

Chiffrement des données sensibles

Sommaire

Description
Mise en œuvre
Activation du chiffrement
Identification des clés de chiffrement
Sauvegarde et restauration de la clé
Retrouver une clé perdue
Déterminer la liste des propriétés qui seront chiffrées
Changer de clé de chiffrement
Désactivation du chiffrement
Information

Contexte

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

Procédure de configuration

La supervision d'un serveur Linux supervisé 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 Serveurs Linux 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 l'**agent SNMP**.

Installation de l'agent SNMP

Installation du démon snmpd

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

# RHEL, Alma, Rocky, Centos, Fedora, OpenSUSE
yum -y install net-snmp

# Arch, Manjaro
pacman -Syy net-snmp
```

Installation des outils 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

# RHEL, Alma, Rocky, Centos, Fedora, OpenSUSE
yum -y install net-snmp-utils

# Arch, Manjaro
# Les utilitaires sont déjà installés avec le packet net-snmp
```

Une fois installé, vous pouvez activer le service snmpd :

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

Configuration du firewall

Vérification des règles pour SNMP du firewall

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 / Fedora) :

- Exécuter la commande suivante :

```
ufw status verbose
```

- Vérifier qu'une règle autorise l'accès au port **161** en **UDP** aux **IP des pollueurs shinken** :
Exemple de retour valide :

```
Status: active

To Action From
---
161/udp ALLOW Anywhere
161/udp (v6) ALLOW Anywhere (v6)
```

- Sinon, passer à l'étape suivante et ajouter la une règle à votre firewall.

Sur les systèmes utilisant **firewalld** (RHEL, Alma, Rocky, Centos, Fedora, OpenSUSE) :

- Exécuter la commande suivante :

```
firewall-cmd --list-all
```

- Vérifier qu'une règle autorise l'accès au port **161/UDP** ou que "**snmp**" se trouve dans la liste des "**services**"

Exemple de retour valide :

```
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ntp snmp ssh
  ports: 80/tcp 7765/tcp 7766/tcp 7767/tcp 7768/tcp 7769/tcp 7770/tcp 7771/tcp 7772/tcp 7773/tcp 7777
/tcp 7780/tcp 50000/tcp
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

- Sinon, passer à l'étape suivante et ajouter la une règle à votre firewall.

Ajout de règle pour SNMP au firewall

Il est possible de passer cette étape si votre firewall est déjà configuré pour autoriser les requêtes SNMP.

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

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

Sur les systèmes utilisant **firewalld** (RHEL, Alma, Rocky, Centos, Fedora, OpenSUSE) :

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

Configuration par script de l'agent

Pour éviter de faire manuellement la configuration, le pack met à disposition un script afin de configurer un serveur Linux 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**" dans le pack.

Il est déconseillé d'utiliser le script si vous avez déjà une configuration SNMP spécifique (non par défaut), car le script va l'**écraser**.



Le script est à exécuter en local sur le serveur Linux à superviser.

- Il faut alors télécharger le dossier "**supervised-host**" sur le serveur Linux, puis **exécuter le script depuis le serveur Linux**.
- 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, il est nécessaire de :

- installer l'agent SNMP et ouvrir les ports SNMP en suivant [ce chapitre](#)
- installer les dépendances sur les hôtes à superviser en suivant [ce chapitre](#).



Avant de déployer le script de configuration sur plusieurs serveurs Linux à superviser, il est fortement conseillé de :

- Faire une installation manuelle sur UN serveur Linux à superviser.
- Appliquer le script de configuration sur UN serveur Linux à superviser.

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 "`supervise`
`d-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 :

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

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
```

Une fois la SNMP configuré, selon le mode d'authentification choisi :

- [Tester la connexion SNMPv1v2](#)
- [Tester la connexion SNMPv3](#)

Configuration pour SELinux

Il est possible que votre serveur Linux supervisé soit configuré avec SELinux et que certains checks du pack n'aient pas les permissions d'accéder aux ressources nécessaires.

Le script peut également être exécuté avec l'option '`--configure-selinux`' afin d'ajouter des règles de lecture au service SNMP (`snmpd`).

```
./configure-host.sh --configure-selinux
```

Configuration manuelle 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
```

Si vous n'avez pas déjà de configuration SNMP,

- Vous pouvez utiliser la [configuration d'exemple](#)
- **Sinon**, suivez la [configuration pas à pas](#).

Configuration d'exemple

Si vous n'avez jamais configuré le serveur SNMP (vous avez le fichier par défaut), vous pouvez utiliser la configuration suivante.

- Copiez la configuration et collez-la dans `/etc/snmp/snmpd.conf`, en écrasant la configuration de base.
- **IMPORTANT** : Cette **configuration minimale** pour un accès en lecture à l'**agent SNMP** supportant le v1, v2 (`v2c`) et v3 (`v3`).

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

#       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



Ensuite, il est **NÉCESSAIRE** de suivre :

- [L'étape Connexion SNMP v3](#) pour finaliser la configuration V3.
- [La configuration nécessaire au check](#) pour le bon fonctionnement des checks.
- [L'installation des dépendances](#) nécessaires aux checks.

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 SNMPv1v2

Il est possible de passer cette étape si vous souhaitez uniquement [configurer la connexion SNMPv3](#).

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
```

i 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.

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

```
#      sec.name      source      community      # Hostname  
com2sec notConfigUser my.host.com public # Hostname  
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

Il est possible de passer cette étape si vous souhaitez uniquement [configurer la connexion SNMPv1v2](#).

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
```

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

i 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 créé à un groupe, et à un modèle de sécurité.

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

i 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
```

i 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
```

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

Test de connexion SNMPv1v2

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

Tester la configuration v2 (les paramètres d'authentification peuvent être à changer) :

```
snmpwalk localhost -v2c -c public 1.3.6.1.4.1
```

Test de connexion SNMPv3

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

Tester la configuration v3 (les paramètres d'authentification peuvent être à changer) :

```

# Tester authPriv
snmpwalk localhost -v3 -l authPriv -u shinken -a SHA -A "shinkenpassword" -x AES -X "shinkenencryptionkey"
1.3.6.1.4.1

# Tester authNoPriv
snmpwalk localhost -v3 -l authNoPriv -u shinken -a SHA -A "shinkenpassword" 1.3.6.1.4.1

# Tester noAuthNoPriv
snmpwalk localhost -v3 -l noAuthNoPriv -u shinken 1.3.6.1.4.1

```

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
```

Installations des dépendances

Certain checks nécessitent des dépendances sur le serveur Linux à superviser. Il faut les installer pour leur bon fonctionnement.

Stats CPU by SNMPvX

Le check CPU Stats SNMPvX utilise le paquet **SysStat**, nécessaire au bon fonctionnement du check. Il faut l'installer avec la commande suivante :

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

# RHEL, Alma, Rocky, Centos, Fedora, OpenSUSE
yum install sysstat

# Arch, Manjaro
pacman -Syy sysstat
```

Erreurs lors de l'utilisation du pack

Pour toute erreur survenue lors de l'exécution des checks, voir la page [Erreurs du pack linux-by-SNMP__shinken](#)