Fichiers Logs

Sommaire

Emplacement et organisation des fichiers de logs

Les fichiers de logs des démons Shinken sont placés dans **/var/log/shinken**.

Chaque instance de démon Shinken possède dans ce dossier son fichier de log.

Par défaut, les démons présents dans l'installation Shinken possèdent les fichiers de logs suivants :

- arbiterd.log
- schedulerd.log
- receiverd.log
- reactionnerd.log
- pollerd.log
- brokerd.log
- synchronizerd.log
- gathererd.log

Lorsque d'autres démons sont ajoutés sur la même machine, les fichiers de logs sont nommés de la façon suivante :

```
<TYPE_DEMON>d-<ID_DEMON>.log
```

Par exemple, un scheduler supplémentaire avec l'id 1 aura le fichier de log suivant :

- /var/log/shinken/schedulerd-1.log

Logs de debug

Les démons Shinken peuvent être démarrés en mode debug pour avoir des logs plus verbeux.

Plusieurs commandes permettent de redémarrer les démons en mode debug :

- Redémarrer tous les démons en mode debug (*option -d*)

```
service-shinken -d restart
```

- Redémarrer tous les démons d'un type en mode debug.

```
service-shinken-<type_demon> -d restart
```

"<type_demon>" correspond au type du démon à redémarrer, et est une valeur parmi les suivantes :

    - arbiter
    - scheduler
    - poller
    - broker
    - reactionner
    - receiver
    - synchronizer.

      Par exemple, pour un Scheduler, la commande est la suivante:

```
service-shinken-scheduler -d restart
```

- Redémarrer une seule instance de démon en mode debug.

```
service-shinken-<type_demon> -d --id <id_demon> restart
```

L'id du démon peut être trouvée à l'aide de la commande shinken-daemons-list (*voir la page* Lister/Activer/Désactiver des démons).

Un démon démarré en mode debug envoie ses logs dans un fichier différent, placé dans **/var/log/shinken** et est nommé :

```
<type_demon>d-<id_demon>.debug.log
```

Pour un scheduler avec l'id 2, le fichier de log en mode debug correspondant est le suivant :

```
/var/log/shinken/schedulerd-2.debug.log
```

Réglage du niveau de log par défaut

Dans les fichiers de logs Shinken, chaque entrée possède une des 4 priorités suivantes :

- DEBUG
- INFO
- WARNING
- CRITICAL

A l'installation, ou lorsqu'un nouveau démon est créé, le niveau de log par défaut est INFO.

Ce niveau de log par défaut peut être modifié dans le fichier .ini du démon concerné, via le paramètre **log_level** :

```
# accepted log level values= DEBUG,INFO,WARNING,ERROR,CRITICAL
log_level=INFO
```

Chaque instance de démon possède un fichier .ini placé dans /etc/shinken/daemons. Ce fichier est nommé selon le type de démon et son id:

```
<type_demon>d-<id_demon>.ini
```

Comme pour les fichiers de logs, les démons préinstallés n'ont pas l'id dans le nom du fichier .ini (*pour rester compatible avec les anciennes versions*). Les fichiers .ini par défaut sont donc les suivants :

- pollerd.ini
- brokerd.ini
- schedulerd.ini
- reactionnerd.ini
- receiverd.ini

Le Synchronizer et l'Arbiter sont des démons centraux avec des rôles particuliers par rapport aux autres démons. Ils ont pour particularité d'avoir des fichiers .ini différents des autres démons :

- **Arbiter**: /etc/shinken/shinken.cfg
- **Synchronizer**: /etc/shinken/synchronizer.cfg

Si le paramètre log_level n'est pas présent dans ces fichiers, il faudra l'ajouter dans les fichiers de surcharge :

- **Arbiter**: /etc/shinken-user/configuration/daemons/arbiters/arbiter_cfg_overload.cfg
- **Synchronizer**: /etc/shinken-user/configuration/daemons/synchronizers/synchronizer_cfg_overload.cfg

Les logs de supervision sont agrégés

Shinken Entreprise peut agréger dans un fichier, les logs contenant seulement les données utiles à la supervision (*alertes de résultats de checks par exemple*). Ce fichier est utile notamment pour les outils externes qui se basent sur les logs de Shinken.

