Surveillance réseau avec le protocole SNMP TD : 1
STI 4A Administration réseaux
Version 2020-2021 avec VM utilisant « systemD »

SOMMAIRE :

1. Généralités

Le but de ce TD est de « monitorer » un élément du réseau en utilisant le protocole « snmp » et ses différentes versions V1, V2c, V3.
En particulier, le but sera d'émettre une alerte dès qu'un fichier (on choisira le fichier en question) dépassera une taille jugée critique.
Puis vous limiterez les accès aux MIBs et vous authentifierez et chiffrerez les échanges avec « snmp V3».

2. Récupérer l'image « Vmware »

Sur la ressource réseau « \\freenas\partage », récupérez la machine virtuelle qui se trouve dans le répertoire « 2019_2020_vm_td » et copiez-la dans votre ressource réseau « \\freenas\votre_login ».

3. Vérification du processus d'initialisation.

Le premier processus à démarrer, lors de la mise en marche de la VM, dans le « Userland » créé par le système d'exploitation est appelé « processus d'initialisation » et son « PID » (Process Identifier) est égal à 1.
C'est la racine de l'arbre des processus.
Pour plus d'information consultez le lien ci-dessous.
https://linuxfr.org/news/systemd-l-init-martyrise-l-init-bafoue-mais-l-init-libere#d%C3%A9marrage-du-syst%C3%A8me

De nos jours il existe selon la distribution et la version de celle-ci deux « processus d'initialisation » que l'on rencontre le plus souvent sur les systèmes « Unix-like » :

- SysVinit : Le processus historique ;
- Systemd : La version plus récente (à partir de 2010).

Ce processus d'initialisation impacte directement ce TD sur « SNMP » car les fichiers d'initialisation des « daemons SNMP» ne sont pas les mêmes.
Pour « SysVinit », il s'agit principalement de « /etc/default/snmpd » ;
Pour « Systemd », il s'agit de « /lib/systemd/system/snmpd.service ».

Donc il faut vérifier quel est le processus d'initialisation utilisé par votre « VM ».

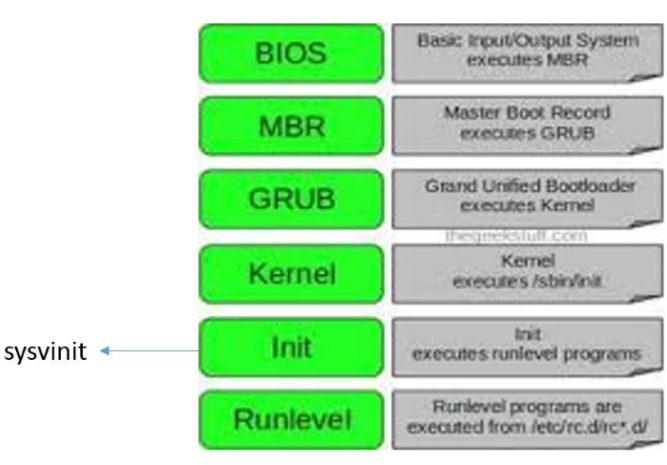
Vérifiez, par exemple, en utilisant une commande du type : pstree|grep «(1)».

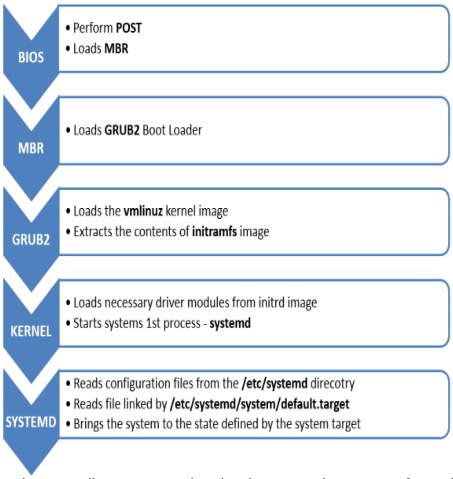
```
martial@martial-ubuntu-light ~ $ pstree -hp|grep "(1)"
init(1)-+-NetworkManager(1156)-+-{NetworkManager}(1157)
```

Il s'agit de "SysVinit"

```
martial@acerfix ~ $ pstree -hp|grep "(1)"
systemd(1)-+-ModemManager(1076)-+-{gdbus}(1137)
```

Il s'agit de "Systemd"





https://medium.com/@Seavievv/booting-process-in-centos7-e1f4a817d32b

Ce support de TD est rédigé pour « SystemD », adaptez-le dans le cas de « SystemVinit ».

4. Vérification des « packages »

4.1. Lancer « vmware workstation »

Lancez « Vmware Workstation » et ajoutez la machine du paragraphe 2. Optimisez les réglages de votre machine virtuelle en fonction des caractéristiques de la machine réelle dont vous disposez (Settings).

4.2. Démarrer l'image ainsi obtenue.

Il existe deux comptes sur cette machine « root » et « insacvl », mot de passe « azerty » pour les deux.

