Sécuriser les communications vers le Synchronizer

Contexte

Afin de sécuriser les communications du Synchronizer, il est possible d'activer le SSL sur le daemon, via des paramètres dédiés à cet effet.

Attention, à la différence des autres daemons, le synchronizer et l'arbiter n'ont pas de fichiers ini dans le répertoire /etc/shinken/daemons. En effet, l'arbiter utilise le fichier /etc/shinken/shinken.cfg et le synchronizer utilise le fichier /etc/shinken/synchronizer.cfg, fichiers qui contiennent à la fois des paramètres globaux mais aussi leurs propres paramètres de configuration.

Important

Attention à ne pas confondre le protocole utilisé pour la communication des démons **ET** le protocole utilisé pour l'accès des utilisateurs /administrateurs aux interfaces Shinken via leurs navigateurs Internet (interface de configuration et interface de visualisation).
Nous traitons ici le paramétrage du protocole de communication du démon.

Paramétrage du SSL

Fichier /etc/shinken/synchronizer.cfg

Pour activer le SSL, sur le serveur hébergeant le démon Synchronizer, il faut tout d'abord modifier le fichier /etc/shinken/synchronizer.cfg qui contient les paramètres du démon.

Ce fichier contient un bloc concernant le paramétrage des ports d'écoutes du démon :

```
#======== Listening address (daemon) =========
# If enabled, the synchronizer daemon will listen in HTTPS instead of HTTP protocol.
# Note: default pem/cert and key files are for sample only. You need to generate
# your own with your PKI.
# by default: 0 (disabled)
use_ssl=1
ca_cert=/etc/shinken/certs/ca.pem
server_cert=/etc/shinken/certs/server.cert
server_key=/etc/shinken/certs/server.key
# Should the synchronizer connections will force the HTTPS certificates name checks
# If enabled and a distant certificate is not the same as the daemon address, then
# the connection will be refused.
hard_ssl_name_check=0
# Which HTTP backend to start the listening daemon with.
# Currently only auto is managed
http_backend=auto
# Which addr to bind for the synchronizer daemon
# by default: 0.0.0.0 (all interfaces)
bind_addr=0.0.0.0
```

Ce fichier contient le paramètre **use_ssl** à passer à **1 pour activer le SSL**.

Les certificats utilisés par défaut sont auto-signés et donc fournis à titre d'exemple, ils ne sont en aucun cas approuvés par une autorité de certification.
Il faut donc que vous placiez vos propres certificats dans le répertoire /etc/shinken/certs/ et modifiez alors les chemins si besoin.

Le paramètre **bind_addr** permet de modifier les IP qui pourront communiquer avec l'interface d'écoute du daemon Synchronizer.
La valeur par défaut est 0.0.0.0 pour que l'interface écoute les requêtes qui sont émises de n'importe quelle IP.

Fichier /etc/shinken/synchronizers/synchronizer-master.cfg

Il faut déclarer le démon Synchronizer auprès de l'Arbiter. Pour cela, sur le serveur central (hébergeant l'Arbiter), le fichier utilisé est /etc/shinken/synchronizers/synchronizer-master.cfg.

La variable use_ssl permet de signaler à l'Arbiter que pour contacter le Synchroniser, il faut utiliser une connexion SSL.

Passez donc le paramètre use_ssl à 1.

Fichier /etc/shinken/modules/synchronizer-import.cfg

Il faut enfin paramétrer le module qui permet à l'Arbiter de communiquer avec le Synchronizer.

Pour cela, sur le serveur central (hébergeant l'Arbiter), le fichier utilisé est /etc/shinken/modules/synchronizer-import.cfg.

Il faut changer l'URL pour que le protocole utilisé lors de la communication soit en SSL.

Pour cela, modifiez le paramétre URL pour y mettre le protocole HTTPS : exemple : https://localhost:7765