Sécuriser les communications vers le Broker

Contexte

La communication entres les démons se fait via le protocole HTTP.

Afin de sécuriser la communication des autres démons vers le Broker, il est possible d'activer le SSL sur ce démon et que ce dernier communique e
HTTPS.

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

Le paramétrage du démon se fait en 2 étapes:

- Sur la machine qui héberge le démon Broker:
  - Le fichier brokerd.ini permet d'initialiser le lancement du démon
  - Il faut donc le modifier pour déclarer l'utilisation du SSL pour que le démon ouvre une porte sécurisée
- Sur la machine qui héberge le démon Arbiter (le "Central"):
  - Déclarer le démon dans un fichier de définition (fichier cfg)

Passage du démon en SSL - Fichier /etc/shinken /daemons/brokerd.ini

Pour activer le SSL, sur le serveur qui héberge le Broker, il faut modifier le fichier /etc/shinken/daemons/brokerd.ini qui contient les paramètres du démon.

Ce fichier contient un bloc concernant le paramétrage des ports d'écoutes du démon (#-- HTTPS configuration –) :

```
[daemon]


################################################
########## Daemon directory and logging #########
################################################
# Directory the daemon will use to chdir into
workdir = /var/run/shinken

# Login directory, for standard logging and debug logging file
logdir  = /var/log/shinken

# Enable log for this daemon
use_local_log=1

# Standard log path
local_log=%(logdir)s/brokerd.log

# accepted log level values= DEBUG,INFO,WARNING,ERROR,CRITICAL
log_level=WARNING
```

```
# unique pid file
pidfile=%(workdir)s/brokerd.pid

# The system user the daemon will run as.
user=shinken

# The system group the daemon will run as.
group=shinken

# Set this parameter to 1 if you allow the daemon to run as root. Never do this unlesss you really understand
why you are doing it and the risk
# that add to your installation.
#idontcareaboutsecurity=0

# Directory to load modules code from
modules_dir=/var/lib/shinken/modules

# Set to 0 if you want to make this daemon NOT run
daemon_enabled=1


#-- External modules watchdog --
# If a module got a brok queue() higher than this value, it will be
# killed and restart. Put to 0 to disable it
max_queue_size=100000


################################################
########### Daemon HTTP(s) server        #########
################################################

# TCP port the daemon will listen to.
port=7772

# Address the daemon will listen to. By default 0.0.0.0=>all interfaces.
host=0.0.0.0

#-- HTTPS  configuration --
# Use or not the HTTPs as listening protocol for the daemon (default HTTP)
use_ssl=0

# Path for the CA certificate.
# NOTE: default file are for example ONLY. Do not use them in production!
#ca_cert=/etc/shinken/certs/ca.pem

# Path for the server certificate
#server_cert=/etc/shinken/certs/server.cert

# Path for the server key
#server_key=/etc/shinken/certs/server.key

# Enable or not the hard name for the HTTPS server name authentification (connection name and certificate mus
# match the exact string to allow connection)
hard_ssl_name_check=0

# Which http backend code to run. Use auto.
http_backend=auto

# Number of threads that will listen to external connection to this daemon. Increase it if your
# daemon will be accessed by lot of other daemons (like for large realm architectures)
daemon_thread_pool_size=64
```

Ce fichier contient donc 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.

Déclaration du démon - Fichier /etc/shinken/brokers/broker-master.cfg

Pour que tous les démons soient informés des caractéristiques du Broker, il faut déclarer ce démon auprès de l'Arbiter.

Pour cela, si vos fichiers de définition sont toujours ceux par défaut (issus de l'installation de Shinken), placez vous sur le serveur "central" (hébergeant l'Arbiter) et modifiez le fichier : /etc/shinken/brokers/broker-master.cfg

La variable **use_ssl** permet de signaler à l'Arbiter que pour contacter le Broker, il faut utiliser une connexion SSL et donc communiquer avec lui via le protocole **HTTPS**.

Passez donc le paramètre **use_ssl** à **1**.