4.3. Installer les paquets suivants :

```
root@insacvl-virtual-machine:~# apt-get install snmp snmpd snmp-mibs-downloader tkmib wireshark
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libc-ares2 liblua5.2-0 libportaudio2 libsmi2ldbl libsnmp-perl
  libwireshark-data libwireshark3 libwiretap3 libwsutil3 perl-tk smistrip
  wireshark-common
Paquets suggérés :
  wireshark-doc
Les NOUVEAUX paquets suivants seront installés :
  libc-ares2 liblua5.2-0 libportaudio2 libsmi2ldbl libsnmp-perl
  libwireshark-data libwireshark3 libwiretap3 libwsutil3 perl-tk smistrip snmp
  snmp-mibs-downloader snmpd tkmib wireshark wireshark-common
0 mis à jour, 17 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 20,6 Mo dans les archives.
Après cette opération, 87,0 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] _
```

apt-get install snmp snmp-mibs-downloader snmpd tkmib

Lors de l'installation on pourra remarquer le téléchargement des MIBS et la création d'un compte "Debian-snmp" (Nom pouvant changer selon la distribution)

```
insacvl@VM-INSA:~$ tail /etc/passwd
nm-openvpn:x:114:121:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin
/nologin
avahi:x:115:122:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:116:123:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/no
login
speech-dispatcher:x:117:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/
false
pulse:x:118:124:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
hplip:x:119:7:HPLIP system user,,,:/var/run/hplip:/bin/false
geoclue:x:120:126::/var/lib/geoclue:/usr/sbin/nologin
insacvl:x:1000:1000:insacvl,,,:/home/insacvl:/bin/bash
sshd:x:121:65534::/run/sshd:/usr/sbin/nologin
Debian-snmp:x:122:128::/var/lib/snmp:/bin/false
```

4.4. Vérifier le bon fonctionnement du "Daemon Snmpd".

```
insacvl@VM-INSA:~$ service snmpd status
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/lib/systemd/system/snmpd.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2019-10-04 08:58:43 CEST; 11min ago
  Process: 831 ExecStartPre=/bin/mkdir -p /var/run/agentx (code=exited, status=0/SUCCESS)
 Main PID: 833 (snmpd)
```


```
 Tasks: 1 (limit: 4630)
 CGroup: /system.slice/snmpd.service
         └─833 /usr/sbin/snmpd -Lsd -Lf /dev/null -u Debian-snmp -g Debian-snmp -I -smux mteTrigger mteTriggerConf -f
oct. 04 08:58:43 VM-INSA systemd[1]: Starting Simple Network Management Protocol (SNMP) Daemon....
oct. 04 08:58:43 VM-INSA systemd[1]: Started Simple Network Management Protocol (SNMP) Daemon..
oct. 04 08:58:43 VM-INSA snmpd[833]: /etc/snmp/snmpd.conf: line 145: Warning: Unknown token: defaultMonitors.
oct. 04 08:58:43 VM-INSA snmpd[833]: /etc/snmp/snmpd.conf: line 147: Warning: Unknown token: linkUpDownNotifications.
oct. 04 08:58:43 VM-INSA snmpd[833]: Turning on AgentX master support.
oct. 04 08:58:43 VM-INSA snmpd[833]: NET-SNMP version 5.7.3
```

Vous remarquez deux “Warnings” venant du fichier “/etc/snmpd.conf” mais pas de souci, vous allez changer son contenu par la suite.

4.5. Arrêter la machine virtuelle

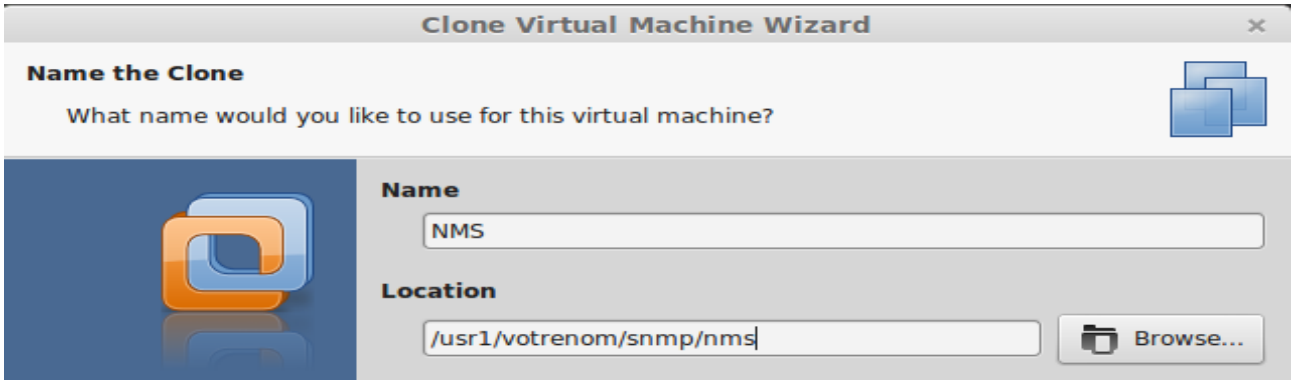
Tapez « Poweroff » dans un terminal

5. Création d'une machine de management NMS (Network Management Station) et d'une machine surveillée MS('Managed Station)

Le réseau sera composé d'une machine NMS (Network Management Station) et d'une station à surveiller qui contiendra l'agent à surveiller que l'on appellera MS (Managed Station).

MS sera la machine virtuelle obtenue au paragraphe 2.

Pour NMS on créera un clone « linké » de MS. Attention !!!! : ne mettez pas cette machine dans votre « home directory » !!!!



Prenez soin de régler « vmware workstation » de manière à voir apparaître dans les onglets des machines virtuelles les mots « MS » et « NMS » ainsi que leur adresse IP respective

6. Configuration de l’agent « SNMP »

6.1. Arrêter la machine « NMS » et actionnez « MS »

6.2. Vérifier que le démon snmpd s'exécute sur MS

```
root@insacvl-virtual-machine:~# service snmpd status
 * snmpd is running
```

Faites afficher le port où le démon snmpd attend, notez ce port.

```
insacvl-mint insacvl # netstat -anp|grep snmp
udp        0      0 127.0.0.1:161           0.0.0.0:*                           1500/snmpd
udp        0      0 0.0.0.0:54657           0.0.0.0:*                           1500/snmpd
unix  2      STREAM     LISTENING     14388    1500/snmpd /var/agentx/master
unix  2      [ ]         DGRAM                    14386    1500/snmpd
```

7. Régler MS pour pouvoir l'interroger à partir de NMS ICI

7.1. Sauvegarder le fichier snmpd.conf original.

cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.org

7.2. Personnaliser le fichier « /etc/snmp/snmpd.conf »

En adaptant le fichier snmpd.conf joint en annexe 13 à vos besoins, personnalisez votre « /etc/snmp/snmpd.conf ».

