

# Synchronizer - DB - Last Flush Time

## Sommaire

- Contexte
- Paramétrage
  - Données utilisées provenant du modèle
    - Données communes pour les checks du modèle
    - Données spécifiques pour ce check
    - Les données DFE ( Duplicate Foreach )
  - Données utilisées provenant du check
  - Données globales
- Résultat
  - Exemple
  - Interprétation
    - Statut
      - Les vérifications communes
      - Les vérifications spécifiques
    - Résultat
    - Résultat Long
    - Description des erreurs
      - Erreur d'un démon bloqué, qui doit être redémarré
      - Un démon spare n'est assigné sur aucun démon master
      - Problème de conflits d'Arbiters
      - Les serveurs ne sont pas à la même heure
      - Erreur de surcharge des disques de logs
      - Le démon a bloqué une tentative de chargement d'objet malveillant
      - Le démon est en cours d'arrêt
      - La dernière connexion de l'Arbiter remonte à trop longtemps
      - Le démon a chargé une configuration enregistrée
      - Erreur de vol de CPU
- Métriques

## Contexte

Le check **Synchronizer - DB - Last Flush Time** vérifie que le démon Synchronizer peut être correctement contacté sur le réseau.

Il donne également la version du démon ( *Résultat court* ), ainsi que les modules opérationnels ( *Résultat long* ).

Pour les versions de Shinken supérieures à la V02.07.00, la mise à jour de Mongo rend ce check non pertinent.

### Shinken < V02.07.00



Synchronizer - DB - Last Flush Time

[OK] - Last Flush Time: 255.00ms

### Shinken > V02.07.00

Statut	Nom de check	Résultat	Résultat Long
	Synchronizer - DB - Last Flush Time	[OK] Mongo 3 is not in MMapV1 mode but in wiredTiger (new format) or in a cluster mode. This indicator is not available.	-

## Paramétrage

Le check utilise la ligne de commande suivante :

```
$PLUGINS_DIR$/check_shinkendb.py -D -H "$HOSTADDRESS$" -P "$_HOSTDB_PORT$" --connection-method "$_HOSTDB_CONNECTION_METHOD$" --ssh-user "$_HOSTDB_SSH_USER$" --ssh-keyfile "$_HOSTDB_SSH_KEY$" --ssh-tunnel-timeout "$_HOSTDB_SSH_TUNNEL_TIMEOUT$" -A last_flush_time -W "$_HOSTDB_LAST_FLUSH_TIME_WARN$" -C "$_HOSTDB_LAST_FLUSH_TIME_CRIT$"
```

## Données utilisées provenant du modèle

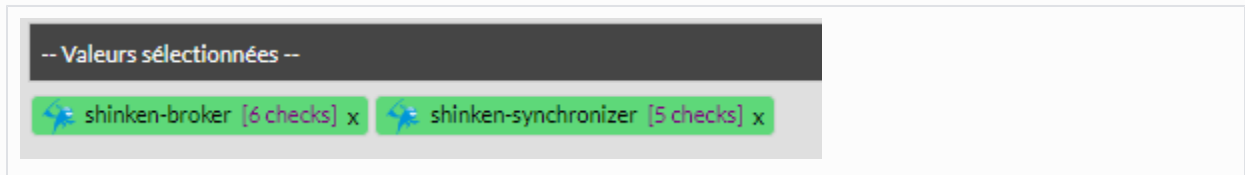
### Données communes pour les checks du modèle

