

Sommaire

List
Overview
 The Action bar
 The title section which contains
 The content section is specific to each type of widget
Configuration
Delete
Favorite widget

Contexte

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

Si vous souhaitez apporter des modifications à ces paramètres,

- Nous vous **conseillons fortement** de les surcharger dans le fichier `/etc/shinken-user/configuration/daemons/brokers/modules/webui/webui_cfg_overload.cfg` (voir la page [Surcharge des paramètres du démon \(synchronizer_cfg_overload.cfg \)](#)).
- Les paramètres sont présents dans ce fichier pour vous indiquer qu'ils existent, mais leur modification dans le fichier de surcharge vous permettra une meilleure gestion (*ne pas modifier ce que l'on livre par défaut, mais le surcharger*).

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
<code>local_log</code>	Texte	---	<code>/var/log/shinken/synchronizerd.log</code>	Emplacement du fichier de log du Synchronizer
<code>human_timestamp_log</code>	Booléen	---	<code>1</code>	Permet d'afficher les logs avec un affichage de la date lisible facilement. <ul style="list-style-type: none">• <code>1</code> => date au format "humain"• <code>0</code> => pour avoir un timestamp, si vous utilisez un système de gestion de log par exemple.

Paramètres du démon

lock_file	Texte	---	<code>/var/run/shinken/synchronizerd.pid</code>	Le chemin vers le fichier qui contient le numéro de PID du démon.
shinken_user	Texte	---	<code>shinken</code>	Utilisateur Unix qui sera utilisé par le démon
shinken_group	Texte	---	<code>shinken</code>	Groupe Unix qui sera utilisé par le démon
daemon_enabled	Booléen	---	<code>1</code>	<p>Définis si le démon est activé ou non.</p> <div style="border: 1px solid red; padding: 10px; margin: 10px 0;"> <p> Pour Activer ou désactiver le Synchronizer, utilisez les commandes suivantes plutôt que modifier le paramètre <code>daemon_enabled</code> :</p> <ul style="list-style-type: none"> • <code>shinken-daemons-disable synchronizer</code> • <code>shinken-daemons-enable synchronizer</code> <p>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 (<i>exécution de <code>sanitize-data</code></i>)</p> </div>
modules_dir	Texte	---	<code>/var/lib/shinken/modules</code>	Emplacement des modules Shinken
share_dir	Texte	---	<code>/var/lib/shinken/share</code>	Emplacement du dossier des fichiers partagés (<i>contiens les icônes affichées dans les listes de l'interface de configuration</i>)
use_ssl	Booléen	---	<code>0</code>	Permet de définir si les autres démons doivent communiquer en SSL lorsqu'ils s'adressent au Synchronizer (<i>actuellement, seul l'Arbiter communique avec le Synchronizer</i>). Ne concerne pas l'interface de configuration.
ca_cert	Texte	---	<code>/etc/shinken/certs/ca.pem</code>	Chemin de l'autorité de certification qui a généré le certificat SSL
server_cert	Texte	---	<code>/etc/shinken/certs/server.cert</code>	<p>Chemin du certificat SSL</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <p> SSL</p> <p>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 surs du plus long terme.</p> </div>
server_key	Texte	---	<code>/etc/shinken/certs/server.key</code>	Chemin de la clé SSL
hard_ssl_name_check	Booléen	---	<code>0</code>	<p>Permet de forcer la vérification du nom du certificat avec le nom du serveur distant.</p> <ul style="list-style-type: none"> • Cette option est désactivée par défaut, car le certificat livré dans l'installation est un certificat auto signé.

http_ba ckend	Texte	---	auto	Permet de définir le moteur HTTP à utiliser. <ul style="list-style-type: none">• Pour le moment, seul le paramètre auto est géré.
bind_ad dr	Texte	---	0.0.0.0	Définis l'interface qui sera en écoute sur le réseau. <ul style="list-style-type: none">• La valeur 0.0.0.0 (<i>par défaut</i>) 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    (français)
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_lqWduRXT8CSTeHgXBZ9N1eKBwuQnh9-
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_lteiBiUgceuJQkbCy94l6Es5yTzCH3PDqjllhy86hE9yekAmkgZkJz

