Exo 2 – 21/10/2022

Consignes :

- Configurer votre agent SNMP sur équipements Linux
- Tester avec les commandes snmpwalk et snmpget le bon fonctionnement

Qu'est-ce que SNMP ?

SNMP (Simple Network Management Protocol) est un protocole de gestion de réseaux, plus précisément un protocole de communication qui va permettre aux administrateurs réseaux la gestion du matériel présent sur le réseau, de les superviser mais aussi de communiquer en cas de diagnostic de problèmes réseaux et/ou matériels, à distance.

SNMP v3 sur Linux

Installation de SNMP

⇨ Commandes d'installation de snmpd, snmp et libsnmp :

```
apt update
apt-get install snmpd snmp libsnmp-dev -y
```

⇨ Arrêt du service snmp :

```
service snmpd stop
```

Ajout d'un utilisateur SNMPv3

⇨ Changement *AuthPassword* par le mot de passe d'authentication.
⇨ Changement *CryptoPassword* par le mot de passe de chiffrement.
⇨ Changement *privUser* par votre l'utilisateur.

```
sudo net-snmp-config --create-snmpv3-user -ro -A AuthPassword -X CryptoPassword -a MD5
    -x AES privUser
```

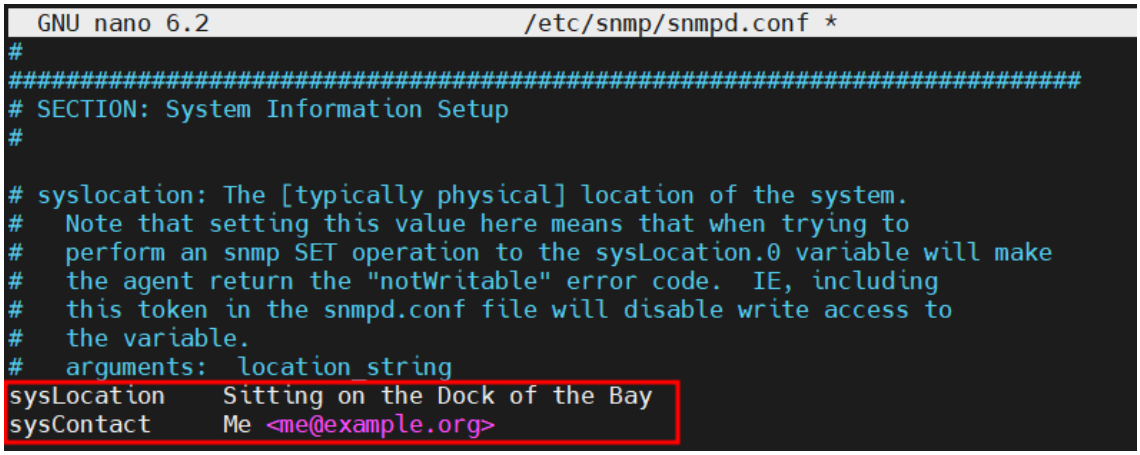
```
root@scw-valentin-clement:~# sudo net-snmp-config --create-snmpv3-user -ro -A AuthPassword -X C
ryptoPassword -a MD5 -x AES privUser
adding the following line to /var/lib/snmp/snmpd.conf:
   createUser privUser MD5 "AuthPassword" AES "CryptoPassword"
adding the following line to /usr/share/snmp/snmpd.conf:
   rouser privUser
```

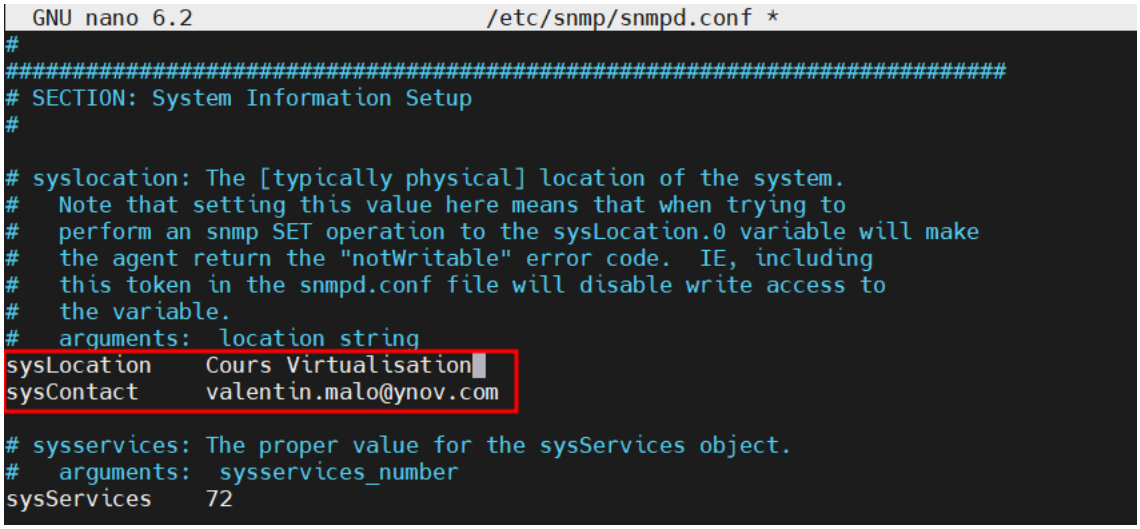
Changement du System Location, System Contact et autoriser SNMP sur toutes les interfaces

