Surcharge des paramètres du démon (synchronizer_cfg_overload.cfg)

Sommaire

Description
Exemple : Surcharge de la configuration de l'interface Web

Description

Le fichier de configuration des paramètres du Synchronizer pouvant être modifiés par les commandes Shinken, il est préférable d'ajuster les paramètres nécessaires dans le fichier suivant : **/etc/shinken-user/configuration/daemons/synchronizers/synchronizer_cfg_overload.cfg**

Les paramètres définis dans ce fichier vont écraser ceux dans les fichiers de configuration du Synchronizer. (*voir la page* Paramètres globaux (synchronizer.cfg))

Exemple : Surcharge de la configuration de l'interface Web

/etc/shinken-user/configuration/daemons/synchronizers/synchronizer_cfg_overload.cfg

```
#*******************************************************************************
#  This file is the overload of the /etc/shinken/synchronizer.cfg file
#  IMPORTANT: You MUST edit this file instead of the /etc/shinken/synchronizer.cfg
#             as the /etc/shinken file can be overwrite by an update
#
#  To set a value, just uncomment it and it will take precedence over the
#  /etc/shinken/synchronizer.cfg one
#*******************************************************************************

#================================================================================
#======== logging =========

# The synchronizer daemon log
#local_log=/var/log/shinken/synchronizerd.log


                                                    # If you disable, the timestamp will be an epoch
integer instead of a human date
#human_timestamp_log=1
#================================================================================



#================================================================================
#======== 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=0
#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 address to bind for the synchronizer daemon
                                                    # by default: 0.0.0.0 (all interfaces)
#bind_addr=0.0.0.0

#================================================================================


#================================================================================
#======== Listening address (Configuration interface) =========

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


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


                                                    # 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

                                                    # Cookie secret password. Is used to crypt cookies
#auth_secret=YOUR-VALUE

                                                    # Master key for CLI access
#master_key=YOUR-VALUE


                                                    # Remote application authentication
                                                    # 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

#================================================================================


#================================================================================
#======== INTERNAL OPTIONS =========

# On source page, some errors or warnings may concern many elements. A summary is shown
# for this error and you can set the number of message who are in this summary.
#number_of_message_in_source_summary=5


#================================================================================
```

```
#================================================================================
#======== 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 secure your mongodb connection you
can enable the ssh use_ssh_tunnel that will
                                                    # allow all mongodb to be encrypted & authenticated
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

                                                    # SSH Timeout used to test if the SSH tunnel is
viable or not, in seconds
                                                    # Default: 2
#mongodb_ssh_tunnel_timeout=2

                                                    # By default bailout the synchronizer if cannot
contact mongodb for more than 120s
#mongodb_retry_timeout=120

                                                    # The time the history will be kept for
synchronizations into database (in minutes)
#sync_history_lifespan=1440

#================================================================================

#================================================================================
#================ Protected fields security ====================
                                                    # Encryption for protected fields
#protect_fields__activate_encryption=0

                                                    # 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
#================================================================================

#================ Synchronizer Authentication External Log ====================
                                                    # Log the synchronizer authentication history in a
file
```

```
                                                        # Enable authentication log or not.
                                                        # by default: 0 (disabled)
# synchronizer__log_users__enabled=0

                                                        # File use for log authentication history
# synchronizer__log_users__file_path=/var/log/shinken/synchronizer/log_users.log

                                                        # Add user name to log.
                                                        # by default: 0 (disabled)
# synchronizer__log_users__add_user_name=0

#================================================================================
#======== Production page =========
                                                        # Timeout for the Arbiter to load a new configuration
#synchronizer__production__apply_new_configuration_timeout=30

#================================================================================
```