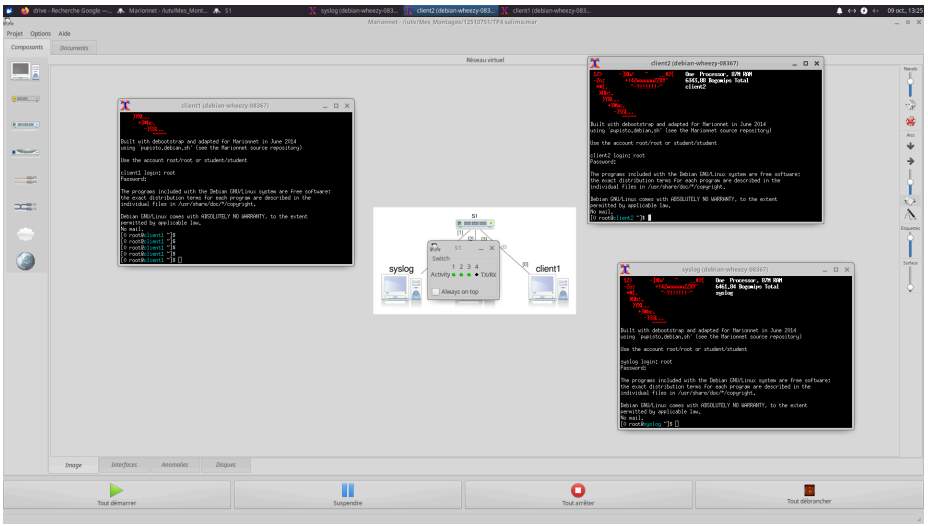
# Compte rendu TP 4 — Syslog sous linux avec le service rsyslog

