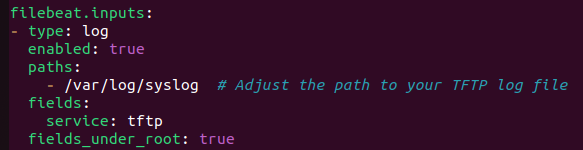
Analyse TFTP

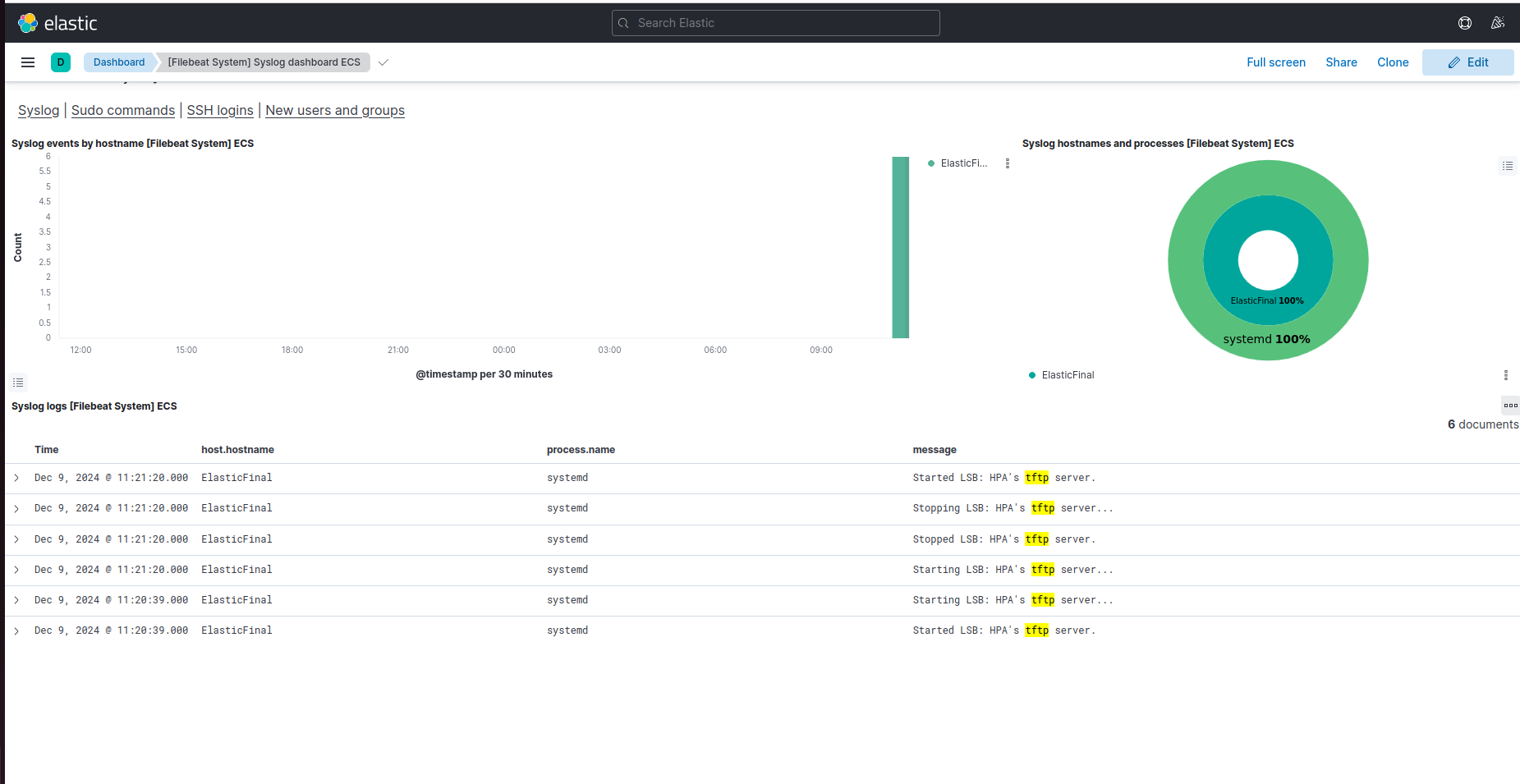
Sudo apt install tftpd-hpa

Dans /etc/default/tftpd-hpa :

TFTP\_OPTIONS="--secure --verbose --create"

Dans /etc/filebeat/filebeat.yml :





### **Contexte et Observations**

* Le tableau de bord **Kibana** affiche les événements de logs liés au service TFTP (HPA's TFTP server) collectés par **Filebeat** et envoyés à **Elasticsearch**.
* Les informations clés observées incluent :
  + **Host** : ElasticFinal.
  + **Processus** : systemd.
  + **Messages de log** : Démarrage et arrêt du serveur TFTP (Starting, Started, Stopping, Stopped).
  + **Représentation graphique** :
    - Une **histogramme temporel** montrant le nombre d'événements par heure.
    - Un diagramme circulaire montrant la répartition par hostname (ElasticFinal) et par processus (systemd).

### **Analyse des Logs**

* **Logs associés à TFTP** :
* Les messages montrent l'état du service TFTP :
* **Starting** : Le processus de démarrage a été initialisé.
* **Started** : Le serveur TFTP est opérationnel.
* **Stopping** : Un processus de fermeture a été demandé.
* **Stopped** : Le serveur TFTP a été arrêté avec succès.
* **Concentration temporelle des événements** :
* Tous les événements sont concentrés dans une courte période (le 9 décembre 2024 entre 11:20 et 11:24).
* Cela suggère que des actions spécifiques ont été exécutées sur le serveur pendant cette période, comme des tests ou une maintenance planifiée.
* **Distribution des logs** :
* La totalité des événements proviennent de l'hôte ElasticFinal, et le processus responsable est systemd.