# TP5 : Syslog

Table des matières

[TP5 : Syslog 1](#_Toc43248593)

[1. Installation du Serveur 1](#_Toc43248594)

[2. Installation Client 1](#_Toc43248595)

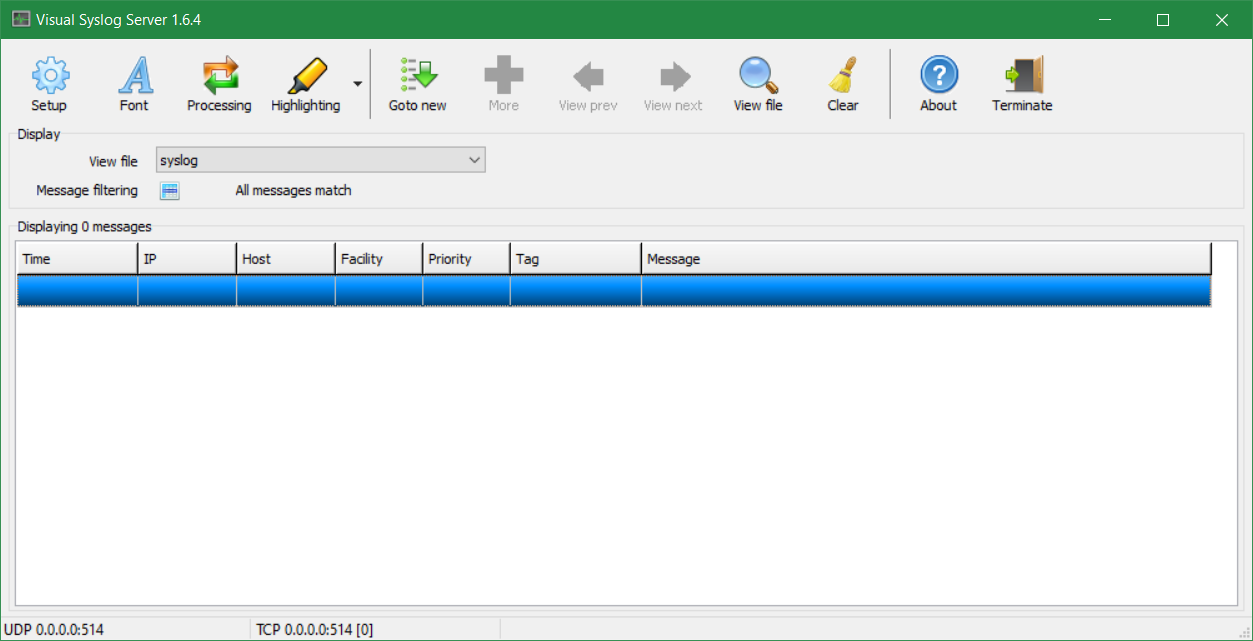
[3. Visual syslog Server 2](#_Toc43248596)

[4. Mise en place de prévention par Mail 3](#_Toc43248597)