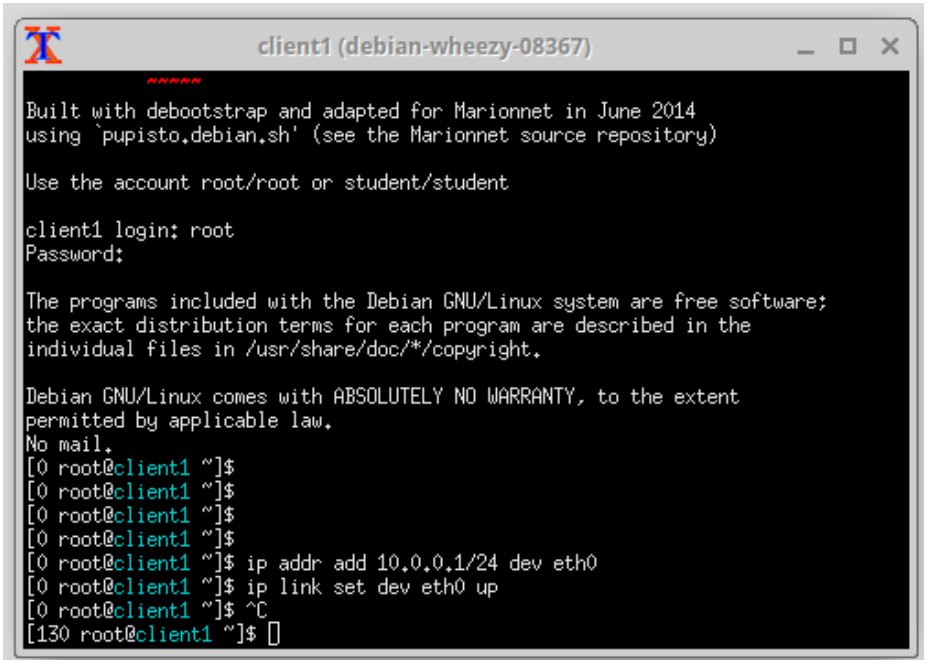
Travail réalisé par Salima Zribi

## Exercice 1-Création du réseau

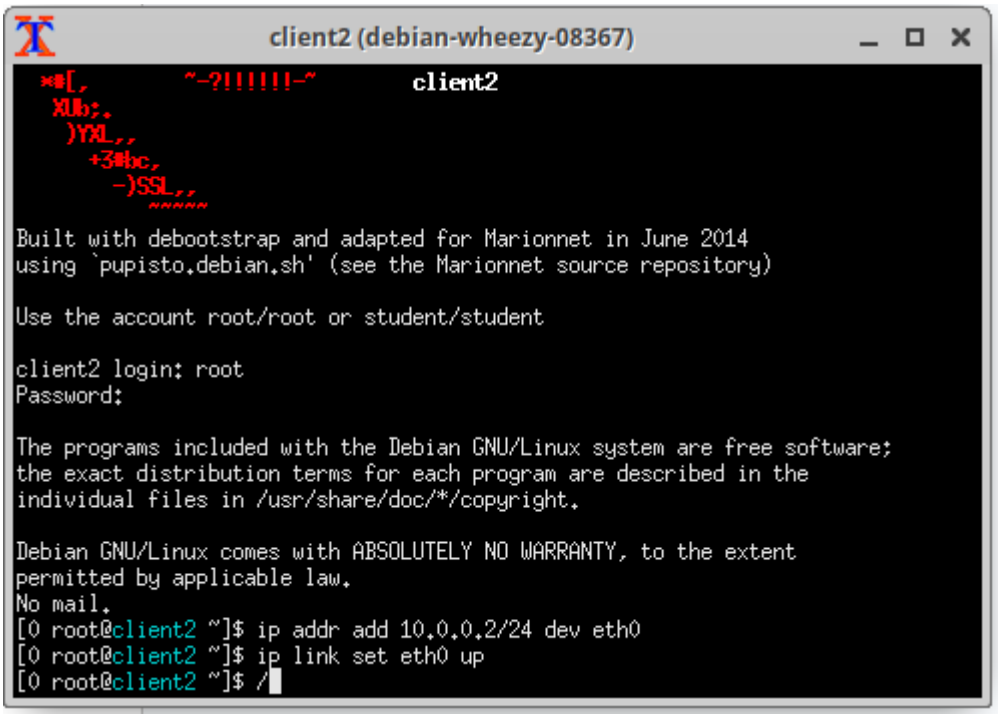
**j'ai créé le réseau avec un switch connecté à 4 machines : client1, client2, NMS, et syslog et j'ai configuré les adresses IP des 4 machines en fait au début j'ai attribué certaines adresses puis je l'ai ais changés au cours du tp car j'ai du refaire le travail dès le début à cause d'un problème survenu**