⇨ Modification du fichier de configuration SNMP dans le chemin /etc/snmp/snmpd.conf

```
nano /etc/snmp/snmpd.conf
```

⇨ Dans le fichier, il faut trouver les 2 lignes *sysLocation* et *sysContact*. *sysLocation* doit être remplacé par l'emplacement du système.





⇨ Toujours le fichier de configuration, vous devez commenter la ligne suivante :

- `agentAddress 127.0.0.1,[ ::1]`

⇨ Et ajouter la ligne suivante en dessous de celle que vous venez de commenter :

- `agentAddress upd :161,upd6 :[ ::1] :161`

```
 GNU nano 6.2                          /etc/snmp/snmpd.conf *

###############################################################################
# SECTION: Agent Operating Mode
#
#   This section defines how the agent will operate when it
#   is running.

# master: Should the agent operate as a master agent or not.
#   Currently, the only supported master agent type for this token
#   is "agentx".
#
#   arguments: (on|yes|agentx|all|off|no)

master  agentx

# agentaddress: The IP address and port number that the agent will listen on.
#   By default the agent listens to any and all traffic from any
#   interface on the default SNMP port (161).  This allows you to
#   specify which address, interface, transport type and port(s) that you
#   want the agent to listen on.  Multiple definitions of this token
#   are concatenated together (using ':'s).
#   arguments: [transport:]port[@interface/address],...

#agentaddress  127.0.0.1,[::1]
agentAddress udp:161,udp6:[::1]:161
```

Cela a pour but de pouvoir lire les différentes informations SNMP en utilisant l'adresse IP des serveurs (n'importe laquelle), sans être limité à une seule d'entre elle (localhost).

Démarrage du service SNMP et des tests des commandes snmpwalk et snmpget

- ⇨ Démarrage du service :

```
service snmpd start
```

- ⇨ Test de la commande SNMPWALK :

```
snmpwalk -v3 -a MD5 -A AuthPassword -X CryptoPassword -l authNoPriv -u privUser
localhost
```

```
root@scw-valentin-clement:~# snmpwalk -v3 -a MD5 -A AuthPassword -X CryptoPassword -l authNoPri
v -u privUser localhost
iso.3.6.1.2.1.1.1.0 = STRING: "Linux scw-valentin-clement 5.15.0-41-generic #44-Ubuntu SMP Wed
Jun 22 14:20:53 UTC 2022 x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (11914) 0:01:59.14
iso.3.6.1.2.1.1.4.0 = STRING: "valentin.malo@ynov.com"
iso.3.6.1.2.1.1.5.0 = STRING: "scw-valentin-clement"
iso.3.6.1.2.1.1.6.0 = STRING: "Cours Virtualisation"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.13.3.1.3
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.92
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The SNMP Management Architecture MIB."
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The management information definitions for the SNMP User-bas
ed Security Model."
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "View-based Access Control Model for SNMP."
iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module for managing TCP implementations"
iso.3.6.1.2.1.1.9.1.3.7 = STRING: "The MIB module for managing UDP implementations"
iso.3.6.1.2.1.1.9.1.3.8 = STRING: "The MIB module for managing IP and ICMP implementations"
iso.3.6.1.2.1.1.9.1.3.9 = STRING: "The MIB modules for managing SNMP Notification, plus filteri
ng."
iso.3.6.1.2.1.1.9.1.3.10 = STRING: "The MIB module for logging SNMP Notifications."
iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (0) 0:00:00.00
```

Il faut savoir que la liste est très longue, il n'y a qu'une partie de toutes les informations que l'on obtient.