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
DB_PORT	l'Hôte ( Onglet Données )	---	27017	<b>27017</b>	Configuration du port de communication avec la base de données.
DB_CONNECTION_METHOD	l'Hôte ( Onglet Données )	---	ssh	<b>ssh</b>	Méthode de connexion au serveur MongoDB  Valeur possible : <ul style="list-style-type: none"><li>• direct</li><li>• ssh</li></ul>
DB_SSH_USER	l'Hôte ( Onglet Données )	---	shinken	<b>shinken</b>	Utilisateur distant avec lequel se connecter au serveur hébergeant MongoDB.
DB_SSH_KEY	l'Hôte ( Onglet Données )	---	~/.ssh/id_rsa	<b>~/.ssh/id_rsa</b>	Clé SSH privée permettant la connexion au serveur hébergeant MongoDB.
DB_SSH_TUNNEL_TIMEOUT	l'Hôte ( Onglet Données )	seconde	5	<b>5</b>	Temps avant le déclenchement d'un timeout lors de la connexion ssh avec la base de données.
DB_USER_NAME	l'Hôte ( Onglet Données )	---	NONE	<b>NONE</b>	Nom de l'utilisateur à utiliser pour l'authentification avec mot de passe à la base MongoDB.  'NONE' est traitée comme une absence de valeur.  Utile uniquement si l'activation par mot de passe a été activé ( voir la page <a href="#">MongoDB - activation de l'authentification par mot de passe</a> ).
DB_USER_PASSWORD	l'Hôte ( Onglet Données )	---	NONE	<b>NONE</b>	Mot de passe de l'utilisateur utilisé pour l'authentification avec mot de passe à la base MongoDB.  'NONE' est traitée comme une absence de valeur.  Utile uniquement si l'activation par mot de passe a été activé ( voir la page <a href="#">MongoDB - activation de l'authentification par mot de passe</a> ).
DB_USE_SSL	l'Hôte ( Onglet Données )	---	false	<b>false</b>	Active le chiffrement SSL/TLS des échanges avec la base.
DB_SSL_CA_FILE	l'Hôte ( Onglet Données )	---	NONE	<b>NONE</b>	Chemin vers le fichier de l'autorité de certification ( CA ) utilisé pour vérifier le certificat SSL de MongoDB.  'NONE' est traitée comme une absence de valeur.
DB_SSL_PEM_KEY_FILE	l'Hôte ( Onglet Données )	---	NONE	<b>NONE</b>	Chemin vers le fichier contenant le certificat SSL du client.  'NONE' est traitée comme une absence de valeur.
DB_SSL_PEM_KEY_PASSWORD	l'Hôte ( Onglet Données )	---	NONE	<b>NONE</b>	Mot de passe du certificat SSL du client.  'NONE' est traitée comme une absence de valeur.

DB_SSL_CRL_FILE	l'Hôte ( Onglet Données )	---	NONE	<b>NONE</b>	Chemin vers le fichier CRL ( <i>liste de révocation</i> ) des certificats SSL à rejeter.  'NONE' est traitée comme une absence de valeur.
DB_SSL_ALLOW_INVALID_HOSTNAMES	l'Hôte ( Onglet Données )	---	false	<b>false</b>	Accepter le certificat SSL de MongoDB même si le nom d'hôte ne correspond pas à celui du serveur.
DB_SSL_ALLOW_INVALID_CERTIFICATES	l'Hôte ( Onglet Données )	---	false	<b>false</b>	Accepter le certificat SSL de MongoDB même s'il est invalide ( <i>par exemple, expiré</i> ).



Si la machine possède les bases de données du Broker et du Synchronizer, alors cela dépendra de l'ordre des modèles dans le champ "Modèles d'hôte hérités".



### Données spécifiques pour ce check

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
DB_LAST_FLUSH_TIME_CRIT	l'Hôte ( Onglet Données )	---	10000	<b>10000</b>	Seuil critique pour le temps de flush de la base de données ( <i>en millisecondes</i> ).
DB_LAST_FLUSH_TIME_WARN	l'Hôte ( Onglet Données )	---	8000	<b>8000</b>	Seuil avertissement pour le temps de flush de la base de données ( <i>en millisecondes</i> ).

### Les données DFE ( Duplicate Foreach )

Pas de données DFE pour ce check.

### Données utilisées provenant du check


Pas de données provenant du check pour ce check.

