

### Veille notion de Syslog sous Linux.

#### Qu'est ce que c'est que le syslog ?

Le syslog est le processus de journalisation qui enregistre les événements afin de permettre de localiser rapidement les défaillances d'un système. Chaque service possède son propre fichier de log qui sont tous stockés dans la partition `/var/log`.

#### A quoi ressemble une ligne d'évènement ?

Dans chaque ligne d'évènement on distingue :

- La date à laquelle l'évènement a été déclenché
- Le processus déclencheur de l'évènement
- Le processus ayant demandé l'ajout du message correspondant au log
- Le niveau de gravité du message (priority)

#### Les types de messages :

Il existe 5 types de messages qui sont les suivantes :

<b><code>/var/log/secure</code></b>	Syslog stocke dans le fichier de log « secure » tous les messages liés à la sécurité y compris ceux de l'authentification.
<b><code>/var/log/maillog</code></b>	Syslog stocke les messages liés aux messageries.
<b><code>/var/log/cron</code></b>	Contient tous les messages liés au démarrage du système.
<b><code>/var/log/boot.log</code></b>	Contient tous les messages liés au démarrage du système.
<b><code>/var/log/messages</code></b>	La plupart des messages log sont enregistré dans le fichier <code>/var/log/messages</code> , sauf les types de messages qu'on a vus précédemment.

## Fonctionnement du syslog

Syslog possède un fichier de configuration « `syslog.conf` » qui est stocké dans le répertoire `/etc`. Ce fichier est sous la forme « `facility.priorité /var/log/fichierlog.log` » :

- La Priorité indique la criticité du message généré par un programme.

Code	Priorité	Description
0	Emergency	Le système est inutilisable
1	Alert	Une action immédiate est requise
2	Critical	Condition critique
3	Errors	Erreurs détectés
4	Warning	Avertissement
5	Notice	Événement normal mais significatif.
6	Info	Message d'information
7	Debug	débogage

- La facility indique le type de message généré par un programme

Type	Description
Kern	Utilisé pour les messages du noyau
user	Utilisateur
mail	Messagerie
cron	le planificateur des tâches
auth	Utilisé pour plusieurs événements de sécurité.
authpriv	Utilisé pour les contrôles d'accès
dæmon	Utilisé par les process système et les daemon.
mark	Pour les messages générés par syslog lui-même contenant un horodatage et la chaîne de caractère "--MARK--"

## Ressources :

[https://fr.wikibooks.org/wiki/Le\\_syst%C3%A8me\\_d%27exploitation\\_GNU-Linux/Les\\_fichiers\\_journaux\\_syslog](https://fr.wikibooks.org/wiki/Le_syst%C3%A8me_d%27exploitation_GNU-Linux/Les_fichiers_journaux_syslog)  
<https://www.linuxtricks.fr/wiki/syslog-les-journaux-systeme-sous-linux>  
<https://sysreseau.net/syslog-la-journalisation-sous-linux/>  
<https://doc.ubuntu-fr.org/syslog-ng>

## Activité

---

Notre application Laravel doit permettre d'inscrire ses évènements dans le syslog.

Autrement dit, nous devons pouvoir référencer des fichiers de logs concernant :

