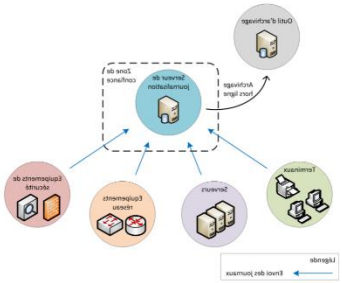
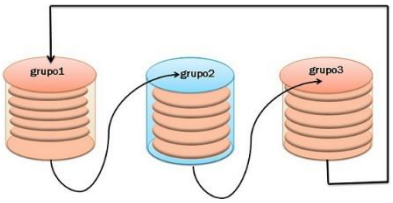


Journalisation



Documentation

1. Définir le rôle des fichiers de journaux.
   En informatique, le concept de sauvegarder les événements de journalisation c'est chaque jour tout est enregistré, on appelle ça l'enregistrement séquentiel dans un fichier ou dans une base de données, mais ça enregistre plus particulièrement les applications, l'activité dans un réseau informatique et bien d'autre…)

2. Définir le rôle d'un serveur syslog.
   Il y a 2 parties la partie syslog qui est un protocole et qui se comporte comme un client, et la 2éme partie le serveur, le client émet des informations sur le réseau sur le port UDP 514 et les serveurs s'occupe de collecter les informations et se chargent de créer les journaux.
   https://www.auditmypc.com/udp-port-514.asp

3. Quel protocole réseau est utilisé par syslog par défaut ?
   Il utilise le protocole UDP 514 il accepte les entrées syslog des hôtes distants.

4. Définir, dans le contexte de syslog les termes : périphérique, relais, collecteur.
   - Périphérique : est une machine ou une application qui génère des messages Syslog.
   - Relais : est une machine ou une application qui reçoit des messages Syslog et les retransmet à une autre machine.
   - Collecteur : est une machine ou une application qui reçoit des messages Syslog, mais qui ne les retransmet pas.
5. Définir, dans le contexte de syslog les termes : origine, priorité.
   - Origine : origine sont des messages orientés, dont des codes qui sont regroupés par des types qui sont appeler des "facilités", soit d'origine de loca10 jusqu'à loca17 bien évidement personnalisable
   - Priorité : La priorité d'un message Syslog est définie par sa fonctionnalité et sa sévérité. Cette priorité et du au résultat d'une multiplication de la fonctionnalité et elle est multiplier par 8 sur les quelle s'ajoute la sévérité.
   - https://ram-0000.developpez.com/tutoriels/reseau/Syslog/#LII-B
6. Expliciter le fonctionnement d'un serveur syslog. Quelques éléments à considérer :
   — Journal c'est un protocole qui sert à envoyer des fichiers du journal système qui ont été traiter soumis à des événements et ils sont envoyés directement au serveur qui lui les stocks.
   — Supervision ce sont plusieurs choses à prendre en compte c'est à dire : il y a 3 notions qui ont un rôle particulier, il y a le périphérique, le relais et le collecteur. Tous les périphériques ou le relais sera considéré comme l'émetteur, quand il envoie un message, Syslog et ses relais ou les collecteurs sera considéré comme un récepteur quand il reçoit le message de Syslog. Sa forme une boucle.
   — Sécurité exige mais le syslog utilise un port UDP 514 c'est un protocole qui s'appelle Datagram c'est un protocole de communication pour la couche réseau internet, la couche transport et la couche session. Mais le port UDP 514 du protocole a été signalé comme virus il ne permet pas de passer par le port mais il parait que dans le passé il a été utiliser pour communiquer avec.

