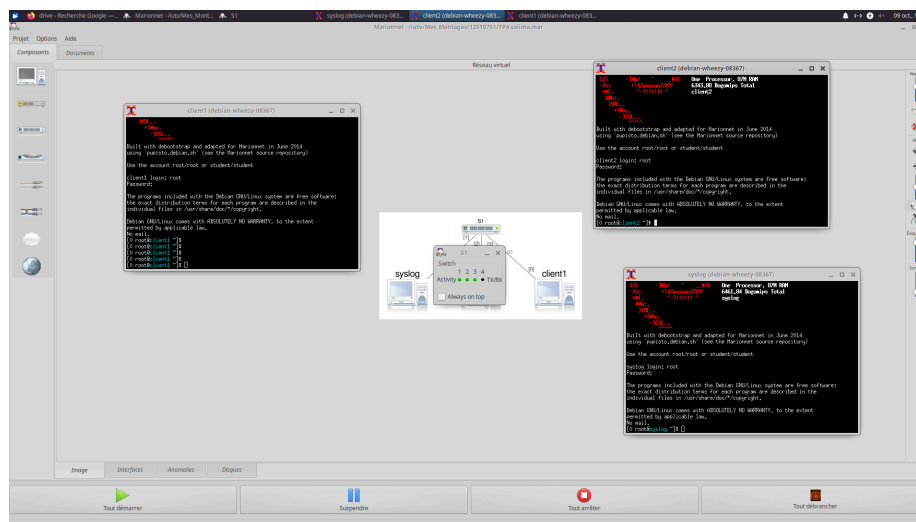


# Compte rendu TP 4 — Syslog sous linux avec le service rsyslog

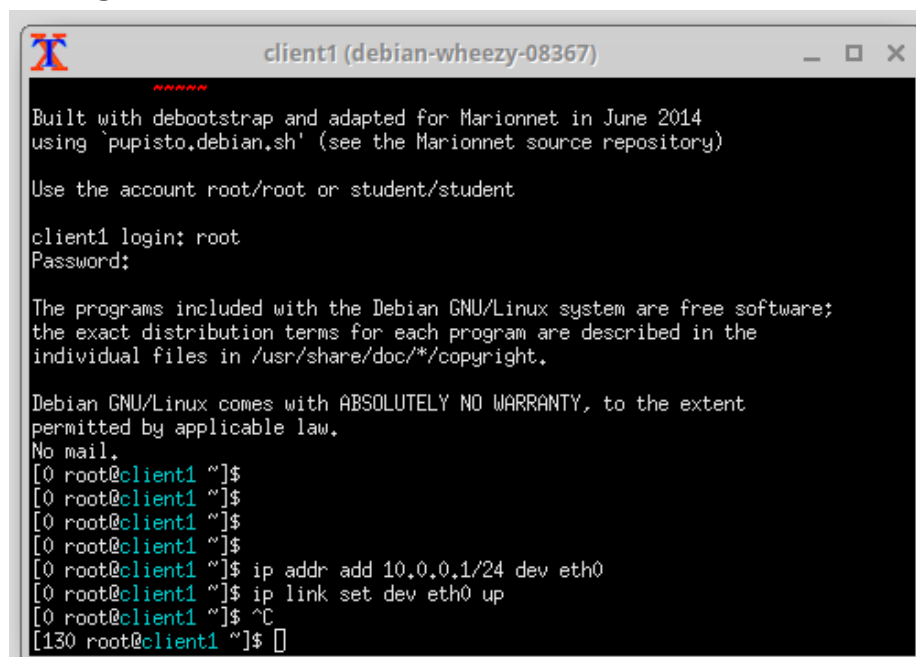
## Travail réalisé par Salima Zribi

### Exercice 1-Création du réseau

j'ai créé le réseau avec un switch connecté à 4 machines : client1, client2, NMS, et syslog et j'ai configuré les adresses IP des 4 machines en fait au début j'ai attribué certaines adresses puis je l'ai ais changés au cours du tp car j'ai du refaire le travail dès le début à cause d'un problème survenu



