**Compte rendu :**

# I.1. Installation, test et configuration de Logstash

## I.1) Installation logstash

Après avoir installer logstash on vérifie sa version pour voir que tout marche bien :

Une image contenant texte, Police, capture d’écran

Le contenu généré par l’IA peut être incorrect.

## I.1.2. Test de Logstash

logstash --path.data /tmp/logstash\_data --log.level=error -e "input { stdin {} } output { stdout { codec => rubydebug } }"

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

## I.1.3. Configuration de Logstash

Personnaliser le lancement de logstash avec la configuration :



Puis saisie d’un log : Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

# I.2. Fonctionnement de Logstash

## I.2.1. Arborescence des fichiers

Une image contenant texte, capture d’écran, menu, Police

Le contenu généré par l’IA peut être incorrect.

## I.2.2. Pipelines Logstash

C’est le fichier de conf lancé par notre pipeline :

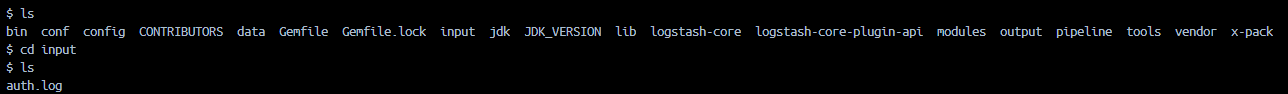
Une image contenant texte, capture d’écran, Police, conception

Le contenu généré par l’IA peut être incorrect.

**II. Exercices**

II.1. Exercice guidé

Création du fichier auth.log avec son contenu sous input :



Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Création du dossier auth sous conf, ainsi que du fichier de configuration logstash.conf :

Une image contenant capture d’écran, texte

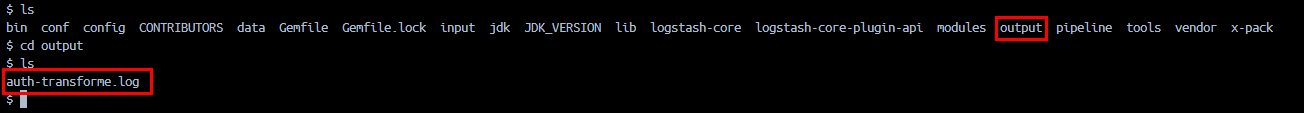
Le contenu généré par l’IA peut être incorrect.

Une image contenant texte, capture d’écran, logiciel

Le contenu généré par l’IA peut être incorrect.

Ici on n’oublie pas de préciser le chemin de notre fichier input et output.

Création du fichier output :



Puis on lance la commande : 

On regarde le résultat dans notre fichier output :

Une image contenant texte, capture d’écran, affichage, logiciel

Le contenu généré par l’IA peut être incorrect.

Comme expliqué dans le TP, on peut voir que « date » et « pid » ne possèdent pas de guillemets car leurs valeurs ont bien été convertis, en date et en nombre.

II.2. Logs multilines

Dans un premier temps on change le contenu du fichier auth.log :

Une image contenant texte, Police, logiciel, capture d’écran

Le contenu généré par l’IA peut être incorrect.

On peut maintenant voir que on a des logs multilines.

Si on relance la configuration précédente avec ses nouveaux logs ont obtient une erreur `\_grokparsefailure`pour la ligne 1 et 5.

Pour résoudre ce problème il nous faut modifier le fichier logstash.conf présente sous conf/auth : Une image contenant texte, capture d’écran, logiciel, affichage

Le contenu généré par l’IA peut être incorrect.

En précisant le codec multilines on indique à logstash que notre intput va être au format multilines.

Cela nous empêche d’avoir l’erreur `\_grokparsefailure` et prend bien en compte tout le log même s’il est sur deux lignes.

Maintenant on peut donc lancer la commande : 

Le résultat dans notre fichier output est affiché dans les erreurs `\_grokparsefailure`, et on peut voir qu’il est précisé pour le log 1 et 5 qu’ils étaient multilines :

Une image contenant texte, capture d’écran, affichage, logiciel

Le contenu généré par l’IA peut être incorrect.