

# Widget 360

## Contexte

**Simple Network Management Protocol** (abrégé **SNMP**), est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.

Une requête SNMP est un datagramme UDP envoyée par le manager à destination du port 161 de l'agent. L'agent répond alors au manager avec la valeur demandée.

Les traps SNMP, elles, sont émises depuis les agents SNMP vers une destination (un serveur de supervision par exemple), qui entendra ces requêtes. Pour les comprendre, ce serveur devra disposer de bases de données avec l'ensemble des informations (OID et Descripteurs) des constructeurs, ces bases sont appelées MIB. Les valeurs pourront alors être interprétées par le serveur de supervision.

Il se peut que vous souhaitiez paramétrer Shinken pour récupérer et interpréter ces traps, nous vous proposons deux moyens, via le module WS Arbiter de Shinken, ou via le module Named Pipe (historique Nagios).

## WS Arbiter

## Module Named Pipe

Il faut que

- tu le copies dans le répertoire `/var/lib/shinken/modules`
- Il faut ensuite rajouter la définition du module :
  - Dans le répertoire `/etc/shinken/modules/`
  - Tu copies le fichier `name-pipe.cfg`
- Ensuite on va accrocher le module au receiver
  - Tu ouvres le fichier `/etc/shinken/receivers/receiver-master.cfg`
  - Et tu ajoutes `named-pipe` a la ligne :
    - `modules`
      - `modules named-pipe`
- Dans l'UI de conf, tu crées le check template en passif
  - C'est l'équivalent du chapitre « On créé un fichier `/etc/shinken/services/snmptrap-service.cfg...` »
- Enfin, tu suis le tutorial <https://mespotesgeek.fr/fr/capture-de-trap-snmpt-sous-shinken/> à partir de « Ajouter le script suivant que l'on appellera `submit_check_res` »