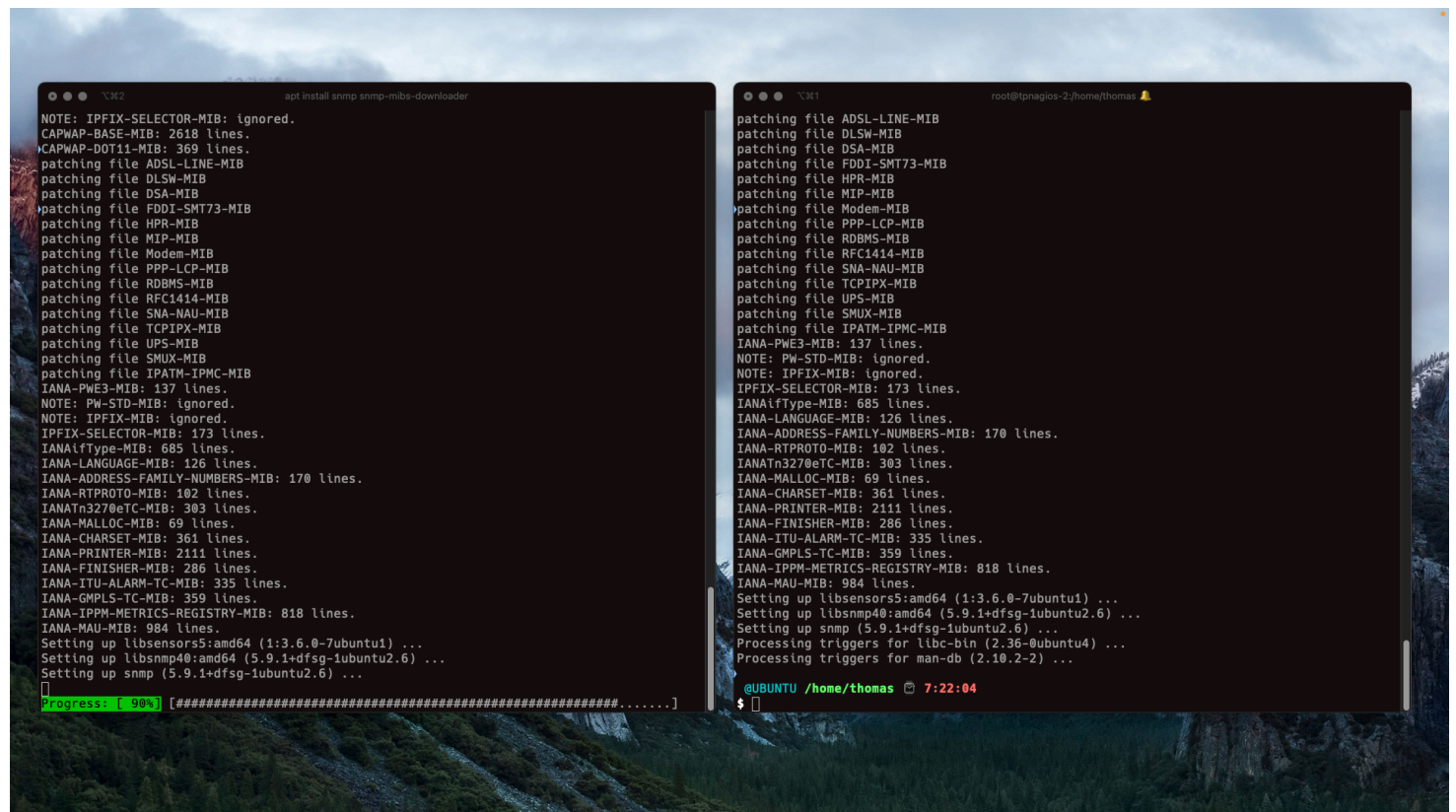


Supervision - Rendu TP02

TP effectué par David TEJEDA et Thomas PEUGNET.

Installation des paquets



```
NOTE: IPFIX-SELECTOR-MIB: ignored.
CAPWAP-BASE-MIB: 2618 lines.
CAPWAP-DOT11-MIB: 369 lines.
patching file ADSL-LINE-MIB
patching file DSLW-MIB
patching file DSA-MIB
patching file FDDI-SMT73-MIB
patching file HPR-MIB
patching file MIP-MIB
patching file Modem-MIB
patching file PPP-LCP-MIB
patching file RDBMS-MIB
patching file RFC1414-MIB
patching file SNA-NAU-MIB
patching file TCPIP-MIB
patching file UPS-MIB
patching file SMUX-MIB
patching file IPATM-IPMC-MIB
IANA-PWE3-MIB: 137 lines.
NOTE: PW-STD-MIB: ignored.
NOTE: IPFIX-MIB: ignored.
IPFIX-SELECTOR-MIB: 173 lines.
IANAifType-MIB: 685 lines.
IANA-LANGUAGE-MIB: 126 lines.
IANA-ADDRESS-FAMILY-NUMBERS-MIB: 170 lines.
IANA-RTPROTO-MIB: 102 lines.
IANATn3270eTC-MIB: 303 lines.
IANA-MALLOC-MIB: 69 lines.
IANA-CHARSET-MIB: 361 lines.
IANA-PRINTER-MIB: 2111 lines.
IANA-FINISHER-MIB: 286 lines.
IANA-ITU-ALARM-TC-MIB: 335 lines.
IANA-GMPLS-TC-MIB: 359 lines.
IANA-IPPM-METRICS-REGISTRY-MIB: 818 lines.
IANA-MAU-MIB: 984 lines.
Setting up libensors5:amd64 (1:3.6.0-7ubuntu1) ...
Setting up libsnmp40:amd64 (5.9.1+dfsg-1ubuntu2.6) ...
Setting up snmp (5.9.1+dfsg-1ubuntu2.6) ...
Progress: [ 90%] [#####.....]
```

```
patching file ADSL-LINE-MIB
patching file DSLW-MIB
patching file DSA-MIB
patching file FDDI-SMT73-MIB
patching file HPR-MIB
patching file MIP-MIB
patching file Modem-MIB
patching file PPP-LCP-MIB
patching file RDBMS-MIB
patching file RFC1414-MIB
patching file SNA-NAU-MIB
patching file TCPIP-MIB
patching file UPS-MIB
patching file SMUX-MIB
patching file IPATM-IPMC-MIB
IANA-PWE3-MIB: 137 lines.
NOTE: PW-STD-MIB: ignored.
NOTE: IPFIX-MIB: ignored.
IPFIX-SELECTOR-MIB: 173 lines.
IANAifType-MIB: 685 lines.
IANA-LANGUAGE-MIB: 126 lines.
IANA-ADDRESS-FAMILY-NUMBERS-MIB: 170 lines.
IANA-RTPROTO-MIB: 102 lines.
IANATn3270eTC-MIB: 303 lines.
IANA-MALLOC-MIB: 69 lines.
IANA-CHARSET-MIB: 361 lines.
IANA-PRINTER-MIB: 2111 lines.
IANA-FINISHER-MIB: 286 lines.
IANA-ITU-ALARM-TC-MIB: 335 lines.
IANA-GMPLS-TC-MIB: 359 lines.
IANA-IPPM-METRICS-REGISTRY-MIB: 818 lines.
IANA-MAU-MIB: 984 lines.
Setting up libensors5:amd64 (1:3.6.0-7ubuntu1) ...
Setting up libsnmp40:amd64 (5.9.1+dfsg-1ubuntu2.6) ...
Setting up snmp (5.9.1+dfsg-1ubuntu2.6) ...
Processing triggers for libc-bin (2.36-0ubuntu4) ...
Processing triggers for man-db (2.10.2-2) ...

@UBUNTU /home/thomas 7:22:04
$
```

A gauche, le manager, à droite l'agent.