Installation et configuration du service

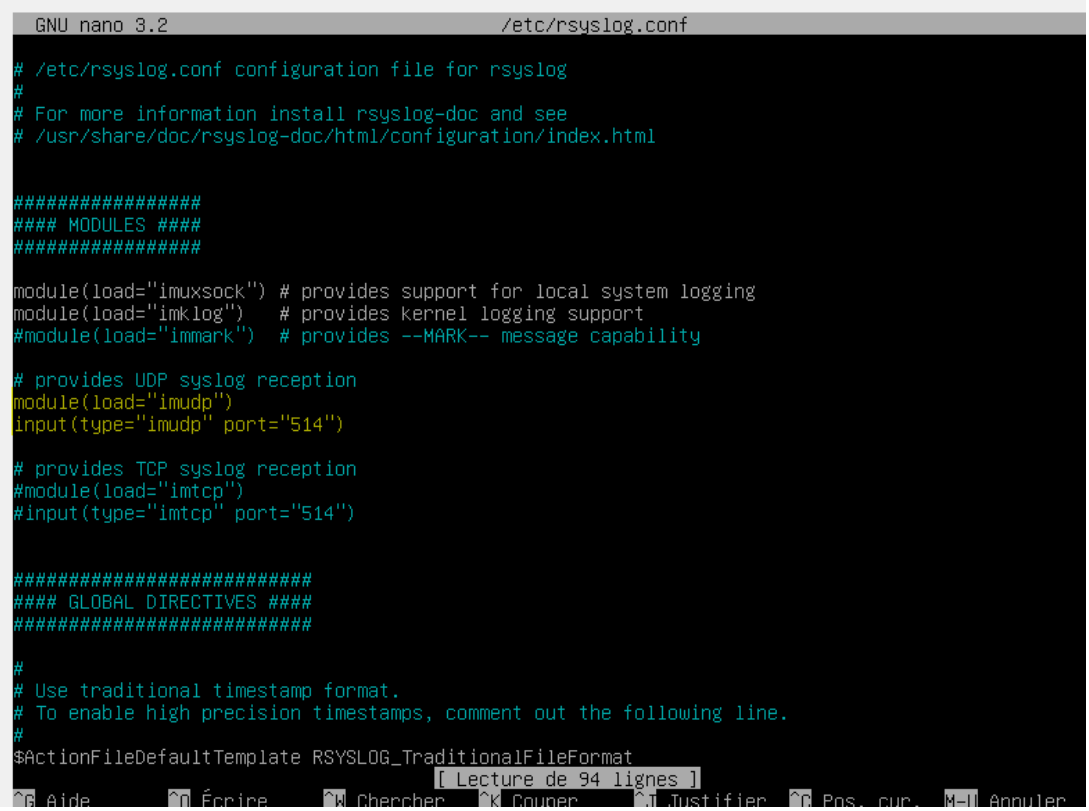
Utilisation de Rsyslog :

Rsyslog est déjà installer sur la machine.

Configuration du serveur syslog :