### Configuration du client 1



## Configuration du client 2

```
client2 (debian-wheezy-08367)
*![, ~-?!!!!!!~ client2
Xlb:.
)YXL,,
+3#bc,
-)SSL,,
#####

Built with debootstrap and adapted for Marionnet in June 2014
using 'pupisto,debian.sh' (see the Marionnet source repository)

Use the account root/root or student/student

client2 login: root
Password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
No mail.
[0 root@client2 ~]$ ip addr add 10.0.0.2/24 dev eth0
[0 root@client2 ~]$ ip link set eth0 up
[0 root@client2 ~]$ /
```

## Configuration du nms

```
nms (debian-wheezy-08367)
Login incorrect
nms login: root
Password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
No mail.
[0 root@nms ~]$ ip addr add 10.0.0.3/24 dev eth0
[0 root@nms ~]$ ip link set dev eth0 up
[0 root@nms ~]$ ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_req=1 ttl=64 time=4.02 ms
64 bytes from 10.0.0.2: icmp_req=2 ttl=64 time=3.11 ms
64 bytes from 10.0.0.2: icmp_req=3 ttl=64 time=3.16 ms
^C
--- 10.0.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2010ms
rtt min/avg/max/mdev = 3.113/3.433/4.025/0.419 ms
[0 root@nms ~]$
```

## Configuration du syslog

```
syslog (debian-wheezy-08367)
12 packets transmitted, 0 received, +9 errors, 100% packet loss, time 11071ms
pipe 3
[1 root@syslog ~]$ ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
From 10.0.0.0 icmp_seq=1 Destination Host Unreachable
From 10.0.0.0 icmp_seq=2 Destination Host Unreachable
From 10.0.0.0 icmp_seq=3 Destination Host Unreachable
From 10.0.0.0 icmp_seq=4 Destination Host Unreachable
From 10.0.0.0 icmp_seq=5 Destination Host Unreachable
From 10.0.0.0 icmp_seq=6 Destination Host Unreachable
^C
--- 10.0.0.1 ping statistics ---
8 packets transmitted, 0 received, +6 errors, 100% packet loss, time 7045ms
pipe 3
[1 root@syslog ~]$ /etc/init.d/rsyslog restart
[ ok ] Stopping enhanced syslogd: rsyslogd already stopped.
[ ok ] Starting enhanced syslogd: rsyslogd.
[0 root@syslog ~]$ rsyslog.conf
-bash: rsyslog.conf: command not found
[127 root@syslog ~]$ /etc/rsyslog.conf
-bash: /etc/rsyslog.conf: Permission denied
[126 root@syslog ~]$ less
Missing filename ("less --help" for help)
[0 root@syslog ~]$ less --help
```

## Exercice 2 - Première analyse du fichier de configuration de rsyslog

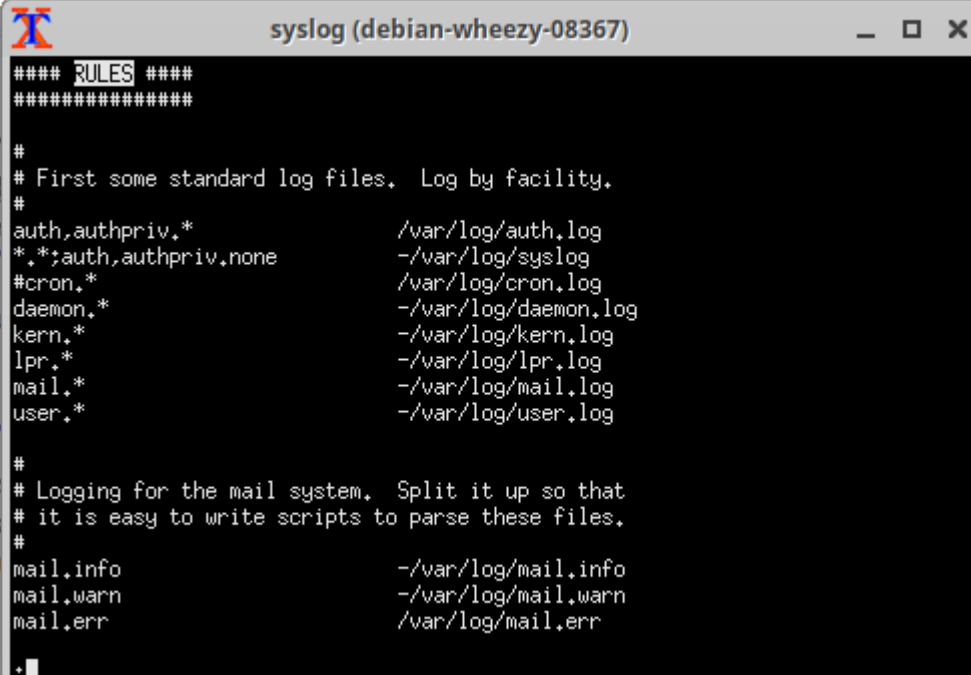
### I 2.1 Démarrer le service rsyslog sur la machine syslog avec la commande

