

RSyslog

Sur une Ubuntu

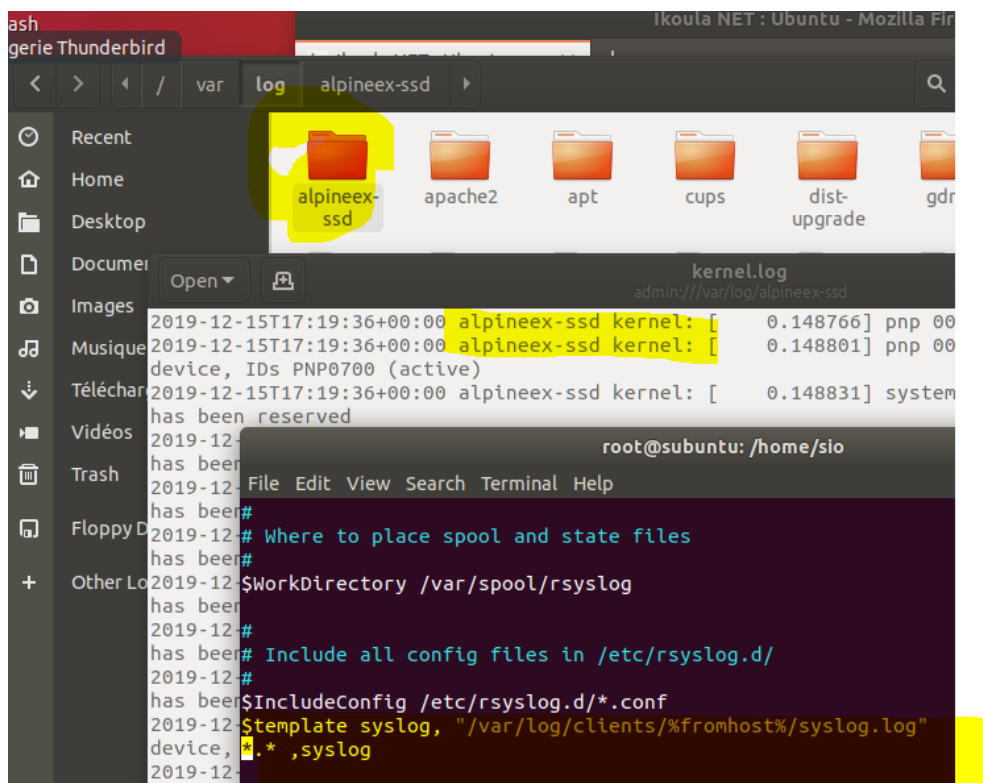
Rsyslog est installé par défaut sur Ubuntu

:

Connaitre la version	<code>rsyslogd -v</code>	<pre>root@subuntu:/home/sio# rsyslogd -v rsyslogd 8.32.0, compiled with: PLATFORM: x86_64-pc-linux-gnu PLATFORM (lsb_release -d): FEATURE_REGEX: Yes GSSAPI Kerberos 5 support: Yes FEATURE_DEBUG (debug build, slow code): No 32bit Atomic operations supported: Yes 64bit Atomic operations supported: Yes memory allocator: system default Runtime Instrumentation (slow code): No uuid support: Yes systemd support: Yes Number of Bits in RainerScript integers: 64</pre>
Checker le service	<code>systemctl status rsyslog</code>	<pre>root@subuntu:/home/sio# systemctl status rsyslog ● rsyslog.service - System Logging Service Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset: Active: active (running) since Sun 2019-12-15 15:17:18 UTC; 10min ago</pre>
Configurer le serveur	<code>vim /etc/rsyslog.conf</code>	<p>Décommenter les lignes pour udp et tcp port :</p> <pre>module(load="imudp") input(type="imudp" port="514") # provides TCP syslog reception module(load="imtcp") input(type="imtcp" port="514")</pre>
	Pour limiter les émetteurs a une adresse IP	
	<code>\$AllowedSender TCP, 127.0.0.1, 192.168.10.0/24, *.example.com</code>	
	Créer un modele pour la reception des messages avec un dossier par client	Ajouter ces deux lignes dans le fichier de config
		<pre>1 \$template syslog, "/var/log/clients/%fromhost%/syslog.log" 2 *.* ?syslog</pre>
Redemarrer le service	<code>systemctl restart rsyslog</code>	
Controler	<code>Ss -tunelp grep 514</code>	<pre>root@subuntu:/home/sio# systemctl restart rsyslog root@subuntu:/home/sio# ss -tunelp grep 514 udp UNCONN 0 0 0.0.0.0:514 0.0.0.0:* users:(("rsyslogd",pid=10749,fd=5)) ino:110901 sk:3 <-> udp UNCONN 0 0 [::]:514 [::]:* users:(("rsyslogd",pid=10749,fd=6)) ino:110902 sk:9 v6only:1 <-> tcp LISTEN 0 25 0.0.0.0:514 0.0.0.0:* users:(("rsyslogd",pid=10749,fd=7)) ino:110908 sk:d <-> tcp LISTEN 0 25 [::]:514 [::]:* users:(("rsyslogd",pid=10749,fd=8)) ino:110909 sk:11 v6only:1 <-></pre>

Configurer le firewall Rsyslog	<pre>sudo ufw allow 514/tcp sudo ufw allow 514/udp</pre>	
Configurer Rsyslog Sur les clients	<pre>vim /etc/rsyslog.conf *. * @ip-address-of-rsyslog-server:514</pre>	

Résultats le dossier Alpineex-ssd est crée et on voit les logs.



Rsyslog est paramétré de base mais on peut gérer les priorités.

- **auth** : Utilisé pour des événements 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 événements des [services](#) mail
- **user** : Facilité par défaut quand aucune n'est spécifiée
- **local7** : Utilisé pour les messages du boot
- ***** : Désigne toutes les facilités, 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 facilités

En plus de ces facilités, nous retrouvons pour chaque facilités 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** : Évènement normaux devant être signalé
- **Info** : Pour information
- **Debug** : Message de débogage