Editer le fichier rsyslog.conf

Nano /etc/rsyslog.conf



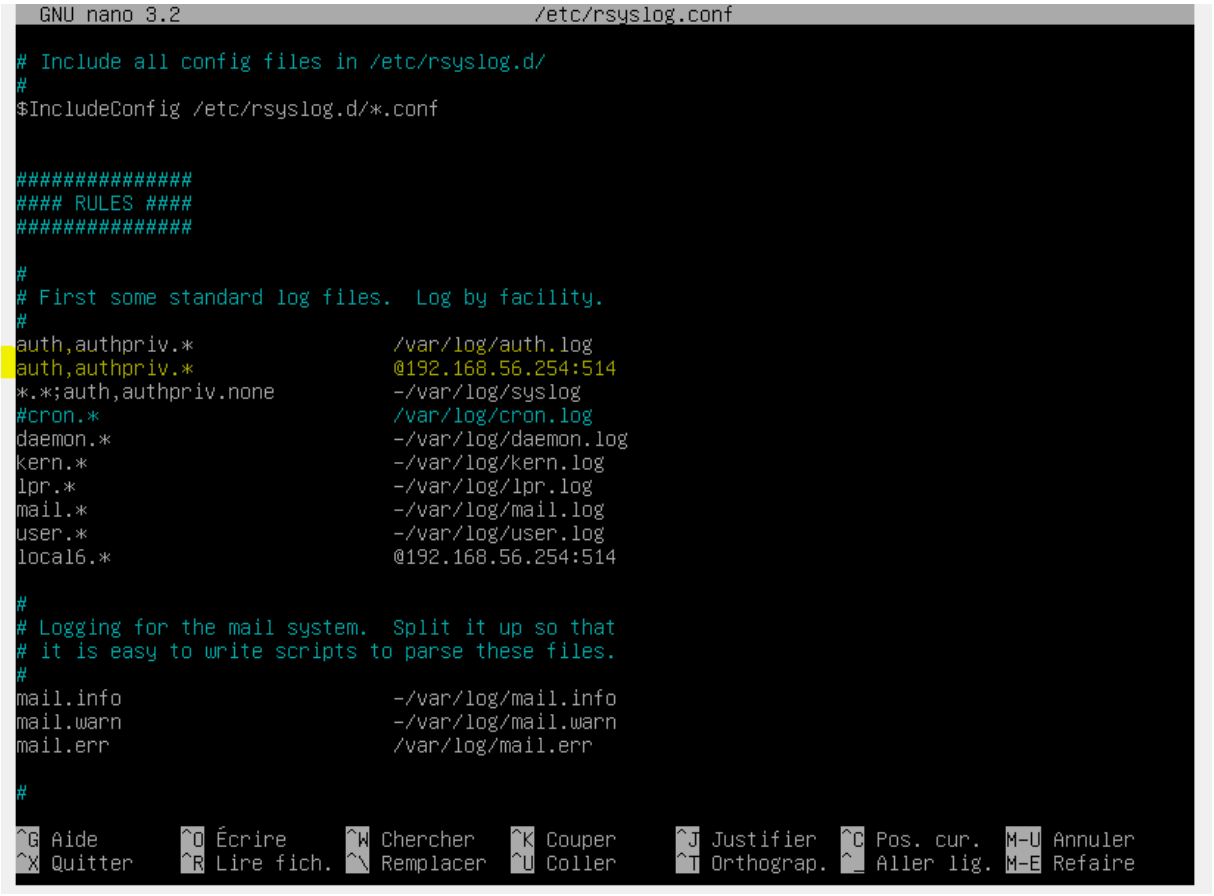
Décocher les # sur les lignes en jaune (c'est pour que le serveur de log puisse écouter sur le port UDP 514). Save la conf.

Faire un test pour savoir si le port UDP et ouvert :

Netstat -nul

```
root@Debian-Gate:~# netstat -u
Connexions Internet actives (sans serveurs)
Proto Recv-Q Send-Q Adresse locale          Adresse distante        Etat
root@Debian-Gate:~# netstat -nul
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale          Adresse distante        Etat
udp        0      0 0.0.0.0:514             0.0.0.0:*
udp        0      0 192.168.56.254:53       0.0.0.0:*
udp        0      0 192.168.1.38:53         0.0.0.0:*
udp        0      0 127.0.0.1:53            0.0.0.0:*
udp        0      0 0.0.0.0:67              0.0.0.0:*
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp6       0      0 :::514                  :::*
udp6       0      0 :::53                   :::*
root@Debian-Gate:~# _
```

On va effectuer un test avec les logs de connexion du serveur root :



Donc on rajoute une ligne sous **auth,authpriv.*** et on rajoute l'IP du serveur de journalisation donc dans mon cas ***192.168.56.254 :514** avec le port

Quelques notions à savoir :

Les **facilites** sont des catégories dans lesquelles les logs vont se "ranger" afin de mieux les archiver et les trier

- **auth** : Utilisé pour des évènements concernant la sécurité ou l'authentification à travers des applications d'accès (type SSH)

