

Editer un groupe utilisateur

Sommaire

[Principes](#)
[Onglet Général](#)

Contexte

Cette page a pour but de décrire la mise en place d'une configuration minimale SNMP pour un hôte supervisé par le pack **linux-by-SNMP__shinken**.

Procédure de configuration

La supervision d'un hôte par un **poller Shinken** se fait par requête/réponse SNMP.

- Sur le **poller shinken**, la sonde SNMP installé est responsable d'envoyer les requêtes et de traiter les réponses.
- Sur les hôtes à superviser, c'est l'**agent SNMP** qui est responsable de répondre aux requêtes.

? Unknown Attachment

Il est donc **essentiel** de correctement installer et configurer sont **agent SNMP**.

Installation de l'agent SNMP

L'agent SNMP sous linux à installer provient du paquet [net-snmp](#).

Il s'installe de la façon suivante :

```
# Ubuntu, Debian
apt-get install snmpd

# Centos, Fedora, OpenSUSE
yum -y install net-snmp

# Arch
pacman -Sy net-snmp
```

Vous pouvez également installer le paquet **net-snmp-utils** (*Utilitaires de gestion de réseau utilisant SNMP, issus du projet NET-SNMP*). L'installation de ce paquet est optionnelle pour le fonctionnement du pack.


```
# Ubuntu, Debian
apt-get install snmp

# Centos, Fedora, OpenSUSE
yum -y install net-snmp-utils
```

Une fois installé, vous pouvez activer le service snmpd :

```
systemctl enable snmpd
systemctl start snmpd
```

Sur certains systèmes, le firewall peut bloquer SNMP. Il faut donc autoriser le trafic sur le port **161/UDP** utilisé par SNMP. (ici le port par défaut est utilisé, si vous avez configuré votre propre port, remplacez 161 par le vôtre)

 Ces commandes sont à effectuer avec un utilisateur ayant les droits root.

Sur les systèmes utilisant **ufw** (Ubuntu/Debian) :

```
ufw allow 161/udp
ufw reload
```

Sur les systèmes utilisant **firewalld** (CentOS, Fedora, OpenSUSE) :

```
firewall-cmd --permanent --add-service=snmp
firewall-cmd --reload
```

Configuration de l'agent

Le fichier principal de configuration SNMP est : **"`/etc/snmp/snmpd.conf`"**.

Par précaution, faites une copie puis éditez le fichier de configuration :

```
cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.bak
vim /etc/snmp/snmpd.conf
```

Configuration minimale

Si vous n'avez pas déjà de configuration SNMP, vous pouvez utiliser la configuration suivante. Sinon, suivez la [configuration pas à pas](#).

Copiez la configuration et collez-la dans **"`/etc/snmp/snmpd.conf`"**, en écrasant la configuration de base. Cette **configuration minimale** pour un accès en lecture à l'**agent SNMP** supportant le v1, v2 et v3.

```
#      sec.name      source      community
com2sec notConfigUser default public

#      groupName      securityModel securityName
group  notConfigGroup v1        notConfigUser
group  notConfigGroup v2c       notConfigUser
group  notConfigGroup usm        shinken

#      name      incl/excl      subtree      mask(optional)
view   shinken   included      .1.3.6.1

#      group      context  sec.model  sec.level  prefix  read      write  notif
access notConfigGroup " "      any       noauth    exact    shinken  none   none

rouser shinken

# Inclus la configuration nécessaire pour le bon fonctionnement des checks.
includeDir /etc/snmp/shinken
```

Cette configuration définit :

- une communauté **"public"** à utiliser pour la connexion SNMP v1 et v2
- un utilisateur **"shinken"** à utiliser pour la connexion SNMP v3



La création de l'utilisateur v3 ne fonctionnera qu'avec l'exécution de la ligne de commande **`net-snmp-create-v3-user`** expliqué [ici](#)



N'oubliez pas d'ajouter également la [configuration nécessaire au check](#).

Configuration pas à pas

Si vous avez déjà votre propre configuration SNMP personnalisée, ou que vous avez des besoins spécifiques, vous pouvez suivre la configuration pas à pas.

Vous trouverez également la documentation de la configuration `snmpd` [ici](#).

Connexion SNMP v1 et v2

La ligne suivante permet de créer une communauté, ici "**public**" et de l'associer à un nouveau nom de sécurité.

```
####  
# First, map the community name "public" into a "security name"  
  
#      sec.name      source      community  
com2sec notConfigUser default      public
```



Par défaut, la communauté est définie à **public** dans **les modèles de supervisions du pack**. Si vous modifiez vos paramètres, il faudra donc les modifier dans l'interface de configuration.



