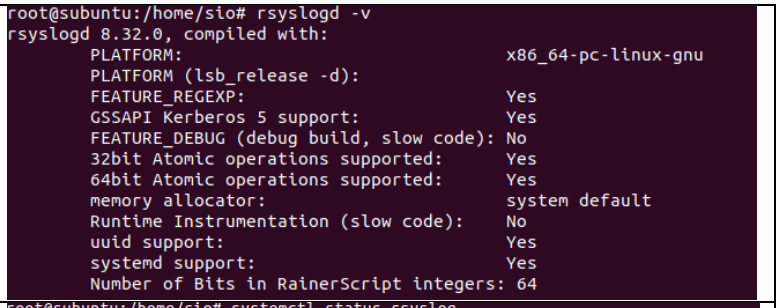
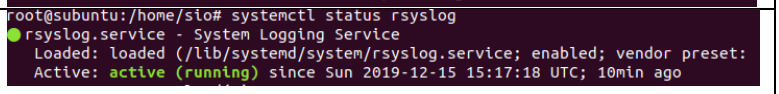
RSyslog

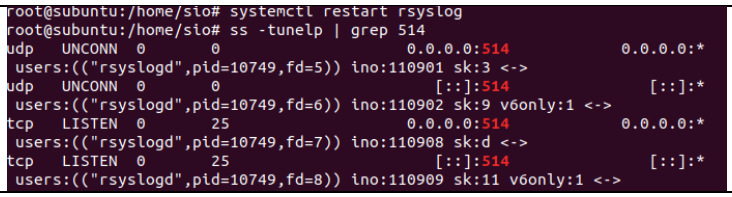
Sur une Ubuntu

Rsyslog est installé par defaut sur Ubuntu

:

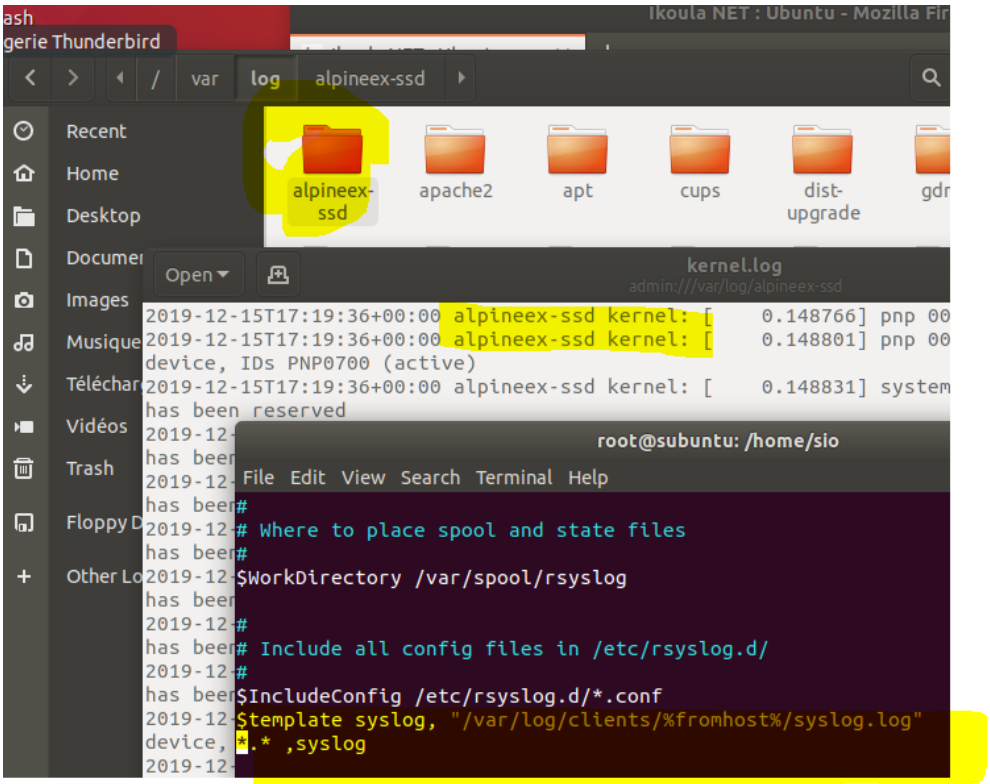
Connaitre la version	rsyslogd -v	
Checker le service	systemctl status rsyslog	

Configurer le serveur	vim /etc/rsyslog.conf	Décommenter les lignes pour **udp** et **tcp** port :
		
		module(load="imudp")
		input(type="imudp" port="514")
		
		# provides TCP syslog reception
		module(load="imtcp")
		input(type="imtcp" port="514")

	Pour limiter les émetteurs a une adresse IP $AllowedSender TCP, 127.0.0.1, 192.168.10.0/24, *.example.com	
	Créer un modele pour la reception des messages avec un dossier par client	Ajouter ces deux lignes dans le fichier de config 1 $template syslog,"/var/log/clients/%fromhost%/syslog.log" 2 *.* ?syslog
Redemarrer le service	systemctl restart rsyslog	
Controler	Ss -tunelp | grep 514	

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

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 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** : Évènement normaux devant être signalé
- **Info** : Pour information
- **Debug** : Message de debogage