Vous pouvez trouver ce fichier sur « https://celene.insa-cvl.fr », cours sti4a administration réseaux ou dans la ressource
« \\freenas\partage\mszpieg\ snmpd_sample.conf»
Demandez au service « snmpd » de relire son fichier de configuration.

```
root@VM-INSA:/home/insacvl# systemctl daemon-reload
root@VM-INSA:/home/insacvl# systemctl restart snmpd.service
root@VM-INSA:/home/insacvl# tail /var/log/syslog
Oct  6 14:09:25 VM-INSA systemd[1]: Reloading.
Oct  6 14:09:30 VM-INSA snmpd[3483]: Received TERM or STOP signal...  shutting down...
Oct  6 14:09:30 VM-INSA systemd[1]: Stopping Simple Network Management Protocol (SNMP) Daemon...
Oct  6 14:09:30 VM-INSA systemd[1]: Stopped Simple Network Management Protocol (SNMP) Daemon..
Oct  6 14:09:30 VM-INSA systemd[1]: Starting Simple Network Management Protocol (SNMP) Daemon...
Oct  6 14:09:30 VM-INSA systemd[1]: Started Simple Network Management Protocol (SNMP) Daemon..
Oct  6 14:09:30 VM-INSA snmpd[3574]: NET-SNMP version 5.7.3
root@VM-INSA:/home/insacvl#
```

Si des erreurs apparaissent, corrigez votre fichier « snmpd.conf »

8. Parcours des MIBs

8.1. Premier parcours des MIBs

On va parcourir les MIBS avec la commande « snmpwalk »

```
root@insacvl-virtual-machine:~# snmpwalk -v1 -c sz localhost|more
iso.3.6.1.2.1.1.1.0 = STRING: "Linux insacvl-virtual-machine 3.13.0-
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: (32961) 0:05:29.61
iso.3.6.1.2.1.1.4.0 = STRING: "root"
iso.3.6.1.2.1.1.5.0 = STRING: "insacvl-virtual-machine"
iso.3.6.1.2.1.1.6.0 = STRING: "Unknown"
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.3.6.1.6.3.11.3.1.1
```

Comprenez les paramètres de la commande « snmpwalk »

Vous pouvez remarquer que les éléments des MIBS apparaissent sous forme brute, c'est-à-dire que l'on voit leur OID. Il est possible de faire une traduction vers des chaînes de caractères, c'est plus explicite.

8.2. Traduire les OID en chaînes de caractères.

Dans le fichier « /etc/snmp/snmp.conf », attention !!!! le nom du fichier est « snmp.conf » qui est utilisé par les clients snmp, et non « snmp**d**.conf » qui lui est utilisé par l'agent « snmp ».

Mettre la dernière ligne de ce fichier en commentaire, celle qui contient le mot

```
# As the snmp packages come without MIB files due to license reasons, loading
# of MIBs is disabled by default. If you added the MIBs you can reenable
# loading them by commenting out the following line.
#mibs :
```

« mibs ». La raison de ce fonctionnement est écrite dans le fichier en question sur les trois premières lignes.
Recommencez la ligne de commande du paragraphe : 8.1

Vous pouvez alors constater que les OID ont été remplacés par des chaînes de caractères plus explicites

```
root@insacvl-virtual-machine:~# snmpwalk -v1 -c sz localhost|more
SNMPv2-MIB::sysDescr.0 = STRING: Linux insacvl-virtual-machine 3.13.0-35-generic
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (104999) 0:17:29.99
SNMPv2-MIB::sysContact.0 = STRING: root
SNMPv2-MIB::sysName.0 = STRING: insacvl-virtual-machine
SNMPv2-MIB::sysLocation.0 = STRING: Unknown
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORID.1 = OID: SNMP-MPD-MIB::snmpMPDCompliance
```

8.3. Mettre « tcpdump » en action.

Mettez « tcpdump » en action et capturez les paquets afin de pouvoir les visualiser sous wireshark en générant le fichier « snmpd.cap »

On mettra un filtre de manière à ne capturer que les paquets émis ou reçus sur le port « snmpd » et sur l'interface « loopback », et on enregistrera ces paquets dans « snmpd.cap »

8.4. En utilisant snmpwalk, chercher un nœud de la MIB appelé « sysDescr » .

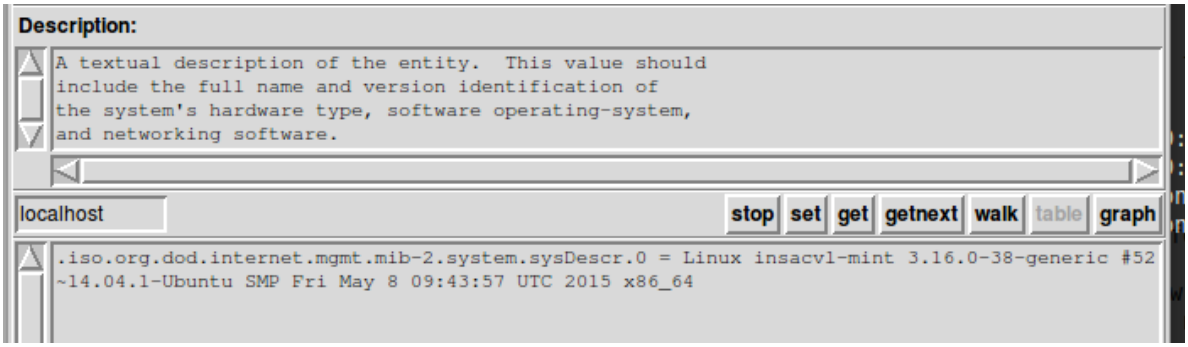
En utilisant snmpwalk et pendant que « tcpdump » capture, cherchez un nœud de la MIB appelé « sysDescr», sur la machine MS à partir de la machine elle-même.

