shinken-receiver (Modèle d'hôte)

Sommaire

Contexte

Le modèle shinken-receiver vous permet de superviser un hôte hébergeant le démon Receiver (*voir la page* Le Receiver).

Receiver

Modèle d'hôte correspondant: ***shinken-receiver*** *(notez que ce modèle hérite du modèle* ***shinken*** *et* ***shinkean-deamon*** *)*

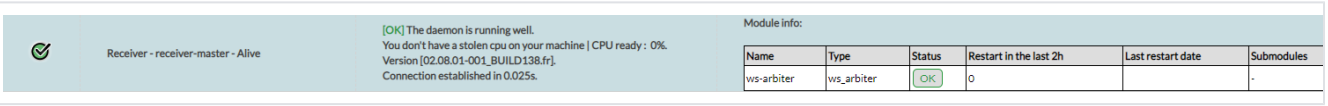
Afin de superviser le démon Receiver, le modèle ***shinken-receiver*** appliqué à votre hôte, attachera plusieurs checks qui vérifieront la santé et la performance de ce démon.

Checks

- **Receiver - KEY - Alive**

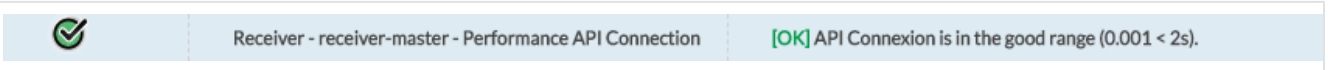
  Vérifie que le démon Receiver peut être correctement contacté sur le réseau (Résultat court) et que les modules sont opérationnels (Résult at long).

  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.



- **Receiver - KEY - Performance API Connection**

  Vérifie la latence de connexion au Receiver et ses performances



Paramètres du check

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

Les données suivantes sont disponibles pour le Receiver:

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 Receiver	http	shinken
CHECK_SHINKEN_TIMEOUT	Timeout utilisé pour établir la connexion avec le Receiver	3	shinken
RECEIVER_PORT	Port utilisé pour établir la connexion avec le Receiver	7773	Locale
RECEIVER_LIST	Liste de Receiver (Multi-démon)	receiver-master$($_HOSTRECEIVER_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))
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

Détail des commandes

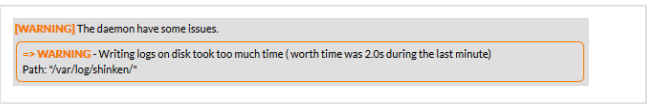
Nom du check	Commande du check	Ligne de commande
Receiver - KEY - Alive	check_shinken_receiver!**alive!$VALUE1$**	$PLUGINSDIR$/check_shinken -H "$HOSTADDRESS$" -p "$ARG2$" --shinkenversion "$SHINKENVERSION$" -t receiver -m $ARG1$ --timeout $_HOSTCHECK_SHINKEN_TIMEOUT$ -w $_HOSTTHRESHOLD_CPU_STOLEN_WARNING$ -c $_HOSTTHRESHOLD_CPU_STOLEN_CRITICAL$
Receiver - KEY - Performance API Connection	check_shinken_receiver!**api_connection!$VALUE1$**	$PLUGINSDIR$/check_shinken -H "$HOSTADDRESS$" -p "$ARG2$" --shinkenversion "$SHINKENVERSION$" -t receiver -m $ARG1$ --timeout $_HOSTCHECK_SHINKEN_TIMEOUT$ -w $_HOSTTHRESHOLD_CPU_STOLEN_WARNING$ -c $_HOSTTHRESHOLD_CPU_STOLEN_CRITICAL$

Description des erreurs de Receiver - 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.



Problème de conflits d'Arbiters

- **Conflit d'Arbiters** :

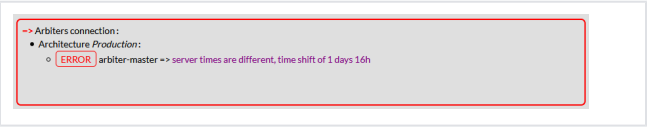
  Si le démon est contacté par des Arbiters qui ne sont pas sur la même architecture (*par exemple un Arbiter de Production, et un autre de l'environnement de Testing*), le check sera mis en **CRITICAL** .

- **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 de vos architectures.

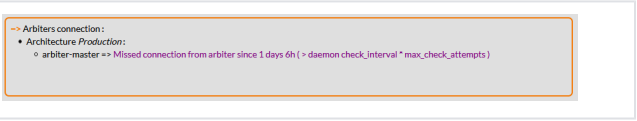
Les serveurs ne sont pas à la même heure

- Si le serveur n'est pas à la même heure que le serveur Arbiter (*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 cohérences des données de supervision.