Nous commentons la ligne `mibs :`


```
root@tpnagios-2:/etc/snmp

@UBUNTU ~ 7:26:24
$ cd /etc/snmp

@UBUNTU /etc/snmp 7:26:31
$ ls
snmp.conf  snmpd.conf  snmpd.conf.d

@UBUNTU /etc/snmp 7:26:33
$ cp snmpd.conf snmpd.conf.old

@UBUNTU /etc/snmp 7:26:43
$ echo "" > snmpd.conf

@UBUNTU /etc/snmp 7:26:49
$ vim snmpd.conf

@UBUNTU /etc/snmp 7:27:03
$ vim snmpd.conf

@UBUNTU /etc/snmp 7:27:05
$ cat snmpd.conf
agentAddress udp:161
rocommunity public
rwcommunity private

@UBUNTU /etc/snmp 7:27:12
$ systemctl restart snmpd

@UBUNTU /etc/snmp 7:27:32
$
```

Surveillance des processus

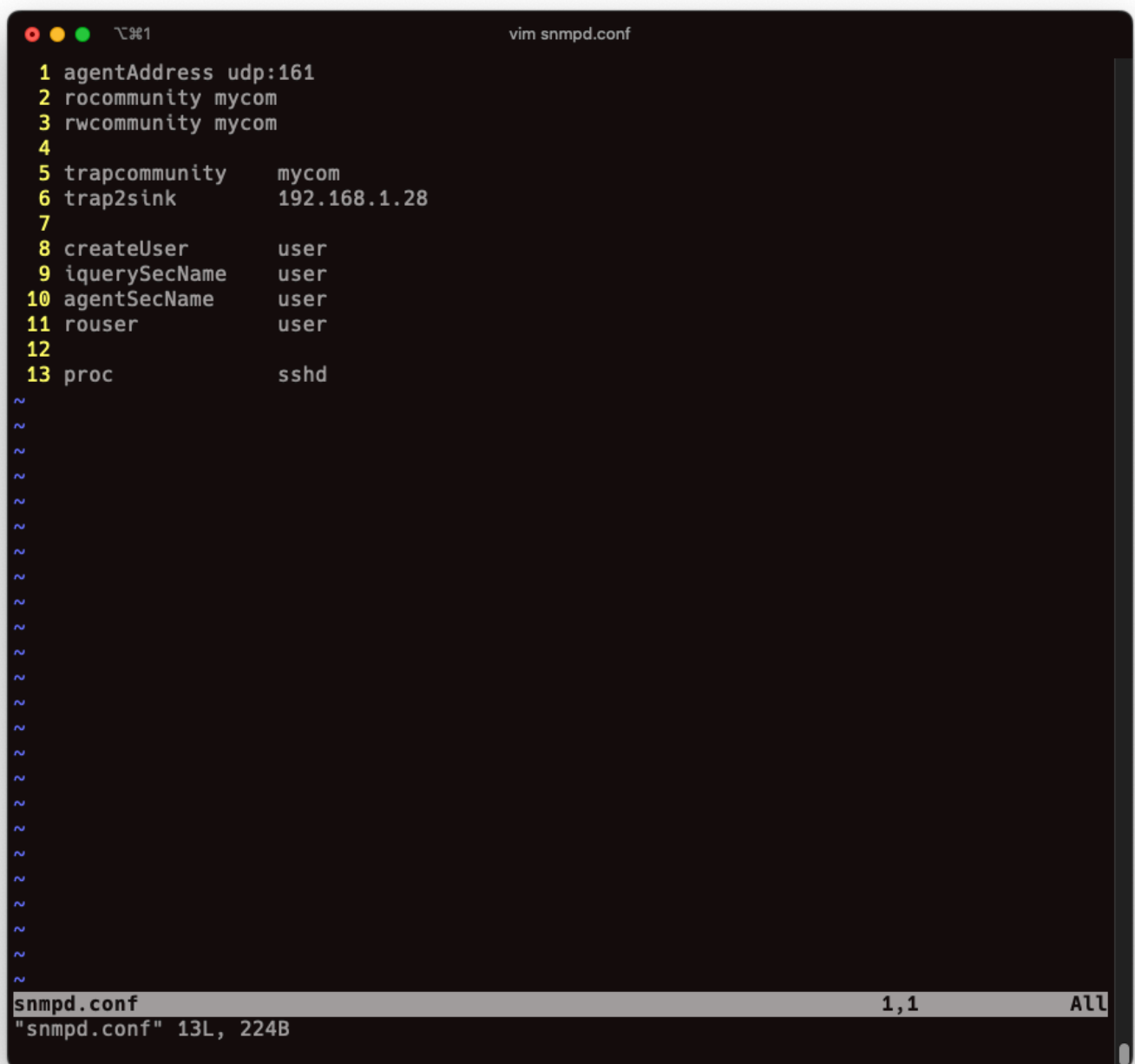
Nous configurons l'agent pour l'envoi de trap snmp au manager, en modifiant la configuration de `/etc/snmp/snmp.conf` sur l'agent.

```
agentAddress      udp:161
rocommunity       mycom
rwcommunity       mycom

trapcommunity     mycom
trap2sink         192.168.1.28

createUser        user
iquerySecName     user
agentSecName      user
rouser            user

proc              sshd
```



The screenshot shows a terminal window with a dark background. At the top, the title bar indicates the file being edited is `vim snmpd.conf`. The main area of the terminal displays the contents of the `snmpd.conf` file, with line numbers 1 through 13 on the left. The configuration is as follows:

```
1 agentAddress udp:161
2 rocommunity mycom
3 rwcommunity mycom
4
5 trapcommunity mycom
6 trap2sink 192.168.1.28
7
8 createUser user
9 iquerySecName user
10 agentSecName user
11 rouser user
12
13 proc sshd
```

Below line 13, there are several lines of tilde characters (~) representing empty lines in the file. At the bottom of the terminal, a status bar shows the filename `snmpd.conf`, the current line and column `1,1`, and the total number of lines and bytes `13L, 224B`.

Nous modifions ensuite le fichier de démarrage de notre service en modifiant la configuration de `/lib/systemd/system/snmpd.service`.

[Unit]

Description=Simple Network Management Protocol (SNMP) Daemon.