- `/etc/init.d/rsyslog restart`

```
syslog (debian-wheezy-08367)
12 packets transmitted, 0 received, +9 errors, 100% packet loss, time 11071ms
pipe 3
[1 root@syslog ~]$ ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
From 10.0.0.0 icmp_seq=1 Destination Host Unreachable
From 10.0.0.0 icmp_seq=2 Destination Host Unreachable
From 10.0.0.0 icmp_seq=3 Destination Host Unreachable
From 10.0.0.0 icmp_seq=4 Destination Host Unreachable
From 10.0.0.0 icmp_seq=5 Destination Host Unreachable
From 10.0.0.0 icmp_seq=6 Destination Host Unreachable
^C
--- 10.0.0.1 ping statistics ---
8 packets transmitted, 0 received, +6 errors, 100% packet loss, time 7045ms
pipe 3
[1 root@syslog ~]$ /etc/init.d/rsyslog restart
[ ok ] Stopping enhanced syslogd: rsyslogd already stopped.
[ ok ] Starting enhanced syslogd: rsyslogd.
[0 root@syslog ~]$ rsyslog.conf
-bash: rsyslog.conf: command not found
[127 root@syslog ~]$ /etc/rsyslog.conf
-bash: /etc/rsyslog.conf: Permission denied
[126 root@syslog ~]$ less
Missing filename ("less --help" for help)
[0 root@syslog ~]$ less --help
```

### I 2.2 on ouvre le fichier de configuration de rsyslog `/etc/rsyslog.conf` sur la machine syslog avec la commande `less /etc/rsyslog.conf`

Puis on tape sur ctrl+w et **/RULES** pour trouver la partie des règles



```
##### RULES #####
#####

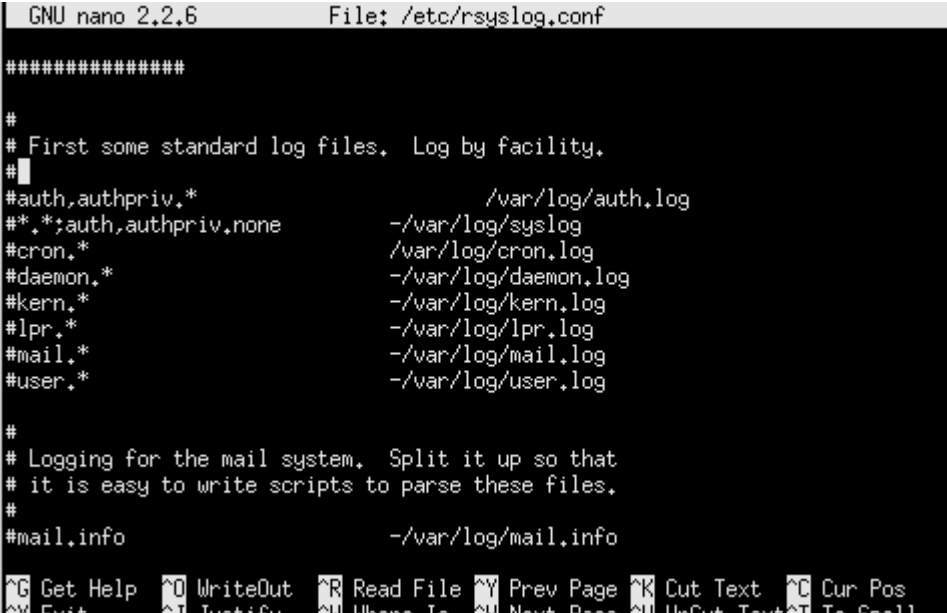
#
# First some standard log files.  Log by facility.
#
auth,authpriv,*                /var/log/auth.log
*.*;auth,authpriv.none         -/var/log/syslog
#cron,*                        /var/log/cron.log
daemon,*                       -/var/log/daemon.log
kern,*                         -/var/log/kern.log
lpr,*                          -/var/log/lpr.log
mail,*                         -/var/log/mail.log
user,*                         -/var/log/user.log

#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
mail.info                     -/var/log/mail.info
mail.warn                    -/var/log/mail.warn
mail.err                     /var/log/mail.err

:|
```