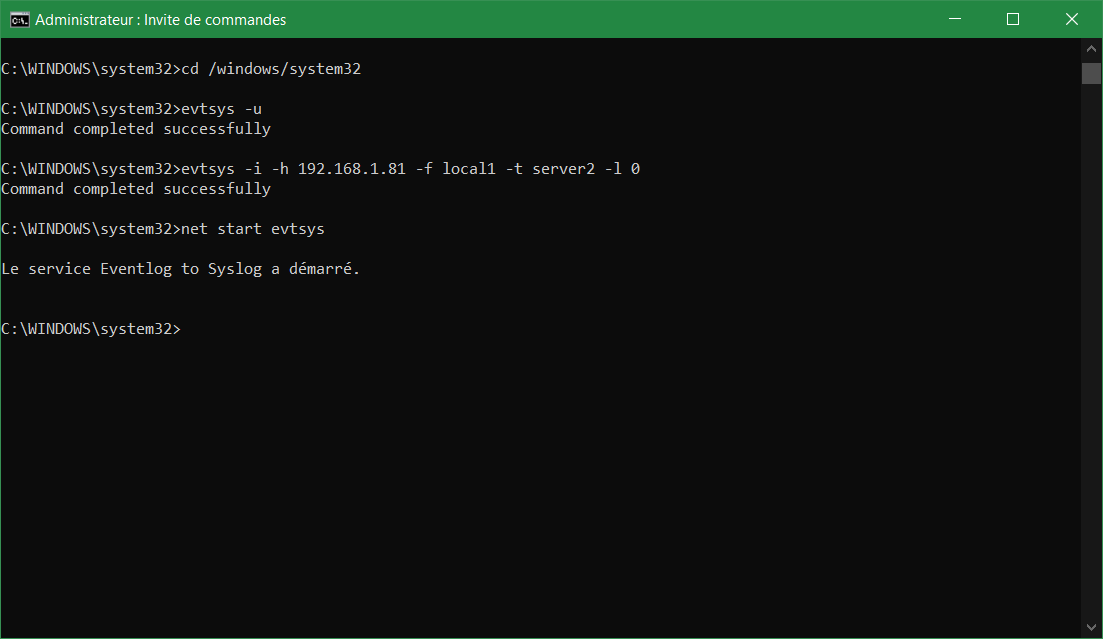
[5. Rotation de fichier de log 4](#_Toc43248598)

## Installation du Serveur

Ceci est le serveur qui va afficher tous les évènements qui vont se produire dans la foulé.



## Installation Client



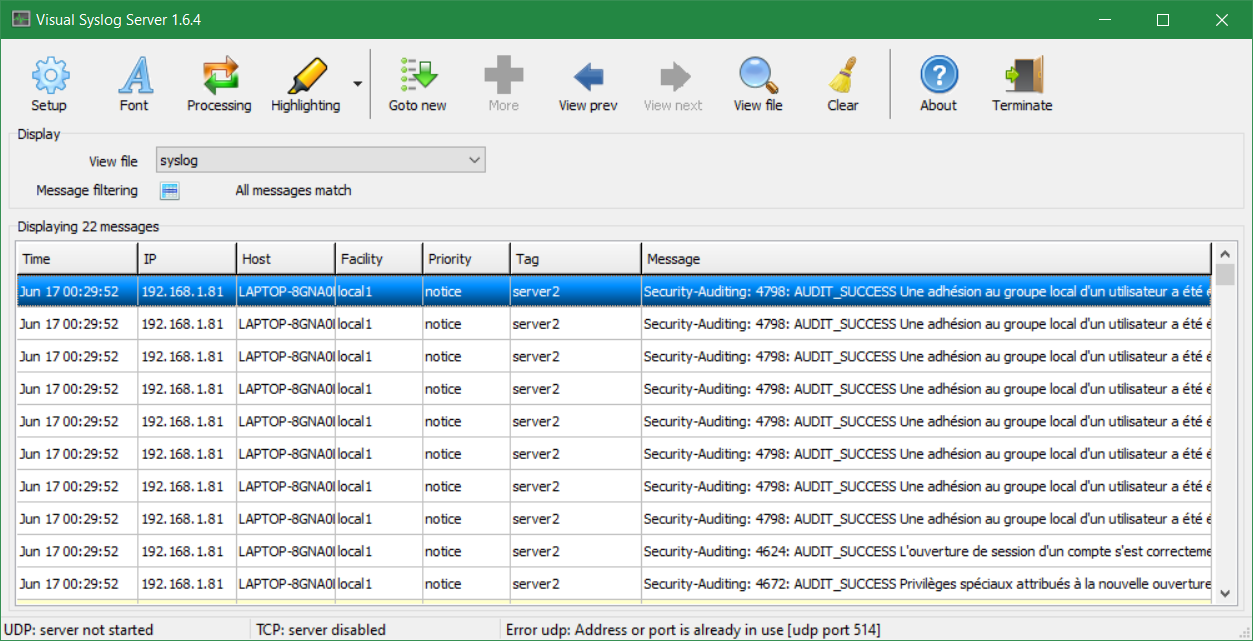
-i Install service

-h host Name of log host(s), separated by a ';'