8.5. Editer le fichier de capture

Éditez avec « wireshark » le fichier « snmpd.cap » ainsi obtenu et vérifiez que c'est bien la version 1 de snmp qui a fait la requête.

8.6. Utiliser le « browser » de MIB « tkmib »

En utilisant « tkmib » faites un « get » sur « sysDescr ». Remarque attention !!! dans les options mettez bien la communauté « sz » et n'oubliez pas de régler correctement **le suffixe de votre « OID »** pour obtenir la bonne chaîne de caractères.



8.7. Refaire les questions 8.3 à 8.6 mais à partir de NMS en consultant la MIB de MS

Attention il faut absolument commenter la ligne « mibs : » qui se trouve dans /etc/snmp/snmp.conf de NMS pour que cela fonctionne !!!

mibs :

De plus le fichier « /etc/snmp/snmpd.conf » de la **VM « MS »** doit être modifier pour être conforme à l'adresse réseau de votre « LAN ».

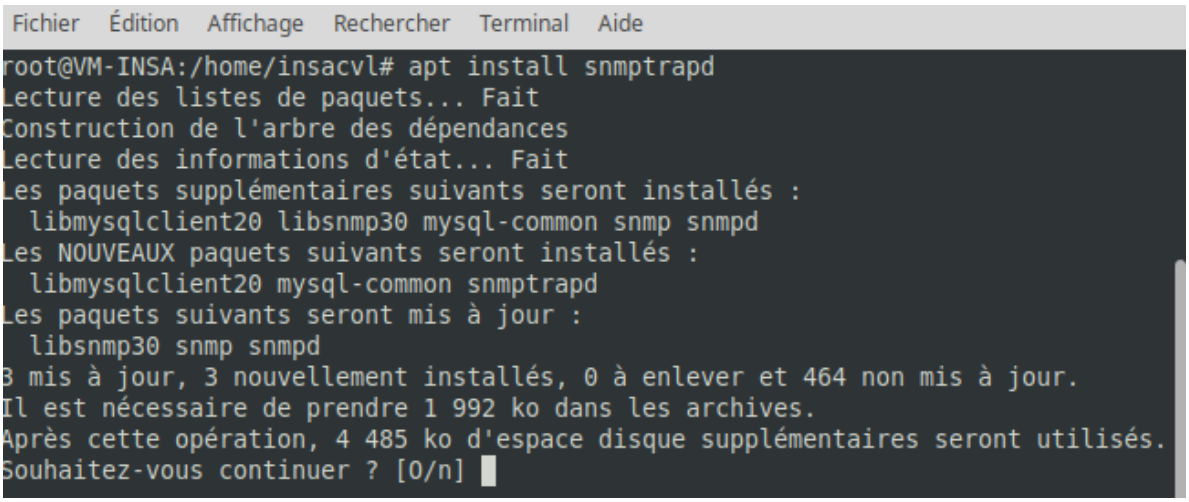
8.8. Editer , sur NMS, le contenu du fichier « snmpd.cap »

Que constatez-vous par rapport aux données que vous avez mises dans snmpd.conf ?

Notez la présence des « OID »..

9. Préparer le démon « snmptrapd » et gérer l'émission de l'alerte « snmp »

Revenez sur MS et téléchargez le paquet snmptrapd



9.1. Modifier les lignes de « /lib/systemd/system/snmpd.service ».

Rappel : pour un système utilisant « SystemVinit » c'est le fichier « /etc/default/snmpd.conf » qui est concerné !!!

Pour vous, il est probable que ce soit le fichier :

« /lib/systemd/system/snmpd.service »

Modifiez la ligne « Environment="MIBS=" » en Environment="MIBS=UCD-SNMP-MIB"

Ajoutez la ligne : PIDFile=/var/run/snmpd.pid et modifiez la ligne « ExecStart » comme suit :

```
ExecStart=/usr/sbin/snmpd -p /var/run/snmpd.pid -Lsd -Lf /dev/null -u Debian-snmp -g Debian-snmp -f
```

```
[Unit]
Description=Simple Network Management Protocol (SNMP) Daemon.
After=network.target
ConditionPathExists=/etc/snmp/snmpd.conf

[Service]
Environment="MIBSDIR=/usr/share/snmp/mibs:/usr/share/snmp/mibs/iana:/usr/share/snmp/mibs/ietf:/usr/share/mibs/site:/usr/share/snmp/mibs:/usr/share/mibs/iana:/usr/share/
mibs/ietf:/usr/share/mibs/netsnmp"
Environment="MIBS="
Type=simple
PIDFile=/var/run/snmpd.pid
ExecStartPre=/bin/mkdir -p /var/run/agentx
ExecStart=/usr/sbin/snmpd -Lsd -Lf /dev/null -u Debian-snmp -g Debian-snmp -I -smux,mteTrigger,mteTriggerConf -f
#ExecStart=/usr/sbin/snmpd -p /var/run/snmpd.pid -Lsd -Lf /dev/null -u Debian-snmp -g Debian-snmp -f
ExecReload=/bin/kill -HUP $MAINPID

[Install]
WantedBy=multi-user.target
~
```

9.2. Vérifier le démarrage du démon snmptrapd

Activez « snmptrapd » à chaque redémarrage du système :

```
root@VM-INSA:/home/insacvl# systemctl enable snmptrapd.service
Synchronizing state of snmptrapd.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable snmptrapd
```

Remettez le service « snmptrapd » en route afin qu'il relise les fichiers de configuration.

