

Receiver - \$KEY\$ - Performance

Sommaire

- Contexte
- Paramétrage
 - Données utilisées provenant du modèle
 - Données communes pour les checks du modèle
 - Provenant du modèle shinken
 - Provenant du modèle shinken-daemon
 - Provenant du modèle shinken-receiver
 - Données spécifiques pour ce check
 - Les données DFE (Duplicate Foreach)
 - Données utilisées provenant du check
 - Données globales
 - Propriétés de l'hôte
- Résultat
 - Exemple
 - Interprétation
 - Statut
 - Résultat
 - Résultat Long
 - Description des erreurs
 - 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
- Métriques

Contexte

Le check **Receiver - \$KEY\$ - Performance API Connection** vérifie la latence de connexion au Receiver et ses performances

Statut	Nom de check	Résultat	Résultat Long
	Receiver - receiver-master - Performance API Connection	OK API Connection is in the good range (0.001 < 2s).	-

Paramétrage

Le check utilise la ligne de commande suivante :

```
$PLUGINSDIR$/check_shinken -H "$HOSTADDRESS$" -p "$ARG2$" --shinkenversion "$SHINKENVERSION$" -t arbiter -m $ARG1$ --timeout "$_HOSTCHECK_SHINKEN_TIMEOUT$" -w "$_HOSTTHRESHOLD_CPU_STOLEN_WARNINGS$" -c "$_HOSTTHRESHOLD_CPU_STOLEN_CRITICAL$"
```

Données utilisées provenant du modèle

Données communes pour les checks du modèle

Provenant du modèle shinken

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
CHECK_SHINKEN_TIMEOUT	l'Hôte (Onglet Données)	seconde	3	3	Temps maximum durant lequel le check va attendre une réponse du démon.

Provenant du modèle shinken-daemon

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
THRESHOLD_CPU_STOLEN_CRITICAL	l'Hôte (Onglet Données)	%	10	10	Seuil de CPU volé sur une machine virtuelle supervisée par VMware avant de déclencher un critique.
THRESHOLD_CPU_STOLEN_WARNING	l'Hôte (Onglet Données)	%	5	5	Seuil de CPU volé sur une machine virtuelle supervisée par VMware avant de déclencher un warning.

Provenant du modèle shinken-receiver

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
RECEIVER_PORT	l'Hôte (Onglet Données)	---	7773	7773	Configuration du port de communication avec le Receiver.

Données spécifiques pour ce check

Pas de données spécifiques pour ce check.

Les données DFE (Duplicate Foreach)

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
RECEIVER_LIST	l'Hôte (Onglet Données)	---	receiver-master\$(\$_HOSTRECEIVER_PORT\$)\$	receiver-master\$(\$_HOSTRECEIVER_PORT\$)\$	Liste de Receivers (Multi-démon) Check(s) impacté(s) : - Receiver - \$KEY\$ - Alive - Receiver - \$KEY\$ - Performance

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
PLUGINS_DIR	Non modifiable (Sauf Admin Shinken)	---	/var/lib/shinken/libexec	/var/lib/shinken/libexec	Chemin absolu du dossier contenant la sonde (non modifiable).

SHINKENVERSION	Non modifiable	---	---	---	Numéro de version du shinken utilisé pour la comparaison avec le shinken surveillé.
----------------	----------------	-----	-----	-----	---

Propriétés de l'hôte

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

Résultat

Exemple

Statut	Nom de check	Résultat	Résultat Long
	Receiver - receiver-master - Performance API Connection	[OK] API Connection is in the good range (0.001 < 2s).	-

Interprétation

Statut

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

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

Situation	Statut
Si un démon est bloqué et doit être redémarré	CRITIQUE
Si le démon a bloqué une tentative de chargement d'objet malveillant	ATTENTION
Si le démon est en cours d'arrêt	ATTENTION
Si la sonde n'a pas eu de réponse avant le temps maximum Si supérieur à CHECK_SHINKEN_TIMEOUT (<i>par défaut : 3 sec</i>)	INCONNU

Résultat

Renvoi au format texte le temps de réponses du démon.

Résultat Long

Pas de résultat long 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]

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 daemon have some issues:

=> There were [3] 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 [2022-02-08 15:48:38]
- [hacker/attack] by [HTTP(s) call "Configuration reception from an Arbiter server" by IP=127.0.0.1] at [2022-02-08 16:25:47]
- [hacker/attack] by [HTTP(s) call "Configuration reception from an Arbiter server" by IP=127.0.0.1] at [2022-02-08 16:25:48]

Le démon est en cours d'arrêt

[WARNING] The receiver is performing a shutdown.

Métriques

Nom	Unité	Description
get_lock_time	seconde	Temps de connexion et d'obtention d'un appel bloquant dans le démon et ainsi voir si les appels bloquants ne sont pas trop long.