- **authpriv** : Utilisé pour les messages relatifs au contrôle d'accès
- **daemon** : Utilisé par les différents processus systèmes et d'application
- **kern** : Utilisé pour les messages concernant le kernel
- **mail** : Utilisé pour les évènements des services mail
- **user** : Facilitie par défaut quand aucune n'est spécifiée
- **local7** : Utilisé pour les messages du boot
- ***** : Désigne toutes les facilities, par soucis de simplicité c'est ce que nous avons spécifié lors de notre première règle de redirection des logs un peu plus haut
- **none** : Désigne aucune facilites

En plus de ces facilites, nous retrouvons pour chaque facilities un niveau de gravité (appelé **Priorité**) qui va du plus grave à la simple information :

- **Emerg** : Urgence, système inutilisable
- **Alert** : Alerte. Intervention immédiate nécessaire
- **Crit** : Erreur système critique
- **Err** : Erreur de fonctionnement
- **Warning** : Avertissement
- **Notice** : Évènements normaux devant être signalé
- **Info** : Pour information
- **Debug** : Message de debogage

Maintenant on test :

```
root@Debian-Gate:~# tail -f /var/log/auth.log
May 28 23:24:11 Debian-Gate systemd-logind[259]: Removed session 31.
May 28 23:24:16 Debian-Gate login[4098]: pam_unix(login:auth): authentication failure; logname=LOGIN
 uid=0 euid=0 tty=/dev/tty1 ruser= rhost=  user=root
May 28 23:24:19 Debian-Gate login[4098]: FAILED LOGIN (1) on '/dev/tty1' FOR 'root', Authentication
failure
May 28 23:24:24 Debian-Gate login[4098]: pam_unix(login:auth): check pass; user unknown
May 28 23:24:24 Debian-Gate login[4098]: pam_unix(login:auth): authentication failure; logname=LOGIN
 uid=0 euid=0 tty=/dev/tty1 ruser= rhost=
May 28 23:24:27 Debian-Gate login[4098]: FAILED LOGIN (2) on '/dev/tty1' FOR 'UNKNOWN', Authenticati
on failure
May 28 23:24:34 Debian-Gate login[4098]: FAILED LOGIN (3) on '/dev/tty1' FOR 'root', Authentication
failure
May 28 23:24:38 Debian-Gate login[4098]: pam_unix(login:session): session opened for user root by LO
GIN(uid=0)
May 28 23:24:38 Debian-Gate systemd-logind[259]: New session 62 of user root.
May 28 23:24:38 Debian-Gate login[4105]: ROOT LOGIN  on '/dev/tty1'
_
```

Comme on peut le voir j'ai effectué plusieurs authentifications avec un faux utilisateur et on peut voir qu'il y a plusieurs FAILED LOGIN (3) donc on peut voir que les logs fonctionnent bien.

Maintenant nous allons passer au log sur apache :

Donc nous allons éditer le fichier de conf de notre vhosts par exemple :

