shinken-arbiter (Modèle d'hôte)

Sommaire

Contexte

Le modèle shinken-arbiter vous permet de superviser un hôte hébergeant le démon Arbiter (*voir la page* L'Arbiter).

Description du modèle

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

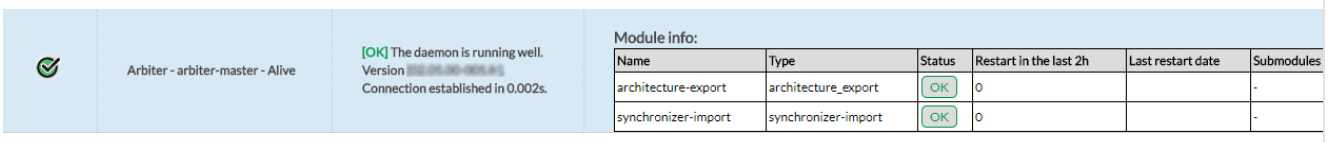
Afin de superviser le démon Arbiter, le modèle ***shinken-arbiter*** appliqué à votre hôte, attachera deux checks qui vérifieront la santé et la performance de ce démon.

Les checks

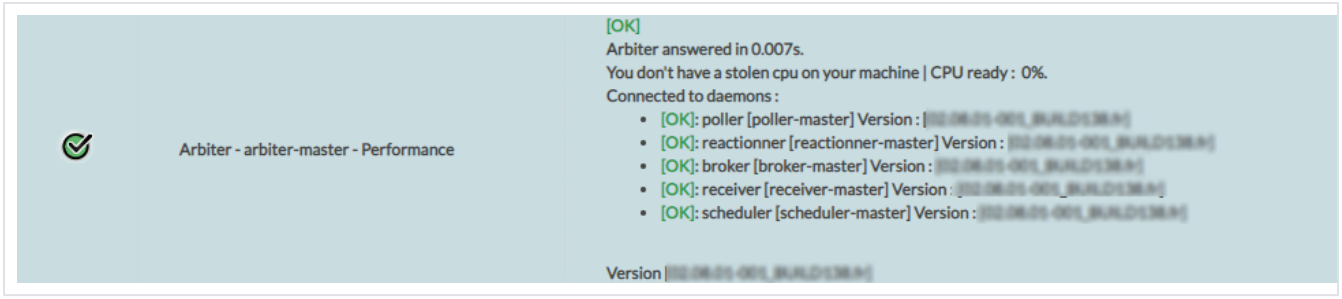
Nom du Check	Description
Arbiter - KEY - Alive	Vérifie que le démon Arbiter peut être correctement contacté sur le réseau ; la version du démon est affichée également (*Résultat court*) et que les modules sont opérationnels (*Résultat long*).
Arbiter - KEY - Performance	Retourne le temps de connexion au démon Arbiter ainsi que la liste des connexions avec les autres démons de l'architecture avec leurs numéros de version (*si possible*). Si certains démons ne sont pas à jours, alors un Warning sera remonté. Si jamais le démon Arbiter est en exécution sur une machine virtuelle supervisée par VMware, alors le pourcentage de temps de vol de CPU (*CPU Ready*) sera affiché.

Exemple de résultat

Arbiter - KEY - Alive



Arbiter - KEY - Performance



Paramétrage des Checks

Les checks de l'Arbiter peuvent être configurés via des données fournies par le modèle.

Les données suivantes sont disponibles:

Nom de la donnée	Description	Valeur par défaut	Hérité du modèle d'hôte ou locale
SHINKEN_PROTOCOL	Protocole utilisé pour établir la connexion avec l'Arbiter	http	shinken
ARBITER_PORT	Port utilisé pour l'établissement de la connexion avec l'Arbiter	7770	Locale
CHECK_SHINKEN_TIMEOUT	Timeout utilisé pour l'établissement de la connexion avec l'Arbiter	3	shinken
ARBITER_LIST	Liste d'Arbiter (*Multi-démon*)	arbiter-master$($_HOSTARBITER_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

