

Poller - \$KEY\$ - Running Well

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-poller
 - Données spécifiques pour ce check
 - Les données DFE (Duplicate Foreach)
 - Données utilisées provenant du check
 - Données globales
- Résultat
 - Exemple
 - Exemple d'un état de santé dégradé du Poller
 - 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

Vérifie que le démon Poller peut être correctement contacté sur le réseau et affiche son numéro de version.

Affiche également le nombre d'éléments qu'il gère dans un tableau, en distinguant les hôtes, les Clusters et les Checks et le Total des éléments. (*Résultat court*)

Présente la liste des démons auxquels le Scheduler doit se connecter, et l'état des connexions (*Résultat long*).

Donne un état des modules chargés (*Résultat long*).

| Statut | Nom de check | Résultat | Résultat Long |
|---|---|--|---------------|
|  | Poller - poller-lab-validationsw1-France - Running Well | <p>[OK] Your poller is running well.</p> <p>Poller</p> <ul style="list-style-type: none">tags: None <p>The latency between the poller and the schedulers are</p> <ul style="list-style-type: none"><code>scheduler-lab-validationsw1-France [lab-validationsw1:9769]: 0.58ms</code><code>scheduler-spare-France-2 [localhost:9769]: 1.14ms</code><code>scheduler-spare-lab-validationsw1-France [lab-validationsw1:9768]: 1.02ms</code> <p>Version [<code>poller-2.10.0-00000000000000000000000000000000</code>]</p> <p>Connection established in 0.016s.</p> | |

Paramétrage

Le check utilise la ligne de commande suivante :

```

$PLUGINDIR$/check_shinken -H "$HOSTADDRESS$" -p "$ARG2$" --shinkenversion "$SHINKENVERSION$" -t scheduler -
m $ARG1$ -l "lck-$LASTSERVICECHECK$" --passive_poller_latency "$_HOSTPASSIVE_POLLER_LATENCY$" --timeout
"$_HOSTCHECK_SHINKEN_TIMEOUT$" -w "$_HOSTTHRESHOLD_CPU_STOLEN_WARNING$" -c
"$_HOSTTHRESHOLD_CPU_STOLEN_CRITICAL$" --scheduler_too_old_retention_save_margin
"$_HOSTSCHEDULER__RETENTION__RENTENTION-IS-TOO-OLD-AFTER_X_MINUTES$"

```

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-poller**

| Nom | Modifiable sur | Unité | Défaut | Valeur par défaut à l'installation de Shinken | Description |
|-------------------------------|------------------------------|-------|--------|---|---|
| POLLER_PORT | l'Hôte (Onglet Données) | --- | 0 | 7771 | Port utilisé pour établir la connexion avec le Poller. |
| NB_CHECK_IN_TIMEOUT_TO LERATE | l'Hôte (Onglet Données) | --- | 0 | 0 | Nombre de checks en timeout provoquant une sortie en erreur du check. |

| | | | | | |
|-------------------------------------|------------------------------|---------|---------------------------------------|--|---|
| POLLER_NB_CHECK_IN_TIMEOUT_TOLERATE | l'Hôte (Onglet Données) | --- | \$_HOSTNB_CHECK_IN_TIMEOUT_TOLERATE\$ | \$_HOSTNB_CHECK_IN_TIMEOUT_TOLERATE\$ | Nombre de checks en timeout provoquant une sortie en erreur du check. |
| ACTIVE_POLLER_LATENCY | l'Hôte (Onglet Données) | seconde | 0.5 | 0.5 | Latence de connexion au-delà de laquelle le check sort en erreur. |

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 |
|-------------|------------------------------|-------|--|---|---|
| POLLER_LIST | l'Hôte (Onglet Données) | --- | poller-master\$(\$_HOSTPOLLER_PORTS)\$ | poller-master\$(\$_HOSTPOLLER_PORTS)\$ | Liste de Pollers. Check(s) impacté(s) : <ul style="list-style-type: none"> • Poller - \$KEY\$ - Running Well • Poller - \$KEY\$ - Performance <p>Note : Cette valeur remplacera dans la commande la valeur \$ARG2\$</p> |

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 | Nom de l'hôte | Adresse de l'hôte |

Résultat

Exemple

| Statut | Nom de check | Résultat | Résultat Long |
|---|---|--|---------------|
|  | Poller - poller-lab-validationsw1-France - Running Well | <p>[OK] Your poller is running well.</p> <p>Poller</p> <ul style="list-style-type: none"> • tags : None <p>The latency between the poller and the schedulers are</p> <ul style="list-style-type: none"> • scheduler-lab-validationsw1-France [lab-validationsw1:9769] : 0.58ms • scheduler-spare-France-2 [localhost:9769] : 1.14ms • scheduler-spare-lab-validationsw1-France [lab-validationsw1:9768] : 1.02ms <p>Version [1.10.0] [1.10.0]</p> <p>Connection established in 0.016s.</p> | - |

Exemple d'un état de santé dégradé du Poller

Lorsque le Poller rencontre des problèmes qui peuvent signifier un fonctionnement dégradé, ces problèmes sont également remontés dans le résultat du check "Poller - Running Well".