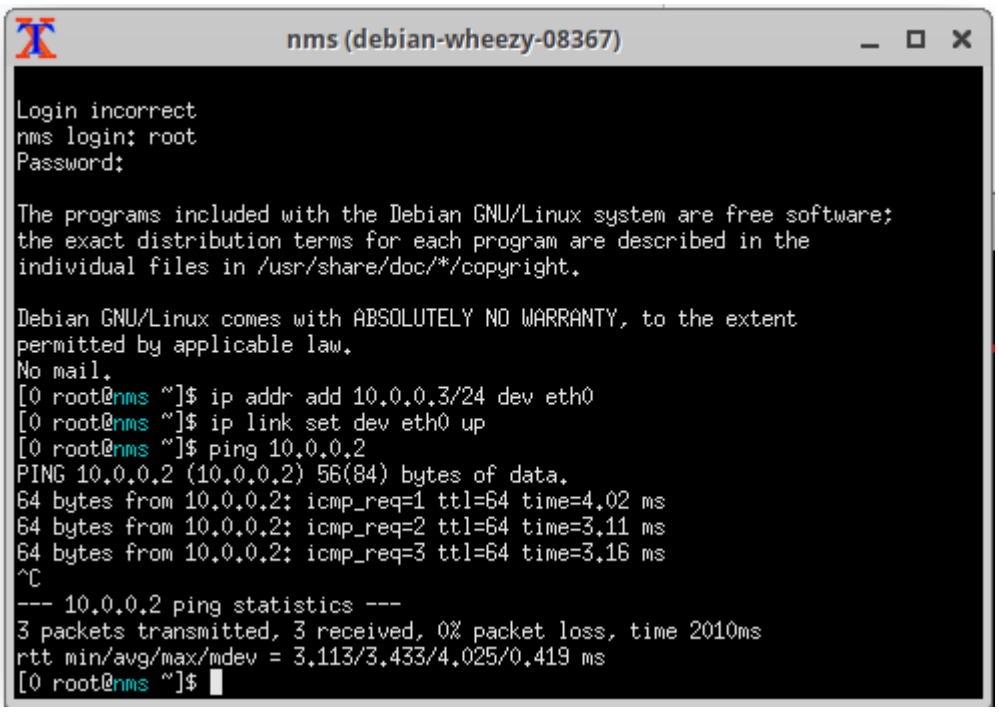

## Configuration du client 1



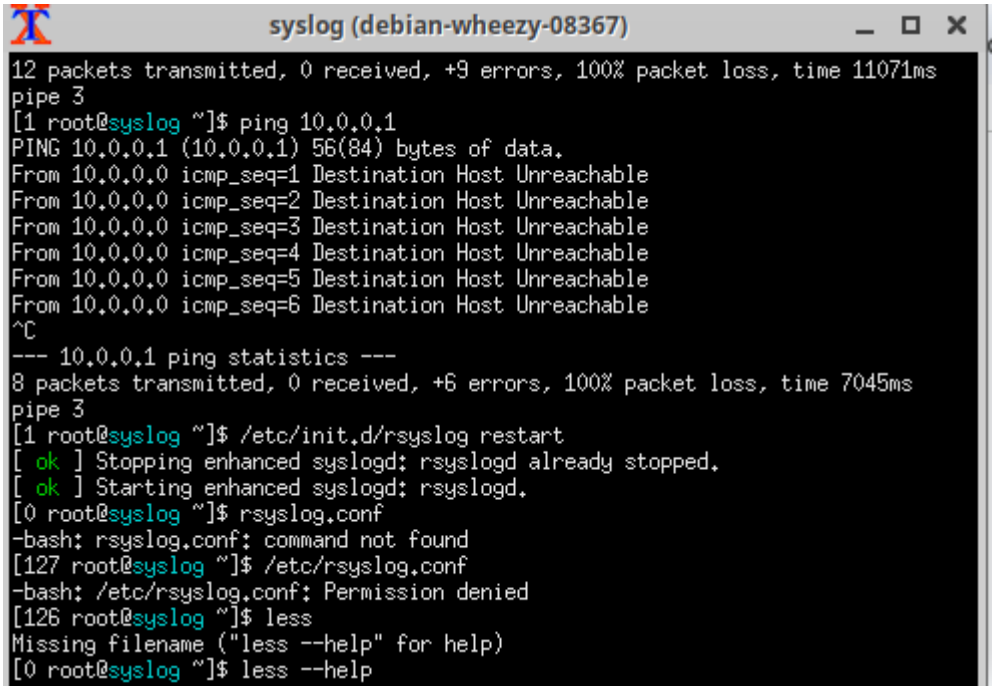
## Configuration du client 2




## Configuration du nms



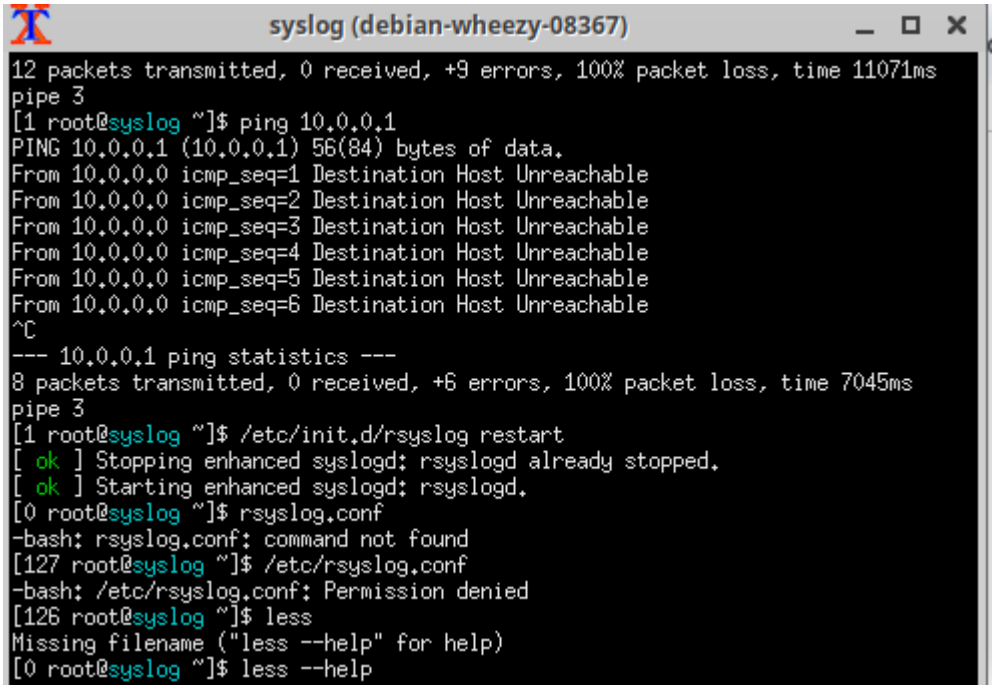