- Nombre de tentative de connexion
- Quand le compte est bloqué

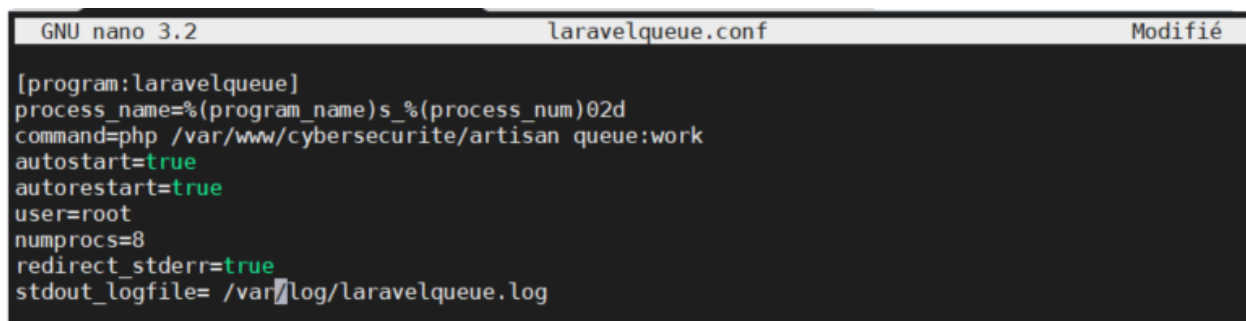
### **Ajustement :**

Avant de mettre en place l'écriture dans le syslog du système, je dois faire persister la commande « php artisan queue:work » afin que les tâches cron se déclenchent correctement. Pour ce faire, j'utilise un package permettant de démarrer automatiquement la commande.

J'installe le package « supervisor » grâce à la commande :

- `sudo apt-get install supervisor`

Ensuite j'ajoute un `laravelqueue.conf` dans le dossier `/etc/supervisor/conf.d` afin de lui indiquer le processus qu'il doit automatiquement lancer.

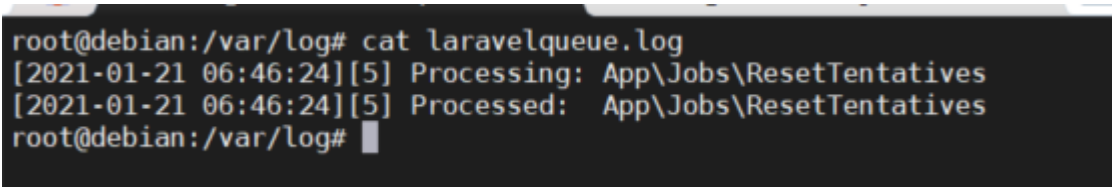


```
GNU nano 3.2      laravelqueue.conf      Modifié
[program:laravelqueue]
process_name=%(program_name)s_%(process_num)02d
command=php /var/www/cybersecurite/artisan queue:work
autostart=true
autorestart=true
user=root
numprocs=8
redirect_stderr=true
stdout_logfile= /var/log/laravelqueue.log
```

Je redémarre le service afin que mon fichier de conf soit pris en compte :

- `sudo /etc/init.d/supervisor restart`

En faisant le test, je peux voir que cela fonctionne correctement :



```
root@debian:/var/log# cat laravelqueue.log
[2021-01-21 06:46:24][5] Processing: App\Jobs\ResetTentatives
[2021-01-21 06:46:24][5] Processed: App\Jobs\ResetTentatives
root@debian:/var/log#
```

Ressources :

<https://blog.elao.com/fr/infra/utiliser-supervisor-pour-controler-ses-services-applicatifs/>

## Mise en place de l'écriture dans le syslog du système et non dans laravel

Modification du fichier rsyslog.conf pour l'écriture dans un fichier de log spécifique :

```
GNU nano 3.2 /etc/rsyslog.conf

# Some "catch-all" log files.
#
*,debug;\
auth,authpriv.none;\
news.none;mail.none     -/var/log/debug
*,info;*,notice;*,warn;\
auth,authpriv.none;\
cron,daemon.none;\
mail,news.none          -/var/log/messages
#
# Emergencies are sent to everybody logged in.
#
*,emerg                  :omusrmsg:*
#
local0.=info             /var/log/securityinfo.log
```

Modification de la manière de faire les logs :

```
AuthController.php x README.md app.php .env
app > Http > Controllers > AuthController.php
43
44     $user->tentatives = $user->tentatives + 1;
45     $user->save();
46     if($user->tentatives > 3) {
47         $user->tentatives = 3;
48         $user->save();
49         $resetJob = (new ResetTentatives($user->id))->delay(Carbon::now()->addSeconds(30));
50         dispatch($resetJob);
51
52         openlog('cybersecrite_app', LOG_NDELAY, LOG_USER);
53         syslog(LOG_INFO|LOG_LOCAL0, "L'utilisateur {$user->email} à atteint son nombre maximal de tentative de connexion ! ");
54         // Log::channel('abuse')->info("L'utilisateur {$user->email} à atteint son nombre maximal de tentative de connexion ! ");
55
56         return response()->json([
57             'success' => false,
58             'type' => 'info',
59             'message' => "Veuillez réessayer dans 30 secondes",
60         ]);
61     }
62
63 }
```