- C'est le module simple-log qui le permet (*voir la page* Module Simple-log).
  - Si le module n'est pas activé, l'agrégation n'aura pas lieu.
  - Il y aura autant de fichiers que de Broker avec le module simple-log.
  - Le module agrégera les logs de son royaume et de tous ses sous-royaumes.
- Ce fichier se situe:
  - par défaut **/var/log/shinken/nagios-export.log**
  - Il ne contient donc pas pas les avertissements et autres messages propres à Shinken.

```
[1622423203] CRITICAL: [scheduler-master] HOST ALERT: Realm FRANCE - Schedulers;UP;HARD;1;OK, worst of [10
OK] states
[1622423205] CRITICAL: [scheduler-master] HOST ALERT: Daemons - FRANCE;UP;HARD;1;OK, worst of [5 OK] states
```

Dans ces fichiers de logs agrégés, les logs de debug ne sont pas présents, pour éviter une surcharge inutile.

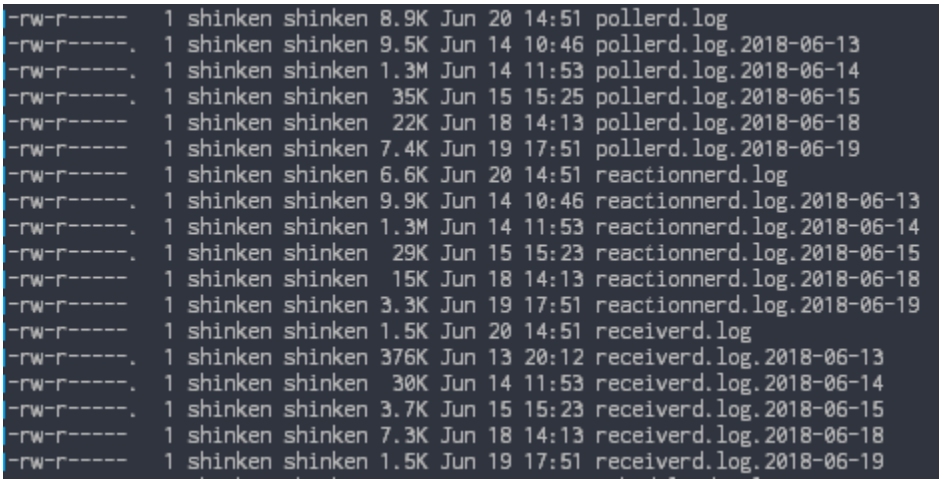
Rotation des logs

Rotation des logs des démons

Les fichiers de logs des démons contiennent seulement les logs de la journée en cours. À chaque nouvelle journée, les démons vident leur fichier de logs après avoir sauvegardé son contenu dans un fichier de sauvegarde.

Chaque fichier de sauvegarde correspond alors à une journée de logs. Pour ne pas consommer trop d'espace disque, uniquement les cinq derniers fichiers sont conservés (*cette durée de cinq jours n'est pas paramétrable à l'heure actuelle*).

Voici l'exemple de l'état du dossier **/var/log/shinken** après plusieurs jours en activité :



Rotation des logs agrégés

Les logs agrégés ont un comportement différent au niveau de leur archivage puisqu'ils ne sont pas gérés par les démons, mais par le module simple-log.

Ces fichiers sont sauvegardés dans le dossier **/var/log/shinken/archives**, toujours en organisant les logs en plaçant une journée par fichier.

À la différence des fichiers de logs des démons où seulement les cinq dernières journées sont conservées, les logs agrégés ne sont pas supprimés.