**Configuration du syslog**




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

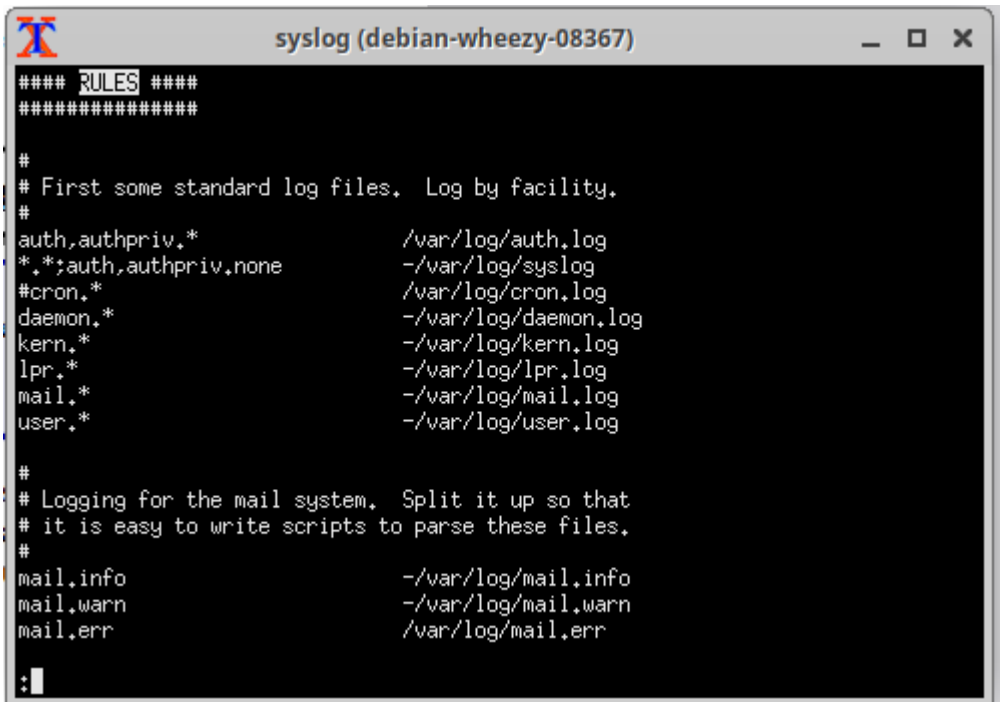
### I 2.1 Démarrer le service rsyslog sur la machine syslog avec la commande

