

shinken-synchronizer (Modèle d'hôte)

Sommaire

Contexte

Description du modèle

Checks

Paramètre du check

Détail des commandes

Description des erreurs de Synchronizer - \$KEY\$ - Alive

Erreur de surcharge des disques de logs

Erreur de vol de CPU

Erreur d'un démon bloqué, qui doit être redémarré

Le démon a bloqué une tentative de chargement d'objet malveillant

Le démon est en cours d'arrêt

Contexte

Le modèle shinken-synchronizer vous permet de superviser un hôte hébergeant le démon Synchronizer (voir la page [Le Synchronizer](#)).

Description du modèle

Modèle d'hôte correspondant: **shinken-synchronizer** (notez que ce modèle hérite du modèle **shinken**, **shinken-deamon** et **shinken-synchronizer-db**)

Afin de superviser le démon Synchronizer, le modèle **shinken-synchronizer** appliqué à votre hôte, attachera plusieurs checks qui vérifieront la santé et la performance de ce démon.

Checks

- Synchronizer - \$KEY\$ - Alive

•

Vérifie que le démon Synchronizer peut être correctement contacté sur le réseau. Son numéro de version est affiché.

Si jamais le démon Arbiter est en exécution sur une machine virtuelle supervisé par VMware, alors le pourcentage de temps de vol de CPU (CPU Ready) sera affiché.

[illegible]

- Synchronizer - \$KEY\$ - Performance API Connection

Vérifie la latence de connexion au Synchronizer et ses performances

 Synchronizer - synchronizer-master - Performance API Connection [OK] API Connexion is in the good range [0.001 < 2s].

- **Synchronizer - DB - Connection**

Vérifie le temps de connexion
à la base de données

	Synchronizer - DB - Connection	[OK] - Connection took 0.003 seconds
---	--------------------------------	--------------------------------------

- Synchronizer - DB - Last Flush Time

Vérifie la durée du dernier "Flush" de la base de données

	Synchronizer - DB - Last Flush Time	[OK] - Last Flush Time: 255.00ms
---	-------------------------------------	----------------------------------



La version V02.07.00 de Shinken est accompagnée d'une mise à jour de MongoDB. Cette nouvelle version comporte notamment un changement de la méthode de sauvegarde des objets au sein de Mongo.

Sur une installation neuve de Shinken, le nouveau format (WiredTiger) est utilisé, ce qui rend le " **Synchronizer - DB - Last Flush Time** " non pertinent. Dans ce cas, ce check aura le résultat suivant:

	Synchronizer - DB - Last Flush Time	[OK] - Mongo 3 is not in MMapV1 mode but in wiredTiger (new format) r mode. This indicator is not available.
--	-------------------------------------	--

Dans le cas d'une mise à jour de Shinken, la méthode de stockage des données dans Mongo n'est pas modifiée et le check "Synchronizer - DB - Last Flush Time" a le même comportement que précédemment.

- **Synchronizer - DB - Open Connections**

Vérifie le nombre de connexions en cours sur la base de données

	Synchronizer - DB - Open Connections	[OK] - 0 percent (127 of 51200 connections) used
--	--------------------------------------	--



Lors de la mise à jour de Shinken une montée de version de MongoDB est effectuée. Le check " **Synchronizer - DB - Lock Time Percentage** " devient obsolète et peut être désactivé. La source "cfg-file-shinken" propose la désactivation du check mais ne peut pas le supprimer automatiquement.

Paramètre du check

Les checks du Synchronizer peuvent être configurés via des données fournies par le modèle.

Les données suivantes sont disponibles pour le Synchronizer:

Nom de la donnée	Description	Valeur par défaut	Hérité du modèle d'hôte ou locale
SHINKEN_PROTocol	Protocole utilisé pour établir la connexion avec le Synchronizer	http	shinken
CHECK_SHINKEN_TIMEOUT	Timeout utilisé pour établir la connexion avec le Synchronizer	3	shinken
SYNCHRONIZER_PORT	Port utilisé pour l'établissement de la connexion avec Synchronizer	7772	Locale
SYNCHRONIZER_LIST	Liste de Synchronizer (Multi-démon)	synchronizer-master\$(\$_HOSTSYNCHRONIZER_PORT\$)\$	Locale - Duplicate For Each (voir la page Dupliquer des checks en fonction d'une liste de valeurs présentes dans la Donnée d'un hôte (duplicate_foreach))
DB_CONNECTION_METHOD	Méthode de connexion au serveur MongoDB ("direct" ou "ssh")	ssh	shinken-synchronizer-db
DB_CONNECTIONS_CRIT	Seuil critique du nombre de connexions en cours sur la base de données (en pourcentage)	80	shinken-synchronizer-db
DB_CONNECTIONS_WARN	Seuil warning du nombre de connexions en cours sur la base de données (en pourcentage)	70	shinken-synchronizer-db
DB_CONNECTION_CRIT	Seuil critique pour le temps de connexion à la base de données (en secondes)	4	shinken-synchronizer-db
DB_CONNECTION_WARN	Seuil warning pour le temps de connexion à la base de données (en secondes)	2	shinken-synchronizer-db
DB_LAST_FLUSH_TIME_CRIT	Seuil critique pour le temps de flush de la base de données (en millisecondes)	10000	shinken-synchronizer-db
DB_LAST_FLUSH_TIME_WARN	Seuil warning pour le temps de flush de la base de données (en millisecondes)	8000	shinken-synchronizer-db
DB_PORT	Port de la base de données	27017	shinken-synchronizer-db
DB_SSH_KEY	Clé SSH privée permettant la connexion au serveur hébergeant MongoDB	~/.ssh/id_rsa	shinken-synchronizer-db

DB_SSH_USER	Utilisateur distant avec lequel se connecter au serveur hébergeant MongoDB	shinken	shinken-synchronizer-db
THRESHOLD_CPU_STOLEN_WARNING	Seuil de CPU volé (en pourcentage) sur une machine virtuelle supervisée par VMware avant de déclencher un warning	5	shinken-deamon
THRESHOLD_CPU_STOLEN_CRITICAL	Seuil de CPU volé (en pourcentage) sur une machine virtuelle supervisée par VMware avant de déclencher un critique	10	shinken-deamon

Voir la page de [Sécurisation des connexions aux bases MongoDB](#) pour plus d'information sur un paramétrage sécurisé.

Détail des commandes

Nom du check	Commande du check	Ligne de commande
Synchronizer - \$KEY\$ - Alive	check_shinken_synchronizer! alive ! \$VALUE1\$	\$PLUGINS_DIR\$/check_shinken -H "\$HOSTADDRESS\$" -p "\$ARG2\$" --shinkenversion "\$SHINKENVERSION\$" -t synchronizer -m \$ARG1\$ --timeout \$_HOSTCHECK_SHINKEN_TIMEOUT\$
Synchronizer - \$KEY\$ - Performance API Connection	check_shinken_synchronizer! api_connection ! \$VALUE1\$	\$PLUGINS_DIR\$/check_shinken -H "\$HOSTADDRESS\$" -p "\$ARG2\$" --shinkenversion "\$SHINKENVERSION\$" -t synchronizer -m \$ARG1\$ --timeout \$_HOSTCHECK_SHINKEN_TIMEOUT\$
Synchronizer - DB - Connection	check_shinken_db_connection	\$PLUGINS_DIR\$/check_shinkendb.py -D -H "\$HOSTADDRESS\$" -P "\$_HOSTDB_PORT\$" --connection-method "\$_HOSTDB_CONNECTION_METHOD\$" --ssh-user "\$_HOSTDB_SSH_USER\$" --ssh-keyfile "\$_HOSTDB_SSH_KEY\$" -A connect -W "\$_HOSTDB_CONNECT_WARN\$" -C "\$_HOSTDB_CONNECT_CRIT\$" --timeout \$_HOSTCHECK_SHINKEN_TIMEOUT\$
Synchronizer - DB - Last Flush Time	check_shinken_db_last_flush	\$PLUGINS_DIR\$/check_shinkendb.py -D -H "\$HOSTADDRESS\$" -P "\$_HOSTDB_PORT\$" --connection-method "\$_HOSTDB_CONNECTION_METHOD\$" --ssh-user "\$_HOSTDB_SSH_USER\$" --ssh-keyfile "\$_HOSTDB_SSH_KEY\$" -A last_flush_time -W "\$_HOSTDB_LAST_FLUSH_TIME_WARN\$" -C "\$_HOSTDB_LAST_FLUSH_TIME_CRIT\$" --timeout \$_HOSTCHECK_SHINKEN_TIMEOUT\$ -w \$_HOSTTHRESHOLD_CPU_STOLEN_WARNING\$ -c \$_HOSTTHRESHOLD_CPU_STOLEN_CRITICAL\$
Synchronizer - DB - Open Connections	check_shinken_db_open_connections	\$PLUGINS_DIR\$/check_shinkendb.py -D -H "\$HOSTADDRESS\$" -P "\$_HOSTDB_PORT\$" --connection-method "\$_HOSTDB_CONNECTION_METHOD\$" --ssh-user "\$_HOSTDB_SSH_USER\$" --ssh-keyfile "\$_HOSTDB_SSH_KEY\$" -A connections -W "\$_HOSTDB_CONNECTIONS_WARN\$" -C "\$_HOSTDB_CONNECTIONS_CRIT\$" --timeout \$_HOSTCHECK_SHINKEN_TIMEOUT\$ -w \$_HOSTTHRESHOLD_CPU_STOLEN_WARNING\$ -c \$_HOSTTHRESHOLD_CPU_STOLEN_CRITICAL\$



