Paramétrage de l'interface de Configuration

Sommaire

Concepts

Pour accéder à cette interface, vous devez pointer votre navigateur Web vers l'adresse affichée durant l'installation.

- Par défaut, l'interface de configuration est accessible sur le port dédié 7766 (via le protocole HTTP). Par exemple : http://172.16.0.1:7766

Ce chapitre explique comment paramétrer l'interface de Configuration.

- Le fichier **/etc/shinken/synchronizer.cfg** contient : des paramètres globaux, les paramètres du daemon synchronizer, ainsi que les paramètres liés à l'interface de configuration.
- Grace aux paramètres de l'interface de configuration, vous pouvez paramétrer :
  - le SSL et certificats
  - le port d'écoute
  - le système SSO (Single Sign On)
  - l'activation des modules
  - la langue

SSL et certificats

L'interface de configuration peut être protégée par un accès HTTPS et des certificats.

Les paramètres se trouvent dans le fichier **/etc/shinken/synchronizer.cfg**.

```
# set the Configuration interface into HTTPs or not (disabled by default)
http_use_ssl=0

# Mandatory is SSL is enabled: server key and certificate
http_ssl_cert=/etc/shinken/certs/server.cert
http_ssl_key=/etc/shinken/certs/server.key
```

Activation du HTTPS

- Pour activer le HTTPS:
  - la propriété est **http_use_ssl**
    - par défaut la valeur est à 0 (pas de HTTPS)
    - mettre la valeur à 1 pour l'activer

Certificats

- Activez les certificats en mettant à jour les 2 paramètres suivant:
  - **http_ssl_cert**=/etc/shinken/certs/server.cert
  - **http_ssl_key**=/etc/shinken/certs/server.key

Les fichiers par défaut /etc/shinken/certs/server.cert et /etc/shinken/certs/server.key (certificats auto-signés non approuvés par une autorité de certification) sont justes des exemples fournis avec l'installation et vous **DEVEZ** les changer par vos propres certificats.

L'accès à l'interface utilisera toujours le port dédié 7766, mais en HTTPS :

- Par Exemple : https://172.16.1.130:7766

Le port d'écoute

Le port de l'interface de configuration peut être modifié.

Le paramètre se trouve dans le fichier **/etc/shinken/synchronizer.cfg**.

```
#======== Listening address (Configuration interface) =========
# Http(s) port to listen the Configuration interface
http_port=7766
```

Pour changer le port il suffit de modifier la valeur 7766 de la propriété **http_port**.

Paramétrage SSO

L'interface de configuration peut être accessible via SSO (Single SignOn).

Les paramètres se trouvent dans le fichier **/etc/shinken/synchronizer.cfg**.

```
                                                    # Remote application authentification
                                                    # if 1: allow the user to be load from a HTTP Header
http_remote_user_enable=0

                                                    # which HTTP header to get user name if
remote_user_enable is 1
http_remote_user_variable=X_Remote_User
                                                    # if remote_user_enable is 1,
                                                    # http_remote_user_case_sensitive to 1 enable case
check on remote user login
                                                    # http_remote_user_case_sensitive to 0 disable case
check on remote user login
                                                    # default value : 1, login is case sensitive
http_remote_user_case_sensitive=1
```

Voici un exemple de paramétrage ici.

Paramétrage du chiffrement des données sensibles

Les paramètres se trouvent dans le fichier **/etc/shinken/synchronizer.cfg**

```
#=============== Protected fields security ====================
                                                    # Encryption for protected fields
protect_fields__activate_encryption=1
                                                    # File containing the encryption key
protect_fields__encryption_keyfile=/etc/shinken/secrets/protected_fields_key
                                                    # List of words contained in protected fields names
                                                    # Default values : PASSWORD,PASSPHRASE,PASSE,
DOMAINUSER,MSSQLUSER,MYSQLUSER,ORACLE_USER,SSH_USER,LOGIN
protect_fields__substrings_matching_fields=PASSWORD,PASSPHRASE,PASSE,DOMAINUSER,MSSQLUSER,MYSQLUSER,
ORACLE_USER,SSH_USER,LOGIN
#==============================================================================
```

Nom du paramètre	Description
protect_fields__activate_encryption	0 = Chiffrage désactivé 1 = Chiffrage activé
protect_fields__encryption_keyfile	Chemin complet du fichier contenant la clé de chiffrement. Ce fichier ne doit être lisible que par l'utilisateur système sous lequel Shinken est lancé, par défaut **shinken**
protect_fields__substring_matching_fields	Liste des mots-clé permettant de déterminer les champs à chiffrer ; toutes les propriétés dont le nom contient l'un de ces mots-clés seront chiffrées

Nous vous conseillons d'utiliser les commandes d'administration du chiffrement des données sensibles, décrites dans la page Protection des données sensibles de l'UI de Configuration plutôt que de modifier directement la configuration ici.

Les modules

Les modules peuvent être chargés dans l'interface de configuration.

Le paramètre définissant le chemin du répertoire des modules se trouve dans le fichier **/etc/shinken/synchronizer.cfg**.

```
 # The path to the modules directory
modules_dir=/var/lib/shinken/modules
```

Langues

La langue de l'interface de configuration peut être changée.

Le paramètre se trouve dans le fichier /etc/shinken/synchronizer.cfg.

```
                                                # Select the lang that will be used by default on the
UIs
                                                # Currently managed:
                                                # -en    (english)
                                                # -fr    (francais)


lang=fr
```

Pour activer une langue :

- utilisez le paramètre **lang**
- A ce jour, 2 langues sont supportées: l'anglais (en) et le francais (fr)

Il est souhaitable que la sortie des démons soient également définies dans la même langue.

