Chiffrement des données sensibles

Description

Le chiffrement des données sensibles de l'interface de Configuration intervient lors du stockage. Cela protège les données dans l'éventualité où quelqu'un accéderait à la base de donnée sans en avoir l'autorisation.

- Les informations chiffrées se basent sur la même liste de mots-clés que celle des données protégées.
- Le chiffrement masque également les données sensibles pour les utilisateurs avec le droit d'administration Shinken.
- Le mécanisme de chiffrement nécessite l'utilisation d'une clé de chiffrement. Pour des raisons de pérennité, cette clé doit être placée par les administrateurs de Shinken dans un lieu sûr et sécurisé.
    - La perte de cette clé rendront les données inaccessibles.

Fonctionnalités principales :

- Stockage chiffré des données sensibles dans la base de données.
- Activation et désactivation du chiffrement à n'importe quel moment.
- Fourniture d'un ensemble de commandes système pour gérer le chiffrement et les clés.
- Activable aussi directement lors d'une installation ou une mise à jour.

⚠ Seul le Synchronizer et sa base de données bénéficient de ce mécanisme de protection.

- Les données sortantes du Synchronizer vers l'Arbiter ne sont pas chiffrées (la transmission de la configuration) et doivent être sécurisées via SSL.
    - Pour cela, voir la page Sécuriser les communications vers le Synchronizer.
- Les données sortantes du Synchronizer vers les navigateurs web ne seront pas chiffrées (en HTTP par défaut) et doivent être sécurisées via SSL .
    - Pour cela, voir la page Paramétrage de l'interface de Configuration

Les principales actions que vous serez amené à effectuer pour mettre en place cette fonctionnalité sont présenté ci-dessous:

Activation du chiffrement

Utilisez la commande shinken-protected-fields-encryption-enable qui vous guidera durant le processus.

Cette opération nécessite le redémarrage du Synchronizer.

N'oubliez pas de sauvegarder la clé de chiffrement générée après l'activation (voir paragraphe suivant).

- Il est important que vous sauvegardiez la clé, car elle vous sera nécessaire lorsque vous restaurerez une sauvegarde de Shinken Entrepris (faite par la commande shinken-backup).
- Par sécurité, la clef est insérée dans la sauvegarde, mais elle n'est pas en clair, afin de bénéficier dans les sauvegardes du même niveau de sécurité que pour la base de données. Référez vous à la page shinken-protected-fields-keyfile-rescue-from-backup, pour plus d'informations.

Identification des clés de chiffrement

Lors de l'activation, il vous sera demandé de choisir un nom pour votre clé. Les clés de chiffrements utilisés par Shinken Entreprise sont composées de deux éléments :

- Un nom, qu'il vous sera demandé de fournir.
- La clé proprement dite, qui sera générée par Shinken Entreprise.

Le fait de nommer les clés vous permettra de les identifier si vous en utilisez plusieurs ; une pour les tests, une pour la production, par exemple.

Notez cependant qu'une seule clé est active pour une configuration à un moment donné.

Le nom est également utilisé par toutes les commandes manipulant les clés et affichant des informations à leur sujet.

Sauvegarde et restauration de la clé

Référez-vous à la page shinken-protected-fields-keyfile-export pour la sauvegarde et à la page shinken-protected-fields-keyfile-restore pour la restauration.

La sauvegarde de la clé dans un endroit sécurisé et séparé de la sauvegarde de la configuration de Shinken Entreprise est de votre responsabilité.

Vous aurez besoin de restaurer la clé de chiffrement à la suite d'une restauration de Shinken via la commande **shinken-restore**.

Retrouver une clé perdue

Si vous perdez la sauvegarde de votre clé ET la clé, il reste un recours **si vous disposez d'une sauvegarde 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.

Changer de clé de chiffrement

Il existe différentes situations nécessitant de générer une nouvelle clé de chiffrement :

- Pour le passage en production suite à une phase de test ou une pré-prod.
- Si vous perdez votre clé, votre support Shinken vous la renvoie mais il est conseillé de régénérer la clé.
- ...

Référez vous à la page shinken-protected-fields-keyfile-migrate pour générer une nouvelle clé.

Désactivation du chiffrement

Pour désactiver le chiffrement de Shinken, veuillez utiliser la commande shinken-protected-fields-encryption-disable . Il sera nécessaire de redémarrer le Synchronizer pour prendre en compte cette opération.

Important

Les commandes d'installation et de mise à jour de Shinken Entreprise permettent d'automatiser la procédure d'activation du chiffrement ; il restera à votre charge la sauvegarde sécurisée de la clé générée lors de l'activation.

Il est très fortement conseillé d'utiliser ces commandes pour manipuler la configuration des champs protégés, plutôt que d'aller directement modifier les paramètres du fichier de configuration du Synchronizer, afin d'éviter tout risque de fausse manipulation pouvant entraîner la perte de vos données.