After=network.target

ConditionPathExists=/etc/snmp/snmpd.conf

[Service]

Type=notify

RuntimeDirectory=agentx

Next line was the original one

ExecStart=/usr/sbin/snmpd -LOW -u Debian-snmp -g Debian-snmp -I -
smux,mteTrigger,mteTriggerConf -f

ExecStart=/usr/sbin/snmpd -LOW -u Debian-snmp -g Debian-snmp -f

ExecReload=/bin/kill -HUP \$MAINPID

Environment="MIBS=ALL"

[Install]

WantedBy=multi-user.target


```
root@tpnagios-1:/etc/snmp

@UBUNTU /etc/snmp 8:06:38
$ snmpwalk 192.168.1.137 1.3.6.1.4.1.2021.2
UCD-SNMP-MIB::prIndex.1 = INTEGER: 1
UCD-SNMP-MIB::prNames.1 = STRING: sshd
UCD-SNMP-MIB::prMin.1 = INTEGER: 1
UCD-SNMP-MIB::prMax.1 = INTEGER: 0
UCD-SNMP-MIB::prCount.1 = INTEGER: 3
UCD-SNMP-MIB::prErrorFlag.1 = INTEGER: noError(0)
UCD-SNMP-MIB::prErrorMessage.1 = STRING:
UCD-SNMP-MIB::prErrFix.1 = INTEGER: noError(0)
UCD-SNMP-MIB::prErrFixCmd.1 = STRING:
>
@UBUNTU /etc/snmp 8:06:40
$
```

Dans le fichier de configuration de l'agent `snmpd.conf`, on ajoute le contenu suivant:

```
notificationEvent      trapService 1.2.3.1.4.1.1000.10.1 -o prNames -o prErrorMessage
monitor                -r 10 -e trapService "erreur service" prErrorFlag ≠ 0
```

Note: Les 2 VMs étant sur un Proxmox, le SSH n'est jamais complètement arrêté tant que nous sommes connectés dessus. Dans un souci de facilité de test sur ce TP, nous avons choisi de superviser le service `cron` en lieu et place de `sshd`.

Nous avons donc une configuration de `snmpd.conf` suivante :

```
agentAddress udp:161
rocommunity mycom
rwcommunity mycom

trapcommunity mycom
trap2sink 192.168.1.28
```

```

createUser user
iquerySecName user
agentSecName user
rouser user

proc cron

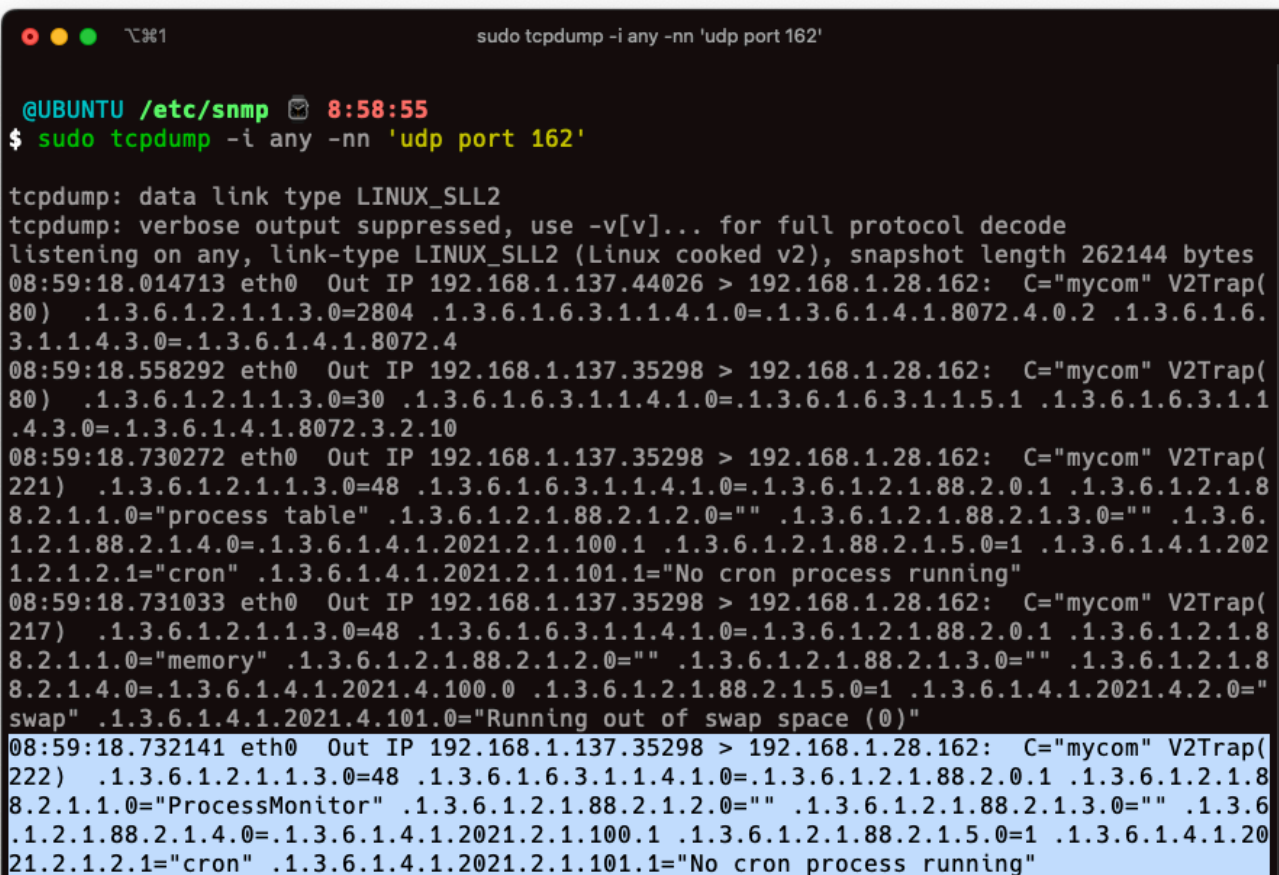
defaultMonitors yes
linkUpDownNotifications yes

monitor -r 5 -o prNames -o prErrorMessage "ProcessMonitor" prErrorFlag ≠ 0

```

Nous effectuons une capture sur l'agent et le manager avec `tcpdump` (Wireshark n'étant pas utilisable sur des VMs étant exclusivement en CLI).