### Exercice 3 — Configuration de rsyslog sur les deux clients

Sur les deux clients : supprimer ou commenter les règles déjà présentes dans le fichier de configuration (toutes les lignes après le commentaire **### RULES ###**).



```
GNU nano 2.2.6      File: /etc/rsyslog.conf

#####

#
# First some standard log files.  Log by facility.
#
#auth,authpriv,*                /var/log/auth.log
#*.*;auth,authpriv.none         -/var/log/syslog
#cron,*                        /var/log/cron.log
#daemon,*                       -/var/log/daemon.log
#kern,*                         -/var/log/kern.log
#lpr,*                          -/var/log/lpr.log
#mail,*                         -/var/log/mail.log
#user,*                         -/var/log/user.log

#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
#mail.info                     -/var/log/mail.info

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page  ^U UnCut Text ^T To Spell
```

1. stocker les messages de la catégorie daemon dans le fichier /var/log/daemon.log;

```
GNU nano 2.2.6      File: /etc/rsyslog.conf      Modified
#####
#
#
# First some standard log files.  Log by facility.
#
#auth,authpriv.*                /var/log/auth.log
#*.;auth,authpriv.none          -/var/log/syslog
#cron.*                          /var/log/cron.log
daemon.*                        /var/log/daemon.log
#kern.*                          -/var/log/kern.log
#lpr.*                           -/var/log/lpr.log
#mail.*                          -/var/log/mail.log
#user.*                          -/var/log/user.log
#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
#mail.info                      -/var/log/mail.info
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

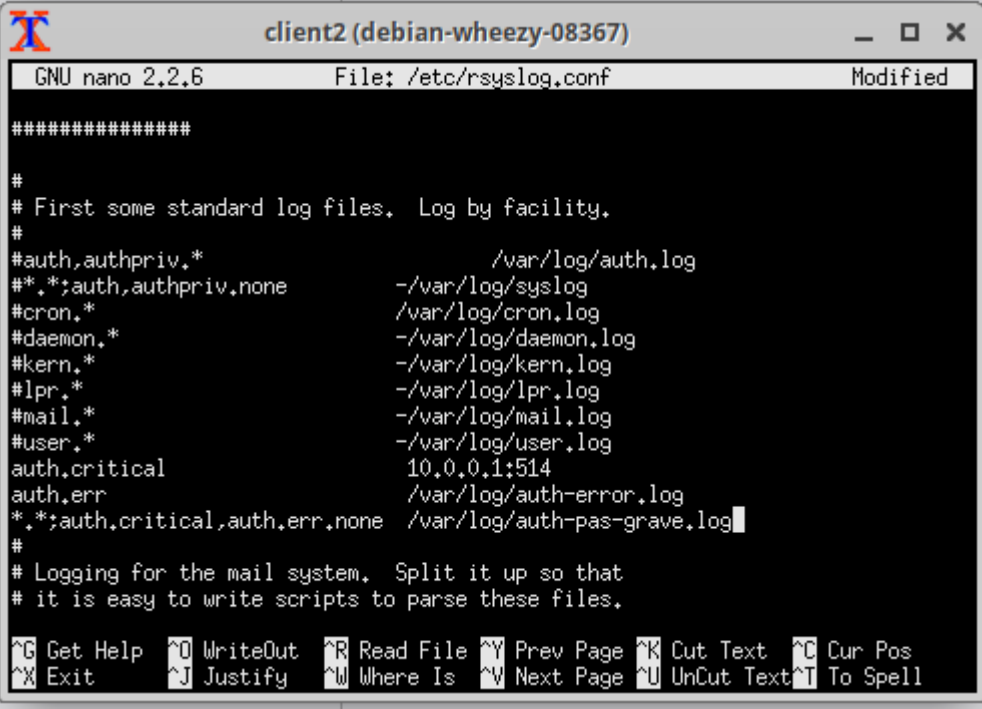
2. stocker tous les messages sauf ceux de la catégorie daemon dans le fichier /var/log/messages.log;

3. et rediriger les messages de la catégorie daemon ayant un niveau error (ou plus grave) vers la machine syslog en utilisant UDP