Vérifiez que les deux démons snmpd et snmptrapd sont actionnés chacun sur leur port respectif.

```
root@VM-INSA:/home/insacvl# systemctl daemon-reload
root@VM-INSA:/home/insacvl# systemctl restart snmptrapd
root@VM-INSA:/home/insacvl# tail /var/log/syslog
Oct  6 14:49:02 VM-INSA kernel: [ 8117.283926] systemd[1]: Started CUPS Scheduler.
Oct  6 14:49:02 VM-INSA kernel: [ 8117.283977] systemd[1]: Started ACPI event daemon.
Oct  6 14:50:34 VM-INSA systemd[1]: message repeated 3 times: [ Reloading.]
Oct  6 14:50:40 VM-INSA snmptrapd[5187]: 2019-10-06 14:50:40 NET-SNMP version 5.7.3 Stopped.
Oct  6 14:50:40 VM-INSA systemd[1]: Stopping Simple Network Management Protocol (SNMP) Trap Daemon....
Oct  6 14:50:40 VM-INSA snmptrapd[5187]: Stopping snmptrapd
Oct  6 14:50:40 VM-INSA systemd[1]: Stopped Simple Network Management Protocol (SNMP) Trap Daemon..
Oct  6 14:50:40 VM-INSA systemd[1]: Started Simple Network Management Protocol (SNMP) Trap Daemon..
Oct  6 14:50:40 VM-INSA snmptrapd[5831]: Warning: no access control information configured.#012  (Config search path: /etc/snmp:/usr/share/snmp
:/usr/lib/x86_64-linux-gnu/snmp)#012This receiver will *NOT* accept any incoming notifications.
Oct  6 14:50:40 VM-INSA snmptrapd[5831]: NET-SNMP version 5.7.3
root@VM-INSA:/home/insacvl# systemctl status snmptrapd.service
● snmptrapd.service - Simple Network Management Protocol (SNMP) Trap Daemon.
   Loaded: loaded (/lib/systemd/system/snmptrapd.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2019-10-06 14:50:40 CEST; 1min 18s ago
 Main PID: 5831 (snmptrapd)
    Tasks: 1 (limit: 4630)
   CGroup: /system.slice/snmptrapd.service
           └─5831 /usr/sbin/snmptrapd -Lsd -f

oct. 06 14:50:40 VM-INSA systemd[1]: Started Simple Network Management Protocol (SNMP) Trap Daemon..
oct. 06 14:50:40 VM-INSA snmptrapd[5831]: Warning: no access control information configured.
                                            (Config search path: /etc/snmp:/usr/share/snmp:/usr/lib/x86_64-linux-gnu/snmp)
                                          This receiver will *NOT* accept any incoming notifications.
oct. 06 14:50:40 VM-INSA snmptrapd[5831]: NET-SNMP version 5.7.3
root@VM-INSA:/home/insacvl#
```

Vous pouvez remarquer que vous obtenez un « Warning » pour le fichier de configuration de « snmptrapd » :

Warning: no access control information configured.

(Config search path:/etc/snmp:/usr/share/snmp:/usr/lib/x86_64-linux-gnu/snmp)

C'est normal vous ne l'avez pas encore configuré, vous le ferez par la suite.

Et pour « snmpd » :

```
root@VM-INSA:/home/insacvl# systemctl restart snmpd.service
root@VM-INSA:/home/insacvl# systemctl status snmpd.service
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/lib/systemd/system/snmpd.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2019-10-06 14:59:46 CEST; 7s ago
  Process: 5900 ExecStartPre=/bin/mkdir -p /var/run/agentx (code=exited, status=0/SUCCESS)
 Main PID: 5901 (snmpd)
    Tasks: 1 (limit: 4630)
   CGroup: /system.slice/snmpd.service
           └─5901 /usr/sbin/snmpd -p /var/run/snmpd -Lsd -Lf /dev/null -u Debian-snmp -g Debian-snmp -f

oct. 06 14:59:46 VM-INSA systemd[1]: Starting Simple Network Management Protocol (SNMP) Daemon....
oct. 06 14:59:46 VM-INSA systemd[1]: Started Simple Network Management Protocol (SNMP) Daemon..
oct. 06 14:59:46 VM-INSA snmpd[5901]: NET-SNMP version 5.7.3
root@VM-INSA:/home/insacvl#
```

9.3. Préparation du fichier « /etc/snmp/snmptrapd.conf »

On peut remarquer un « warning » : « no access control information configured. »

Qu'en pensez-vous ? Corrigez le problème. Inspirez-vous de l'annexe 13.2 et comprenez son contenu.