On obtient le résultat suivant :



```

@UBUNTU /etc/snmp 8:58:55
$ sudo tcpdump -i any -nn 'udp port 162'

tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
08:59:18.014713 eth0 Out IP 192.168.1.137.44026 > 192.168.1.28.162: C="mycom" V2Trap(
80) .1.3.6.1.2.1.1.3.0=2804 .1.3.6.1.6.3.1.1.4.1.0=.1.3.6.1.4.1.8072.4.0.2 .1.3.6.1.6.
3.1.1.4.3.0=.1.3.6.1.4.1.8072.4
08:59:18.558292 eth0 Out IP 192.168.1.137.35298 > 192.168.1.28.162: C="mycom" V2Trap(
80) .1.3.6.1.2.1.1.3.0=30 .1.3.6.1.6.3.1.1.4.1.0=.1.3.6.1.6.3.1.1.5.1 .1.3.6.1.6.3.1.1
.4.3.0=.1.3.6.1.4.1.8072.3.2.10
08:59:18.730272 eth0 Out IP 192.168.1.137.35298 > 192.168.1.28.162: C="mycom" V2Trap(
221) .1.3.6.1.2.1.1.3.0=48 .1.3.6.1.6.3.1.1.4.1.0=.1.3.6.1.2.1.88.2.0.1 .1.3.6.1.2.1.8
8.2.1.1.0="process table" .1.3.6.1.2.1.88.2.1.2.0="" .1.3.6.1.2.1.88.2.1.3.0="" .1.3.6.
1.2.1.88.2.1.4.0=.1.3.6.1.4.1.2021.2.1.100.1 .1.3.6.1.2.1.88.2.1.5.0=1 .1.3.6.1.4.1.202
1.2.1.2.1="cron" .1.3.6.1.4.1.2021.2.1.101.1="No cron process running"
08:59:18.731033 eth0 Out IP 192.168.1.137.35298 > 192.168.1.28.162: C="mycom" V2Trap(
217) .1.3.6.1.2.1.1.3.0=48 .1.3.6.1.6.3.1.1.4.1.0=.1.3.6.1.2.1.88.2.0.1 .1.3.6.1.2.1.8
8.2.1.1.0="memory" .1.3.6.1.2.1.88.2.1.2.0="" .1.3.6.1.2.1.88.2.1.3.0="" .1.3.6.1.2.1.8
8.2.1.4.0=.1.3.6.1.4.1.2021.4.100.0 .1.3.6.1.2.1.88.2.1.5.0=1 .1.3.6.1.4.1.2021.4.2.0="
swap" .1.3.6.1.4.1.2021.4.101.0="Running out of swap space (0)"
08:59:18.732141 eth0 Out IP 192.168.1.137.35298 > 192.168.1.28.162: C="mycom" V2Trap(
222) .1.3.6.1.2.1.1.3.0=48 .1.3.6.1.6.3.1.1.4.1.0=.1.3.6.1.2.1.88.2.0.1 .1.3.6.1.2.1.8
8.2.1.1.0="ProcessMonitor" .1.3.6.1.2.1.88.2.1.2.0="" .1.3.6.1.2.1.88.2.1.3.0="" .1.3.6
.1.2.1.88.2.1.4.0=.1.3.6.1.4.1.2021.2.1.100.1 .1.3.6.1.2.1.88.2.1.5.0=1 .1.3.6.1.4.1.20
21.2.1.2.1="cron" .1.3.6.1.4.1.2021.2.1.101.1="No cron process running"

```


Pour répondre à une demande spécifique du TP concernant `sshd`, pour savoir que le nombre de processus `sshd` varie lors des connexions des utilisateurs, un regard à la commande nous explique tout.

De notre côté:

```
$ pgrep sshd
178
335
12185
12205
```

Surveillance du disque

Nous ajoutons la ligne suivante dans le fichier `snmpd.conf` de l'agent:

```
file /tmp/fileToWatch 10
```

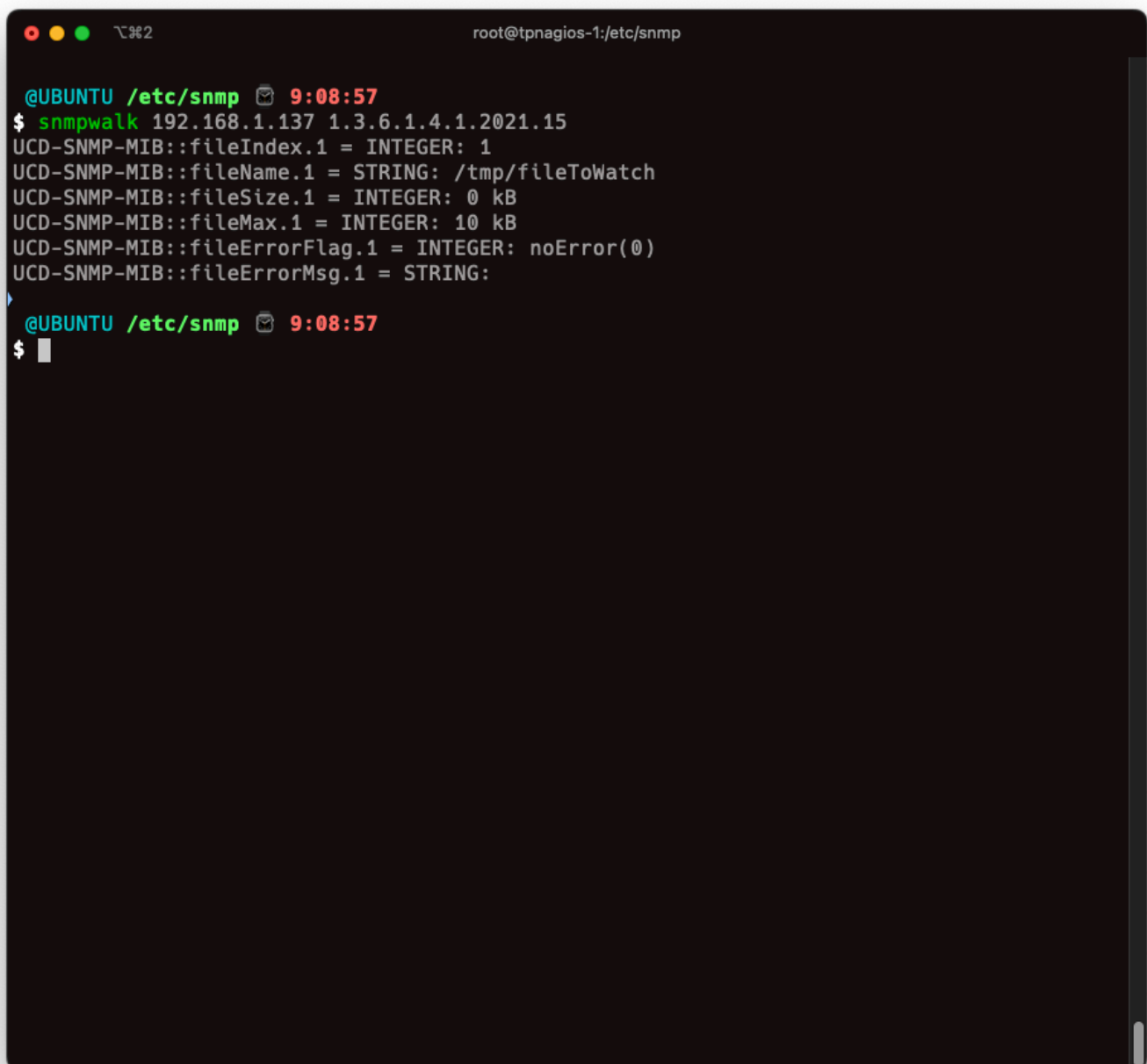
Nous redémarrons le service `snmpd`:

```
$ systemctl restart snmpd
```