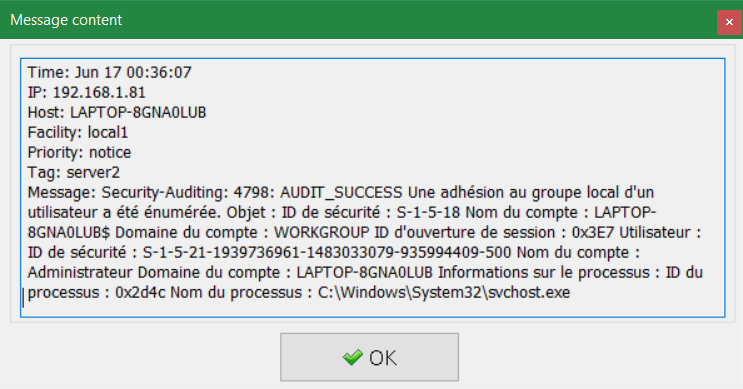
-f facility Facility level of syslog message

## Visual syslog Server

Après toute cette mise en place nous pouvons voir que maintenant que le serveur syslog est en place.



Celui-ci nous renvoi qu’un utilisateur a été créé et qu’il c’est connecter au serveur de LOG.



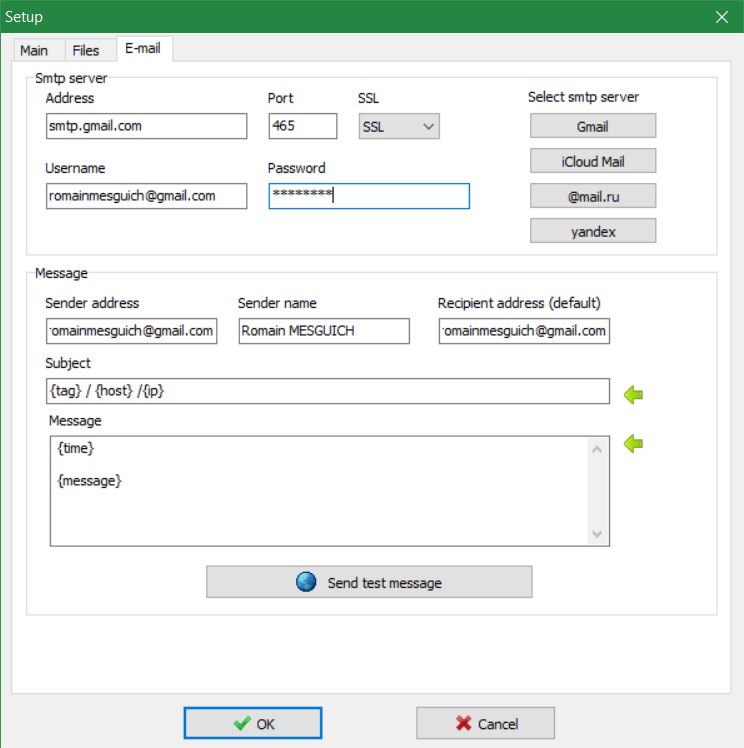
Nous pouvons voir l’IP de la machine ainsi que le Numéro de sécurité se référent au message.

Nous pouvons voir ici qu’il y a 3 niveau de message :

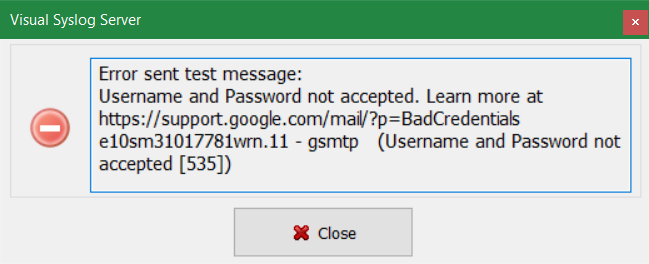


## Mise en place de prévention par Mail

Nous pouvons créer une alerte par mail, c’est-à-dire que dès qu’il y a une alerte nous sommes prévenu par email.



Malheureusement ce genre de mesure ne fonctionne pas avec les comptes ayant activer la double authentification.



## Rotation de fichier de log

Nous mettons en place maintenant des fichiers de Logs. Il sera créé un fichier toute les 5 heures par jours avec comme nom de fichier syslog(date).

