrée avec la clé définie dans la configuration**
✗	✓	Nom différent	**Lors du redémarrage du Synchronizer, la base sera chiffrée avec la clé définie dans la configuration**
✗	✓	**Aucune incohérence**	**Lors du redémarrage du Synchronizer, la base sera chiffrée avec la clé définie dans la configuration**
✗	✗	Clé différente	**Aucune conséquence**
✓	✗	Clé différente	**Le synchronizer refusera de démarrer car il ne dispose pas de la bonne clé pour déchiffrer les données**
✓	✗	Nom différent	**Le synchronizer refusera de démarrer car il ne dispose pas de la bonne clé pour déchiffrer les données**
✓	✗	**Aucune incohérence**	**Le synchronizer démarrera et désactivera le chiffrement de la base**
✓	✓	Clé différente	**Le synchronizer refusera de démarrer car il ne dispose pas de la bonne clé pour travailler**
✓	✓	Nom différent	**Le synchronizer refusera de démarrer car il ne dispose pas de la bonne clé pour travailler**
✓	✓	**Aucune incohérence**	**Le synchronizer démarrera et ne modifiera pas l'état de la base**

Refus de démarrage du Synchronizer en cas de problème

Lorsque le Synchronizer ne peut pas démarrer à cause de problèmes liés au chiffrement de données sensibles, il affichera l'un des messages d'erreurs suivants :

Encryption is activated but there no key file is defined in the configuration

Le Synchronizer est configuré pour chiffrer les données, mais l'entrée **protect_fields__encryption_keyfile** dans le fichier de configuration du Synchronizer est manquante ou vide.

Solution: Utilisez la commande **shinken-healthcheck** pour vérifier si la base est effectivement chiffrée et le nom de la clé utilisée.

- Si la base est chiffrée, alors **shinken-healthcheck** vous donne le nom de la clé, et vous pouvez alors la restaurer avec la commande shinken-protected-fields-keyfile-restore
- Si la base de données n'est pas chiffrée, alors vous pouvez utiliser la commande shinken-protected-fields-encryption-disable pour revenir dans l'état correct.

Cela restaurera les bons champs dans le fichier automatiquement, sans que vous ayez a manipuler le fichier.

Note: Si vous n'utilisez que les commandes d'administration des champs protégés, cette erreur ne devrait pas se produire.

Cannot read the protected fields secret file <fichier> : <cause>

Le fichier contenant la clé de chiffrement n'est pas lisible pour la raison indiquée dans le message d'erreur.

Il peut s'agir du fait que le fichier n'existe pas ou bien que le compte Linux "shinken" sous lequel fonctionne le Synchronizer n'a pas les droits d'accès au fichier.

- Si c'est un problème de droits Linux, redonnez au fichier indiqué dans le message d'erreur des droits permettant à l'utilisateur Linux de le lire (et uniquement cet utilisateur).
- Si le fichier n'existe pas vous pouvez le restaurer avec la commande shinken-protected-fields-keyfile-restore.

The key contained in the keyfile does not have the right structure

Le fichier contenant la clé de chiffrement ne contient pas d'information utilisable par le Synchronizer. Il peut s'agit d'un fichier corrompu, auquel cas utilisez la commande shinken-protected-fields-keyfile-restore pour régénérer un fichier contenant les bonnes informations.

The Protected Fields key file was modified

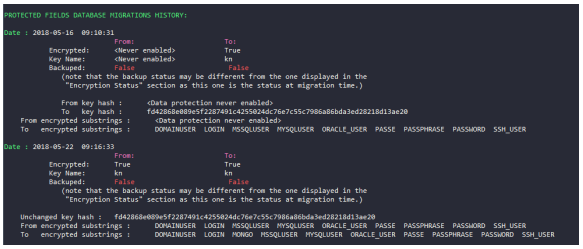
Cette erreur se produit lorsque la clé décrite dans les fichiers de configuration est différente de celle utilisée pour le chiffrement des données. Deux cas peuvent se produire :

- Le nom de la clé est différent. Dans ce cas le log contient les deux noms, ce qui vous permet de restaurer la bonne clé avec la commande shinken-protected-fields-keyfile-restore
- La clé elle-même a changé alors que le nom reste identique. Cela signifie que le fichier contenant la clé a été corrompu et la meilleure solution est de la restaurer avec la commande shinken-protected-fields-keyfile-restore

Si cela s'avérait nécessaire, référez vous à la page Paramétrage de l'interface de Configuration pour connaitre les paramètres liés au chiffrement, même si nous vous déconseillons de les modifier manuellement.

Vous pouvez utiliser la commande suivante, qui vous donnera l'historique des cinq dernières modifications concernant le chiffrement des données :

```
$ shinken-healthcheck --show-history
```



La copie d'écran montre que :

- le 16 / 05 le chiffrage a été activé avec la clé nommée **kn**
- le 22 / 05 la liste des données protégées a été modifiée

Dans les deux cas, la clé n'était pas sauvegardée au moment de la migration.

En cas de perte de la sauvegarde de la clé

Si vous perdez la sauvegarde de votre clé ET la clé, il reste un recours **si vous disposez d'un backup de la configuration effectué avec shinken-backup**.

Nous vous conseillons alors de vous référer à la documentation de la commande shinken-protected-fields-keyfile-rescue-from-backup qui vous permettra de restaurer votre clé avec l'aide du support Shinken.

Cette solution ne doit être utilisée qu'en dernier recours et ne doit pas remplacer les sauvegardes dont vous êtes responsable.

Il est fortement recommandé de changer la clé de chiffrement utilisée (shinken-protected-fields-keyfile-migrate) après cette manipulation.