Puis, nous exécutons la commande suivante depuis notre manager, pour tester le bon fonctionnement de notre configuration:

```
$ snmpwalk 192.168.1.137 1.3.6.1.4.1.2021.15
```

Nous obtenons le résultat suivant :

A terminal window with a dark background. The title bar shows three colored circles (red, yellow, green) and the text 'root@tpnagios-1:/etc/snmp'. The prompt is '@UBUNTU /etc/snmp' followed by a clock icon and the time '9:08:57'. The user enters '\$ snmpwalk 192.168.1.137 1.3.6.1.4.1.2021.15'. The output is: 'UCD-SNMP-MIB::fileIndex.1 = INTEGER: 1', 'UCD-SNMP-MIB::fileName.1 = STRING: /tmp/fileToWatch', 'UCD-SNMP-MIB::fileSize.1 = INTEGER: 0 kB', 'UCD-SNMP-MIB::fileMax.1 = INTEGER: 10 kB', 'UCD-SNMP-MIB::fileErrorFlag.1 = INTEGER: noError(0)', and 'UCD-SNMP-MIB::fileErrorMsg.1 = STRING:'. The prompt '\$' is visible again on the next line.

```
root@tpnagios-1:/etc/snmp

@UBUNTU /etc/snmp 9:08:57
$ snmpwalk 192.168.1.137 1.3.6.1.4.1.2021.15
UCD-SNMP-MIB::fileIndex.1 = INTEGER: 1
UCD-SNMP-MIB::fileName.1 = STRING: /tmp/fileToWatch
UCD-SNMP-MIB::fileSize.1 = INTEGER: 0 kB
UCD-SNMP-MIB::fileMax.1 = INTEGER: 10 kB
UCD-SNMP-MIB::fileErrorFlag.1 = INTEGER: noError(0)
UCD-SNMP-MIB::fileErrorMsg.1 = STRING:
$
```

Nous augmentons la taille de notre fichier par l'exécution de cette commande pendant quelques secondes:

```
while true; do echo "AAAAAA" >> /tmp/fileToWatch; done;
```

Quelques secondes après, nous obtenons le résultat suivant:

```

021.2.1.2.1="cron" .1.3.6.1.4.1.2021.2.1.101.1="No cron process running"
^C
16 packets captured
18 packets received by filter
0 packets dropped by kernel

@UBUNTU /etc/snmp 9:14:04
$ sudo tcpdump -i any -nn 'udp port 162'

tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
09:14:10.300299 eth0 Out IP 192.168.1.137.45112 > 192.168.1.28.162: C="mycom" V2Trap(
80) .1.3.6.1.2.1.1.3.0=5706 .1.3.6.1.6.3.1.1.4.1.0=.1.3.6.1.4.1.8072.4.0.2 .1.3.6.1.6.
3.1.1.4.3.0=.1.3.6.1.4.1.8072.4
09:14:10.891738 eth0 Out IP 192.168.1.137.41718 > 192.168.1.28.162: C="mycom" V2Trap(
80) .1.3.6.1.2.1.1.3.0=30 .1.3.6.1.6.3.1.1.4.1.0=.1.3.6.1.6.3.1.1.5.1 .1.3.6.1.6.3.1.1.
4.3.0=.1.3.6.1.4.1.8072.3.2.10
09:14:11.114161 eth0 Out IP 192.168.1.137.41718 > 192.168.1.28.162: C="mycom" V2Trap(
221) .1.3.6.1.2.1.1.3.0=53 .1.3.6.1.6.3.1.1.4.1.0=.1.3.6.1.2.1.88.2.0.1 .1.3.6.1.2.1.8
8.2.1.1.0="process table" .1.3.6.1.2.1.88.2.1.2.0="" .1.3.6.1.2.1.88.2.1.3.0="" .1.3.6.
1.2.1.88.2.1.4.0=.1.3.6.1.4.1.2021.2.1.100.1 .1.3.6.1.2.1.88.2.1.5.0=1 .1.3.6.1.4.1.202
1.2.1.2.1="cron" .1.3.6.1.4.1.2021.2.1.101.1="No cron process running"
09:14:11.114985 eth0 Out IP 192.168.1.137.41718 > 192.168.1.28.162: C="mycom" V2Trap(
217) .1.3.6.1.2.1.1.3.0=53 .1.3.6.1.6.3.1.1.4.1.0=.1.3.6.1.2.1.88.2.0.1 .1.3.6.1.2.1.8
8.2.1.1.0="memory" .1.3.6.1.2.1.88.2.1.2.0="" .1.3.6.1.2.1.88.2.1.3.0="" .1.3.6.1.2.1.8
8.2.1.4.0=.1.3.6.1.4.1.2021.4.100.0 .1.3.6.1.2.1.88.2.1.5.0=1 .1.3.6.1.4.1.2021.4.2.0="
swap" .1.3.6.1.4.1.2021.4.101.0="Running out of swap space (0)"
09:14:11.115972 eth0 Out IP 192.168.1.137.41718 > 192.168.1.28.162: C="mycom" V2Trap(
252) .1.3.6.1.2.1.1.3.0=53 .1.3.6.1.6.3.1.1.4.1.0=.1.3.6.1.2.1.88.2.0.1 .1.3.6.1.2.1.8
8.2.1.1.0="fileTable" .1.3.6.1.2.1.88.2.1.2.0="" .1.3.6.1.2.1.88.2.1.3.0="" .1.3.6.1.2.
1.88.2.1.4.0=.1.3.6.1.4.1.2021.15.1.100.1 .1.3.6.1.2.1.88.2.1.5.0=1 .1.3.6.1.4.1.2021.1
5.1.2.1="/tmp/fileToWatch" .1.3.6.1.4.1.2021.15.1.101.1="/tmp/fileToWatch: size exceeds
10kb (= 2486kb)"
09:14:11.116197 eth0 Out IP 192.168.1.137.41718 > 192.168.1.28.162: C="mycom" V2Trap(
222) .1.3.6.1.2.1.1.3.0=53 .1.3.6.1.6.3.1.1.4.1.0=.1.3.6.1.2.1.88.2.0.1 .1.3.6.1.2.1.8
8.2.1.1.0="ProcessMonitor" .1.3.6.1.2.1.88.2.1.2.0="" .1.3.6.1.2.1.88.2.1.3.0="" .1.3.6
.1.2.1.88.2.1.4.0=.1.3.6.1.4.1.2021.2.1.100.1 .1.3.6.1.2.1.88.2.1.5.0=1 .1.3.6.1.4.1.20
21.2.1.2.1="cron" .1.3.6.1.4.1.2021.2.1.101.1="No cron process running"