Penser à mettre en place une suppression des logs, suivant le nombre de jours voulant être gardés (*en fonction des outils qui utilisent ces fichiers*).

Informations utiles contenues dans les logs

Chaque démon a un rôle particulier. Par conséquent, chaque fichier de logs possède des informations particulières sur la supervision. Cette section liste les informations utiles qui peuvent être trouvées dans chaque fichier de log.

Arbiter

Dans les logs de l'Arbiter, on trouve l'ensemble des données relatives à l'ensemble de l'architecture de Shinken : l'état des démons et les détails concernant l'envoi de la configuration aux autres démons. Ce fichier est très utile dans le cas d'une architecture haute disponible, utilisant des spares. On peut y trouver quel démon est tombé, quel démon est passé en Spare et à quelle heure.

Exemple d'envoi de la configuratio aux autres démons

```
[2018-06-27 16:14:08] INFO: [arbiter] [Architecture-Export] Someone ask me to map the architecture [Shinken-lab-vm5]
[2018-06-27 16:14:08] INFO: [arbiter] And arbiter is launched with the hostname: from an arbiter point of view of addr:lab-vm5
[2018-06-27 16:14:08] INFO: [arbiter] Begin to dispatch configurations to satellites
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All]  Dispatching shards and satellites
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All]     Dispatching 1/1 shards to schedulers
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All]     Shards will be dispatched to schedulers in this order: scheduler-master (spare:False),
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All] DISPATCH SHARD    Dispatching shard [0]
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All] SEND SHARD   Trying to send shard 0 to scheduler scheduler-master
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All] SENT TIME   Shard [0] sent time is 0.10s (size=0.621MB, speed=6.340MB/s)
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All] SHARD SENT TO SCHEDULER   Dispatch OK of shard [0] - flavor [637621] in scheduler scheduler-master
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH] SHARD ALL SENT   All 1 schedulers shards are dispatched.
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All] SATELLITE ORDER  Dispatching reactionner satellite with be done in this order: reactionner-master (spare:False)
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All] SATELLITE SENT START Trying to send shard [0] to reactionner reactionner-master
[2018-06-27 16:14:08] INFO: [arbiter] [Architecture-Export] Old host [33d29aa6c5fc4e308d39e9c6de93516f] disabled on synchronizer.
[2018-06-27 16:14:08] INFO: [arbiter] [Architecture-Export] Old host [a50ffa8b2945401e9f620f04b07d78ea] disabled on synchronizer.
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All] SATELLITE SENT OK  Dispatch OK of shard [0:637621] to reactionner reactionner-master
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All] SATELLITES ALL SENT  No more reactionner sent need for this realm
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All] SATELLITE ORDER  Dispatching poller satellite with be done in this order: poller-master (spare:False),
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All] SATELLITE SENT START Trying to send shard [0] to poller poller-master
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All] SATELLITE SENT OK  Dispatch OK of shard [0:637621] to poller poller-master
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All] SATELLITES ALL SENT  No more poller sent need for this realm
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All] SATELLITE ORDER  Dispatching broker satellite with be done in this order: broker-master (spare:False),
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All] SATELLITE SENT START Trying to send shard [0] to broker broker-master
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All] SATELLITE SENT OK  Dispatch OK of shard [0:637621] to broker broker-master
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All] SATELLITES ALL SENT  No more broker sent need for this realm
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All] SATELLITE ORDER  Dispatching receiver satellite with be done in this order: receiver-master (spare:False),
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All] SATELLITE SENT START Trying to send shard [0] to receiver receiver-master
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All] SATELLITE SENT OK  Dispatch OK of shard [0:637621] to receiver receiver-master
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All] RECEIVER INVENTORY UPDATE Sending 16 hostnames to the receiver receiver-master
[2018-06-27 16:14:08] INFO: [arbiter]  (http://172.16.0.5:7773/)
[2018-06-27 16:14:08] INFO: [arbiter] [DISPATCH][All] SATELLITES ALL SENT  No more receiver sent need for this realm
```

