Chiffrement des données sensibles

Description

Le chiffrement des données permet de protéger les informations sensibles de l'interface de Configuration, tant au niveau du stockage que de l'interface utilisateur. Cela permet de protéger les données dans le cas où quelqu'un accéderait à la base de donnée sans en avoir l'autorisation.

- Les informations chiffrées sont la valeur de propriétés et de données, dont la liste est configurable.
- Le mécanisme de chiffrement nécessite l'utilisation d'une clé de chiffrement, qui, pour des questions de pérennité, doit être mise en sécurité par l'administrateur (rangée dans un endroit sécurisé), **car sans la clé, les données ne seront plus accessibles**.

Fonctionnalités principales :

- Stockage chiffré des données sensibles dans la base de données
- Possibilité de choisir les données à sécuriser.
- Activation et désactivation du chiffrement à n'importe quel moment.
- Fourniture d'un ensemble de commandes shell pour gérer le chiffrement et les clés.
    - Certaines commandes nécessitent une confirmation de l'utilisateur mais proposent une option pour pré-valider la confirmation dans le cas par exemple d'utilisation de la commande par script.
- Activable aussi directement lors d'une installation ou une mise à jour .

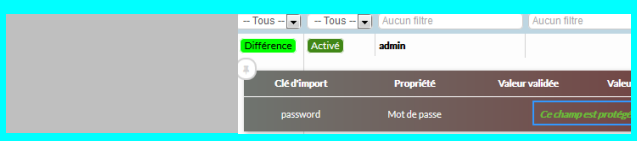
⚠ Seul le Synchronizer et sa base de donnée bénéficient de ce mécanisme de protection. Les données sortantes du Synchronizer vers l'Arbiter ne sont pas chiffrées (la transmission de la configuration) et doivent être sécurisées via SSL.

⚠ Même sans l'activation de cette fonctionnalité les Administrateurs de SI ne pourront voir les mots de passes dans le synchronizer.

Mise en œuvre

L'utilisation de cette fonctionnalité ne change en rien la manière d'utiliser Shinken mais les utilisateurs finaux utilisant l'interface de configuration ne pourront pas voir les propriétés chiffrées :

- Dans les pages d'édition, leur valeur est cachée par **des étoiles**.
- Dans les autres pages, un texte "Ce champ est protégé" est affiché en lieu et place de la véritable valeur.



Voici les principales actions que vous serez amené à effectuer pour mettre en place cette fonctionnalité :

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 Entreprise (faite par un 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 chiffrement 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.

Veuillez noter que 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'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.

Déterminer la liste des propriétés qui seront chiffrées

Une fois le chiffrement activé, assurez-vous que la liste des propriétés chiffrées correspond à vos besoins avec la commande shinken-protected-fields-properties-manage qui vous permettra de voir quelles propriétés seront chiffrées, ainsi que de la modifier le cas échéant.

Cette liste est modifiable alors que le chiffrement est actif ; mais la prise en compte des modifications nécessitera le redémarrage du Synchronizer.

Changer de clé de chiffrement

Il existe différentes situations nécessitant de chiffrer une base avec une nouvelle clé :

- En pré-prod ou en phase de test, la clé utilisée est connue par trop de monde ; pour le passage en production, il faut donc utiliser une nouvelle clé
- Si vous perdez votre clé et que votre support Shinken vous la renvoie, il est conseillé de rechiffrer votre base avec une nouvelle clé
- ...

Référez vous à la page shinken-protected-fields-keyfile-migrate

Désactivation du chiffrement

Veuillez utiliser la commande shinken-protected-fields-encryption-disable . Il est nécessaire de redémarrer le Synchronizer pour prendre en compte cette opération.

Information

En outre les commandes **shinken-healthcheck, shinken-backup** et **shinken-restore** gérer le chiffrement.

Enfin, 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.