### Données globales

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
HOSTADDRESS	l'Hôte ( Onglet Général )	---	Nom de l'hôte	<b>Nom de l'hôte</b>	Adresse de l'hôte

## Résultat

### Exemple

Statut	Nom de check	Résultat	Résultat Long
	Synchronizer - DB - Last Flush Time	[OK] Mongo 3 is not in MMapV1 mode but in wiredTiger (new format) or in a cluster mode. This indicator is not available.	-

## Interprétation

### Statut

Il peut prendre deux valeurs **OK** / **CRITIQUE** / **ATTENTION** / **INCONNU**.

- Le statut va dépendre du retour de sonde et de la configuration spécifique du check pour les données suivantes :
  - `HOSTCHECK_SHINKEN_TIMEOUT`
  - `DB_LAST_FLUSH_TIME_CRIT`
  - `DB_LAST_FLUSH_TIME_WARN`
- Voici un tableau récapitulatif du statut attendu suivant le retour de sonde :

### Les vérifications communes

Situation	Statut
Démon bloqué et qui doit être redémarré	<b>CRITIQUE</b>
Démon spare non assigné sur un démon master	<b>CRITIQUE</b>
Problème de conflits d'Arbiters	<b>CRITIQUE</b>
Les serveurs ne sont pas à la même heure	<b>CRITIQUE</b>
Erreur de surcharge des disques de logs	<b>ATTENTION</b>
Démon qui bloque une tentative de chargement d'objet malveillant	<b>ATTENTION</b>
Démon est en cours d'arrêt	<b>ATTENTION</b>
Dernière connexion de l'Arbiter remonte à trop longtemps	<b>ATTENTION</b>
Le démon a chargé une configuration enregistrée, en attendant d'être contacté par l'Arbiter	<b>ATTENTION</b>

### Les vérifications spécifiques

Situation	Statut
Si la sonde n'a pas eu de réponse avant le temps maximum <ul style="list-style-type: none"><li>Si <b>supérieur</b> à <code>HOSTCHECK_SHINKEN_TIMEOUT</code> ( <i>par défaut : 3 sec</i> )</li></ul>	<b>INCONNU</b>
Le temps de connexion à la base de données : <ul style="list-style-type: none"><li>Si c'est <b>supérieur</b> à <code>DB_LAST_FLUSH_TIME_CRIT</code> ( <i>par défaut : 10000 ms</i> )</li></ul>	<b>CRITIQUE</b>
Le temps de connexion à la base de données : <ul style="list-style-type: none"><li>Si c'est <b>supérieur</b> à <code>DB_LAST_FLUSH_TIME_WARN</code> ( <i>par défaut : 8000 ms</i> )</li></ul>	<b>ATTENTION</b>

### Résultat

Renvoi au format texte :

- Le temps nécessaire pour réaliser un flush sur la base de données.

### Résultat Long

Pas de données spécifiques pour ce check.

## Description des erreurs

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 au 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 ]

Un démon spare n'est assigné sur aucun démon master

**Un spare n'est pas assigné à un démon master :**

Lorsqu'un démon Broker spare n'est assigné par aucun démon master, il est inutile, et remonte en erreur dans le check, tout comme dans la commande shinken-healthcheck, afin qu'il soit rapidement identifié et corrigé.

**SPARE [CRITICAL]**

No master is using this spare daemon → **UNUSED**

Problème de conflits d'Arbiters

### • Conflits d'Arbiters :

Si le démon est contacté par des Arbiters qui ne sont pas sur la même architecture ( *par exemple un Arbitre de Production et un autre de l'environnement de Testing* ), le check sera mis en **CRITICAL** .