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




### 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**

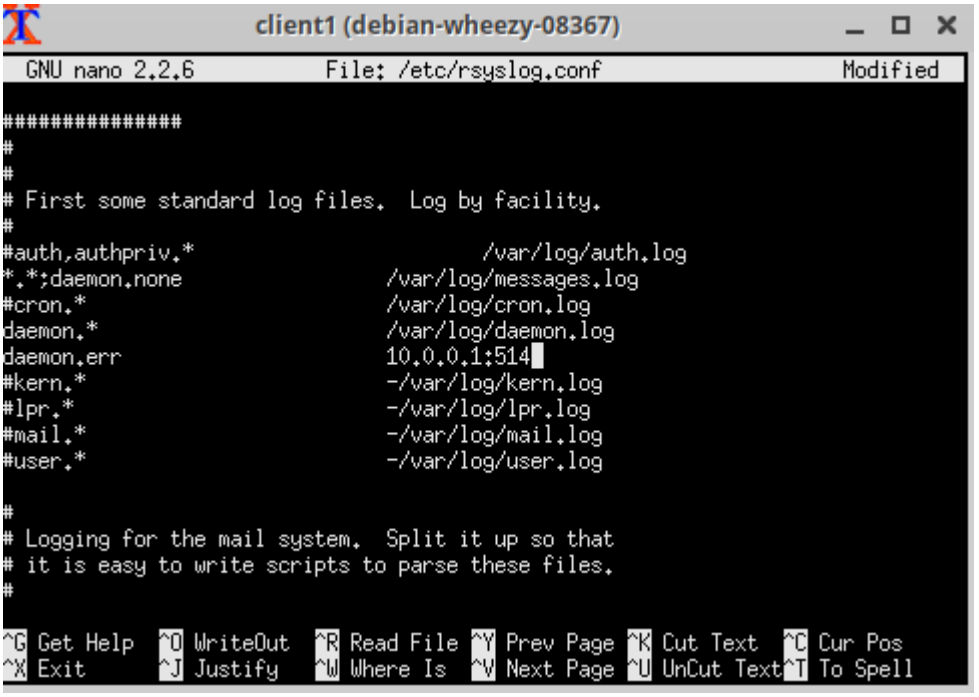



## Exercice 3 — Configuration de rsyslog sur les deux clients

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

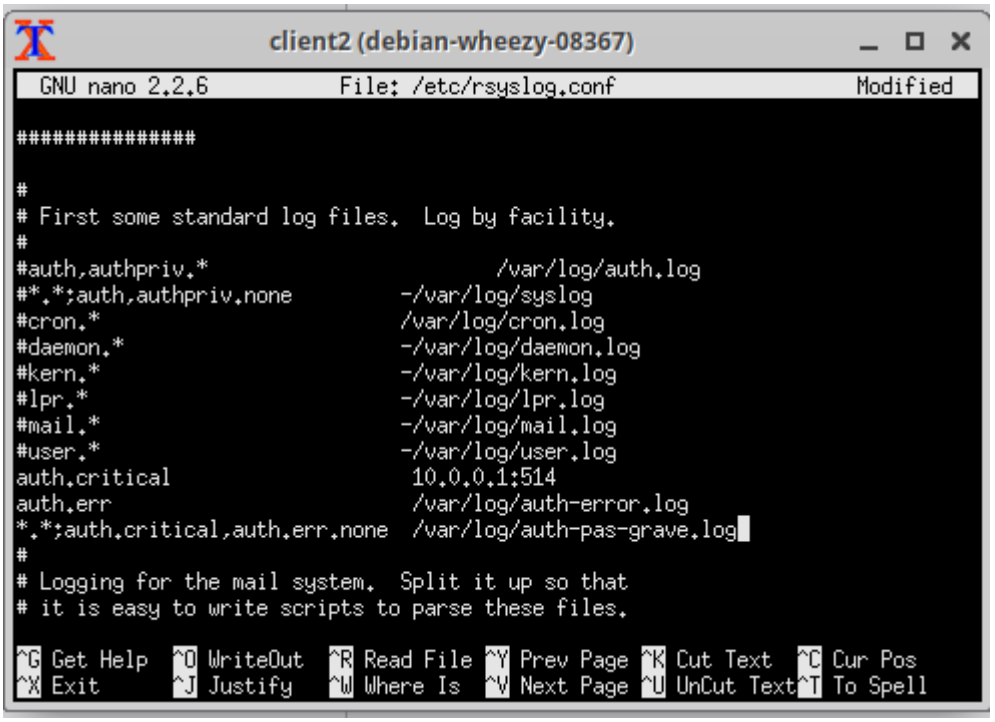
**1. stocker les messages de la catégorie daemon dans le fichier /var/log/daemon.log;**