- `snmpwalk -v3 -a MD5 -A AuthPassword -X CryptoPassword -l authNoPriv -u privUser localhost | grep "ynov"`

```
root@scw-valentin-clement:~# snmpwalk -v3 -a MD5 -A AuthPassword -X CryptoPassword -l authNoPriv -u privUser localhost |
grep "ynov"
iso.3.6.1.2.1.1.4.0 = STRING: "valentin.malo@ynov.com"
iso.3.6.1.2.1.25.4.2.1.5.4736 = STRING: "--color=auto ynov"
```

⇨ Test de la commande SNMPGET :

- `snmpwalk -v3 -a MD5 -A AuthPassword -X CryptoPassword -l authNoPriv -u privUser localhost iso.3.6.1.2.1.1.4.0`

```
root@scw-valentin-clement:~# snmpget -v3 -a MD5 -A AuthPassword -X CryptoPassword -l authNoPriv -u privUser localhost iso
.3.6.1.2.1.1.4.0
iso.3.6.1.2.1.1.4.0 = STRING: "valentin.malo@ynov.com"
```

⇨ Les 2 commandes à la suite :

```
root@scw-valentin-clement:~# snmpwalk -v3 -a MD5 -A AuthPassword -X CryptoPassword -l authNoPriv -u privUser localhost |
grep "ynov"
iso.3.6.1.2.1.1.4.0 = STRING: "valentin.malo@ynov.com"
iso.3.6.1.2.1.25.4.2.1.5.4770 = STRING: "--color=auto ynov"
root@scw-valentin-clement:~# snmpget -v3 -a MD5 -A AuthPassword -X CryptoPassword -l authNoPriv -u privUser localhost iso
.3.6.1.2.1.1.4.0
iso.3.6.1.2.1.1.4.0 = STRING: "valentin.malo@ynov.com"
```

Test avec SNMPv1

```
root@scw-valentin-malo:~# snmpwalk -v1 127.0.0.1 -c cours
iso.3.6.1.2.1.1.1.0 = STRING: "Linux scw-valentin-malo 5.15.0-41-generic #44-Ubuntu SMP
Wed Jun 22 14:20:53 UTC 2022 x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (9373) 0:01:33.73
iso.3.6.1.2.1.1.4.0 = STRING: "valentin.malo@ynov.com"
iso.3.6.1.2.1.1.5.0 = STRING: "scw-valentin-malo"
iso.3.6.1.2.1.1.6.0 = STRING: "Cours Virtualisation"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.13.3.1.3
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.92
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The SNMP Management Architecture MIB."
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The management information definitions for the SNMP U
ser-based Security Model."
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "View-based Access Control Model for SNMP."
iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module for managing TCP implementations"
iso.3.6.1.2.1.1.9.1.3.7 = STRING: "The MIB module for managing UDP implementations"
iso.3.6.1.2.1.1.9.1.3.8 = STRING: "The MIB module for managing IP and ICMP implementatio
ns"
iso.3.6.1.2.1.1.9.1.3.9 = STRING: "The MIB modules for managing SNMP Notification, plus
filtering."
iso.3.6.1.2.1.1.9.1.3.10 = STRING: "The MIB module for logging SNMP Notifications."
iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.6 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.7 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.8 = Timeticks: (0) 0:00:00.00
```

```
root@scw-valentin-malo:~# snmpwalk -v1 127.0.0.1 -c cours .1.3.6.1.2.1.1.1.0
iso.3.6.1.2.1.1.1.0 = STRING: "Linux scw-valentin-malo 5.15.0-41-generic #44-Ubuntu SMP
Wed Jun 22 14:20:53 UTC 2022 x86_64"
```

On récupère grâce à la commande snmpwalk, le OID de la cible : iso.3.6.1.4.1.8072.3.2.10

```
root@scw-valentin-malo:~# snmpwalk -v1 127.0.0.1 -c cours
iso.3.6.1.2.1.1.1.0 = STRING: "Linux scw-valentin-malo 5.15.0-41-generic #44-Ubuntu SMP
Wed Jun 22 14:20:53 UTC 2022 x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (9373) 0:01:33.73
iso.3.6.1.2.1.1.4.0 = STRING: "valentin.malo@ynov.com"
iso.3.6.1.2.1.1.5.0 = STRING: "scw-valentin-malo"
iso.3.6.1.2.1.1.6.0 = STRING: "Cours Virtualisation"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
```