Lorsque certains checks ont un temps d'exécution supérieur aux différents seuils définis, ils sont répertoriés dans le résultat du check "Poller - Running Well" pour permettre d'avertir des potentielles erreurs sur ces checks ou du Poller.

Dans l'exemple, le check signale que 10 checks ont pris plus que 10 secondes pour s'exécuter pendant les 20 dernières minutes, et ont leur exécution a donc été arrêtée de force.

[WARNING] You have 10 (> 0 tolerate) check(s) that timed out in the last 20m 0s.

The last actions that timed out :

| Nb | Last | Host | Check | Timeout |
|----|----------|----------|----------|---------|
| 1 | 16:49:59 | LAB-VM23 | sleep 7 | 10s |
| 1 | 16:49:58 | LAB-VM23 | sleep 6 | 10s |
| 1 | 16:49:58 | LAB-VM23 | sleep 2 | 10s |
| 1 | 16:49:58 | LAB-VM23 | sleep 10 | 10s |
| 1 | 16:49:58 | LAB-VM23 | sleep 5 | 10s |

Poller [ACTIVE]
 • tags : None

La durée de temps (en secondes) durant laquelle les checks sont conservés dans l'ensemble des checks en timeout est configurable dans le fichier de configuration du Poller concerné.

Il est également possible de définir un seuil de tolérance afin d'afficher un avertissement seulement lorsqu'il y a plus qu'un certain nombre de checks en timeout. Pour cela, il faut modifier la donnée NB_CHECK_IN_TIMEOUT_TOLERATE dans l'hôte concerné dans la configuration.

```

/etc/shinken/pollers/mon_poller.cfg

define poller {
    ...
    keep_timeout_time    1200
    ...
}
```

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 :
 - THRESHOLD_CPU_STOLEN_CRITICAL
 - THRESHOLD_CPU_STOLEN_WARNING
 - SCHEDULER__RETENTION__RENTENTION-IS-TOO-OLD-AFTER_X_MINUTES
 - CHECK_SHINKEN_TIMEOUT
- Voici un tableau récapitulatif du statut attendu suivant le retour de sonde :

Les vérifications communes

| Situation | Statut |
|--|------------------|
| Démon bloqué et qui doit être redémarré | CRITIQUE |
| Démon spare non assigné sur un démon master | CRITIQUE |
| Problème de conflits d'Arbiters | CRITIQUE |
| Les serveurs ne sont pas à la même heure | CRITIQUE |
| Erreur de surcharge des disques de logs | ATTENTION |
| Démon qui bloque une tentative de chargement d'objet malveillant | ATTENTION |

| | |
|---|------------------|
| Démon est en cours d'arrêt | ATTENTION |
| Dernière connexion de l'Arbiter remonte à trop longtemps | ATTENTION |
| Le démon a chargé une configuration enregistrée, en attendant d'être contacté par l'Arbiter | ATTENTION |

Les vérifications spécifiques

| Situation | Statut |
|--|------------------|
| Le temps de connexion à la base de données : <ul style="list-style-type: none"> • Si c'est supérieur à THRESHOLD_CPU_STOLEN_CRITICAL (<i>par défaut : 10%</i>) | CRITIQUE |
| Le temps de connexion à la base de données : <ul style="list-style-type: none"> • Si c'est supérieur à THRESHOLD_CPU_STOLEN_WARNING (<i>par défaut : 5%</i>) | ATTENTION |
| Le temps de connexion à la base de données : <ul style="list-style-type: none"> • Si c'est supérieur à SCHEDULER_RETENTION_RENTENTION-IS-TOO-OLD-AFTER_X_MINUTES (<i>par défaut : 5%</i>) | ATTENTION |
| Si la sonde n'a pas eu de réponse avant le temps maximum <ul style="list-style-type: none"> • Si supérieur à CHECK_SHINKEN_TIMEOUT (<i>par défaut : 3 sec</i>) | INCONNU |

Résultat

Renvoi au format texte :

- Une mention qui indique si le Poller est actif ou passif. Dans l'exemple, on a affaire à un Poller actif.
- La liste des tags du Poller. Dans l'exemple, aucun tag n'est défini sur le Poller.
- La latence de connexion avec le ou les Schedulers du royaume et des sous-royaumes

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]

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 Arbiter de Production et un autre de l'environnement de Testing*), le check sera mis en **CRITICAL** .

=> **Arbiters CONFLICT**

Architecture List :

1. Production [**100** arbiters]

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

2. Testing [**100** arbiters]

- 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 [**100** arbiters]

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

2. Production [**100** arbiters]

- 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 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 cohérence des données de supervision.

=> Arbiters connection :

- Architecture *Production*:

- **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*) :
 - 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 [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

| Nom | Unité | Description |
|---------------------|-------|---|
| nb_check_in_timeout | --- | Nombre de checks qui sont entrés en timeout sur le Poller pendant les 20 dernières minutes. Cette durée est configurable dans le fichier de configuration du Poller, avec l'option <i>keep_timeout_time</i> (<i>par défaut 1200s</i>) |