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 peux être dû:
  - les Arbiters MASTER et SPARE sont réellement éteints.
  - les Arbiter 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.

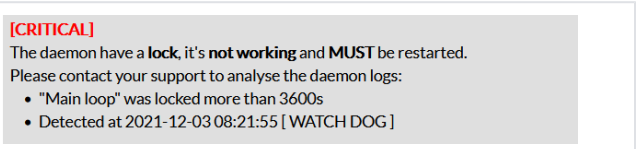


Le temps pris en compte comme limite de dernière connexion est de *check_interval * max_check_attempts* du démon (*définis dans sa configuration*).

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

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

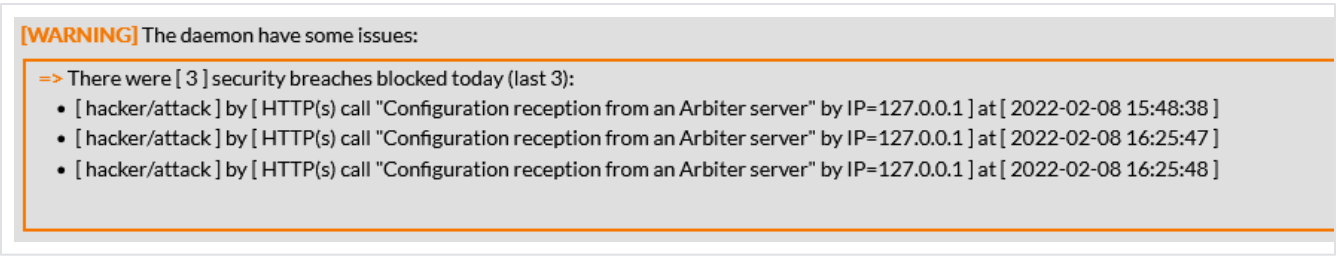


Le démon a bloqué une tentative de chargement d'objet malveillant

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.

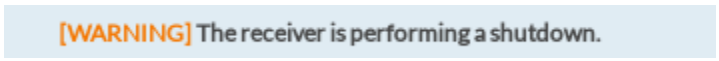
Un message est remonté :

- 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.



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

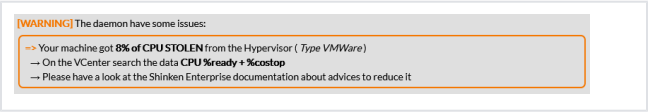


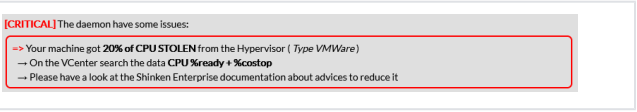
Description des erreurs de Receiver - KEY - Performance

Erreur de vol de CPU

Seulement si votre machine virtuelle est hébergé sur un hyperviseur VMWare

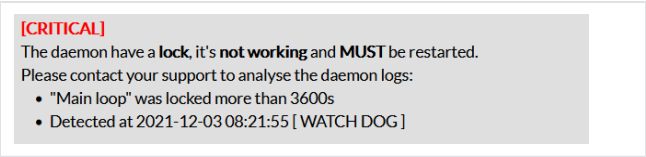
- Si la VM se fait voler trop de temps de calcul (*CPU Stolen*), le check sera mis en **WARNING** ou en **CRITIQUE** (*en fonction du taux de vol fixé par défaut ou indiqué par l'utilisateur*).
  - Vous pouvez avoir plus d'information sur cet indicateur et comment réduire la parte de temps de la VM sur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





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

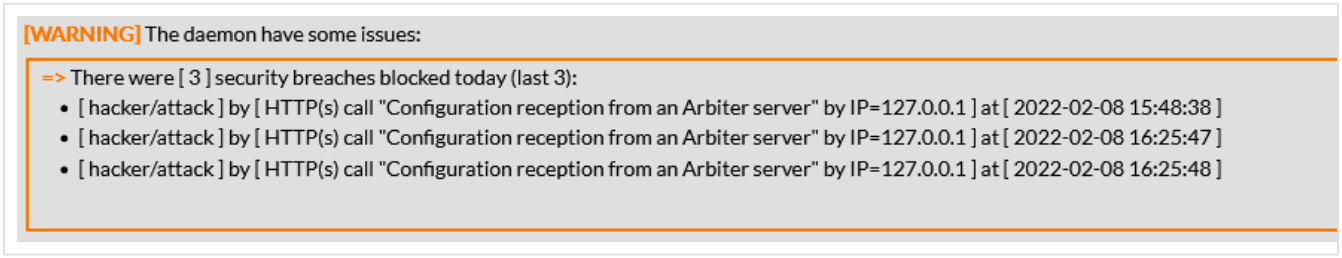


Le démon a bloqué une tentative de chargement d'objet malveillant

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.



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