# 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

#####
```

Les paramètres sont les suivants :

Nom	Type	Unité	Défaut	Commentaire
-----	------	-------	--------	-------------

http_port	Entier positif	---	7766	Le port utilisé par l'interface
lang	Texte	---	<i>dépend de la version installée</i>	Langue de l'interface. La valeur par défaut est "fr" pour un installateur FR, "en" pour un installateur US.
http_use_ssl	Booléen	---	0	Permet de définir si l'interface sera accessible par HTTP (<i>valeur "0"</i>) ou HTTPS (<i>valeur "1"</i>)
http_ssl_cert	Texte	---	<i>/etc/shinken/certs /server.cert</i>	Certificat SSL
http_ssl_key	Texte	---	<i>/etc/shinken/certs /server.key</i>	Clé du certificat SSL
auth_secret	Texte	---	<i>générée lors de l'installation</i>	Clé générée à l'installation permettant de chiffrer les cookies
master_key	Texte	---	<i>générée lors de l'installation</i>	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 (<i>Single-Sign-One</i>) 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

```
#####
##### Mongoddb database connection #####
# database type. currently only mongoddb is managed.
data_backend=mongoddb

# mongoddb uri definition for connecting to the mongoddb database. You can find the mongoddb uri
# syntax at https://docs.mongoddb.com/manual/reference/connection-string/
mongoddb_uri=mongoddb://localhost/?safe=false

# mongoddb database to use for this daemon.
mongoddb_database=synchronizer

# If you want to securize your mongoddb connection you can enable the ssh use_ssh_tunnel that will
# allow all mongoddb to be encrypted & authenticated with SSH
# Should use a SSH tunnel (Default 0=False)
mongoddb_use_ssh_tunnel=0

# If the SSH connection goes wrong, then retry use_ssh_retry_failure time
# Default: 1
mongoddb_use_ssh_retry_failure=1

# SSH user/keyfile in order to connect to the mongoddb server.
# Default: shinken
mongoddb_ssh_user=shinken

# Default: ~shinken/.ssh/id_rsa
mongoddb_ssh_keyfile=~shinken/.ssh/id_rsa

# Timeout to wait for mongoddb queries, in seconds
# Default: 120
mongoddb_mongo_timeout=120

# By default bailout the sychronizer if cannot contact mongoddb for more than 120s
mongoddb_retry_timeout=120

# Each database request will be tried X times before considering it as an error and abort
# Default : 15
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
synchronizer__database__wait_X_seconds_before_reconnect=5

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

#####
```

Les paramètres sont les suivants :

Nom	Type	Unité	Défaut	Commentaire
data_backend	Texte	---	mongoddb	Moteur de base de données utilisé. Pour le moment, seule "mongoddb" est gérée.
mongoddb_uri	Texte	---	mongoddb://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	Définis 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	Définis 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
synchronizer_database_retry_connection_X_times_before_considering_an_error	Entier positif	---	15	Nombre de tentatives à effectuer avant de considérer une requête en base de donnée comme étant en erreur
synchronizer_database_wait_X_seconds_before_reconnect	Entier positif	Seconde	5	Temps d'attente entre chaque tentative de requête vers la base de données
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	---	<ul style="list-style-type: none">• 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'installateur. 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 lesquelles 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

#####
```

Les logs d'activité des utilisateurs (authentication et session)

Les paramètres suivants permettent au Synchronizer de créer un fichier de log supplémentaire pour y recenser l'activité des utilisateurs (*authentication et session*), qu'elles soient réussites ou non, ainsi que les déconnexions.

- Nous vous conseillons fortement de les surcharger dans le fichier `/etc/shinken-user/configuration/daemons/synchronizers/synchronizer_cfg_overload.cfg`.
- Ils sont présents dans ce fichier pour vous indiquer qu'ils existent, mais leur modification dans le fichier de surcharge vous permettra une meilleure gestion (*ne pas modifier ce que l'on livre par défaut, mais le surcharger*).

`/etc/shinken/synchronizer.cfg`

```

#===== Synchronizer Authentication and Session External Log =====
# Log the synchronizer authentication and session
history in a file

# Enable authentication and session 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 and session 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
<code>synchronizer_log_users_enabled</code>	Booléen	---	0	Permet d'activer (valeur "1") ou désactiver (valeur "0") les logs d'authentification et de session de l'interface de configuration.
<code>synchronizer_log_users_file_path</code>	Texte	---	<code>/var/log/shinken/synchronizer/log_users.log</code>	Définit le fichier utilisé pour écrire les logs.
<code>synchronizer_log_users_add_user_name</code>	Booléen	---	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_t imeout	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 (<i>Vérification de la configuration, Application de la configuration...</i>)