Test et vérification après 3 tentatives d'échecs :

```
3. secu@debian: /var/www/cybersecu x 4. secu@debian: /var/log
root@debian:/var/log/web# cd ..
root@debian:/var/log# ls
alternatives.log      faillog               messages              syslog.2.gz
alternatives.log.1    cups                 fontconfig.log        syslog.3.gz
alternatives.log.2.gz daemon.log            gdm3                 mysql                unattended-upgrades
apache2               daemon.log.1         hp                    private              user.log
apt                   debug               installer             securityinfo.log     user.log.1
auth.log              debug.1             kern.log              speech-dispatcher    web
auth.log.1            dpkg.log            kern.log.1            supervisor           wtmp
boot.log              dpkg.log.1          laravelqueue.log      syslog
btm                   dpkg.log.2.gz       lastlog               syslog.1
root@debian:/var/log# cat securityinfo.log
Jan 21 08:44:15 debian cybersecrite_app: L'utilisateur admin@gmail.com à atteint son nombre maximal de tentative de connexion !
root@debian:/var/log#
```

```
3. secu@debian: /var/www/cybersecu x 4. secu@debian: /var/log
root@debian:/var/log# cat securityinfo.log
Jan 21 08:44:15 debian cybersecrite_app: L'utilisateur admin@gmail.com à atteint son nombre maximal de tentative de connexion !
Jan 21 08:46:57 debian cybersecrite_app: L'utilisateur admin@gmail.com à atteint son nombre maximal de tentative de connexion !
root@debian:/var/log#
```

```
rd 37 from systemd. [v8.1901.0]
Jan 21 10:15:58 debian rsyslogd: [origin software="rsyslogd" swVersion="8.1901.0" x-pid="30279" x-info="https://www.rsyslog.com"] start
Jan 21 10:15:58 debian systemd[1]: Started System Logging Service.
Jan 21 10:16:52 debian cybersecurite_app: L'utilisateur admin@gmail.com à atteint son nombre maximal de tentative de connexion !
Jan 21 10:17:01 debian CRON[30385]: (root) CMD ( cd / && run-parts --report /etc/cron.hourly)
Jan 21 10:20:11 debian systemd[1]: Started Session 37 of user secu.
Jan 21 10:20:12 debian systemd[1]: session-37.scope: Succeeded.
root@debian: /var/log#
```

### **Veille notion de SIEM.**

#### **### Qu'est-ce que c'est que le SIEM ?**

L'abréviation SIEM signifie Security Information and Event Management, une combinaison des deux concepts SIM (Security Information Management) et SEM (Security Event Management). Ensemble, ces deux concepts informatiques couvrent l'ensemble de la sécurité informatique.

SIEM peut se traduire en français par systèmes de gestion des informations et des événements de sécurité. Dans ce cadre, un SIEM tient toujours compte des exigences spécifiques à l'entreprise en définissant clairement et de façon individuelle les processus et les événements liés à la sécurité, la façon d'y réagir et un ordre de priorité.

Par conséquent, le Security Information and Event Management peut également être considéré comme un ensemble de règles pour les normes de sécurité applicables et comme un guide visant à maintenir la qualité dans le fonctionnement informatique d'une entreprise

#### **### A quoi sert le SIEM ?**

Son objectif est de pouvoir réagir aux menaces aussi rapidement et précisément que possible. Pour ce faire, les systèmes de SIEM tentent de détecter en temps réel les attaques ou les tendances d'attaques en collectant et en analysant les messages habituels, les notifications d'alarme et les fichiers journaux de façon centralisée. Différents appareils, composants et applications du réseau d'entreprise concerné servent de sources dans ce cadre tels que :

- les pare-feu (logiciels et matériels) ;
- les interrupteurs ;
- les routeurs ;
- les serveurs (serveur de fichiers, FTP, VPN, Proxy, etc.) ;
- les IDS et IPS.

