

EzParse - Exploitation

Liens pour installation et exploitation (en anglais):

<https://media.readthedocs.org/pdf/ezparse/master/ezparse.pdf>

Avant propos :

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

`http://localhost:59599/`

notre serveur Ezparse est accessible en intranet ici :

`http://ezparse.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 Ezparse :

Paramétrage pour les logs Lille3


The screenshot shows the 'Paramétrage actuel' (Current configuration) page in the EzParse web interface. The page title is 'Paramétrage actuel par défaut (modifié)' and there is a checkbox for 'Mémoriser mes paramètres' (Save my parameters) which is checked. The interface has three tabs: 'Fichiers de logs', 'Concevoir mon format de log' (active), and 'Paramètres'. The main area is titled 'Copiez/collez vos lignes de log ici' and contains a large empty text box. Below this are three input fields: 'Type de log' (a dropdown menu with 'EZproxy' selected), 'Parseur par défaut' (a text box with 'Exemple: dspace'), and 'Format de date' (a text box with 'Exemple: DD/MMM/YYYY:HH:mm:ss Z'). Below these is a 'Format de log' field with a help icon and the text '%h %l %u-%{ezproxy-session}i %t "%r" %s %b'. At the bottom, there is an 'Analyse du format' section with the text 'Basée sur la première ligne de log'. A 'Traiter les lignes' button with a refresh icon is located at the bottom right of the configuration area.

Depot du fichier dans l'autre onglet :

Paramétrage actuel par défaut (modifié) Mémoriser mes paramètres

Fichiers de logs Concevoir mon format de log Paramètres

tri automatique

Nom de fichier	Taille
 ezp201601.log	157.1 MB
1 fichiers sélectionnés	
157.1 MB au total	

Traitements via les API :

EzParse 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-ezparse-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-ezparse-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 fichiers de log d'un répertoire et générer 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 caractères '_' et '+' dans la zone UID : la ligne n'est donc pas analysée du tout pour non conformité au LogFormat

Pour Lille DS, donc, il faut apporter une modification pour dire à EzPaarse que tous les caractères 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/ezparse-project/ezparse/raw/master/misc/windows/ezPAARSE-Render.ots>

-La macro Excel proposé par Couperin ici :

<https://github.com/ezparse-project/ezparse/raw/master/misc/windows/ezPAARSE-Render.xltm>

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

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

From:

<https://wikis.univ-lille.fr/dsi-exploit/> - **DSI - Exploitation / Intégration**

Permanent link:

<https://wikis.univ-lille.fr/dsi-exploit/dom-doc/ezproxy/ezparse/ezparseexploit>

Last update: **2018/03/21 13:13**