Nano /etc/apache2/sites-available/site1_vhosts.conf

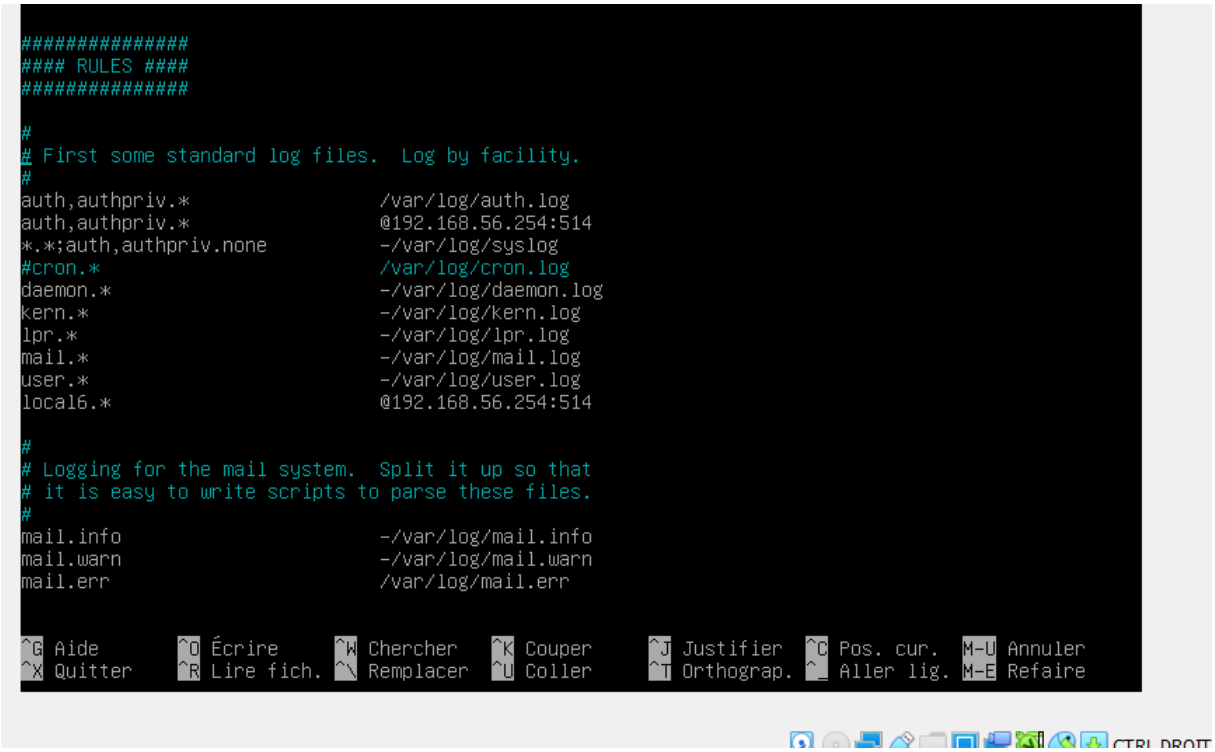
```
 GNU nano 3.2                /etc/apache2/sites-available/site1_vhosts.conf

<VirtualHost *:80>
        ServerAdmin webmaster@site1.gate.hyp
        DocumentRoot "/var/www/vhosts/site1/"
        ServerName site1.gate.hyp
        ErrorLog "|/usr/bin/logger -t apache -p local6.info"
        CustomLog "|/usr/bin/logger -t apache -p local6.info" combined
        #ErrorLog "/var/log/apache2/site1_error_log"
        #Customlog "/var/log/apache2/site1_access_log" combined
        LogLevel info
</VirtualHost>
```

Donc comme on peut le voir j'ai commenté les chemins qui pointe sur apache2.

Je renvoie tout dans **|/usr/bin/logger -t apache -p local6.info** donc on utilise logger gérer les logs en ligne de commande. Et pour local6 c'est le code facilité graviter pour de l'information et pour finir LogLevel info pour générer des logs plus facilement.