```
client1 (debian-wheezy-08367)
GNU nano 2.2.6      File: /etc/rsyslog.conf      Modified
#####
#
#
# First some standard log files.  Log by facility.
#
#auth,authpriv.*                /var/log/auth.log
*.;daemon.none                  /var/log/messages.log
#cron.*                          /var/log/cron.log
daemon.*                        /var/log/daemon.log
daemon.err                      10.0.0.1:514
#kern.*                          -/var/log/kern.log
#lpr.*                           -/var/log/lpr.log
#mail.*                          -/var/log/mail.log
#user.*                          -/var/log/user.log
#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

client2 propose un service ssh. On souhaite donc configurer le service rsyslog sur client2 selon les spécifications suivantes :

1. rediriger les messages de la catégorie auth ayant un niveau critical (ou plus grave) vers la machine syslog en utilisant UDP ;
2. stocker les messages de la catégorie auth ayant un niveau égal à error dans le fichier /var/log/auth-error.log;
3. stocker les messages de la catégorie auth ayant un niveau de gravité autres que ceux décrits dans les deux premières clauses dans le fichier /var/log/auth-pas-grave.log.



The screenshot shows a terminal window titled 'client2 (debian-wheezy-08367)'. Inside, the GNU nano 2.2.6 editor is open to the file /etc/rsyslog.conf. The file content is as follows:

```
#####
#
# First some standard log files.  Log by facility.
#
#auth,authpriv.*                  /var/log/auth.log
#*.;auth,authpriv.none            -/var/log/syslog
#cron.*                            /var/log/cron.log
#daemon.*                         -/var/log/daemon.log
#kern.*                           -/var/log/kern.log
#lpr.*                            -/var/log/lpr.log
#mail.*                           -/var/log/mail.log
#user.*                           -/var/log/user.log
auth,critical                     10.0.0.1:514
auth,err                          /var/log/auth-error.log
*.;auth,critical,auth,err,none    /var/log/auth-pas-grave.log
#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
```

At the bottom of the editor, there is a status bar with various keyboard shortcuts: ^G Get Help, ^O WriteOut, ^R Read File, ^Y Prev Page, ^K Cut Text, ^C Cur Pos, ^X Exit, ^J Justify, ^W Where Is, ^V Next Page, ^U UnCut Text, ^T To Spell.