Testez le bon fonctionnement de vos modifications :

Résultat :

```
root@VM-INSA:/home/insacvl# systemctl restart snmptrapd.service
root@VM-INSA:/home/insacvl# systemctl status snmptrapd.service
● snmptrapd.service - Simple Network Management Protocol (SNMP) Trap Daemon.
   Loaded: loaded (/lib/systemd/system/snmptrapd.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2019-10-06 15:05:42 CEST; 10s ago
 Main PID: 5921 (snmptrapd)
    Tasks: 1 (limit: 4630)
   CGroup: /system.slice/snmptrapd.service
           └─5921 /usr/sbin/snmptrapd -Lsd -f

oct. 06 15:05:42 VM-INSA systemd[1]: Started Simple Network Management Protocol (SNMP) Trap Daemon..
oct. 06 15:05:42 VM-INSA snmptrapd[5921]: NET-SNMP version 5.7.3
root@VM-INSA:/home/insacvl#
```

10. Surveillance de la taille d'un fichier

10.1. Créer un script « /usr/bin/sz.sh »

Créez un script « /usr/bin/sz.sh » comme joint en annexe paragraphe 13.3.
!!!!! N'oubliez pas de lui donner les droits 755

10.2. Préparer le fichier à surveiller :

mkdir -p /home/szpieg

touch /home/szpieg/essai

chmod 755 -R /home/szpieg

10.3. Activer les lignes de surveillance du fichier dans snmpd.conf.

Dans le fichier snmpd.conf ajoutez les lignes suivantes :

```
monitor -S -r 1  -o fileName -o fileErrorMsg "fileTable" fileErrorFlag != 0
file  /home/szpieg/essai 2
rwuser sz
```


```
iquerySecName sz
agentSecName sz
```

Attention : si le compte utilisateur (ici sz) n'est pas créé correctement des erreurs du genre

```
4804705:Oct  5 14:21:26 VM-INSA snmpd[871]: disman:event:trigger:monitor:
4804771-Oct  5 14:21:26 VM-INSA snmpd[871]: Trigger query (walk) failed: 16
4804839-Oct  5 14:21:26 VM-INSA snmpd[871]: failed to run mteTrigger query
```

apparaissent ce qui peut compliquer votre recherche lors de votre travail de débogage !

10.4. Relancer la machine.

Faites un « reboot » afin de vérifier que tous les services démarrent correctement à la mise en route de la VM.

```
root@VM-INSA:/home/insacvl# systemctl status snmpd.service
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/lib/systemd/system/snmpd.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2019-10-06 15:19:46 CEST; 6min ago
  Process: 915 ExecStartPre=/bin/mkdir -p /var/run/agentx (code=exited, status=0/SUCCESS)
 Main PID: 916 (snmpd)
    Tasks: 1 (limit: 4630)
   CGroup: /system.slice/snmpd.service
           └─916 /usr/sbin/snmpd -p /var/run/snmpd -Lsd -Lf /dev/null -u Debian-snmp -g Debian-snmp -f

oct. 06 15:23:59 VM-INSA snmpd[916]: Connection from UDP: [127.0.0.1]:47422->[127.0.0.1]:161
oct. 06 15:23:59 VM-INSA snmpd[916]: Connection from UDP: [127.0.0.1]:47422->[127.0.0.1]:161
root@VM-INSA:/home/insacvl# systemctl status snmptrapd.service
● snmptrapd.service - Simple Network Management Protocol (SNMP) Trap Daemon.
   Loaded: loaded (/lib/systemd/system/snmptrapd.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2019-10-06 15:19:46 CEST; 6min ago
 Main PID: 911 (snmptrapd)
    Tasks: 1 (limit: 4630)
   CGroup: /system.slice/snmptrapd.service
           └─911 /usr/sbin/snmptrapd -Lsd -f

oct. 06 15:19:46 VM-INSA systemd[1]: Started Simple Network Management Protocol (SNMP) Trap Daemon..
oct. 06 15:19:47 VM-INSA snmptrapd[911]: NET-SNMP version 5.7.3
```

10.5. Vérification de la bonne prise en compte, dans la MIB, du fichier « essai » à surveiller.

Saisissez la ligne de commande ci-contre :

```
root@VM-INSA:/home/insacvl# snmpwalk -c sz -v1 localhost FileTable
UCD-SNMP-MIB::fileIndex.1 = INTEGER: 1
UCD-SNMP-MIB::fileName.1 = STRING: /home/szpieg/essai
UCD-SNMP-MIB::fileSize.1 = INTEGER: 0 kB
UCD-SNMP-MIB::fileMax.1 = INTEGER: 2 kB
UCD-SNMP-MIB::fileErrorFlag.1 = INTEGER: noError(0)
UCD-SNMP-MIB::fileErrorMsg.1 = STRING:
root@VM-INSA:/home/insacvl#
```

Vérifiez que vos résultats sont identiques.

Bien que tout semble correct, l'agent « SNMP » ne générera aucun événement car il faut activer le paramètre « trapsink » dans le fichier « /etc/snmp/snmpd.conf »

Donc ajoutez, dans ce fichier, la ligne :

```
trapsink localhost sz
```

Puis redémarrez le service « snmpd »

10.6. Faire varier la taille du fichier « /home/szpieg/essai »

Faites varier le fichier /home/szpieg/essai en faisant varier sa taille alternativement d'une valeur inférieure à 4Ko à une valeur supérieure à 4Ko (ATTENTION snmp

arrondit la taille du fichier au multiple de 2Ko inférieur, donc l'alerte ne sera effective que si le fichier copié à une taille supérieure ou égale à 4Ko !!!)

Exemple de fichier test.sh :

```
while true
do
echo bonjour >
/home/szpieg/essai
sleep 2
cp /etc/wgetrc
/home/szpieg/essai
sleep 2
done
```

Faites fonctionner votre script en arrière plan :

```
./testsz.sh&
```

Puis lancez la commande suivante :

```
watch -d snmpwalk -c sz -v1 localhost FileTable
```

Vous devriez voir la taille du fichier « /home/szpieg/essai » varier.

Arrêtez la commande « watch » mais pas la commande « ./testsz.sh& »

Visualisez le contenu du fichier /tmp/snmp.trap :

```
watch -d tail -n2  /tmp/snmp.trap
```

Une « trap » doit apparaître toutes les 4 secondes.