**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**




**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.**



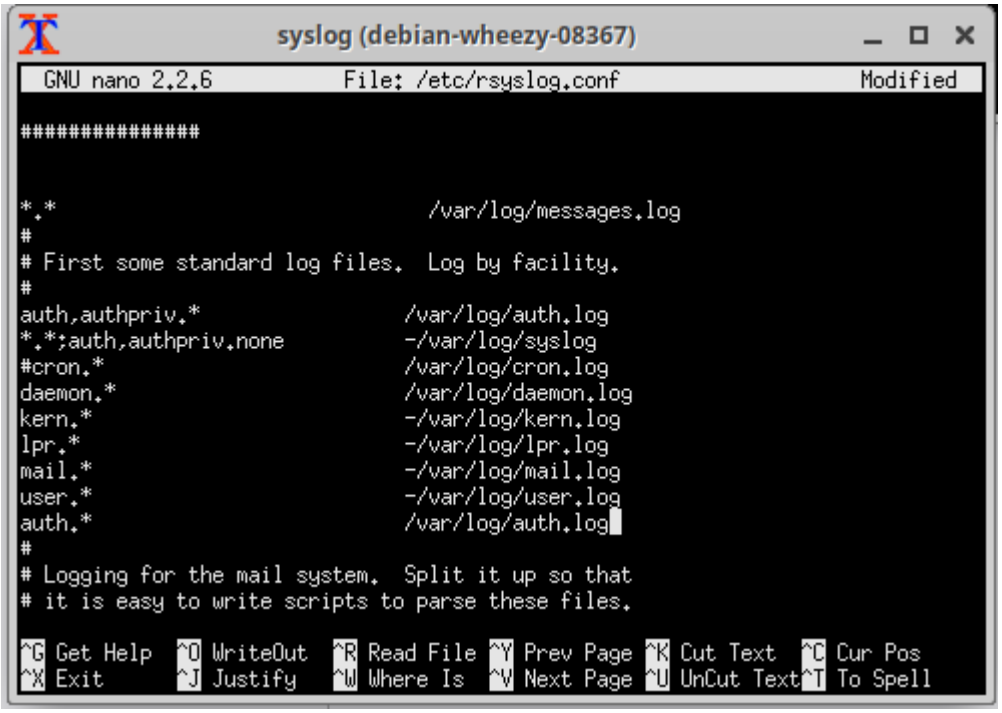

## Exercice 4 — Configuration du serveur rsyslog

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


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

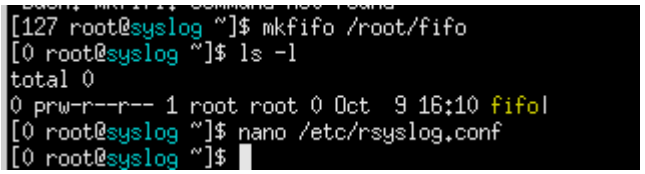
**3) Les messages (reçus ou générés par la machine syslog) des catégories auth et daemon seront stockés dans les fichiers /var/log/auth.log et /var/log/daemon.log respectivement.**