## Exercice 4 — Configuration du serveur rsyslog

- 1) J'ai trouvé les deux lignes qui activent la réception des messages udp sur le port 514 et je les ais décommentés

```
#####
#### MODULES ####
#####

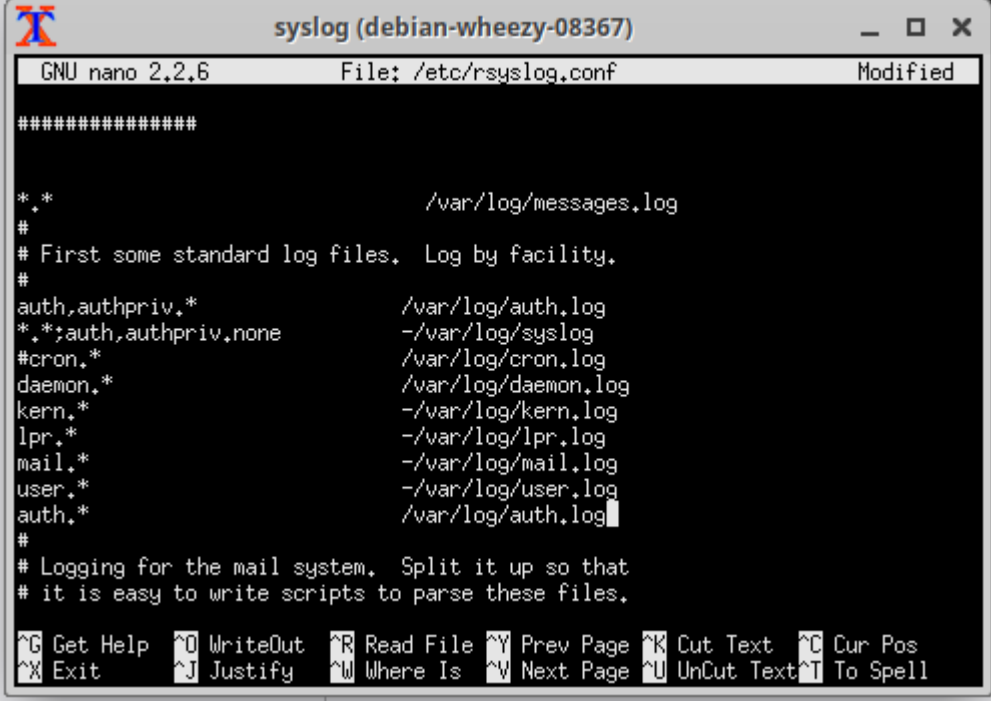
$ModLoad imuxsock # provides support for local system logging
$ModLoad imklog   # provides kernel logging support
#$ModLoad immark  # provides --MARK-- message capability

# provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
```

- 2) Tout message (reçu ou généré par la machine syslog) est stocké dans le fichier /var/log/messages.log

3) Les messages (reçus ou générés par la machine syslog) des catégories auth et daemon seront stockés dans les fichiers /var/log/auth.log et /var/log/daemon.log respectivement.

j'ai fait la même démarche que dans l'exercice 3 mais cette fois dans la machine syslog



```
#####
*.*                               /var/log/messages.log
#
# First some standard log files.  Log by facility.
#
auth,authpriv.*                  /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
#cron.*                          /var/log/cron.log
daemon.*                        /var/log/daemon.log
kern.*                          -/var/log/kern.log
lpr.*                           -/var/log/lpr.log
mail.*                          -/var/log/mail.log
user.*                          -/var/log/user.log
auth.*                          /var/log/auth.log
#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^N Next Page  ^U UnCut Text ^T To Spell
```

## Exercice 5 — Envoi de notifications SNMP

### Création du tube

```
[127 root@syslog ~]$ mkfifo /root/fifo
[0 root@syslog ~]$ ls -l
total 0
0 prw-r--r-- 1 root root 0 Oct  9 16:10 fifo
[0 root@syslog ~]$ nano /etc/rsyslog.conf
[0 root@syslog ~]$
```

Configuration pour que les messages auth de gravité emerg et les messages daemon de gravité emerg soient envoyés au tube

```
#####
auth.emerg;daemon.emerg      |/root/fifo
```