Des agents logiciels – des programmes informatiques travaillant de façon autonome et conçus spécialement pour transmettre les données – veillent à ce que cette abondance de données soit collectée et transmise à une station de SIEM centrale. Pour réduire la quantité de données à transmettre, un prétraitement des informations par les agents est par ailleurs prévu dans de nombreux systèmes. Dans la station de SIEM centrale, les informations sont enregistrées et structurées puis mises en relation et analysées sur cette base et de façon générale. Des ensembles de règles définies de façon concrète, des technologies d'IA – en particulier l'apprentissage automatique – et des modèles de corrélation sont notamment utilisés pour l'analyse et l'évaluation.

#### #### Notes

Les modèles de corrélation servent à établir des contextes pour les informations enregistrées dans le journal et les événements de sécurité survenus. Il existe par exemple des modèles pour l'analyse de la structure des données d'entrée générant un graphique des événements avec des relations directes et indirectes entre les différents événements. Nous pouvons visualiser et inspecter les différents résultats d'analyse et indicateurs dans un tableau de bord clair que nous pouvons généralement personnaliser entièrement afin de répondre de façon optimale aux exigences de l'entreprise.

#### ### Avantages :

- Maintenir les éventuels dommages à un niveau aussi faible que possible
- La réaction en temps réel aux événements de sécurité enregistrés
- Les algorithmes et les outils d'IA automatisés détectent les menaces à un moment où les mesures de sécurité habituelles n'agissent pas encore voire pas du tout.
- Les solutions de SIEM documentent et archivent automatiquement de façon inviolable l'ensemble des événements de sécurité. (RGPD : prouver que les lois applicables en matière de sécurité et de protection des données ont été observées et respectées)
- optimiser les ressources humaines : du fait du haut degré d'automatisation lié à la surveillance et à l'analyse en temps réel, les employés du service informatique peuvent se consacrer à d'autres tâches.

#### ### Cas d'utilisations :

Le Security Information and Event Management est par conséquent souvent utilisé par les entreprises traitant des données clients sensibles ou devant veiller à un fonctionnement informatique sans accroc.

- Cas utilisation 1 : attaque par force brute
- Cas utilisation 2 : tentatives d'accès par VPN

#### ### Conclusion :

Le SIEM nous permet en outre d'atteindre quasiment les mêmes enjeux que la supervision :

- Être réactif en étant averti d'une panne avant ses utilisateurs ;
- Être proactif en planifiant, contrôlant et budgétisant les ressources matériels ou logiciels ;
- Justifier un niveau de service en assurant des niveaux de SLA\* et une amélioration constante ;

#### ### LEXIQUE :

- SLA\* : Disponibilité /performance sur une période donnée/ taux de réussite/ congestion etc.

### ### Ressources :

- <https://www.nomios.fr/signification-siem-security-information-and-event-management/>
- <https://www.logpoint.com/fr/comprendre/c-est-quoi-le-siem/>
- <https://www.expert-com.com/siem-definition/>
- <https://www.ionos.fr/digitalguide/serveur/securite/quest-ce-que-le-siem/>



## Activité

### Logs :

Pour :