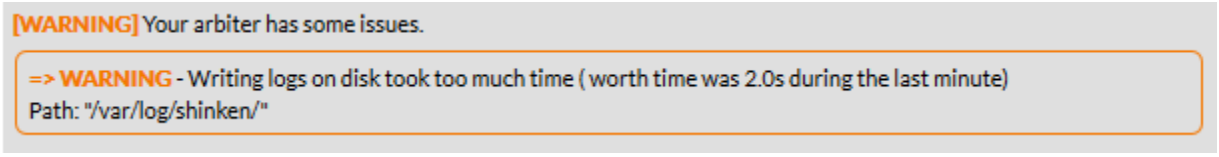
Détail des commandes

Nom du check	Commande du check	Ligne de commande
Arbiter - KEY - Alive	check_shinken_arbiter!**alive!$VALUE1$**	$PLUGINSDIR$/check_shinken -H "$HOSTADDRESS$" -p "$ARG2$" --shinkenversion "$SHINKENVERSION$" -t arbiter -m $ARG1$ --timeout $_HOSTCHECK_SHINKEN_TIMEOUT$ -w $_HOSTTHRESHOLD_CPU_STOLEN_WARNING$ -c $_HOSTTHRESHOLD_CPU_STOLEN_CRITICAL$
Arbiter - KEY - Performance	check_shinken_arbiter!**stats!$VALUE1$**	$PLUGINSDIR$/check_shinken -H "$HOSTADDRESS$" -p "$ARG2$" --shinkenversion "$SHINKENVERSION$" -t arbiter -m $ARG1$ --timeout $_HOSTCHECK_SHINKEN_TIMEOUT$ -w $_HOSTTHRESHOLD_CPU_STOLEN_WARNING$ -c $_HOSTTHRESHOLD_CPU_STOLEN_CRITICAL$

Description des erreurs de Arbiter - KEY - Alive

Erreur de surcharge des disques de logs

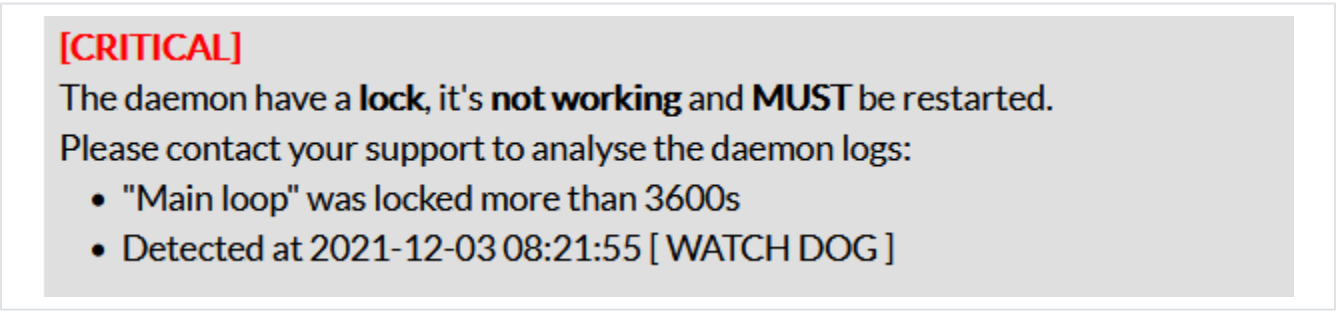
- En cas de disques trop lent sur le volume des logs, le check sera mis en **WARNING** avec l'erreur suivante.



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

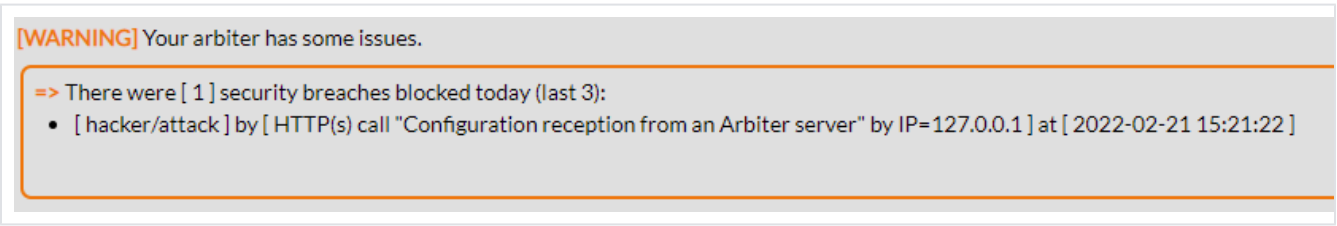


Le démon a bloqué une tentative de chargement d'objet malveillant

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.