On fait une configuration sur la machine syslog pour afficher le contenu du tube créé

```
syslog (debian-wheezy-08367)
GNU nano 2.2.6 File: /usr/local/bin/rsyslog-snmpp
#!/bin/bash

while true
do
    cat /root/fifo
done

[ Read 7 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

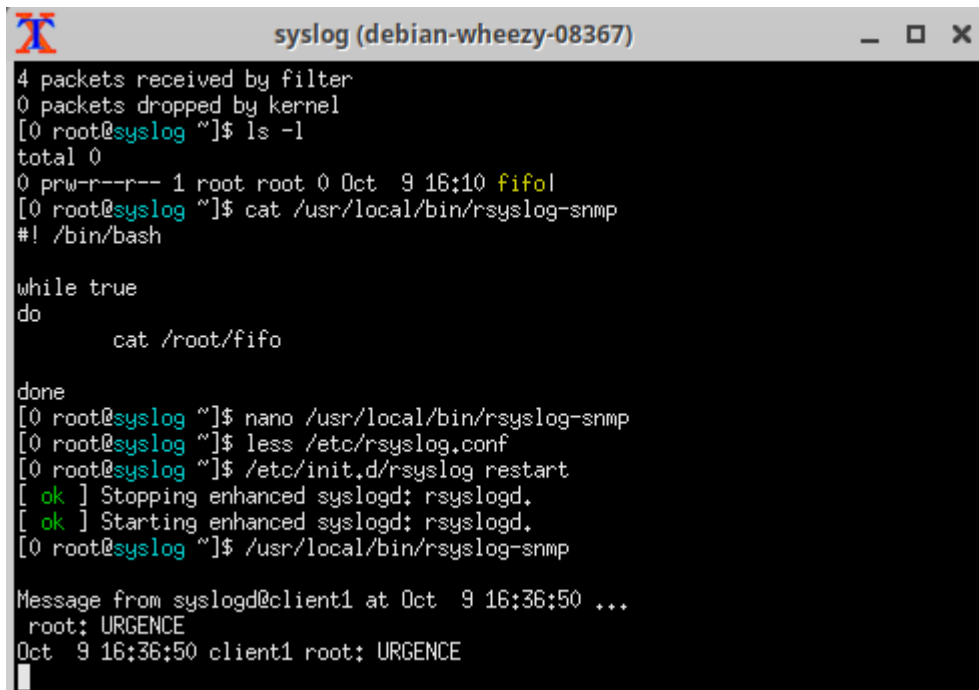
Maintenant à partir de la machine client on introduit dans le tube un message daemon.err

```
client1 (debian-wheezy-08367)
^C
--- 10.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3019ms
rtt min/avg/max/mdev = 3.375/3.636/4.010/0.239 ms
[0 root@client1 ~]$ sudo less /etc/rsyslog.conf
[0 root@client1 ~]$ logger -p daemon.err URGENCY
[0 root@client1 ~]$ sudo less /etc/rsyslog.conf
[0 root@client1 ~]$ sudo less /etc/rsyslog.conf
[0 root@client1 ~]$ nano /etc/rsyslog.conf
[0 root@client1 ~]$ nano /etc/rsyslog.conf
[0 root@client1 ~]$ logger -p daemon.err URGENCY
[0 root@client1 ~]$ /etc/init.d/rsyslog restart
Usage: /etc/init.d/rsyslog {start|stop|rotate|restart|force-reload|status}
[3 root@client1 ~]$ /etc/init.d/rsyslog restart
[ ok ] Stopping enhanced syslogd: rsyslogd.
[ ok ] Starting enhanced syslogd: rsyslogd.
[0 root@client1 ~]$ logger -p daemon.err URGENCY
[0 root@client1 ~]$ logger -p daemon.err URGENCY
[0 root@client1 ~]$ logger -p daemon.err URGENCY
[0 root@client1 ~]$ logger -p daemon.emerg URGENCY

Message from syslogd@client1 at Oct  9 16:36:50 ...
root: URGENCY
[0 root@client1 ~]$
```



On observe le contenu du tube sous forme de message dans la machine syslog



```
syslog (debian-wheezy-08367)
4 packets received by filter
0 packets dropped by kernel
[0 root@syslog ~]$ ls -l
total 0
0 prw-r--r-- 1 root root 0 Oct  9 16:10 fifo
[0 root@syslog ~]$ cat /usr/local/bin/rsyslog-snmpp
#!/bin/bash

while true
do
    cat /root/fifo
done
[0 root@syslog ~]$ nano /usr/local/bin/rsyslog-snmpp
[0 root@syslog ~]$ less /etc/rsyslog.conf
[0 root@syslog ~]$ /etc/init.d/rsyslog restart
[ ok ] Stopping enhanced syslogd: rsyslogd.
[ ok ] Starting enhanced syslogd: rsyslogd.
[0 root@syslog ~]$ /usr/local/bin/rsyslog-snmpp

Message from syslogd@client1 at Oct  9 16:36:50 ...
root: URGENCY
Oct  9 16:36:50 client1 root: URGENCY
```

NB: on s'est arrêtés à ce niveau- là du tp