EzPaarse - Exploitation

Liens pour installation et exploitation (en anglais):
https://media.readthedocs.org/pdf/ezpaarse/master/ezpaarse.pdf

Avant propos :

Après installation, l'interface web d'Ezpaarse est accessible ici :

```
http://localhost:59599/
```

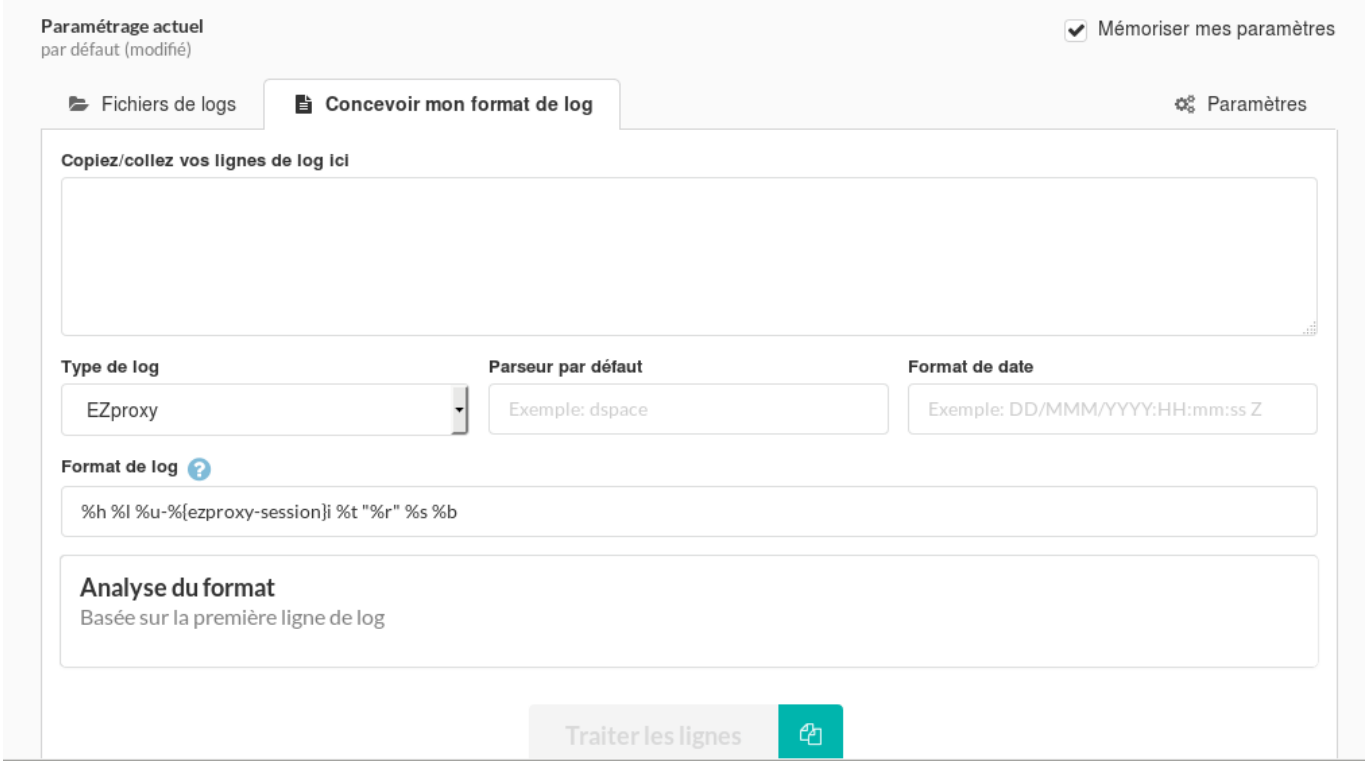
notre serveur Ezpaarse est accessible en intranet ici :

```
http://ezpaarse.univ-lille.fr:59599/
```

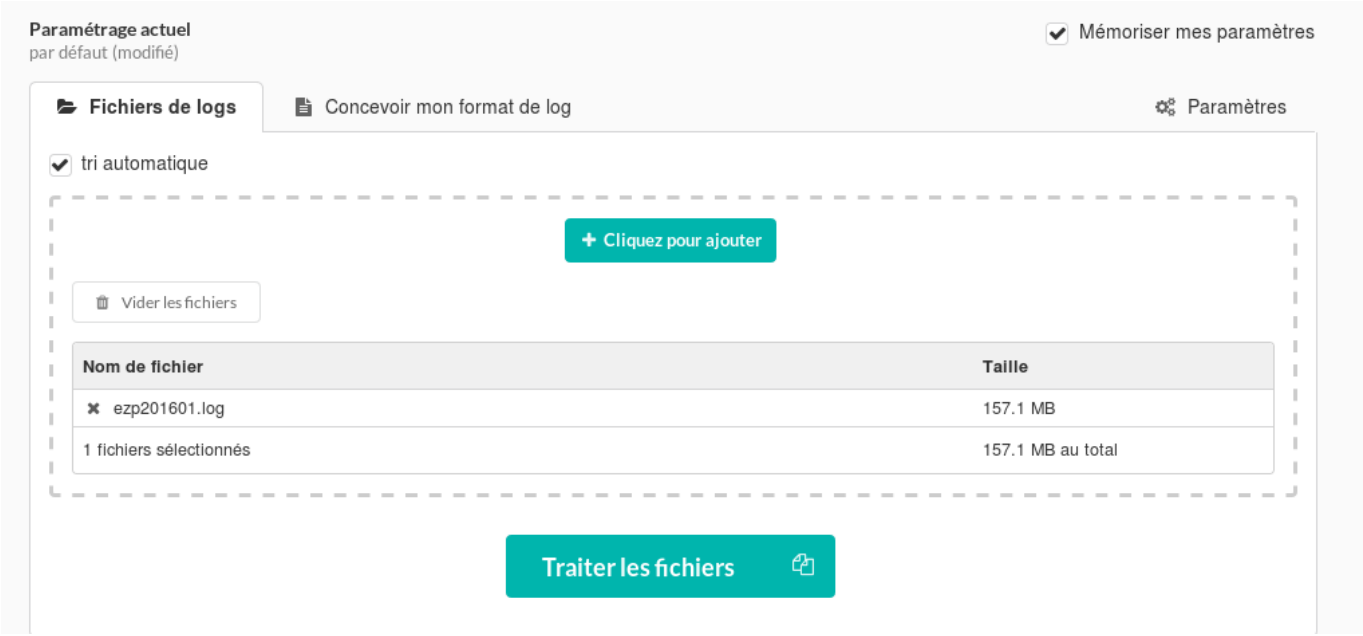
Il faut créer au moins un premier compte administrateur via l'interface web (même si tout peut se faire via API)

