NFA083 – Apache2, Fichiers de Log

Sami Taktak

sami.taktak@cnam.fr

Centre d'Étude et De Recherche en Informatique et Communications
Conservatoire National des Arts et Métiers

mai 2013

le cnam

Fichiers journaux du Serveur HTTP Apache

- Aide à la gestion du serveur web
- Enregistre les informations sur l'activité et les performances
- Enregistre les erreurs pouvant survenir
- Fonctionnalités de journalisation souples et complètes

```
10.0.2.2 - alice [02/May/2013:15:51:10 +0200] "GET /prive2/ HTTP/1.1" 200 648
 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:20.0) Gecko/20100101 Firefox/20.0"
10.0.2.2 - - [02/May/2013:15:51:15 +0200] "GET /prive2/.htaccess HTTP/1.1" 403
 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:20.0) Gecko/20100101 Firefox/20.0"
10.0.2.2 - - [02/May/2013:15:51:24 +0200] "GET /.htpasswd HTTP/1.1" 403 503
 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:20.0) Gecko/20100101 Firefox/20.0"
10.0.2.2 - - [02/May/2013:15:53:05 +0200] "GET /.htpasswd HTTP/1.1" 403 504
 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:20.0) Gecko/20100101 Firefox/20.0"
10.0.2.2 - - [02/May/2013:15:53:10 +0200] "GET /passwd HTTP/1.1" 200 310
 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:20.0) Gecko/20100101 Firefox/20.0"
```

le cnam

Journal des Accès

- Enregistre toutes les requêtes que traite le serveur
- Localisation et contenu du journal des accès définis par la directive `CustomLog`
- Définition d'un format de journal grâce à la directive `LogFormat`
- Format d'un journal référencé par un nom

Exemple :

```
LogFormat "%h %l %u %t \"%r\" %>s %b" common
CustomLog logs/access_log common
```

Journal des Accès

```
LogFormat "%h %l %u %t \"%r\" %>s %b" common
CustomLog logs/access_log common
```

- Syntaxe :
  `LogFormat "chaîne de format" nom_format`
- Chaîne de Format : dans le style de `printf` langage C
  - Décrit les champs d'informations composant les messages enregistrés dans le journal
  - Symbole % suivit d'un caractère remplacé par le champ de la requête correspondant
  - `%h` : hôte distant (*remote host*)
  - `%t` : heure de réception de la requête
- `http://httpd.apache.org/docs/2.2/mod/mod_log_config.html`

Journal des Accès

- Présence de modificateurs placés juste après le signe % :
  - Champ imprimé que pour des réponses avec code d'erreur spécifique
    `"%400,501{User-agent}i"` : enregistre le `User-agent` lors d'erreur 400 et 501 uniquement
  - "<" et ">" précise si la requête originale ou finale doit être considérée si une redirection interne a été effectuée
- Caractères spéciaux :
  - caractères non-imprimables et spéciaux remplacés par une chaîne d'échappement `\xhh`
  - `hh` : représentation hexadécimale du caractère
    exemple : \x1B : Fin de support (ASCII)
  - caractères '"' et '\' échappés en plaçant un \ devant : \" et \\
  - les caratères d'espacement (retour à la ligne, tabulation) : utilise le style C (`\n`, `\t`)

le cnam

Journal des Accès

```
LogFormat "%h %l %u %t \"%r\" %>s %b" common
CustomLog logs/access_log common
```

- LogFormat définie le format `common`
- CustomLog définit un nouveau fichier journal `logs/access_log` au format `common`
- Connu sous le nom de *Common Log Format* (CLF) pour Format de journalisation standard

Exemple d'entrée du journal :

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET
 /apache_pb.gif HTTP/1.0" 200 2326
```

le cnam

Exemple d'entrée de journal CLF

```
LogFormat "%h %l %u %t \"%r\" %>s %b" common

10.0.0.2 - alice [23/May/2013:11:34:23 +0200] "GET
 /apache_pb.gif HTTP/1.1" 200 2326
```

- `10.0.0.2 (%h)` : l'adresse IP du client (l'hôte distant)
- `- (%l)` : portion d'information correspondante non disponible
- `alice (%u)` : identifiant utilisateur issu d'une authentification HTTP ; identifiant n'est pas fiable si statut de la requête 401
- `[23/May/2013:11:34:23 +0200] (%t)` : heure de réception de la requête par le serveur
- `"GET /apache_pb.gif HTTP/1.1"` : requête du client placée entre guillemets
- `200 (%>s)` : code de statut retourné au client
- `2326 (%b)` : taille de l'objet retourné

Format de Journalisation Combiné

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\"
 \"%{User-agent}i\"" combined

10.0.0.2 - alice [23/May/2013:11:34:23 +0200] "GET
 /NFA083/TP/TP5.pdf HTTP/1.1" 200 2326 "http://localhost:
 8080/NFA083/TP/" "Mozilla/5.0 (X11; Linux x86_64; rv:20.0)
 Gecko/20100101 Firefox/20.0"
```

- `"http://localhost:8080/NFA083/TP/"` (`\"\%{Referer}i\"`) : en-tête `Referer` de la requête HTTP ; indique le site depuis lequel le client prétend avoir lancé sa requête
- `"Mozilla/5.0 (X11; Linux x86_64; rv:20.0) Gecko/2010 0101 Firefox/20.0"` : en-tête `User-Agent` de la requête HTTP

Journal des erreurs

- journal des erreurs du serveur
- nom et la localisation sont définis par la directive `ErrorLog`
- journal le plus important
- informations de diagnostic et erreurs enregistrées dans ce journal
- journal à consulter en cas d'erreur au lancement ou en cours d'exécution

Exemple Journal des erreurs

```
[Thu May 02 15:51:24 2013] [error] [client 10.0.2.2]
 client denied by server configuration: /var/www/.h
 tpasswd
```

- premier champ : date et l'heure du message
- second champ : sévérité de l'erreur
- troisième champ : adresse IP du client
- message d'erreur indiquant que l'accès à cette ressource a été interdit

Directive LogLevel

- `emerg` : urgences ; système inutilisable
- `alert` : mesures a prendre immédiatement
- `crit` : conditions critiques
- `error` : erreurs
- `warn` : avertissements
- `notice` : evènement important mais normal
- `info` : informations
- `debug` : messages de débogage

Exemple : `LogLevel crit`