Il faut préciser en syntaxe une option parmi la liste proposée :

```
root@scw-valentin-malo:~# snmpget -h
USAGE: snmpget [OPTIONS] AGENT OID [OID]...

  Version:  5.9.1
  Web:      http://www.net-snmp.org/
  Email:    net-snmp-coders@lists.sourceforge.net

OPTIONS:
  -h, --help            display this help message
  -H                    display configuration file directives understood
  -v 1|2c|3             specifies SNMP version to use
  -V, --version         display package version number
SNMP Version 1 or 2c specific
  -c COMMUNITY          set the community string
SNMP Version 3 specific
  -a PROTOCOL           set authentication protocol (MD5|SHA|SHA-224|SHA-256|SHA-384|SHA-512)
  -A PASSPHRASE         set authentication protocol pass phrase
  -e ENGINE-ID          set security engine ID (e.g. 800000020109840301)
  -E ENGINE-ID          set context engine ID (e.g. 800000020109840301)
  -l LEVEL              set security level (noAuthNoPriv|authNoPriv|authPriv)
  -n CONTEXT            set context name (e.g. bridge1)
  -u USER-NAME          set security name (e.g. bert)
  -x PROTOCOL           set privacy protocol (DES|AES|AES-192|AES-256)
  -X PASSPHRASE         set privacy protocol pass phrase
  -Z BOOTS,TIME         set destination engine boots/time
General communication options
  -r RETRIES            set the number of retries
  -t TIMEOUT            set the request timeout (in seconds)
Debugging
  -d                    dump input/output packets in hexadecimal
  -D[TOKEN[,...]]       turn on debugging output for the specified TOKENs
                           (ALL gives extremely verbose debugging output)
General options
  -m MIB[:...]          load given list of MIBs (ALL loads everything)
  -M DIR[:...]          look in given list of directories for MIBs
    (default: $HOME/.snmp/mibs:/usr/share/snmp/mibs:/usr/share/snmp/mibs/iana:/usr/share/snmp/mibs/ietf)
  -P MIBOPTS            Toggle various defaults controlling MIB parsing:
                          u:  allow the use of underlines in MIB symbols
                          c:  disallow the use of "--" to terminate comments
                          d:  save the DESCRIPTIONs of the MIB objects
                          e:  disable errors when MIB symbols conflict
                          w:  enable warnings when MIB symbols conflict
```

```
root@scw-valentin-malo:~# snmpget -V agent OID iso.3.6.1.4.1.8072.3.2.10
NET-SNMP version: 5.9.1
```

```
root@scw-valentin-malo:~# snmpget -v 2c 127.0.0.1 -c cours .1.3.6.1.2.1.1.1.0
iso.3.6.1.2.1.1.1.0 = STRING: "Linux scw-valentin-malo 5.15.0-41-generic #44-Ubuntu SMP
Wed Jun 22 14:20:53 UTC 2022 x86_64"
```

Différences entre snmpget et snmpwalk

Ces 2 commandes sont des éléments de la suite Net-SNMP qui permettent d'implémenter et d'utiliser SNMP dans les réseaux IPv4 et IPv6.

- SNMPGET permet de consulter les informations d'un participant au réseau à l'aide du Simple Network Management Protocol. Cette consultation est effectuée à l'aide du type de messages SNMP « GET » qui va exiger plusieurs données spécifiques sur le système cible.

Pour se faire, il est nécessaire d'indiquer comme arguments l'hôte (nom ou IP), le nom de communauté (SNMPv1 ou SNMPv2) ou les informations d'authentification (SNMPv3) et le numéro d'identification approprié (OID).

```
snmpget [Options] [Community-String/Informations d'authentification] [Nom de l'hôte /Adresse de l'hôte] [Object Identifier]
```

- SNMPWALK permet non seulement de consulter un ensemble de données spécifique sur un appareil cible compatible SNMP, mais aussi les ensembles de données subséquents.

Afin d'interroger un arbre d'information complet (base MIB complète), snmpwalk utilise des messages de type « GETNEXT » qui vont demander des informations aux agents jusqu'à ce que la base MIB concerné soit atteinte. D'un point de vue syntaxe, l'utilisation de snmpwalk n'est pas si différente des interrogations simples de snmpget.

```
snmpwalk [Options] [Community-String/Informations d'authentification] [Nom de l'hôte/Nom de l'adresse] [Object Identifier]
```

SNMPGET permet de récupérer la valeur OID tandis que SNMPWALK permet de récupérer toutes les valeurs d'un OID.