Exemple d'erreur à l'envoi de la configuration

```
[2018-06-27 16:13:12] INFO: [arbiter] [DISPATCH][All]  Dispatching shards and satellites
[2018-06-27 16:13:12] INFO: [arbiter] [DISPATCH][All]     Dispatching 1/1 shards to schedulers
[2018-06-27 16:13:12] INFO: [arbiter] [DISPATCH][All]     Shards will be dispatched to schedulers in this order: scheduler-master (spare:False),
[2018-06-27 16:13:12] INFO: [arbiter] [DISPATCH][All] DISPATCH SHARD    Dispatching shard [0]
[2018-06-27 16:13:12] INFO: [arbiter] [DISPATCH][All] SEND SHARD   Trying to send shard 0 to scheduler scheduler-master
[2018-06-27 16:13:12] ERROR: [arbiter] Failed sending configuration for scheduler-master: Connexion error to http://172.16.0.5:7768/ : Failed connect to 172.16.0.5:7768; Connection refuse
[2018-06-27 16:13:12] INFO: [arbiter] [DISPATCH][All] SENT TIME   Shard [0] sent time is 0.00s (size=0.621MB, speed=190.863MB/s)
[2018-06-27 16:13:12] ERROR: [arbiter] [DISPATCH][All] SHARD NOT SENT   shard [0] - flavor [637621] dispatching error for scheduler scheduler-master
[2018-06-27 16:13:12] ERROR: [arbiter] [DISPATCH] MISSING SHARDS  All schedulers shards are not dispatched. 1 are missing
[2018-06-27 16:13:12] ERROR: [arbiter] [DISPATCH][All] UNMANAGED SHARD   shard [0] is unmanaged. We will sent it to a new scheduler.
[2018-06-27 16:13:13] WARNING: [arbiter] [DISPATCH][All] MISSING SATELLITE   Missing satellite reactionner for shard 0:
[2018-06-27 16:13:13] INFO: [arbiter] [DISPATCH][All] A SATELLITE    The reactionner reactionner-master seems to be waiting for a conf
[2018-06-27 16:13:13] WARNING: [arbiter] [DISPATCH][All] MISSING SATELLITE   Missing satellite poller for shard 0:
[2018-06-27 16:13:13] INFO: [arbiter] [DISPATCH][All] A SATELLITE    The poller poller-master seems to be waiting for a conf
[2018-06-27 16:13:13] WARNING: [arbiter] [DISPATCH][All] MISSING SATELLITE   Missing satellite broker for shard 0:
[2018-06-27 16:13:13] WARNING: [arbiter] [DISPATCH][All] MISSING SATELLITE   Missing satellite receiver for shard 0:
```

Broker

Ce fichier contient entre autres les informations liées à la gestion des données. Le broker est utilisé pour consommer les données de supervision récupérées par le Scheduler, et donc contiendra des informations supplémentaires sur la connexion entre les démons en cas d'erreur :

- Schedulers
- Poller
- Reactionners
- Receivers

C'est principalement dans ce fichier qu'on trouvera aussi les informations liées à **l'interface de Visualisation**.

Poller

Le Poller est chargé d'exécuter les vérifications des checks et des hôtes. On utilise souvent ce fichier pour déterminer pourquoi un check ou un hôte n'a pas son statut à jour.

En cas d'erreur d'une commande (*syntaxe invalide, script introuvable*), des informations pourront être trouvées dans les logs du Poller.

Aussi, on y trouvera des informations supplémentaires lorsque le démon n'arrive pas à communiquer avec le Scheduler.

