Modèle shinken-broker-db

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

Fonctionnalités principales :

- Stockage chiffré des données sensibles dans la base de données
- Possibilité de choisir les données sécurisées.
- Activation et désactivation du chiffrement à n'importe quel moment
- Gestion des clés de chiffrement.
- Possibilité d'automatisation par activation en ligne de commande Activation lors
  - d'une nouvelle installation.
  - lors d'une mise à jour depuis une version antérieure.

⚠ Seul le Synchronizer et sa base de donnée bénéficie 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.

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

? Unknown Attachment

? Unknown Attachment

? Unknown Attachment

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

Activation du chiffrement

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).

- **Il est important que vous sauvegardiez la clef de votre clé car elle vous sera nécessaire lorsque vous restaurer une sauvegarde de Shinken Entreprise (faite par un shinken-backup)**.
- **Pour des raisons de sécurité, la clef n'est pas stocké en clair dans la sauvegarde. Ceci met le même niveau de la base de données sur les les sauvegardes**.

Sauvegarde de la clé

Veuillez 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.

Nous vous conseillons de stocker la clef exportée dans un emplacement sécurisé.

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.

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.

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.

Si la sauvegarde n'est pas effectuée, la restauration d'une sauvegarde, le changement des propriétés protégées ou la désactivation du chiffrement ne seront pas possible.

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 :

shinken-protected-fields-encryption-enable	pour activer le chiffrement
shinken-protected-fields-encryption-disable	pour le désactiver
shinken-protected-fields-keyfile-generate	pour générer une nouvelle clé
shinken-protected-fields-keyfile-export	pour exporter une version de la clé, à sauvegarder manuellement et de manière sécurisée
shinken-protected-fields-keyfile-restore	pour restaurer une version sauvegardée de la clé et l'utiliser
shinken-protected-fields-properties-manage	pour visualiser la liste des propriétés chiffrées, ajouter ou supprimer un motif et en visualiser les conséquences

shinken-protected-fields-keyfile-rescue-from-backup	Cet outil est disponible dans le cas où vous auriez 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 shinken-protected-fields-keyfile-restore

Toutes ces commandes vous guident dans leur utilisation.

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.