Il est possible de changer le champ "**source**" pour restreindre l'accès à la communauté définit, pour une adresse ou une plage d'adresse.

```
#      sec.name      source      community      # Hostname  
com2sec notConfigUser my.host.com      public  
com2sec notConfigUser 192.0.0.123      public      # Address  
com2sec notConfigUser 10.10.10.0/255.255.255.0      public      # IP/MASK
```

Ensuite, il est nécessaire de rattacher le nom de sécurité créée à un groupe, et à un modèle de sécurité.

```
#      groupName      securityModel securityName  
group  notConfigGroup v1      notConfigUser  
group  notConfigGroup v2c      notConfigUser
```

Connexion SNMP v3

La connexion SNMP v3 nécessite la mise en place d'un utilisateur qui sera utilisé pour se connecter sur les hôtes supervisés.

Voici un exemple de création d'un utilisateur sur la machine supervisée qui sera interrogée par le pack en SNMP v3.

Arrêtez le service SNMP pour pouvoir lancer la commande de création d'un utilisateur :

```
service snmpd stop
```

Créez votre utilisateur avec ses informations d'identification :

```
net-snmp-create-v3-user -ro -A shinkenpassword -a SHA -X shinkenencryptionkey -x AES shinken
```

Redémarrez le service SNMP :


```
service snmpd start
```

Test de connexion en local :

```
snmpwalk -u shinken -A shinkenpassword -a SHA -X shinkenencryptionkey -x AES -l authPriv 127.0.0.1 -v3
```

À noter qu'ici, nous avons défini :

- **shinken**: nom de l'utilisateur côté serveur SNMPv3
- **shinkenpassword**: mot de passe de l'utilisateur. Attention : il ne peut pas être plus petit que 8 caractères.
- **shinkenencryptionkey**: clé de chiffrement pour cet utilisateur
- **AES**: protocole de chiffrement de l'utilisateur
- **SHA**: méthode de hashage des informations de l'utilisateur

 Ces **paramètres sont par défaut dans le pack et seront utilisés dans les modèles de supervisions** pour interroger les équipements supervisés. Si vous créez vos propres paramètres, il faudra donc les modifier dans l'interface de configuration.

Ensuite, il est nécessaire de rattacher l'utilisateur créée à un groupe, et à un modèle de sécurité.

```
#      groupName      securityModel securityName
group notConfigGroup usm              shinken
```

 usm signifie User Security Model et a été introduit et utilisé pour SNMP v3

Autorisations d'accès aux données

Quelle que soit la version de SNMP configuré, V1, V2 ou V3, **il est essentiel de configurer l'accès aux données**.

Une fois les utilisateurs, noms de sécurités, et groupes créés, il faut ajouter une vue pour leur donner accès aux données.

```
#      name          incl/excl    subtree      mask(optional)
view  shinken        included    .1.3.6.1
```

 Ici la vue "**shinken**" définit l'accès à l'arbre ".1.3.6.1". L'ensemble des OIDs qui commencent par ".1.3.6.1" sont donc inclus.

Pour finir, il faut donner l'accès à la vue au groupe défini plus tôt.

```
#      group          context  sec.model  sec.level  prefix  read  write  notif
access notConfigGroup    ""      any       noauth    exact  shinken  none  none
```

 Ici seulement les droits de lectures ont été donnés au groupe "**notConfigGroup**"

Configuration nécessaire aux checks

Les checks du pack **linux-by-SNMP__shinken** nécessitent la configuration ci-dessous pour fonctionner.

```

# linux-by-SNMP__shinken snmpd configuration file
# This file is essential for checks to work
# The file must be installed on hosts supervised by Shinken
# It must be included from the main snmpd configuration file

# check : Disks Usage by SNMP
includeAllDisks 10%

# check : Ntp Sync by SNMP
extend shinken__linux-by-snmp__ntp-sync__ntpq /bin/sh -c "export LC_LANG=C && unset LANG && ntpq -p ; date
+'%H:%M:%S.%3N'"

# check : Ntp Sync Chrony by SNMP
extend shinken__linux-by-snmp__ntp-sync__chrony__chronyc /bin/sh -c "export LC_LANG=C && unset LANG &&
chronyc tracking ; date +'%H:%M:%S.%3N'"

# check : Stats CPU by SNMP
extend shinken__linux-by-snmp__stats-cpu__processes-cpu-time /bin/sh -c "export LC_LANG=C && unset LANG &&
awk '{ut[\\$1]=\\$14; st[\\$1]=\\$15} END { system("\\sleep 1\\"); for (p in ut) { getline < (\\\"/proc/\\\" p \\\"
/stat\\"); split(\\$0, d, \\\" \\"); printf \\\"%s %d %d %d %d\\n\\\", p, ut[p], st[p], d[14], d[15] } }' /proc/[0-9]*
/stat"
extend shinken__linux-by-snmp__stats-cpu__processes-cpu /bin/sh -c "export LC_LANG=C && unset LANG && ps -eo
pcpu,pid,args --sort=-pcpu --no-headers"
extend shinken__linux-by-snmp__stats-cpu__frequency /bin/sh -c "export LC_LANG=C && unset LANG && cat /proc
/cpuinfo | grep 'cpu MHz' | uniq | cut -d ' ' -f 3"
extend shinken__linux-by-snmp__stats-cpu__mpstat /bin/sh -c "export LC_LANG=C && unset LANG && mpstat -P ALL
1 1"