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



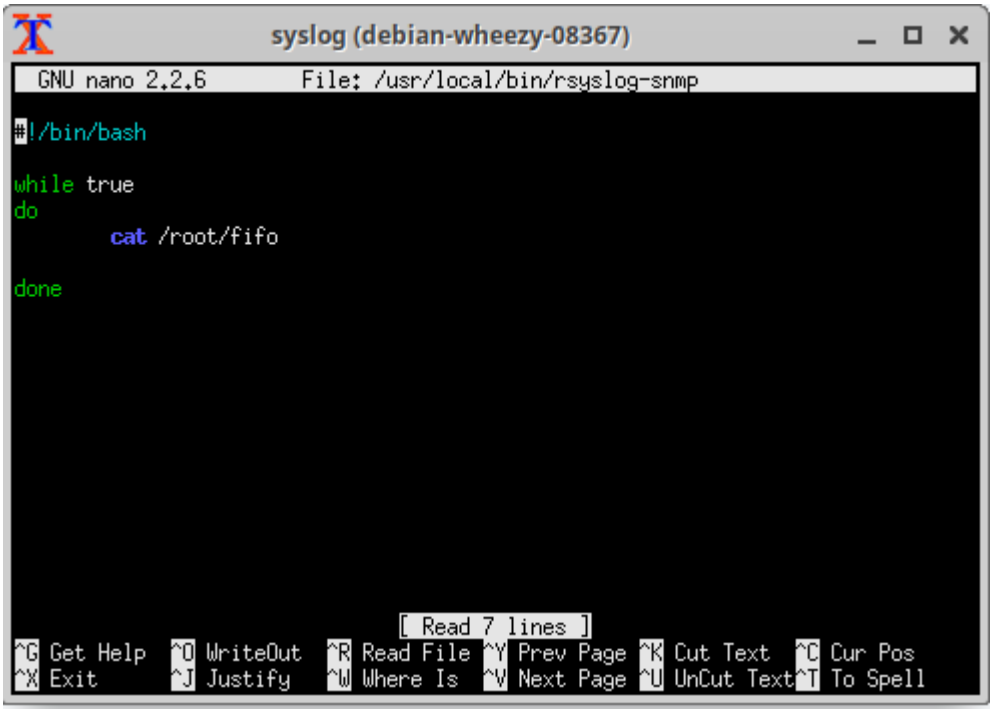

## Exercice 5 — Envoi de notifications SNMP

**Création du tube**

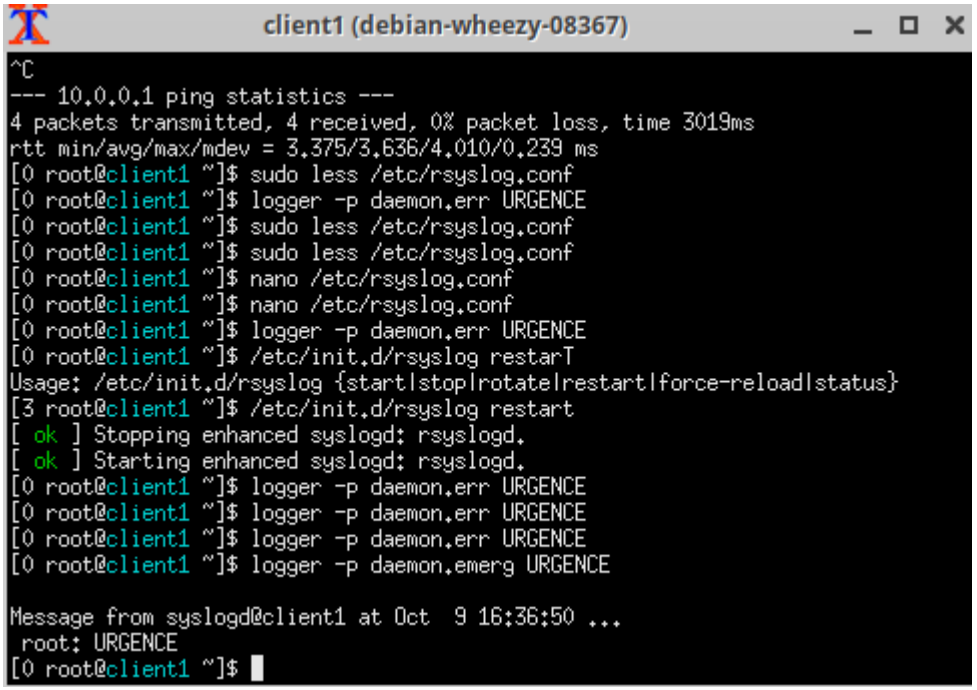



**Configuration pour que les messages auth de gravité emerg et les messages daemon de gravité emerg soient