Puis on repart dans le fichier de conf nano **/etc/rsyslog.conf**



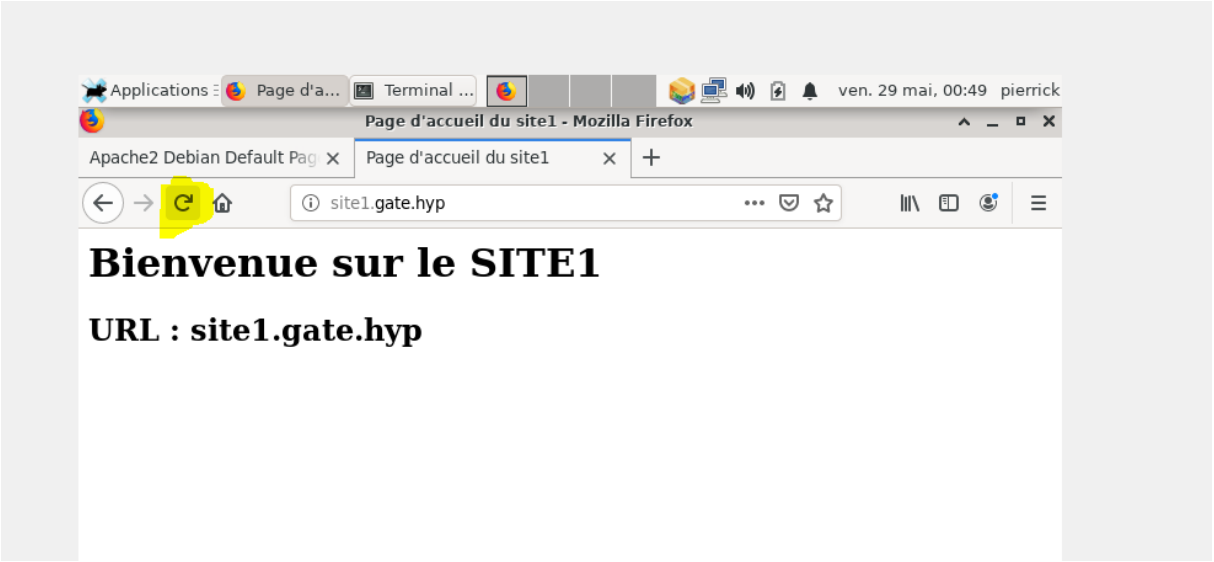
Et on rajoute le **local6.* avec l'ip @192.168.56.254 :514**

Une fois fini on redémarre le service apache2 et rsyslog

Systemctl restart apache2

Systemctl restart rsyslog.service

On passe sur une page de test avec un client :



On prend un client et on recharge plusieurs fois la page web pour que des logs soit envoyer sur le serveur.

On se retrouve sur le serveur :

```
root@Debian-Gate:~# tail -f /var/log/messages
May 28 17:18:38 Debian-Gate apache: 192.168.56.10 - - [28/May/2020:17:18:38 +0200] "GET / HTTP/1.1"
200 476 "-" "Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0"
May 28 17:18:38 Debian-Gate apache: 192.168.56.10 - - [28/May/2020:17:18:38 +0200] "GET / HTTP/1.1"
200 476 "-" "Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0"
May 28 17:18:39 Debian-Gate apache: 192.168.56.10 - - [28/May/2020:17:18:39 +0200] "GET / HTTP/1.1"
200 476 "-" "Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0"
May 28 17:18:39 Debian-Gate apache: 192.168.56.10 - - [28/May/2020:17:18:39 +0200] "GET / HTTP/1.1"
200 476 "-" "Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0"
May 28 17:18:39 Debian-Gate apache: 192.168.56.10 - - [28/May/2020:17:18:39 +0200] "GET / HTTP/1.1"
200 476 "-" "Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0"
May 28 17:18:40 Debian-Gate apache: 192.168.56.10 - - [28/May/2020:17:18:40 +0200] "GET / HTTP/1.1"
200 476 "-" "Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0"
May 28 17:18:40 Debian-Gate apache: 192.168.56.10 - - [28/May/2020:17:18:40 +0200] "GET / HTTP/1.1"
200 476 "-" "Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0"
May 28 18:34:02 Debian-Gate apache: 192.168.56.10 - - [28/May/2020:18:34:02 +0200] "GET / HTTP/1.1"
200 477 "-" "Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0"
May 29 00:00:06 Debian-Gate rsyslogd:  [origin software="rsyslogd" swVersion="8.1901.0" x-pid="3298"
 x-info="https://www.rsyslog.com"] rsyslogd was HUPed
May 29 00:49:44 Debian-Gate apache: 192.168.56.10 - - [29/May/2020:00:49:44 +0200] "GET / HTTP/1.1"
200 477 "-" "Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0"
```

Tail -f /var/log/messages nous affiches quand la page a été ouverte et on remarque que j'ai charger la page a 00H49 et 44 secondes