```

En vérifiant avec, à nouveau avec notre manager, notre commande `snmpwalk 192.168.1.137 1.3.6.1.4.1.2021.15`, nous obtenons le résultat suivant:

```
root@tpnagios-1:/etc/snmp

@UBUNTU /etc/snmp 9:08:57
$ snmpwalk 192.168.1.137 1.3.6.1.4.1.2021.15
UCD-SNMP-MIB::fileIndex.1 = INTEGER: 1
UCD-SNMP-MIB::fileName.1 = STRING: /tmp/fileToWatch
UCD-SNMP-MIB::fileSize.1 = INTEGER: 0 kB
UCD-SNMP-MIB::fileMax.1 = INTEGER: 10 kB
UCD-SNMP-MIB::fileErrorFlag.1 = INTEGER: noError(0)
UCD-SNMP-MIB::fileErrorMsg.1 = STRING:

@UBUNTU /etc/snmp 9:08:57
$ snmpwalk 192.168.1.137 1.3.6.1.4.1.2021.15
UCD-SNMP-MIB::fileIndex.1 = INTEGER: 1
UCD-SNMP-MIB::fileName.1 = STRING: /tmp/fileToWatch
UCD-SNMP-MIB::fileSize.1 = INTEGER: 2486 kB
UCD-SNMP-MIB::fileMax.1 = INTEGER: 10 kB
UCD-SNMP-MIB::fileErrorFlag.1 = INTEGER: error(1)
UCD-SNMP-MIB::fileErrorMsg.1 = STRING: /tmp/fileToWatch: size exceeds 10kb (= 2486kb)

@UBUNTU /etc/snmp 9:11:32
$
```

Traitement des notifications sur le Manager

Nous commençons par installer `snmptrapd` sur notre manager:

```
$ apt install snmptrapd
```

Puis, nous ajoutons en fin de fichier `/etc/snmp/snmptrapd.conf` la ligne suivante:

```
authCommunity log,execute mycom
```

Ensuite, nous exécutons la commande suivante sur notre agent:

```
$ snmptrap -v 2c -c mycom 192.168.1.28 '' UCD-SNMP-MIB::ucdStart UCD-SNMP-MIB::ucdavis.0 s
"Test Trap"
```

Nous obtenons, sur notre agent, le résultat suivant:

```
tcpdump -i any -nn 'udp port 162'

@UBUNTU /etc/snmp 9:23:33
$ tcpdump -i any -nn 'udp port 162'
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
09:23:45.927902 eth0 In IP 192.168.1.137.37517 > 192.168.1.28.162: C="mycom" V2Trap(8
0) .1.3.6.1.2.1.1.3.0=775611 .1.3.6.1.6.3.1.1.4.1.0=.1.3.6.1.4.1.2021.251.1 .1.3.6.1.4.
1.2021.0="Test Trap"
```

Puis, en analysant le fichier `/var/log/syslog` sur notre manager, nous obtenons le résultat suivant:

```
root@tpnagios-1:/etc/snmp
Mar 28 09:09:01 tpnagios-1 systemd[1]: Starting Clean php session files...
Mar 28 09:09:01 tpnagios-1 systemd[1]: phpsessionclean.service: Deactivated successfully.
Mar 28 09:09:01 tpnagios-1 CRON[6084]: (root) CMD ( [ -x /usr/lib/php/sessionclean ] && if [ ! -d /run/systemd/system ]; then /usr/lib/php/sessi
onclean; fi)
Mar 28 09:09:01 tpnagios-1 systemd[1]: Finished Clean php session files.
Mar 28 09:17:01 tpnagios-1 slapd[1780]: slap_global_control: unrecognized control: 1.3.6.1.4.1.4203.666.5.16
Mar 28 09:17:01 tpnagios-1 CRON[6157]: (root) CMD ( cd / && run-parts --report /etc/cron.hourly)
Mar 28 09:22:11 tpnagios-1 slapd[1780]: slap_global_control: unrecognized control: 1.3.6.1.4.1.4203.666.5.16
Mar 28 09:22:11 tpnagios-1 slapd[1780]: message repeated 3 times: [ slap_global_control: unrecognized control: 1.3.6.1.4.1.4203.666.5.16]
Mar 28 09:22:11 tpnagios-1 slapd[1780]: slap_global_control: unrecognized control: 1.3.6.1.4.1.4203.666.5.16
Mar 28 09:22:11 tpnagios-1 slapd[1780]: slap_global_control: unrecognized control: 1.3.6.1.4.1.4203.666.5.16
Mar 28 09:22:12 tpnagios-1 slapd[1780]: slap_global_control: unrecognized control: 1.3.6.1.4.1.4203.666.5.16
Mar 28 09:22:15 tpnagios-1 slapd[1780]: message repeated 98 times: [ slap_global_control: unrecognized control: 1.3.6.1.4.1.4203.666.5.16]
Mar 28 09:22:16 tpnagios-1 systemd[1]: Reloading.
Mar 28 09:22:16 tpnagios-1 systemd[1]: Starting Daily apt download activities...
Mar 28 09:22:16 tpnagios-1 systemd[1]: apt-daily.service: Deactivated successfully.
Mar 28 09:22:16 tpnagios-1 systemd[1]: Finished Daily apt download activities.
Mar 28 09:22:16 tpnagios-1 systemd[1]: Reloading.
Mar 28 09:22:16 tpnagios-1 systemd[1]: Starting Message of the Day...
Mar 28 09:22:16 tpnagios-1 systemd[1]: motd-news.service: Deactivated successfully.
Mar 28 09:22:16 tpnagios-1 systemd[1]: Finished Message of the Day.
Mar 28 09:22:16 tpnagios-1 systemd[1]: Listening on sockets for SNMP trap messages.
Mar 28 09:22:16 tpnagios-1 slapd[1780]: slap_global_control: unrecognized control: 1.3.6.1.4.1.4203.666.5.16
Mar 28 09:22:45 tpnagios-1 systemd[1]: Starting Simple Network Management Protocol (SNMP) Trap Daemon....
Mar 28 09:22:46 tpnagios-1 systemd[1]: Started Simple Network Management Protocol (SNMP) Trap Daemon..
Mar 28 09:32:23 tpnagios-1 systemd[1]: Stopping Simple Network Management Protocol (SNMP) Trap Daemon....
Mar 28 09:32:23 tpnagios-1 systemd[1]: snmptrapd.service: Deactivated successfully.
Mar 28 09:32:23 tpnagios-1 systemd[1]: Stopped Simple Network Management Protocol (SNMP) Trap Daemon..
Mar 28 09:32:23 tpnagios-1 systemd[1]: Starting Simple Network Management Protocol (SNMP) Trap Daemon....
Mar 28 09:32:23 tpnagios-1 systemd[1]: Started Simple Network Management Protocol (SNMP) Trap Daemon..
Mar 28 09:39:01 tpnagios-1 slapd[1780]: slap_global_control: unrecognized control: 1.3.6.1.4.1.4203.666.5.16
Mar 28 09:39:01 tpnagios-1 systemd[1]: Starting Clean php session files...
Mar 28 09:39:01 tpnagios-1 CRON[6708]: (root) CMD ( [ -x /usr/lib/php/sessionclean ] && if [ ! -d /run/systemd/system ]; then /usr/lib/php/sessi
onclean; fi)
Mar 28 09:39:01 tpnagios-1 systemd[1]: phpsessionclean.service: Deactivated successfully.
Mar 28 09:39:01 tpnagios-1 systemd[1]: Finished Clean php session files.

@UBUNTU /etc/snmp 9:42:30
```

Nous ajoutons la ligne suivante à notre fichier `snmptrapd.conf` sur notre manager:

```
traphandle default /bin/traitement-notification
```

A noter que `traitement-notification` est le nom de notre script qui va s'exécuter pour chaque trap reçu.

