Paramètres globaux (synchronizer.cfg)

Sommaire

Cette page explique les paramètres présents dans le fichier **/etc/shinken/synchronizer.cfg**

Si vous souhaitez apporter des modifications à ces paramètres, il est conseillé de modifier le fichier suivant : **/etc/shinken-user/configuration /daemons/synchronizers/synchronizer_cfg_overload.cfg**

Configuration des logs

La partie des logs du Synchronizer se gère avec ces paramètres :

/etc/shinken/synchronizer.cfg

```
#=============================================================================
#======== logging =========

# The synchronizer can have it's own local 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
#=============================================================================
```

Les paramètres sont les suivants :

Nom	Type	Unité	Défaut	Commentaire
`local_log`	Texte	---	**/var/log/shinken /synchronizerd.log**	Emplacement du fichier de log du Synchronizer
`human_timestamp_log`	Booléen	---	**1**	Permet d'afficher les logs avec un affichage de la date lisible facilement. • **1** => date au format "humain" • **0** => pour avoir un timestamp, si vous utilisez un système de gestion de log par exemple.

Paramètres du démon

Les paramètres suivants permettent de configurer le démon sur le serveur :

/etc/shinken/synchronizer.cfg

```
#=============================================================================
#======== System synchronizer daemon parameters (user, group, pid, ...) =========


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


# User that will be used by the synchronizer
shinken_user=shinken
shinken_group=shinken

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


# 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) =========

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

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

Les paramètres sont les suivants :

Nom	Type	Unité	Défaut	Commentaire	

`lock_file`	Texte	---	**/var/run/shinken/synchronizerd.pid**	Le chemin vers le fichier qui contient le numéro de PID du démon.	
`shinken_user`	Texte	---	**shinken**	Utilisateur Unix qui sera utilisé par le démon	
`shinken_group`	Texte	---	**shinken**	Groupe Unix qui sera utilisé par le démon	
`daemon_enabled`	Booléen	---	**1**	Défini si le démon est activé ou non. Pour Activer ou désactiver le Synchronizer, utiliser les commandes suivantes plutôt que de modifier le paramètre daemon_enabled : • shinken-daemons-disable synchronizer • shinken-daemons-enable synchronizer Ces commandes permettent de vérifier que le Synchronizer est dans un état correct avant de démarrer afin de ne pas corrompre la base de données (*exécution de sanatize-data*)	
`modules_dir`	Texte	---	**/var/lib/shinken/modules**	Emplacement des modules Shinken	
`share_dir`	Texte	---	**/var/lib/shinken/share**	Emplacement du dossier des fichiers partagés (*contiens les icônes affichées dans les listes de l'interface de configuration*)	
`use_ssl`	Booléen	---	**0**	Permet de définir si les autres démons doivent communiquer en SSL lorsqu'ils s'adressent au Synchronizer (*actuellement, seul l'Arbiter communique avec le Synchronizer*). Ne concerne pas l'interface de configuration.	
`ca_cert`	Texte	---	**/etc/shinken/certs/ca.pem**	Chemin de l'autorité de certification qui a généré le certificat SSL	
`server_cert`	Texte	---	**/etc/shinken/certs/server.cert**	Chemin du certificat SSL **SSL** Par défaut un certificat auto signé est livré afin de pouvoir mettre en place rapidement et facilement une sécurité sur les communications des démons. Il est conseillé d'utiliser vos propres certificats sur du plus long terme.	
`server_key`	Texte	---	**/etc/shinken/certs/server.key**	Chemin de la clé SSL	
`hard_ssl_name_check`	Booléen	---	**0**	Permet de forcer la vérification du nom du certificat avec le nom du serveur distant. • Cette option est désactivée par défaut, car le certificat livré dans l'installation est un certificat auto signé.	

`http_backend`	Texte	---	**auto**	Permet de définir le moteur HTTP à utiliser. • Pour le moment, seul le paramètre auto est géré.	
`bind_addr`	Texte	---	**0.0.0.0**	Défini l'interface qui sera en écoute sur le réseau. • La valeur 0.0.0.0 (*par défaut*) permet d'écouter sur toutes les interfaces.	

Configuration de l'interface de configuration

Les paramètres suivants permettent de configurer l'interface accessible depuis votre navigateur :

/etc/shinken/synchronizer.cfg

```
#===============================================================================
#======== 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=fr


# 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=AUTH-SECRET-
_RqRGhiNimAebzJRAY6Hx3mGGbxSlq_gx7Jirdz9ki4co8rK9yeQ8f_1qWDuRXT8CSTeHgXBZ9N1eKBwuQnh9-
5sWmZJn5e2MHOOk0jC7gIUFzfUeJsSHVRx3YLEBRpIP9WjYfGoPNkPq4tE64aZlR1Mukj_iRnC-
D8KX4P0zHKj_BJP_aws_ZzKR5l36rGrPozfdW0KryhdDTrwEg-me34MM22uQDjk_jYAF--ZHRMGgE5jY3gd_fXXlBEH29Ao