Traitement via l'interface Web de Ezpaarse :

Paramétrage pour les logs Lille3



Depot du fichier dans l'autre onglet :



Traitements via les API :

EzPaarse est accessible aussi via webservice. Ce qui est pratique pour automatiser le traitement des logs.

exemple d'appel ici :

```
curl -X POST --proxy "" --no-buffer -H 'Log-Format-ezproxy: %h %<[-]> %u
[%t] "%r" %s %b' --data-binary @test/dataset/sd.2012-11-30.300.log
http://127.0.0.1:59599 -v
```

Traiter 1 fichier de logs

Les Logs du ezproxy Lille3 sont comme cela :

```
LogFormat %h %l %u-%{ezproxy-session}i %t “%r” %s %b
```

Ici, on veut traiter le fichier ezp201601.log qui se situe dans le chemin /mnt/hgfs/Documents/logs/ et on veut générer un rapport csv sous le nom rapport-ezpaarse-2016-01.csv:

```
curl -v -X POST http://localhost:59599   -H "Accept:text/csv"  -H "Traces-
Level:info"  -H "Log-Format-ezproxy:%h %l %u-%{ezproxy-session}i %t \"%r\"
%s %b"  -H "Crypted-Fields:host,login"  -F
"files[]=@/mnt/hgfs/Documents/logs/ezp201601.log;type=text/x-log"> rapport-
ezpaarse-2016-01.csv
```

Remarquez comme on protège les **“** avec un \ (échappe) lorsque l'on décrit le format. En effet comme le bloc de description commence et fini par un guillemet, il faut bien préciser que les **“** intermédiaire font parti de la description du format.

Ne pas mettre le \ lorsqu'on utilise l'interface web de ezpaarse.

Traiter tous les fichiers de logs d'un répertoire

La commande ecbulkmaker va lire tous les fichier de log d'un repertoire et génerer les rapports Ezpaarse CSV dans un répertoire de destination

```
/usr/local/ezpaarse/bin/ecbulkmaker -H "Log-Format-ezproxy:%h %l %u-
%{ezproxy-session}i %t \"%r\" %s %b" /mnt/hgfs/Documents/logs/2016/
/mnt/hgfs/Documents/ezpaarse/2016/
```

Ici, les fichiers de logs sont dans `/mnt/hgfs/Documents/logs/2016/` et les fichiers générés sont dans `/mnt/hgfs/Documents/ezpaarse/2016/`

On précise en paramètre le format des logs :

Pour Lille SHS

```
-H “Log-Format-ezproxy:%h %l %u-%{ezproxy-session}i %t \”%r\” %s %b”
```

Pour Lille DS

```
-H “Log-Format-ezproxy:%h %{ezproxy-groups}i %l %u %t ”%r“ %s %b”
```

Depuis mai 2017, dans les logs de Lille DS, en lieu et place de l'UID figure le groupe d'appartenance sous une certaine forme : etudiant_lille2+SCDDoc

Or, EzPaarse, par défaut n'accepte pas les caractére '_' et '+' dans la zone UID : la ligne n'est donc pas analysée du tout pour non conformitée au LogFormat

Pour Lille DS, donc , il faut apporter une modification pour dire à EzPaarse que tous les caractéres sont acceptés dans un uid avec le regex **<.*>** :

```
-H “Log-Format-ezproxy:%h %{ezproxy-groups}i<.*> %l %u %t ”%r“ %s %b”
```

Pour Lille ST

```
-H “Log-Format-ezproxy:%h ”%{ezproxy-groups}i“ %u %t ”%r“ %s %b ”%{Referer}i“
”%{user-agent}i“ ”%{Cookie}i“ %{ezproxy-session}i
```

Même souci pour Lille ST, donc on ajoute un regex là où peut y avoir des caractères inattendus :

```
-H “Log-Format-ezproxy:%h ”%{ezproxy-groups}i<.*>” %u %t “%r” %s %b “%{Referer}i<.*>” “%{user-agent}i<.*>” “%{Cookie}i<.*>” %{ezproxy-session}i<.*>
```

Visualisation de tableaux de bord :

Ce rapport CSV peut être exploité de 4 manières :

-La macro LibreOffice proposé par Couperin ici :

https://github.com/ezpaarse-project/ezpaarse/raw/master/misc/windows/ezPAARSE-Render.ots

-La macro Excel proposé par Couperin ici :

https://github.com/ezpaarse-project/ezpaarse/raw/master/misc/windows/ezPAARSE-Render.xltm

-Via une instance EzMesure (LogsStash/ElasticSearch/Kibana) ⇒ la prochaine étape...

-Via une instance locale LogsStash/ElasticSearch/Kibana ⇒ AGimus ⇒la prochaine étape...