Puis, nous créons le script avec le contenu suivant:

```
#!/bin/bash
```

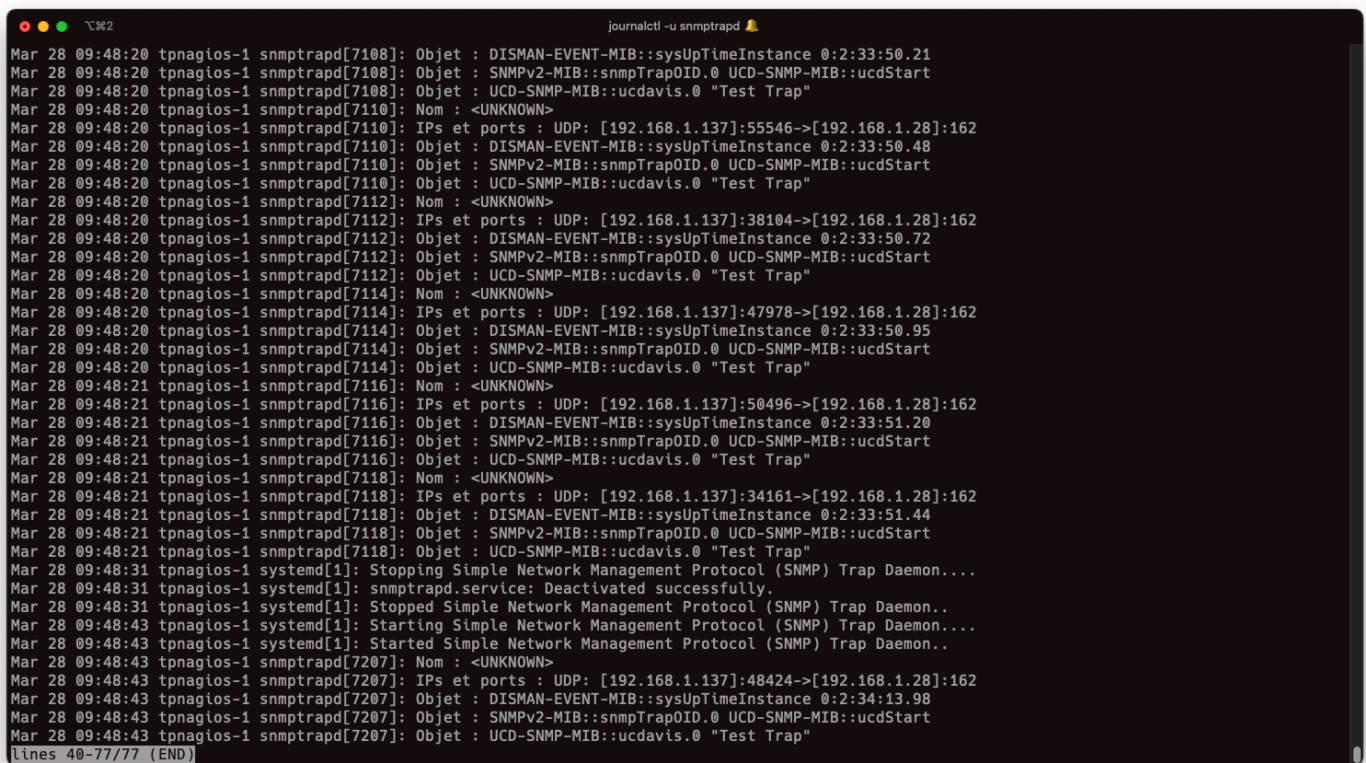
```
read nom
echo "Nom : "$nom
read ip
echo "IPs et ports : "$ip
while read obj; do
    echo "Objet : "$obj
done
```

Nous lui appliquons les permissions nécessaires:

```
$ chmod +x /bin/traitement-notification
```