# Master key for CLI access
master_key=MASTERKEY-KUMi_DY49LtZTLI3XMiabDT5f_OyErn-8oH1Ew0z7kv86y5zNjm2bJ-Wf50cfy5Hwc1BTMBhA747p0_sKwd-
YAtbD2D9mmBY8ecBAvMmXIqRCaAe86GyBrQzQRaLz6_x38rjBT1ImAcwZwwE1U1tiI3qhLS4cRsRZHCP_DcKJ2XTDbYL7eoeBdc9FRUApTmP6
S5xdonY6_lteiBiUgceuJQkbCy94l6Es5yTzCH3PDqj11hy86hE9yekAmkgZkJz


# 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_UserSurcharge des paramètres du démon # 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


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

Les paramètres sont les suivants :

Nom	Type	Unité	Défaut	Commentaire

`http_port`	Entier positif	---	**7766**	Le port utilisé par l'interface
`lang`	Texte	---	***dépend de la version installé***	Langue de l'interface. La valeur par défaut est "**fr**" pour un installeur FR, "**en** " pour un installeur US.
`http_use_ssl`	Booléen	---	**0**	Permet de définir si l'interface sera accessible par HTTP (*valeur "**0**"*) ou HTTPS (*valeur "**1**"*)
`http_ssl_cert`	Texte	---	**/etc/shinken/certs /server.cert**	Certificat SSL
`http_ssl_key`	Texte	---	**/etc/shinken/certs /server.key**	Clé du certificat SSL
`auth_secret`	Texte	---	***générée lors de l'installation***	Clé générée à l'installation permettant de chiffrer les cookies
`master_key`	Texte	---	***générée lors de l'installation***	Clé générée à l'installation permettant un accès CLI
`http_remote_user_enable`	Booléen	---	**0**	Permet de s'authentifier par un en-tête. Cette option permet de configurer un accès SSO (*Single-Sign-One*) aussi appelé authentification unique.
`number_of_message_in_source_summary`	Entier positif	---	**5**	Permet de configurer le nombre de messages d'erreur ou d'avertissements dans le résumé d'une source

Configuration de la base de données du Synchronizer

La base de données utilisée est MongoDB. Pour la configurer, vous aurez besoin de modifier les paramètres suivants :

/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

# Timeout to wait for mongodb queries, in seconds
# Default: 120
mongodb_mongo_timeout=120

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

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

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

Les paramètres sont les suivants :

Nom	Type	Unité	Défaut	Commentaire
`data_backend`	Texte	---	**mongodb**	Moteur de base de données utilisé. Pour le moment, seule "mongodb" est gérée.
`mongodb_uri`	Texte	---	**mongodb://localhost/?safe=false**	Adresse de connexion à la base de données. La syntaxe est celle de mongo
`mongodb_database`	Texte	---	**synchronizer**	Le nom de la base de données utilisée
`mongodb_use_ssh_tunnel`	Booléen	---	**0**	Défini si la connexion à la base de données est directe ou doit être encapsulé dans un tunnel SSH.

`mongodb_use_ssh_retry_failure`	Booléen	---	**1**	Défini le nombre d'essais à réaliser si la connexion à la base de données est perdue
`mongodb_ssh_user`	Texte	---	**shinken**	L'utilisateur qui sera utilisé si la connexion à la base de données est encapsulée dans un tunnel SSH
`mongodb_ssh_keyfile`	Texte	---	**~shinken/.ssh/id_rsa**	La clé SSH qui sera utilisée si la connexion à la base de données est encapsulée dans un tunnel SSH
`mongodb_mongo_timeout`	Entier positif	---	**120**	Temps de connexion maximum avant que la connexion ne soit considérée comme trop longue et cause un échec de connexion
`sync_history_lifespan`	Entier positif	Minute	**1440**	Le nombre de minutes durant lesquelles les derniers imports seront conservés dans la base de données. La valeur par défaut est de 1440 minutes soit 45 heures.

Si votre base de données n'est pas hébergée sur le même serveur que le Synchronizer, il est préférable d'utiliser le tunnel SSH afin de ne pas exposer le port de la base de données sur le serveur distant.

Protection des données sensibles (*paramètres à ne pas modifier*)

La modification manuelle de ces paramètres peut entraîner une corruption de la base de données. La protection des données sensibles est configurable (*voir la page Protection des données sensibles de l'UI de Configuration*).

