# Surcharge des paramètres du démon ( synchronizer_cfg_overload.cfg )

**Sommaire**



## Concept

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 comment is used by Shinken to recognize this file, please do not edit or remove it.
# If done so, several parts of Shinken, like sanitize, may not work properly.
# __OVERRIDE_TYPE__ synchronizer_cfg_overload
#  #

#  #
#      DAEMON LOGS PARAMETERS      #
#  #

#  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
#
#           ...     : 0 => timestamp
#           ...     : 1 => human date
#
# human_timestamp_log=1

#  Set logging level for the Synchronizer daemon.
#
#           ...     : accepted values: DEBUG,INFO,WARNING,ERROR,CRITICAL
#           Default : INFO ( info, warning and error logs will be shown )
#
# log_level=INFO

#  #
#      EXTERNAL AUTHENTICATION LOGS PARAMETERS      #
#  #

#  Log the synchronizer authentication and Session history in a file
#
#           ...     : 1 => Enable
#           Default : 0 => Disable
#
# synchronizer__log_users__enabled=0

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

#  Add user name to log
#
```

```
#           ...     : 1 => Enable
#           Default : 0 => Disable
#
# synchronizer__log_users__add_user_name=0

#  The logs files will be daily rotated up to the number of configurated days.
#  All log files older than the configured number of days will be deleted automatically.
#
#           Default : 7 (days)
#
# synchronizer__log_users__logs_rotation__nb_days_before_deletion=7

#  #
#      SYSTEM AND SECURITY      #
#  #

#   System daemon parameters (user, group, pid, ...)   #

#  Run or not the daemon
#
#           ...     : 0 => Disable
#           ...     : 1 => Enable
#
# daemon_enabled=1

#  Lock file (with pid) for the synchronizer daemon
#
# lock_file=/var/run/shinken/synchronizerd.pid

#  User used by the synchronizer
#
# shinken_user=shinken

#
# shinken_group=shinken

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

#  The path to the share files
#
# share_dir=/var/lib/shinken/share

#   Listening address (daemon)   #

#  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.
#
#           Default : 0.0.0.0 => (all interfaces)
#
# bind_addr=0.0.0.0

#  Enable HTTPS.
#
#           ...     : 1 => Use HTTPS
#           Default : 0 => Use HTTP
#
# use_ssl=0

#  Paths to pem/cert and key files
#  Note: default pem/cert and key files are for sample only. You need to generate
#  your own with your PKI.
#
# ca_cert=/etc/shinken/certs/ca.pem

#
```

```
# server_cert=/etc/shinken/certs/server.cert

#
# server_key=/etc/shinken/certs/server.key

#  Force the HTTPS certificates name checks by the synchronizer connections
#  If enabled and a distant certificate is not the same as the daemon address, then
#  the connection will be refused.
#
#           ...     : 0 => Disable
#           Default : 1 => Enable
#
# hard_ssl_name_check=0

#  #
#      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

    #  username/password to authenticate to MongoDB.
#  Both parameters must be provided for authentication to function correctly.
#
# synchronizer__database__username=

#
# synchronizer__database__password=

    #  Secure your mongodb connection
#  enable the ssh that will
#  allow all mongodb to be encrypted & authenticated with SSH
#
#           ...     : 1 => Enable
#           Default : 0 => Disable
#
# mongodb_use_ssh_tunnel=0

#  If the SSH connection goes wrong,
#  then retry use_ssh_retry_failure time
#
#           ...     : 0 => Disable
#           Default : 1 => Enable
#
# mongodb_use_ssh_retry_failure=1

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

#
# mongodb_ssh_keyfile=~shinken/.ssh/id_rsa

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

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

```
#           Default : 120 (in seconds)
#
# mongodb_retry_timeout=120

#  Each database request will be tried X times before considering it as an error and abort
#
#           Default : 15 (in seconds)
#
# synchronizer__database__retry_connection_X_times_before_considering_an_error=15

#  We will wait X seconds between each try or any database request
#
#           Default : 5 (in seconds)
#
# synchronizer__database__wait_X_seconds_before_reconnect=5

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

#  #
#      ADDRESS AND SECURITY      #
#  #

#   Listening address (Configuration interface)   #

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

#  set the Configuration interface into HTTPs or not (disabled by default).
#
#           ...     : 1 => Use HTTPS
#           Default : 0 => Use HTTP
#
# 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

#   Cypher keys   #

#  Cookie secret password. Is used to crypt cookies.
#
# auth_secret=TO_CHANGE

#  Master key for CLI access.
#
# master_key=TO_CHANGE

#   SSO authentication   #

#  Remote application authentication.
#
#           ...     : 1 => allow the user to be load from a HTTP Header
#           Default : 0 => Disable
#
# http_remote_user_enable=0

#  From which HTTP header get user name if remote_user_enable is 1.
#
# http_remote_user_variable=X-Remote-User

#  Case sensitivity of login if remote_user_enable is 1.
#
```

```
#           ...     : 0 => disable case check on remote user login
#           Default : 1 => enable case check on remote user login
#
# http_remote_user_case_sensitive=1

#  #
#      INTERFACE CONFIGURATION PARAMETERS      #
#  #

#   Language   #

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

#   Sources   #

#  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

#   Production page   #

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