10.7. Vérifier l'arrivée d'alertes

Chaque alerte est reportée dans le fichier « syslog » donc un « tail /var/log/syslog » doit vous donner le résultat suivant :

```
root@VM-INSA:/home/insacvl# tail /var/log/syslog |grep snmptrapd
Oct  6 15:46:13 VM-INSA snmptrapd[911]: 2019-10-06 15:46:13 VM-INSA [192.168.37.141] (via UDP: [127.0.0.1]:58787->[127.0.0.1]:162) TRAP, SNMP v1, community sz#012#011DI
SMAN-EVENT-MIB::dismanEventMIBNotificationPrefix Enterprise Specific Trap (DISMAN-EVENT-MIB::mteTriggerFired) Uptime: 0:03:14.16#012#011DISMAN-EVENT-MIB::mteHotTrigger.
0 = STRING: fileTable#011DISMAN-EVENT-MIB::mteHotTargetName.0 = STRING: #011DISMAN-EVENT-MIB::mteHotContextName.0 = STRING: #011DISMAN-EVENT-MIB::mteHotOID.0 = OID: UCD
-SNMP-MIB::fileErrorFlag.1#011DISMAN-EVENT-MIB::mteHotValue.0 = INTEGER: 1#011UCD-SNMP-MIB::fileName.1 = STRING: /home/szpieg/essai#011UCD-SNMP-MIB::fileErrorMsg.1 = ST
RING: /home/szpieg/essai: size exceeds 2kb (= 4kb)
Oct  6 15:46:17 VM-INSA snmptrapd[911]: 2019-10-06 15:46:17 VM-INSA [192.168.37.141] (via UDP: [127.0.0.1]:58787->[127.0.0.1]:162) TRAP, SNMP v1, community sz#012#011DI
SMAN-EVENT-MIB::dismanEventMIBNotificationPrefix Enterprise Specific Trap (DISMAN-EVENT-MIB::mteTriggerFired) Uptime: 0:03:18.16#012#011DISMAN-EVENT-MIB::mteHotTrigger.
0 = STRING: fileTable#011DISMAN-EVENT-MIB::mteHotTargetName.0 = STRING: #011DISMAN-EVENT-MIB::mteHotContextName.0 = STRING: #011DISMAN-EVENT-MIB::mteHotOID.0 = OID: UCD
-SNMP-MIB::fileErrorFlag.1#011DISMAN-EVENT-MIB::mteHotValue.0 = INTEGER: 1#011UCD-SNMP-MIB::fileName.1 = STRING: /home/szpieg/essai#011UCD-SNMP-MIB::fileErrorMsg.1 = ST
RING: /home/szpieg/essai: size exceeds 2kb (= 4kb)
Oct  6 15:46:21 VM-INSA snmptrapd[911]: 2019-10-06 15:46:21 VM-INSA [192.168.37.141] (via UDP: [127.0.0.1]:58787->[127.0.0.1]:162) TRAP, SNMP v1, community sz#012#011DI
SMAN-EVENT-MIB::dismanEventMIBNotificationPrefix Enterprise Specific Trap (DISMAN-EVENT-MIB::mteTriggerFired) Uptime: 0:03:22.16#012#011DISMAN-EVENT-MIB::mteHotTrigger.
0 = STRING: fileTable#011DISMAN-EVENT-MIB::mteHotTargetName.0 = STRING: #011DISMAN-EVENT-MIB::mteHotContextName.0 = STRING: #011DISMAN-EVENT-MIB::mteHotOID.0 = OID: UCD
-SNMP-MIB::fileErrorFlag.1#011DISMAN-EVENT-MIB::mteHotValue.0 = INTEGER: 1#011UCD-SNMP-MIB::fileName.1 = STRING: /home/szpieg/essai#011UCD-SNMP-MIB::fileErrorMsg.1 = ST
RING: /home/szpieg/essai: size exceeds 2kb (= 4kb)
root@VM-INSA:/home/insacvl#
```

De plus chaque alerte déclenche le script /usr/bin/sz.sh par « snmptrapd », donc la date de chaque alerte doit être inscrite dans /tmp/snmp.trap

```
root@VM-INSA:/home/insacvl# tail /tmp/snmp.trap
dimanche 6 octobre 2019, 15:45:45 (UTC+0200)
dimanche 6 octobre 2019, 15:45:49 (UTC+0200)
dimanche 6 octobre 2019, 15:45:53 (UTC+0200)
dimanche 6 octobre 2019, 15:45:57 (UTC+0200)
dimanche 6 octobre 2019, 15:46:01 (UTC+0200)
```


10.8. Mettre « tcpdump » en action et capturer les paquets.

On mettra un filtre de manière à ne capturer que les paquets émis ou « éventuellement » reçus sur le port « snmptrapd » et sur l'interface « loopback », on enregistrera ces paquets dans « snmptrapd.cap »

10.9. Analyser les paquets d'alerte

Mettez fin au processus de capture « tcpdump » et analysez le fichier « snmptrapd.cap ».

10.10. Envoyer ces alertes sur NMS

A vous de jouer ...

