shinken-protected-fields-encryption-enable

Sommaire

Description

Cette commande permet d'activer le chiffrement sur le Synchronizer.

- Elle affichera un texte explicatif des possibilités de protection des champs et vous demandera ensuite une confirmation pour être sûr que vous voulez vraiment activer le chiffrement.
  - Si aucune clé de chiffrement n'existe, elle est générée
  - Si une clé a déjà était mise en place (par l'activation puis désactivation), elle sera réutilisée
- Lors de l'activation:
  - Si le Synchronizer est démarré, il sera redémarré et le chiffrement activé.
  - S'il est stoppé, le chiffrement prendra effet au prochain redémarrage.

Options

Option courte	Description
-h	Affiche l'aide de la commande
-q	Mode silencieux : n'affiche que le minimum d'informations nécessaires
-y	Force l'activation du chiffrement sans demander la confirmation (utile lors de l'automatisation d'une installation)

Exemples

```
$ shinken-protected-fields-encryption-enable

This command will enable encryption and restart the synchronizer to encrypt the protected fields.

Checking consistency between the synchronizer configuration file and the currently running configuration... DONE

You can review the list of Shinken properties which will be protected using the following command :

        shinken-protected-fields-data-manage

You can remove or add substrings to that list and review which Shinken properties would become protected or unprotected
before committing using the following commands or a combination :

        shinken-protected-fields-data-manage --add substring1 --add substring2 ...

        shinken-protected-fields-data-manage --remove substring1 --remove substring2 ...


        Are you sure you want to proceed and enable encryption (if you answer negatively you can still re-run this command later) ? (y/N) y

In order to enable encryption, an secret key is required.
It will be generated now, but it can be changed at a later stage, assuming this one is still available.

This key must have a name in order to identify it easily if you have several of them.
Enter your key name: secret key

Enabling encryption with key named 'secret key'...


Now stopping the Synchronizer...  OK

Encryption enabled

Now restarting the Synchronizer...  OK

Your protected data is now encrypted, using the key generated with the key name you provided : secret key

 * You now need to make a backup of your key using the following command command :

      shinken-protected-fields-keyfile-export

 * NOTE : If you lose your key, you won't be able to restore a backup and you will have to contact your support.
```

Si le chiffrement est déjà activé, le lancement de la commande **shinken-protected-fields-encryption-enable** expliquera qu'une clé est déjà activée et comment migrer la base vers une nouvelle clé de chiffrement.

```
$ shinken-protected-fields-encryption-enable

This command will enable encryption and restart the synchronizer to encrypt the protected fields.

Checking consistency between the synchronizer configuration file and the currently running configuration... DONE

Encryption already enabled with the key named secret key

Nothing to do.

However if you want to encrypt your protected fields with a new key, please use the following command :

        shinken-protected-fields-keyfile-migrate
```