Nous envoyons maintenant une notification `snmptrap` depuis notre agent, et observons le résultat suivant dans le journal:

```
$ snmptrap -v 2c -c mycom 192.168.1.28 '' UCD-SNMP-MIB::ucdStart UCD-SNMP-MIB::ucdavis.0 s "Test Trap"
```



```
journalctl -u snmptrapd
Mar 28 09:48:20 tpnagios-1 snmptrapd[7108]: Objet : DISMAN-EVENT-MIB::sysUpTimeInstance 0:2:33:50.21
Mar 28 09:48:20 tpnagios-1 snmptrapd[7108]: Objet : SNMPv2-MIB::snmpTrapOID.0 UCD-SNMP-MIB::ucdStart
Mar 28 09:48:20 tpnagios-1 snmptrapd[7108]: Objet : UCD-SNMP-MIB::ucdavis.0 "Test Trap"
Mar 28 09:48:20 tpnagios-1 snmptrapd[7110]: Nom : <UNKNOWN>
Mar 28 09:48:20 tpnagios-1 snmptrapd[7110]: IPs et ports : UDP: [192.168.1.137]:55546->[192.168.1.28]:162
Mar 28 09:48:20 tpnagios-1 snmptrapd[7110]: Objet : DISMAN-EVENT-MIB::sysUpTimeInstance 0:2:33:50.48
Mar 28 09:48:20 tpnagios-1 snmptrapd[7110]: Objet : SNMPv2-MIB::snmpTrapOID.0 UCD-SNMP-MIB::ucdStart
Mar 28 09:48:20 tpnagios-1 snmptrapd[7110]: Objet : UCD-SNMP-MIB::ucdavis.0 "Test Trap"
Mar 28 09:48:20 tpnagios-1 snmptrapd[7112]: Nom : <UNKNOWN>
Mar 28 09:48:20 tpnagios-1 snmptrapd[7112]: IPs et ports : UDP: [192.168.1.137]:38104->[192.168.1.28]:162
Mar 28 09:48:20 tpnagios-1 snmptrapd[7112]: Objet : DISMAN-EVENT-MIB::sysUpTimeInstance 0:2:33:50.72
Mar 28 09:48:20 tpnagios-1 snmptrapd[7112]: Objet : SNMPv2-MIB::snmpTrapOID.0 UCD-SNMP-MIB::ucdStart
Mar 28 09:48:20 tpnagios-1 snmptrapd[7112]: Objet : UCD-SNMP-MIB::ucdavis.0 "Test Trap"
Mar 28 09:48:20 tpnagios-1 snmptrapd[7114]: Nom : <UNKNOWN>
Mar 28 09:48:20 tpnagios-1 snmptrapd[7114]: IPs et ports : UDP: [192.168.1.137]:47978->[192.168.1.28]:162
Mar 28 09:48:20 tpnagios-1 snmptrapd[7114]: Objet : DISMAN-EVENT-MIB::sysUpTimeInstance 0:2:33:50.95
Mar 28 09:48:20 tpnagios-1 snmptrapd[7114]: Objet : SNMPv2-MIB::snmpTrapOID.0 UCD-SNMP-MIB::ucdStart
Mar 28 09:48:20 tpnagios-1 snmptrapd[7114]: Objet : UCD-SNMP-MIB::ucdavis.0 "Test Trap"
Mar 28 09:48:21 tpnagios-1 snmptrapd[7116]: Nom : <UNKNOWN>
Mar 28 09:48:21 tpnagios-1 snmptrapd[7116]: IPs et ports : UDP: [192.168.1.137]:50496->[192.168.1.28]:162
Mar 28 09:48:21 tpnagios-1 snmptrapd[7116]: Objet : DISMAN-EVENT-MIB::sysUpTimeInstance 0:2:33:51.20
Mar 28 09:48:21 tpnagios-1 snmptrapd[7116]: Objet : SNMPv2-MIB::snmpTrapOID.0 UCD-SNMP-MIB::ucdStart
Mar 28 09:48:21 tpnagios-1 snmptrapd[7116]: Objet : UCD-SNMP-MIB::ucdavis.0 "Test Trap"
Mar 28 09:48:21 tpnagios-1 snmptrapd[7118]: Nom : <UNKNOWN>
Mar 28 09:48:21 tpnagios-1 snmptrapd[7118]: IPs et ports : UDP: [192.168.1.137]:34161->[192.168.1.28]:162
Mar 28 09:48:21 tpnagios-1 snmptrapd[7118]: Objet : DISMAN-EVENT-MIB::sysUpTimeInstance 0:2:33:51.44
Mar 28 09:48:21 tpnagios-1 snmptrapd[7118]: Objet : SNMPv2-MIB::snmpTrapOID.0 UCD-SNMP-MIB::ucdStart
Mar 28 09:48:21 tpnagios-1 snmptrapd[7118]: Objet : UCD-SNMP-MIB::ucdavis.0 "Test Trap"
Mar 28 09:48:31 tpnagios-1 systemd[1]: Stopping Simple Network Management Protocol (SNMP) Trap Daemon....
Mar 28 09:48:31 tpnagios-1 systemd[1]: snmptrapd.service: Deactivated successfully.
Mar 28 09:48:31 tpnagios-1 systemd[1]: Stopped Simple Network Management Protocol (SNMP) Trap Daemon..
Mar 28 09:48:43 tpnagios-1 systemd[1]: Starting Simple Network Management Protocol (SNMP) Trap Daemon....
Mar 28 09:48:43 tpnagios-1 systemd[1]: Started Simple Network Management Protocol (SNMP) Trap Daemon..
Mar 28 09:48:43 tpnagios-1 snmptrapd[7207]: Nom : <UNKNOWN>
Mar 28 09:48:43 tpnagios-1 snmptrapd[7207]: IPs et ports : UDP: [192.168.1.137]:48424->[192.168.1.28]:162
Mar 28 09:48:43 tpnagios-1 snmptrapd[7207]: Objet : DISMAN-EVENT-MIB::sysUpTimeInstance 0:2:34:13.98
Mar 28 09:48:43 tpnagios-1 snmptrapd[7207]: Objet : SNMPv2-MIB::snmpTrapOID.0 UCD-SNMP-MIB::ucdStart
Mar 28 09:48:43 tpnagios-1 snmptrapd[7207]: Objet : UCD-SNMP-MIB::ucdavis.0 "Test Trap"
```

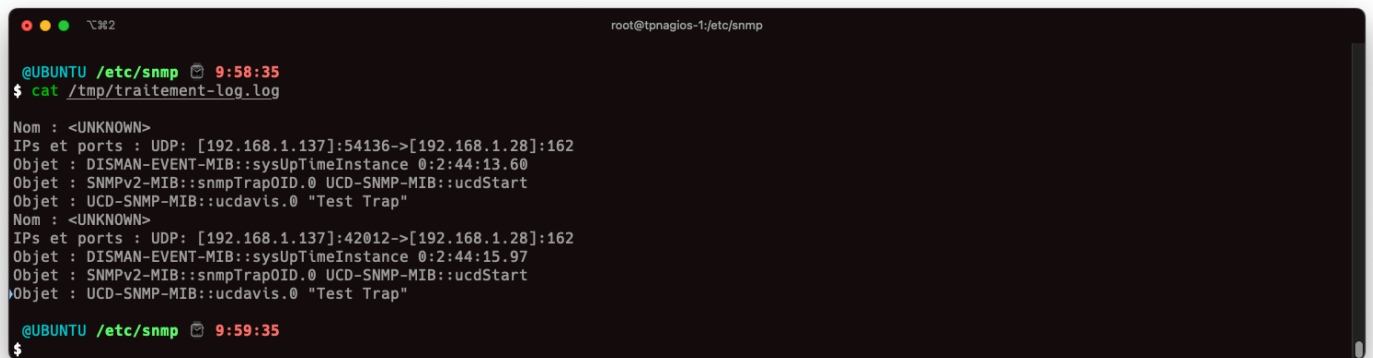
Nous pouvons donc bien en conclure que le script est bien exécuté lors de l'envoi de notre notification par notre agent.

Note: Etant donné le fonctionnement des mails Postfix assez compliqué au vu des dernières mises à jour, nous allons modifier le script de traitement des notifications pour simplement écrire dans un fichier ce qui aurait dû être présent dans un mail.

Nous modifions donc le contenu de notre fichier `/bin/traitement-notification` pour avoir le contenu suivant:


```
#!/bin/bash
logFile="/tmp/traitement-log.log"
echo "Date de réception: $(date)" >> $logFile
read nom
echo "Nom : "$nom >> $logFile
read ip
echo "IPs et ports : "$ip >> $logFile
while read obj; do
    echo "Objet : "$obj >> $logFile
done
```

Nous envoyons à nouveau une notification SNMP, et obtenons le résultat suivant dans notre fichier /tmp/traitement-log.log :



```
@UBUNTU /etc/snmp 9:58:35
$ cat /tmp/traitement-log.log
Nom : <UNKNOWN>
IPs et ports : UDP: [192.168.1.137]:54136->[192.168.1.28]:162
Objet : DISMAN-EVENT-MIB::sysUpTimeInstance 0:2:44:13.60
Objet : SNMPv2-MIB::snmpTrapOID.0 UCD-SNMP-MIB::ucdStart
Objet : UCD-SNMP-MIB::ucdavis.0 "Test Trap"
Nom : <UNKNOWN>
IPs et ports : UDP: [192.168.1.137]:42012->[192.168.1.28]:162
Objet : DISMAN-EVENT-MIB::sysUpTimeInstance 0:2:44:15.97
Objet : SNMPv2-MIB::snmpTrapOID.0 UCD-SNMP-MIB::ucdStart
Objet : UCD-SNMP-MIB::ucdavis.0 "Test Trap"
@UBUNTU /etc/snmp 9:59:35
$
```

En amélioration, nous pourrions mettre à jour le nom de notre agent, afin de ne pas avoir `<UNKNOWN>` figurant parmi les logs.