```

Copiez cette configuration et enregistrez-la dans un fichier : ***"/etc/snmp/shinken/linux-by-SNMP__shinken.conf"***

```

mkdir -p /etc/snmp/shinken/
vim /etc/snmp/shinken/linux-by-SNMP__shinken.conf

```

Il faut ensuite inclure ce fichier depuis la configuration principale snmpd.
Dans le fichier ***"/etc/snmp/snmpd.conf"*** :

```

vim /etc/snmp/snmpd.conf

```

Assurez vous d'avoir la ligne suivante, sinon ajoutez la :

```

includeDir /etc/snmp/shinken

```

Test en local

Sur votre machine locale, vous pouvez exécuter les commandes suivantes pour tester votre configuration SNMP.

Tester la configuration v2 :

```

snmpwalk localhost -v2c -c public 1.3.6.1.4.1

```

Déploiement sur plusieurs hôtes à superviser

Pour éviter un déploiement manuel de la configuration sur de nombreuses machines, shinken propose un script afin de configurer une hôte à superviser.

Le script permet d'**écraser** la configuration existante pour une configuration minimale en SNMP, v1, v2 et v3, et de faire fonctionner les checks du pack.

Le script est livré dans le dossier ***"supervised-host"*** livré dans le pack.



Le script est à exécuter en local sur l'hôte à superviser. Il faut alors télécharger le dossier "**supervised-host**" sur l'hôte, puis **exécuter le script depuis l'hôte**.

L'outil **ne permet donc pas de déployer** sur votre parc de machines. Pour automatiser le déploiement, vous devez intégrer notre dossier "**supervised-host**" dans vos solutions de déploiement (*Virtual Box, Docker, Ansible, Terraform, AWS EC2, ...*).

Prérequis avant d'exécuter le script

Avant d'exécuter le script, veuillez installer l'agent SNMP et ouvrir les ports SNMP en suivant [ce chapitre](#).



Avant de déployer le script de configuration sur plusieurs hôtes, il est fortement conseillé de :

- Faire une installation manuelle sur UN hôte
- Appliquer le script de configuration sur UN hôte

Exécuter le script

Le script va **ÉCRASER** ("**/etc/snmp/snmpd.conf**") pour la remplacer par la configuration minimale **SNMP** livré avec le pack. Un fichier de sauvegarde ("**/etc/snmp/snmpd.conf.bak**") sera généré avant d'écraser la configuration par défaut.

```
./configure-host.sh --override-default-conf
```

N'hésitez pas à vous approprier la configuration avant d'exécuter le script, en modifiant le fichier "**snmpd-template.conf**" dans le dossier "**supervised-host**" afin que la configuration s'adapte à vos besoins.



Vous pouvez ajouter les options suivantes en ligne de commande afin de configurer les paramètres de connexion SNMP v1 v2 et v3 :

argument	description	Pour version SNMP	Valeur par défaut	Variable de modèle d'hôte correspondant
-c	Communauté	V1 V2	public	<i>LINUX-BY-SNMP__V1V2-COMMUNITY</i>
-a	Protocole pour l'identification	V3	SHA	<i>LINUX-BY-SNMP__V3-PROTOCOL-AUTH</i>
-A	Mot de passe	V3	shinkenpassword	<i>LINUX-BY-SNMP__V3-PASSPHRASE-AUTH</i>
-x	Protocole de confidentialité	V3	AES	<i>LINUX-BY-SNMP__V3-PROTOCOL-PRIV</i>
-X	Clef de chiffrement	V3	shinkenencryptionkey	<i>LINUX-BY-SNMP__V3-PASSPHRASE-PRIV</i>
-u	Nom d'utilisateur	V3	shinken	<i>LINUX-BY-SNMP__V3-LOGIN</i>

Toutes les valeurs par défaut sont celles utilisées par **les modèles de supervisions du pack**.

Exemple :

```
./configure-host.sh --override-default-conf -u my_new_user -a SHA -A my_new_password -c my_community
```

Erreurs lors de l'utilisation du pack

Pour toute erreur survenue lors de l'exécution des checks, voir la page [Erreurs communes](#).