=> **Arbiters CONFLICT**

Architecture List :

#### 1. Production [ **shinken** ]

- arbiter-master : last connection 11s ago. Defined on the server with uuid d2a358b0-cae3-4ce8-bc3f-edd241627bac (/var/lib/shinken/server.uuid)

#### 2. Testing [ **shinken** ]

- arbiter-master : last connection 12s ago. Defined on the server with uuid 785e0227-455a-449d-b8f1-516897000e3b (/var/lib/shinken/server.uuid)

### • Conflit d'Arbiters qui ont le même nom d'Architecture :

Comme dans le cas précédent, le démon est contacté par des Arbiters d'architectures différentes, mais qui ont le même nom. On sort également en **CRITICAL** mais en avertissant que les noms sont identiques, et en indiquant où changer le nom des architectures.

=> **Arbiters CONFLICT**

Architecture List :

1. Production [XXXXXXXXXX]

- o arbiter-master : last connection 33s ago. Defined on the server with uuid d2a358b0-cae3-4ce8-bc3f-edd241627bac (/var/lib/shinken/server.uuid)

2. Production [XXXXXXXXXX]

- o arbiter-master : last connection 10s ago. Defined on the server with uuid 785e0227-455a-449d-b8f1-516897000e3b (/var/lib/shinken/server.uuid)

NOTE:

*Some architecture have the same name. We advise you to change it in the configuration of their architecture\_export module.*

Les serveurs ne sont pas à la même heure

Si le serveur n'est pas à la même heure que le serveur Arbitre ( *qui fait office de référence* ), une erreur **CRITICAL** sera levée, car des temps différents sur les différents serveurs va avoir des effets **désastreux** sur la cohérence des données de supervision.

=> Arbiters connection:

• Architecture Production:

- o **ERROR** arbiter-master => server times are different, time shift of 1 days 16h

Erreur de surcharge des disques de logs

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

**[WARNING]** The daemon 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/"

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

[WARNING] The daemon have some issues:

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

- [ hacker/attack ] by [ HTTP(s) call "Configuration reception from an Arbiter server" by IP=127.0.0.1 ] at [ 2022-02-21 14:44:39 ]

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 broker is performing a shutdown.

La dernière connexion de l'Arbiter remonte à trop longtemps

Si la dernière connexion de l'Arbiter remonte à trop de temps, le démon va lever un **WARNING** . Ceci peut être dû :

- Les Arbiters MASTER et SPARE sont réellement éteints
- Les Arbiters MASTER et SPARE sont en train d'envoyer des configurations à d'autres démons, et ne peuvent donc pas contacter ce démon pour l'instant.

=> Arbiters connection :

- Architecture *Production* :
  - arbiter-master => Missed connection from arbiter since 1 days 6h ( > daemon check\_interval \* max\_check\_attempts )



Le temps pris en compte comme limite de dernière connexion est de  $check\_interval * max\_check\_attempts$  du démon ( *définis dans sa configuration* ).

Les valeurs par défauts sont de  $60s * 3$ , soit 3 minutes.

Le démon a chargé une configuration enregistrée

Lorsque le module *last-configuration-recorder* est actif, pour les démons de type

- Broker,
- Poller,
- Reactionner,
- Receiver et
- Scheduler,

Au démarrage, le démon charge la précédente configuration qu'il a reçue de l'Arbiter, en attendant que ce dernier le contacte.

- Il permet un redémarrage du démon **même si l'Arbiter ne peut pas joindre le démon** ( *ex : coupure réseau* ),
- Cela permet aussi de rendre le **redémarrage du démon plus rapide**, dans le cas où l'Arbiter **n'a pas changé de version** de configuration.

Un **WARNING** indique que le démon n'a pas encore été contacté par l'Arbiter.

Arbiters connection:

Architecture List :

1. Shinken-Production [loaded from retention]

- **WARNING** arbiter-master : loaded from retention 52s ago [waiting for Arbiter connection].

Erreur de vol de CPU

Seulement si la machine virtuelle est hébergée sur un hyperviseur VMWare

- 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 ).
  - on peut avoir plus d'informations sur cet indicateur et comment réduire la perte 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

## Métriques

Pas de métriques pour ce check