10.11. Parcourir la MIB en version SNMPv2c

10.12. Parcourir la MIB en version SNMPv3

Modifiez le contenu de snmpd.conf afin de pouvoir interroger la MIB en snmpv3 avec une authentification md5.
Avant toute modification, sauvegardez le fichier précédant dans « /etc/snmp/snmpd.conf.V1 »

10.13. Mettre « tcpdump » en action.

Mettez « tcpdump » en action et capturez les paquets afin de pouvoir les visualiser sous wireshark en générant le fichier « snmpv2c.cap »

11. SNMPv3 authentification et cryptage

11.1. Créer des utilisateurs « SNMPv3 »

Arrêtez le démon « snmpd » puis ajoutez les lignes (Pour snmpv3) suivantes au fichier /etc/snmp/snmpd.conf.

```
file  /home/szpieg/essai 2

# Pour snmpv3
createUser user1
createUser user2 MD5 azertyuiop
createUser user3 MD5 azertyuiop DES azertyuiop

rouser user1 noauth 1.
rouser user2 auth 1.
rwuser user3 priv 1.
```

11.2. Interroger la MIB en « SNMPv3 »

Redémarrez le démon « snmpd »

Testez le bon fonctionnement avec les trois « users » comme ci-dessous :

```
insacvl-mint insacvl # snmpwalk -v 3 -u user1 localhost sysDescr
SNMPv2-MIB::sysDescr.0 = STRING: Linux insacvl-mint 3.16.0-38-generic #52~14.04.1-Ubuntu SMP Fri May 8 09:43:57 UTC 2015 x86_64
insacvl-mint insacvl # snmpwalk -v 3 -u user2 -a MD5 -A 'azertyuiop'  localhost -l auth sysDescr
SNMPv2-MIB::sysDescr.0 = STRING: Linux insacvl-mint 3.16.0-38-generic #52~14.04.1-Ubuntu SMP Fri May 8 09:43:57 UTC 2015 x86_64
insacvl-mint insacvl # snmpwalk -v 3 -u user3 -a MD5 -A 'azertyuiop' -x DES -X 'azertyuiop' -l authPriv localhost sysDescr
SNMPv2-MIB::sysDescr.0 = STRING: Linux insacvl-mint 3.16.0-38-generic #52~14.04.1-Ubuntu SMP Fri May 8 09:43:57 UTC 2015 x86_64
insacvl-mint insacvl #
```

11.3. Capturer les paquets.

Faites trois fichiers de capture des paquets avec « tcpdump », un par « user ».
Analysez le résultat avec « Wireshark ». Concluez !
Testez avec les algorithmes SHA et AES.

11.4. Protéger les pass-phrases et les secrets partagés

Visualisez le contenu du fichier /var/lib/snmp/snmpd.conf.
Que constatez-vous pour les différents « users » SNMPv3.
Retournez dans le fichier /etc/snmp/snmpd.conf et enlevez les lignes « createUser ». Redémarrez le démon « snmpd », les « users » SNMPv6 sont-ils toujours fonctionnels.Concluez.

11.5. Création utilisateurs SNMPv3 méthode alternative

Créez et testez un utilisateur « user4 » SNMPv3 en utilisant la commande « snmpusm ». USM → User-based Security Model.

12. View Access Control Model (VACM)

12.1. Limitation de la zone d'accès de la MIB

Dans « snmpd.conf » modifiez la vue « tout » comme suit :

```
#view tout    included  .1
view tout excluded .1
view tout included sysUpTime.0
#view tout included .1.3.6.1.2.1.92.1.3.2.1.9.7.100.101.102.97.117.108.116.1.2
#view tout included NOTIFICATION-LOG-MIB::nlmLogVariableIpAddressVal."default".1.2
#view tout included nlmLogVariableIpAddressVal."default".1.2
view tout included IpAddressVal
```

Dé-commentez alternativement les 4 dernières lignes, redémarrez à chaque fois le démon « snmpd » et faites un « snmpwalk ». Que constatez-vous ?
Pour les lignes où les valeurs « 1.2 » apparaissent en suffixe, testez-les sans le « 1.2 ». Que constatez vous ?

12.2. View et SNMPv3

Dans « snmpd.conf » ajoutez les lignes :

```
createUser user5 MD5 azertyuiop DES azertyuiop
rwuser user5 priv -V tout
```

Faites un « snmpwalk » avec le compte « user5 », que constatez-vous ?

12.3. Commande « snmpset »

Ajoutez à la vue « tout » la variable « sysName », modifiez cette variable avec « tkmib » et le compte « user5 »

13. Annexes

13.1. Fichier « snmpd.conf » exemple

```
#       sec.name  source          community
com2sec  local     localhost        sz
com2sec  localnet  192.168.241.0/24 public
# Second, map the security names into group names:

#               sec.model  sec.name
group  RWGroup    v1         local
group  ROGroup    v1         localnet

####
# Third, create a view for us to let the groups have rights to:

#           incl/excl subtree                          mask
view tout    included  .1

####
# Finally, grant the 2 groups access to the 1 view with different
# write permissions:
#                context sec.model sec.level match  read   write  notif
access ROGroup ""        v1       noauth    exact  tout     none   none
access RWGroup ""        v1       noauth    exact  tout     tout    none
#rwuser sz
#trapsink localhost sz
#agentSecName sz
#monitor -S -r 1  -o fileName -o fileErrorMsg "fileTable" fileErrorFlag != 0
#file  /home/szpieg/essai 2
```

13.2. Fichier « /etc/snmp/snmptrapd.conf »

traphandle default /usr/bin/sz.sh
disableAuthorization yes
pidFile /var/run/snmptrapd.pid

13.3. Contenu du fichier « /usr/bin/sz.sh »

date >> /tmp/snmp.trap

13.4. Afficher les comptes snmpV3.

Il faut un compte user ici “sz” bien configuré.

root@VM-INSA:/home/insacvl# snmpwalk -v3 -csz -usz -a MD5 -A 'azertyuiop' -x DES -X 'azertyuiop' -l authPriv localhost .1.3.6.1.6.3.15.1.2.2.1.3
SNMP-USER-BASED-SM-MIB::usmUserSecurityName."........ps..]...."."sz" = STRING: sz
SNMP-USER-BASED-SM-MIB::usmUserSecurityName."........ps..]...."."ceciestuntest" = STRING: ceciestuntest