

La surcharge des propriétés pour un check

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.

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 sécurité, doit être gérée par l'administrateur (stockage sécurisé d'une sauvegarde).

Fonctionnalités principales :

- Stockage chiffré des données sensibles dans la base de données
- Les données sensibles ne transitent pas en clair sur le réseau entre le navigateur Web et le Synchronizer (si SSL est activé)
- **Nombreux mécanismes** permettant d'éviter la perte de données
- Choix des données à chiffrer (nécessite le redémarrage du Synchronizer)
- Activation et désactivation du chiffrement à n'importe quel moment (nécessite le redémarrage du Synchronizer)
- Activation lors d'une nouvelle installation, lors d'une mise à jour depuis une version antérieure de Shinken Entreprise totalement automatisable.
- Gestion des clés de chiffrement.



Seul le Synchronizer bénéficie de cette fonctionnalité. Les données sortant du Synchronizer ne sont pas chiffrées (la transmission de la configuration à l'Arbiter en particulier)

Mise en œuvre

L'utilisation de cette fonctionnalité est transparente pour les utilisateurs excepté sur les points suivants :

- Les propriétés chiffrées ne sont pas affichées dans l'interface :
 - Dans les pages d'édition, leur valeur est remplacée par un champ de type "Mot de passe"
 - 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 amenés à effectuer pour mettre en place cette fonctionnalité :



Déterminer la liste des propriétés qui seront chiffrées

Avant toute chose, 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 ; cela nécessite le redémarrage du synchronizer.

Activation du chiffrement

Une fois la liste des propriétés établies, veuillez utiliser la commande **shinken-protected-fields-encryption-enable** qui vous guidera durant le processus. La désactivation peut se faire ensuite à n'importe quel moment avec la commande **shinken-protected-fields-encryption-disable**.

Ces deux opérations nécessitent le redémarrage du synchronizer.

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

Sauvegarde de la clé

Veillez utiliser la commande `shinken-protected-fields-keyfile-export` qui vous donnera toutes les informations nécessaires concernant la sauvegarde et la restauration éventuelle, si cela se révèle nécessaire.

Il est de votre responsabilité de stocker l'export généré à un emplacement sécurisé.

Désactivation du chiffrement

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



Veillez 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.

Si la sauvegarde n'est pas effectuée, la perte de l'intégralité des données de configuration de Shinken est presque certaine.

Shinken Entreprise fournit cependant des outils décrits ci-dessous pour cela.

Pour l'administrateur, Shinken fournit un certain nombre de commandes permettant l'administration du chiffrement :

<code>shinken-protected-fields-encryption-enable</code>	pour activer le chiffrement
<code>shinken-protected-fields-encryption-disable</code>	pour le désactiver
<code>shinken-protected-fields-keyfile-generate</code>	pour générer une nouvelle clé
<code>shinken-protected-fields-keyfile-export</code>	pour exporter une version de la clé, à sauvegarder manuellement et de manière sécurisée
<code>shinken-protected-fields-keyfile-restore</code>	pour restaurer une version sauvegardée de la clé et l'utiliser
<code>shinken-protected-fields-properties-manage</code>	pour visualiser la liste des propriétés chiffrées, ajouter ou supprimer un motif et en visualiser les conséquences
<code>shinken-protected-fields-keyfile-rescue-from-backup</code>	Cet outil est disponible dans le cas où vous avez perdu une clé. Il permet d'exporter une version chiffrée de la clé stockée dans une sauvegarde Shinken, afin de l'envoyer au support Shinken, qui vous renverra la clé exportée que vous pourrez restaurer avec la commande <code>shinken-protected-fields-keyfile-restore</code>

Toutes ces commandes vous guident dans leur utilisation.

En outre les commandes `shinken-healthcheck`, `shinken-backup` et `shinken-restore` savent 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.

