Chapitre 5
Gestion des logs sous Apache

1. Activation et configuration

Le service Apache possède nativement des fonctions de journalisation (écriture dans des fichiers logs) permettant de collecter diverses informations, telles que :

– l'état du service,

– les erreurs de configuration,

– les dépendances non satisfaites,

– d'autres informations liées aux applications hébergées.

La journalisation est primordiale pour assurer un suivi opérationnel du service, mais peut également constituer une véritable problématique en matière de stockage et de performance.

Il s'agit donc de paramétrer cette journalisation en fonction de ses propres besoins, de l'environnement (production, intégration, recette) et d'utiliser des modules d'Apache spécifiques apportant une granularité supplémentaire.

1.1 Journaux d'erreur

Par défaut, Apache enregistre des informations liées aux arrêts/démarrage du service ainsi qu'aux erreurs via la directive `ErrorLog`.

Cette directive est documentée dans le chapitre Configuration de base d'Apache, à la section Directives Core.

```
ErrorLog "/var/log/apache2.4/error_log"
```

La directive `ErrorLog` nous permet ici de préciser où seront enregistrées les informations du service.

1.1.1 Utilisation de LogLevel

Par défaut, lors d'un redémarrage de service, voici le niveau de journalisation observé dans le fichier /var/log/apache2.4/error_log :

```
[Mon Oct 20 12:21:32 2014] [notice] [pid 20911] event.c(2855):
[client AH00494: SIGHUP received.  Attempting to restart
[Mon Oct 20 12:21:33.001849 2014] [mpm_event:notice] [pid
20911:tid 139883230811904] AH00489: Apache/2.4.10 (Unix)
ENI_server configured -- resuming normal operations
[Mon Oct 20 12:21:33.001875 2014] [core:notice] [pid 20911:tid
139883230811904] AH00094: Command line:
'/opt/prod/apache2.4/bin/httpd'
```

Nous pouvons constater que seules des informations de niveau « notice » sont enregistrées dans le fichier de logs.

Les principaux niveaux sont :

Niveau	Description
`emerg`	Urgences - le système est inutilisable
`alert`	Des mesures doivent être prises immédiatement
`crit`	Conditions critiques
`error`	Erreurs
`warn`	Avertissements
`notice`	Événements importants mais normaux

Niveau	Description
info	Informations
debug	Messages de débogage

Passons à présent en mode info grâce à la directive LogLevel :

```
LogLevel info
```

Après redémarrage du service, on a :

```
[Mon Oct 20 12:32:19.475407 2014] [mpm_event:notice] [pid
20911:tid 139883230811904] AH00494: SIGHUP received.  Attempting
to restart
[Mon Oct 20 12:32:19.478174 2014] [unique_id:info] [pid 20911:tid
139883230811904] AH01566: using ip addr 127.0.1.1
[Mon Oct 20 12:32:20.000686 2014] [session_crypto:info] [pid
20911:tid 139883230811904] AH01849: The crypto library 'openssl'
was loaded successfully
[Mon Oct 20 12:32:20.001547 2014] [mpm_event:notice] [pid
20911:tid 139883230811904] AH00489: Apache/2.4.10 (Unix)
ENI_server configured -- resuming normal operations
[Mon Oct 20 12:32:20.001557 2014] [mpm_event:info] [pid 20911:tid
139883230811904] AH00490: Server built: Nov 16 2014 14:12:11
[Mon Oct 20 12:32:20.001565 2014] [core:notice] [pid 20911:tid
139883230811904] AH00094: Command line:
'/opt/prod/apache2.4/bin/httpd'
```

Avec un LogLevel debug, on a :

```
[Mon Oct 20 12:23:29.238600 2014] [mpm_event:notice] [pid
20911:tid 139883230811904] AH00494: SIGHUP received. Attempting
to restart
[Mon Oct 20 12:23:29.241396 2014] [unique_id:info] [pid 20911:tid
139883230811904] AH01566: using ip addr 127.0.1.1
[Mon Oct 20 12:23:30.000857 2014] [session_crypto:info] [pid
20911:tid 139883230811904] AH01849: The crypto library 'openssl'
was loaded successfully
[Mon Oct 20 12:23:30.000903 2014] [:debug] [pid 20911:tid
139883230811904] mod_security2.c(595): SecServerSignature: Changed
server signature to "ENI_server".
[Mon Oct 20 12:23:30.001706 2014] [mpm_event:notice] [pid
20911:tid 139883230811904] AH00489: Apache/2.4.10 (Unix)
ENI_server configured -- resuming normal operations
[Mon Oct 20 12:23:30.001717 2014] [mpm_event:info] [pid 20911:tid
```

```
139883230811904] AH00490: Server built: Nov 16 2014 14:12:11
[Mon Oct 20 12:23:30.001725 2014] [core:notice] [pid 20911:tid
139883230811904] AH00094: Command line:
'/opt/prod/apache2.4/bin/httpd'
[Mon Oct 20 12:23:30.002052 2014] [mpm_event:debug] [pid 15151:tid
139883131455232] event.c(2009): AH02471: start_threads: Using
epoll
[Mon Oct 20 12:23:30.002212 2014] [mpm_event:debug] [pid 15150:tid
139883131455232] event.c(2009): AH02471: start_threads: Using
epoll
[Mon Oct 20 12:23:30.002680 2014] [mpm_event:debug] [pid 15152:tid
139883131455232] event.c(2009): AH02471: start_threads: Using epoll
```

La quantité d'information collectée n'est donc pas la même en fonction du niveau choisi via la directive `LogLevel`.