Lors de la mise à jour de Shinken une montée de version de MongoDB est effectuée. Le check "Synchronizer - DB - Lock Time Percentage" devient obsolète et peut être désactivé. La source "cfg-file-shinken" propose la désactivation du check mais ne peut pas le supprimer automatiquement.

Description des erreurs de Synchronizer - \$KEY\$ - Alive

Erreur de surcharge des disques de logs

- Disque des logs trop lent :

En cas de disques trop lent sur le volume des logs, le check sera mis en **WARNING** avec l'erreur suivante.

```
[WARNING] The synchronizer have some issues.
=> WARNING - Writing logs on disk took too much time ( worth time was 2.0s during the last minute)
Path: "/var/log/shinken/"
```

Erreur de vol de CPU

Seulement si votre machine virtuelle est hébergé sur un hyperviseur VMWare

- Votre machine à du vol de CPU :
 - Si la VM se fait voler trop de temps de calcul (*CPU Stolen*), le check sera mis en **WARNING** ou en **CRITIQUE** (*en fonction du taux de vol fixé par défaut ou indiqué par l'utilisateur*).
 - Vous pouvez avoir plus d'information sur cet indicateur et comment réduire la part de temps de la VM sur la page [Machine VMWare avec un fort taux de CPU Stolen \(%ready + %costop\)](#)

[WARNING] The daemon have some issues:

- => Your machine got **8% of CPU STOLEN** from the Hypervisor (Type VMWare)
- => On the VCenter search the data **CPU %ready + %costop**
- => Please have a look at the Shinken Enterprise documentation about advices to reduce it

[CRITICAL] The daemon have some issues:

- => Your machine got **20% of CPU STOLEN** from the Hypervisor (Type VMWare)
- => On the VCenter search the data **CPU %ready + %costop**
- => Please have a look at the Shinken Enterprise documentation about advices to reduce it

Erreur d'un démon bloqué, qui doit être redémarré

- Si un démon est dans un état bloqué, il doit être redémarré. Si c'est le cas:
 - les checks seront en **ERROR** avec le message suivant,
 - il faut ouvrir un ticket à votre support pour analyser le blocage

[CRITICAL]

The daemon have a **lock**, it's **not working** and **MUST** be restarted.
Please contact your support to analyse the daemon logs:

- "Main loop" was locked more than 3600s
- Detected at 2021-12-03 08:21:55 [WATCH DOG]

Le démon a bloqué une tentative de chargement d'objet malveillant

Il est possible qu'un démon puisse détecter et bloquer une tentative d'injection d'objet malveillant par le biais de l'une de ses routes.

Un message est remonté :

- le nombre total de ces tentatives que le démon a bloqué ce jour (*le compte commence à minuit*) ;
- pour chacune des tentatives (*maximum 3*) :
 - descriptif de l'objet que l'attaquant essaye de charger,
 - sa provenance de l'attaque, par exemple le nom de la route utilisée, et l'IP à la source de l'attaque,
 - sa date.

[WARNING] The synchronizer have some issues.

=> There were [1] security breaches blocked today (last 3):

- [hacker/attack] by [HTTP(s) call "/get_whole_configuration" by IP=127.0.0.1] at [2022-02-21 14:44:52]

Le démon est en cours d'arrêt

Lorsque le démon est en cours d'arrêt, le check le signale, et les informations relatives aux modules ne sont plus disponibles

[WARNING] The synchronizer is performing a shutdown.