/etc/shinken/synchronizer.cfg

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

Les paramètres sont les suivants :

Nom	Type	Unité	Défaut	Commentaire
`protect_fields__activate_encryption`	Booléen	---	**0**	Définit si la protection est active
`protect_fields__encryption_keyfile`	Texte	---	**/etc/shinken/secrets/protected_fields_key**	Chemin de la clé de protection

`protect_fields__substrings_matching_fields`	Texte	---	• **PASSWORD,** • **PASSPHRASE,** • **PASSE,** • **DOMAINUSER,** • **MSSQLUSER,** • **MYSQLUSER,** • **ORACLE_USER,** • **SSH_USER,** • **LOGIN**	Chaîne de caractère générant une protection des données

La définition de ces paramètres est volontairement peu détaillée, car ils sont modifiés par les commandes Shinken adéquates. Ces commandes sont expliquées dans la page indiquée dans l'avertissement précédent.

Architecture de Shinken (*paramètres à ne pas modifier*)

Les paramètres suivants sont gérés par Shinken. Ils peuvent être modifiés par les commandes Shinken ou par l'installeur. Il est conseillé de ne pas modifier les valeurs. Les paramètres sont modifiables (*voir la page* Surcharge des paramètres du démon (synchronizer_cfg_overload.cfg)).

Les paramètres suivants permettent au Synchronizer de connaître les dossiers dans lesquels seront placés les fichiers de configurations (modules, démons, packs, données globales, fichier de surcharge)

/etc/shinken/synchronizer.cfg

```
#=============================================================================
#======== Modules and architecture =========

# sub directories to load. do not edit
cfg_dir=modules
cfg_dir=arbiters
cfg_dir=schedulers
cfg_dir=pollers
cfg_dir=reactionners
cfg_dir=brokers
cfg_dir=receivers
cfg_dir=realms
cfg_dir=synchronizers
cfg_dir=sources
cfg_dir=listeners
cfg_dir=analyzers
cfg_dir=taggers
cfg_dir=discovery_rules
cfg_file=synchronizer_discovery.cfg
packs_dir=packs

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

[...]

#=============================================================================
#======== Global DATA and default properties =========
# You will find global DATA into this directory
cfg_dir=resource.d

# Load default properties for types (like hosts). Do not edit theses files, they are overwritten at every
update.
cfg_dir=_default/default_element_properties

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

[...]


#=============================================================================
#======== User parameters customizations =========

# If you need to customise a value in this file, set it in this file
cfg_file=/etc/shinken-user/configuration/daemons/synchronizers/synchronizer_cfg_overload.cfg


# If you need to customise element (host, check, ...) default properties value, set it in this directory
cfg_dir=/etc/shinken-user/configuration/default_element_properties

# For your custom global DTA
cfg_dir=/etc/shinken-user/configuration/global-data

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

Log Externe d'Authentification

Les paramètres suivants permettent au Synchronizer de créer un fichier de log pour y recenser toutes les tentatives de connexion qu'elles soient réussies ou non ainsi que les déconnexions.

Ces paramètres ne sont là que pour avertir l'utilisateur qu'ils peuvent être modifiés dans le fichier */etc/shinken-user/configuration/daemons /synchronizers/synchronizer_cfg_overload.cfg* .

/etc/shinken/synchronizer.cfg

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

                                                        # Enable authentication log or not.
                                                        # by default: 0 (disabled)
# /!\ Need be change in the file: /etc/shinken-user/configuration/daemons/synchronizers
/synchronizer_cfg_overload.cfg
# synchronizer__log_users__enabled=0

                                                        # File use for log authentication history
# /!\ Need be change in the file: /etc/shinken-user/configuration/daemons/synchronizers
/synchronizer_cfg_overload.cfg
# synchronizer__log_users__file_path=/var/log/shinken/synchronizer/log_users.log

                                                        # Add user name to log.
                                                        # by default: 0 (disabled)
# /!\ Need be change in the file: /etc/shinken-user/configuration/daemons/synchronizers
/synchronizer_cfg_overload.cfg
# synchronizer__log_users__add_user_name=0
```

Nom	Type	Unité	Défaut	Commentaire
`synchronizer__log_users__enabled`	Texte	---	**0**	Permet d'activer (valeur "**1**") ou désactiver (valeur "**0**") les logs d'authentification de l'interface de configuration.
`synchronizer__log_users__file_path`	Booléen	---	**/var/log/shinken/synchronizer/log_users.log**	Définie le fichier utilisé pour écrire les logs.
`synchronizer__log_users__add_user_name`	Texte	---	**0**	Permet d'activer (valeur "**1**") ou désactiver (valeur "**0**") l'ajout du nom d'utilisateur dans les logs.

Page de Production

Les paramètres suivants permettent de configurer la page de Production

/etc/shinken/synchronizer.cfg

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

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

Nom	Type	Unité	Défaut	Commentaire
`synchronizer__production__apply_new_configuration_timeout`	Entier positif	---	**30**	Permet de définir un temps d'attente avant que l'Arbiter soit considéré comme indisponible lors d'une action dans la page de Production (*Vérification de la configuration, Application de la configuration…*)