En effet, pour un simple redémarrage de service :

– Trois lignes sont écrites dans le fichier de logs avec un LogLevel par défaut (`warn`).
– Six lignes pour un LogLevel positionné à `info`.
– Neuf lignes pour un LogLevel positionné à `debug`.

Bien entendu, il s'agit de sélectionner le niveau de journalisation en fonction du besoin. Ainsi, compte tenu de la quantité d'information collectée par les différents LogLevel, et notamment en mode `debug`, il convient de l'activer uniquement dans le cadre d'une analyse « bas niveau » du service pour effectuer un diagnostic.

Car un fichier log d'erreur est efficace à condition d'y trouver uniquement les informations utiles, voire en cas de fort trafic, uniquement celles qui sont critiques.

Il est important de noter que la volumétrie d'événements journalisés a également un impact direct sur la performance et la maintenance des plates-formes :

– nombre d'accès disque lors de l'écriture des logs,
– trafic réseau, dans le cas d'une externalisation logs,
– volumétrie importante des fichiers logs, et donc utilisation de l'espace disque

1.1.2 Utilisation de ErrorLogFormat

Un autre moyen pour optimiser la journalisation des erreurs d'Apache est d'utiliser la directive `ErrorLogFormat`.

Comme abordé dans le chapitre Configuration de base d'Apache, il est possible de sélectionner les chaînes de format que nous souhaitons voir apparaître dans les fichiers de logs.

Pour illustrer un cas d'erreur, nous avons chargé le module `mod_security` sans le module `mod_unique_id` qui est une dépendance.

Ci-dessous, la sortie de logs par défaut lors d'un redémarrage de service et après une requête HTTP :

```
[Mon Oct 20 13:26:27 2014] [notice] [pid 20911] [client AH00494:
SIGHUP received.  Attempting to restart
[Mon Oct 20 13:26:27.342048 2014] [mpm_event:notice] [pid
20911:tid 139883230811904] AH00489: Apache/2.4.10 (Unix)
ENI_server configured -- resuming normal operations
[Mon Oct 20 13:26:27.342064 2014] [core:notice] [pid 20911:tid
139883230811904] AH00094: Command line:
'/opt/prod/apache2.4/bin/httpd'
[Mon Oct 20 13:26:36.780030 2014] [:error] [pid 16356:tid
139883125167872] ModSecurity: ModSecurity requires mod_unique_id
to be installed.
```

Utilisons la directive `ErrorLogFormat` ci-dessous :

```
ErrorLogFormat "[%t] [%l] [pid %P] [client %a] %M"
```

`[%t]` affiche l'heure entre `[` et `]`, sans les microsecondes.

`[%l]` affiche la sévérité du message entre `[` et `]`.

`[pid %P]` affiche « pid » suivi du numéro du PID entre `[` et `]`.

`[client %a]` affiche adresse IP et port clients.

`%M` affiche le message (obligatoire).

Nous obtenons :

```
[Mon Oct 20 13:26:02 2014] [notice] [pid 20911] [client AH00494:
SIGHUP received.  Attempting to restart
[Mon Oct 20 13:26:02 2014] [notice] [pid 20911] [client AH00489:
```

```
Apache/2.4.10 (Unix) ENI_server configured -- resuming normal
operations
[Mon Oct 20 13:26:02 2014] [notice] [pid 20911] [client AH00094:
Command line: '/opt/prod/apache2.4/bin/httpd'
[Mon Oct 20 13:26:09 2014] [error] [pid 16264] [client
ModSecurity: ModSecurity requires mod_unique_id to be installed.
```

L'information reste tout aussi lisible que précédemment, mais avec un message épuré.

Ici, l'objectif est de montrer qu'il est possible de formater les entrées du fichier ErrorLog de manière à ne stocker que l'essentiel.

Mais la directive `ErrorLogFormat` permet également de mettre en évidence des informations supplémentaires qui peuvent être importantes à journaliser.

Dans le cadre de l'hébergement de plusieurs sites web, avec des noms de domaine différents, l'ajout du nom du « ServerName » ayant généré une erreur permettra d'affiner le diagnostic :

```
ErrorLogFormat "[%t] [%v] [%l] [pid %P] [client %a] %M"
```

Le résultat obtenu :

```
[Mon Oct 20 13:34:56 2014] [vm-compilation-eni] [error] [pid
16467] [client ModSecurity: ModSecurity requires mod_unique_id to
be installed.
[Mon Oct 20 13:35:29 2014] [eni.labs] [error] [pid 16465] [client
ModSecurity: ModSecurity requires mod_unique_id to be installed.
```

1.2 Module mod_log_config

Le module `mod_log_config` permet de journaliser les requêtes traitées par le serveur en dehors de celles inscrites dans l'ErrorLog.

1.2.1 Utilisation de la directive LogFormat

Comme cela a été vu dans le chapitre Configuration de base d'Apache, la directive `LogFormat` permet de définir le formatage des fichiers de logs concernant les requêtes traitées par le serveur Apache. Tout comme pour les ErrorLog, il est possible d'optimiser la quantité d'information journalisée et de faire apparaître certaines informations en fonction de ses besoins.