envoyés au tube**

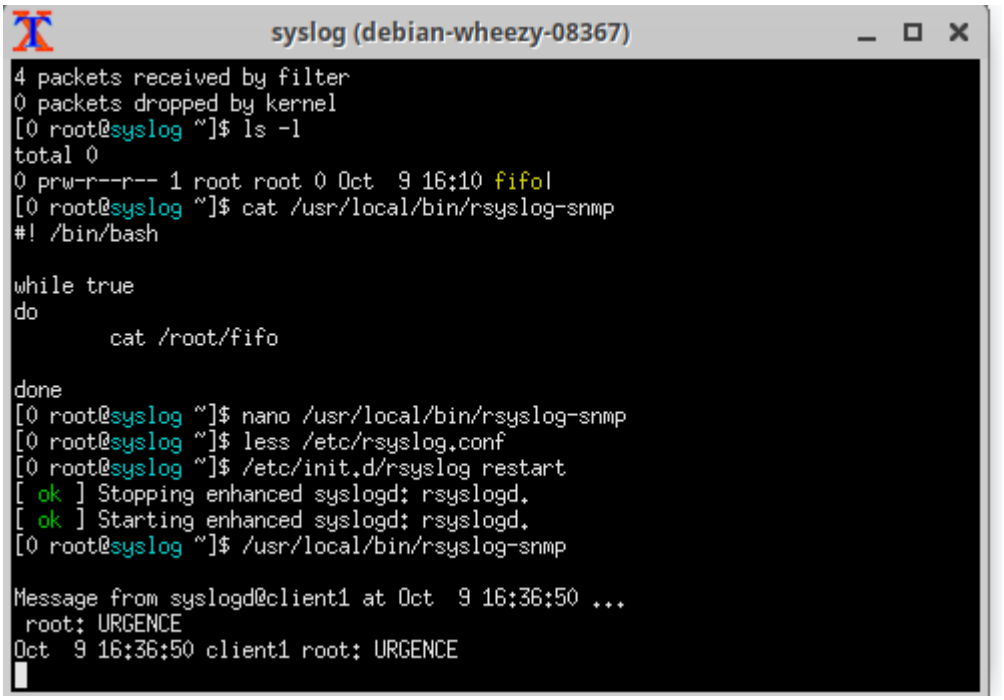

**On fait une configuration sur la machine syslog pour afficher le contenu du tube créé**




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



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




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