Pour cela, dans le fichier /etc/shinken/shinken.cfg

- il faut dé-commenter ou rajouter la ligne
  - language=fr
  - A ce jour, 2 langues sont supportées: l'anglais (en) et le francais (fr)

Accès à la base de données MongoDB

L'interface de Configuration à besoin de MongoDD afin de stocker la configuration.

Les paramètres se trouvent dans le fichier **/etc/shinken/synchronizer.cfg**.

```
#================================================================================
#======== Mongodb database connection =========
                                                # database type. currently only mongodb is managed.
data_backend=mongodb

                                                # mongodb uri definition for connecting to the
mongodb database. You can find the mongodb uri
                                                # syntax at https://docs.mongodb.com/manual/reference
/connection-string/
mongodb_uri=mongodb://localhost/?safe=false

                                                # mongodb database to use for this daemon.
mongodb_database=synchronizer

                                                # If you want to securize your mongodb connection you
can enable the ssh use_ssh_tunnel that will
                                                # allow all mongodb to be encrypted & authentificated
with SSH
                                                # Should use a SSH tunnel (Default 0=False)
mongodb_use_ssh_tunnel=0

                                                # If the SSH connection goes wrong, then retry
use_ssh_retry_failure time
                                                # Default: 1
mongodb_use_ssh_retry_failure=1

                                                # SSH user/keyfile in order to connect to the mongodb
server.
                                                # Default: shinken
mongodb_ssh_user=shinken

                                                # Default: ~shinken/.ssh/id_rsa
mongodb_ssh_keyfile=~shinken/.ssh/id_rsa
                                                                                                #
By default bailout the sychronizer if cannot contact mongodb for more than 120s
mongodb_retry_timeout=120

                                                # SSH Timeout used to test if the SSH tunnel is
viable or not, in seconds
                                                # Default: 5
mongodb_ssh_tunnel_timeout=5
```

Pour plus de sécurité, Il est possible d'utiliser un tunnel SSH pour se connecter à la base mongo.

- Le paramétrage de mongoDB permet de définir sur quel adresse ce dernier écoute les requêtes.
  - En n'autorisant seulement l'adresse 127.0.0.1, cela évite d'ouvrir la base au monde extérieur.
  - mais si le Synchronizer se trouve sur un autre serveur, il faut lui donner la possibilité de se connecter.
- Le tunnel SSH va permettre au Synchronizer de se connecter comme si ses requêtes étaient local au serveur mongo (en 127.0.0.1)

Pour cela il faut activer les options suivantes :

Nom du paramètre	Description
`mongodb_use_ssh_tunnel`	Activation du tunnel ou non (0 ou 1). Par défaut, il n'est pas activé (à 1)
`mongodb_use_ssh_retry_failure`	Spécifie le nombre supplémentaire de tentatives lors de l'établissement du tunnel SSH
`mongodb_ssh_user`	L'utilisateur utilisé pour établir la connexion
`mongodb_ssh_keyfile`	Une clé ssh publique présent sur le serveur Shinken (par défaut ~/.ssh/id_rsa.pub) qui sera utilisé pour établir le tunnel.
mongodb_ssh_tunnel_timeout	Timeout utilisé pour tester le tunnel SSH avant de le fournir à la connexion mongo

Paramétrage du délai d'attente de l'initialisation du Synchronizer

Nom du paramètre	Description	Valeur par défaut
wait_time_http_process_is_ready	Permet de définir le temps d'attente maximum (en secondes) que le Synchronizer attend pour le démarrage et l'initialisation de ses données. Cette valeur ne devrait pas nécessiter de modification.	180

Gestion des cookies

Les cookies sont chiffrés par l'interface afin que les utilisateurs ne puissent pas les forger et récupérer le compte d'un autre utilisateur. Pour cela, il utilise la clé de chiffrement contenue dans le paramètre

auth_secret

```
auth_secret=AUTH-SECRET-_O9ZyyQS-6ba9U0_ftOA41WIwt08tMvUEivMlrUUBnE8yNXhvqB6BOzcxVAk4XZ3Ku9YBQD4-
jUmvAWOJ8fSFDY43uID0F83b8sgERemlyE4QtUjHraPvyj6IpSAGQ2WKyBhaUY8jrkuEf_ny1_pYLeAuHW7a3BM_5qKpyEOhs9QMkjyYZ2S7E
FcdWNpApkq8I41svgcoPxUA-fJG2Lb9pqQyLyNAQ3-8nzEirFwwX4aKaBkIz7Sizr5Ah0lBbiI
```

Ce paramètre est généré lors de l'installation et n'a pas à être modifié par les administrateurs.

Ce paramètre doit rester le même que sur l'interface de visualisation si elle est située sur le même serveur que le synchronizer.

Paramètres internes de communications entre processus

Pour des raisons de performance, le processus du synchronizer a besoin de dialoguer avec le processus de l'interface de configuration. Pour protéger ces accès particuliers qui ne reposent pas sur des droits utilisateurs normaux (un appel avec un utilisateur même shinken admin sera refusé) une clé partagée est définie dans la configuration. Elle est générée lors de l'installation, et n'a pas à être modifiée par les administrateurs.

Clé de communication privée
master_key=MASTERKEY-t-F7MIXFNXWLeF6V4S6f_VjxmqaXOHbKwdfYqW7CP-El70s9JKGCijS- vZZyI8OL1NRfDqBQq3ziYRjFvX02b5BFFRSUnrQ5SZIPqdnYzFg6F7mtMB8NrPsBiBPsqz-fDFKIKwGUPe4GvWI-K5fKXOMDebDQy- Oww1tXl_U_Yl86iXPxfAXjhl7O4LEGV5l54w7KfU1m1in3Sifv642NQ8SGSFqnOxBhVcwUo8G7J8ScOHhY1j3HSaD53m84hln7