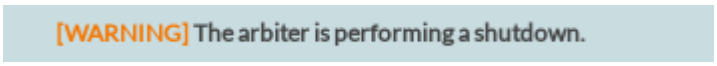
Un message est remonté :

- 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

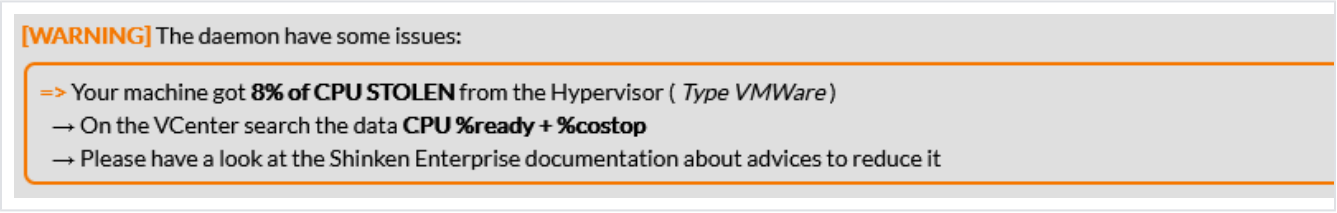
Lorsque le démon est en cours d'arrêt, le check le signale, et les informations relatives aux modules ne sont plus disponibles

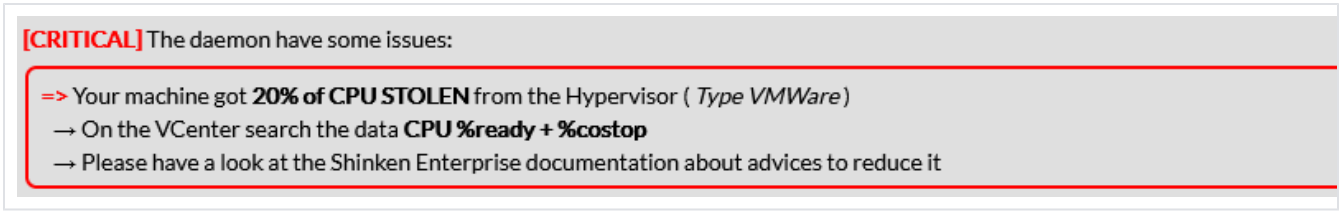


Description des erreurs de Arbiter - KEY - Performance

Erreur de 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 parte de temps de la VM sur la page Machine VMWare avec un fort taux de CPU Stolen (%ready + %costop)



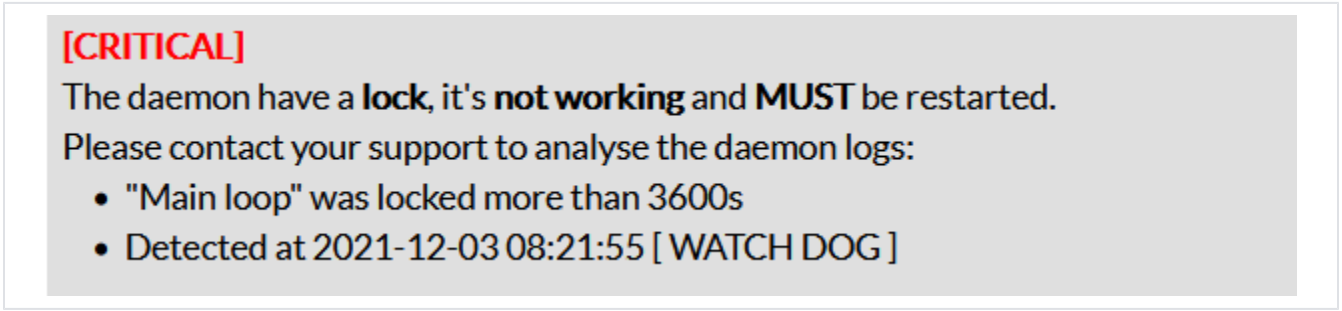


Les serveurs ne sont pas à la même heure

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.

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

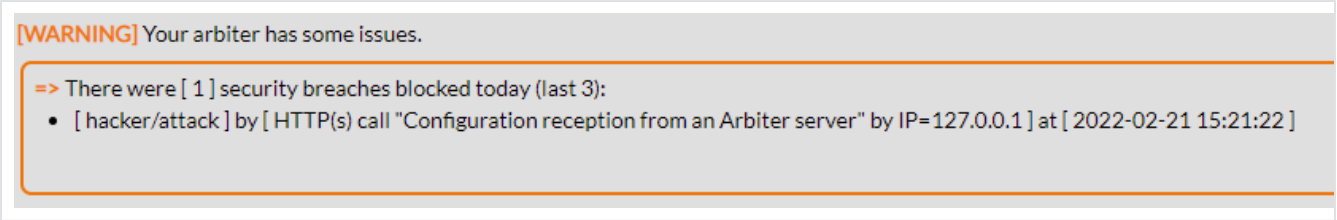


Le démon a bloqué une tentative de chargement d'objet malveillant

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