Spécificités liées aux logs du Poller Windows

Suite à des contraintes techniques liées aux différences au point de vue système entre Windows et Linux, la convention de nommage des fichiers de logs du Poller sous Windows est légèrement différente :

- Le fichier de log du jour courant comporte également la date en suffixe comme c'est le cas pour les fichiers de logs archivés.
- Le Poller utilise des workers pour répartir la charge au niveau système créée par l'exécution des sondes. Sous Windows, chaque Worker possède son fichier de log, nommé de la forme suivante :

```
pollerd.log.worker<id_du_worker>.2019-02-19
```

- Les logs des workers du Poller Windows sont conservés un jour de moins que les logs du Poller Windows.

Reactionner

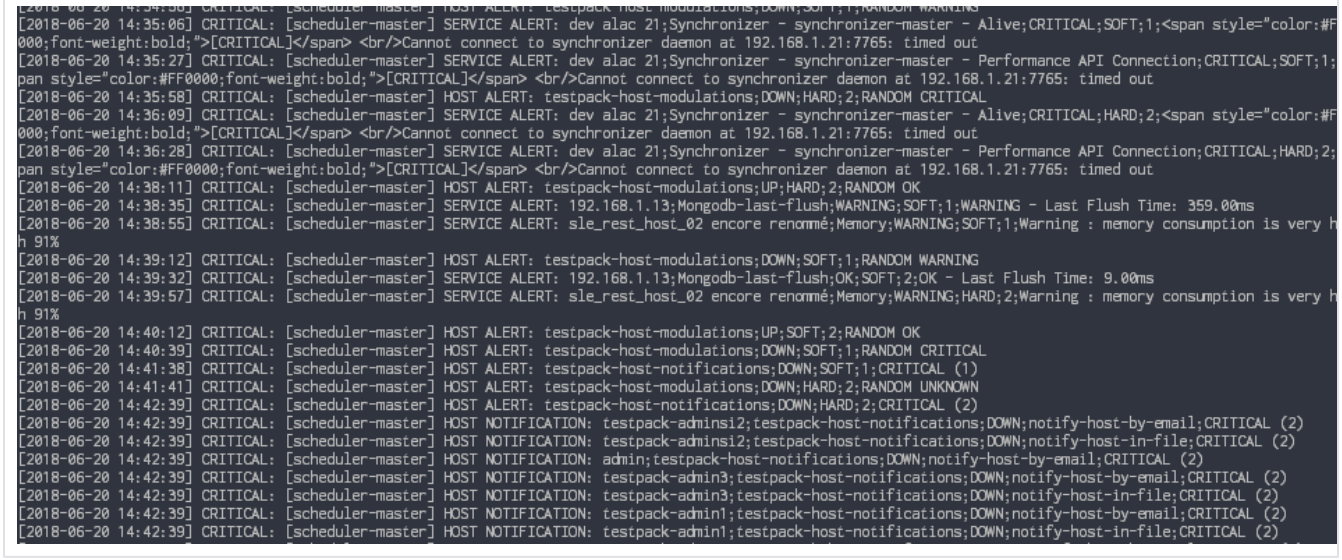
Le Reactionner est lui chargé d'exécuter les commandes de notifications et de gestionnaires d'événements. On utilise les logs du Reactionner pour avoir plus d'informations sur l'exécution d'une notification ou d'un gestionnaire d'événement en cas d'erreur.

Receiver

Dans les logs du Receiver, on trouve les événements liés aux checks passifs.

Scheduler

Le Scheduler ordonnance l'exécution des checks et des commandes. On trouve dans ce fichier l'ensemble des retours de checks, le déclenchement de l'envoi de notifications et des gestionnaires d'événements:



Synchronizer

On trouve dans ce fichier les alertes et messages concernant l'Interface de Configuration.

Gatherer

Dans ce fichier, il y aura les informations concernant le démarrage et l'arrêt du Gatherer (*qui sert à récupérer des statistiques système et de Virtualisation*), ainsi que les erreurs potentielles de ces récupérations, par exemple si l'ESXi ne permet pas de récupérer les informations de consommation CPU de la machine virtuelle.