- Nombre de tentative user
- Blocage du compte

```
AuthController.php X ResetTentatives.php README.md app.php
app > Http > Controllers > AuthController.php
40 $user = User::where('email', $request->email)->first();
41 if(!$user || !Hash::check($request->password, $user->password)){
42
43     if($user) {
44         $tentative = $user->tentatives + 1;
45         $user->tentatives = $tentative;
46         $user->save();
47
48         openlog('cybersecurite_app', LOG_NDELAY, LOG_USER);
49         syslog(LOG_INFO|LOG_LOCAL0, "il y a eu {$tentative} tentative de connexion au compte {$user->email}");
50
51         if($user->tentatives > 3) {
52             $user->tentatives = 3;
53             $user->save();
54             $resetJob = (new ResetTentatives($user->id))->delay(Carbon::now()->addSeconds(30));
55             dispatch($resetJob);
56
57             openlog('cybersecurite_app', LOG_NDELAY, LOG_USER);
58             syslog(LOG_INFO|LOG_LOCAL0, "L'utilisateur {$user->email} à atteint son nombre maximal de tentative de connexion !");
59             // Log::channel('abuse')->info("L'utilisateur {$user->email} à atteint son nombre maximal de tentative de connexion !");
60
61             return response()->json([
62                 'success' => false,
63                 'type' => 'info',
64                 'message' => "Veuillez réessayer dans 30 secondes",
65             ]);
66         }
67     }
68 }
```

Pour :

- Déblocage du compte
- 

```
EXPLORATEUR ... AuthController.php ResetTentatives.php X README.md app.php
> Éditeurs ouverts
> CYBERSECURITE [SSH: 192.168.1.11]
  > app
  > Console
  > Exceptions
  > Http
  > Controllers
    > AuthController.php M
    > Controller.php
  > Middleware
    > Kernel.php
  > Jobs
    > ResetTentatives.php M
  > Models
  > Providers
  > bootstrap
  > config
  > database
  > documentation
    > cours-secu-03-04-12-2020.pdf
    > cours-secu-03-12-2020.pdf
    > cours-secu-21-22-01-2021.pdf
  > public
  > resources
  > routes
  > storage

app > Jobs > ResetTentatives.php
14 {
15     use Dispatchable, InteractsWithQueue, Queueable, SerializesModels;
16
17     public $userId;
18
19     /**
20      * Create a new job instance.
21      *
22      * @return void
23      */
24     public function __construct($userId)
25     {
26         $this->userId = $userId;
27     }
28
29     /**
30      * Execute the job.
31      *
32      * @return void
33      */
34     public function handle()
35     {
36         $user = User::whereId($this->userId)->first();
37         $user->tentatives = 0;
38         $user->save();
39         openlog('cybersecurite_app', LOG_NDELAY, LOG_USER);
40         syslog(LOG_INFO|LOG_LOCAL0, "Le compte {$user->email} a été débloqué !");
41     }
42 }
```

Suivre en temps réel les logs :

<https://www.malekal.com/comment-lire-les-logs-sur-linux-en-temps-reel-avec-tail-multitail/>

```
root@debian:/var/log# ls
alternatives.log      auth.log.1            daemon.log.1          faillog               kern.log.1            private               syslog.2.gz           web
alternatives.log.1    boot.log              debug                 fontconfig.log        laravelqueue.log      securityinfo.log      syslog.3.gz           wtmp
alternatives.log.2.gz bttmp                 debug.1               gdm3                  lastlog               speech-dispatcher     syslog.4.gz
apache2               bttmp.1              dpkg.log              hp                     messages              supervisor            unattended-upgrades
apt                   cups                 dpkg.log.1            installer             messages.1            syslog               user.log
auth.log              daemon.log            dpkg.log.2.gz         kern.log              mysql                 syslog.1              user.log.1
root@debian:/var/log# tail -f -n 10 securityinfo.log
Jan 22 06:47:52 debian cybersecurite_app: il y a eu 1 tentative de connexion au compte admin@gmail.com
Jan 22 06:47:54 debian cybersecurite_app: il y a eu 2 tentative de connexion au compte admin@gmail.com
Jan 22 06:47:55 debian cybersecurite_app: il y a eu 3 tentative de connexion au compte admin@gmail.com
Jan 22 06:47:57 debian cybersecurite_app: il y a eu 4 tentative de connexion au compte admin@gmail.com
Jan 22 06:47:57 debian cybersecurite_app: L'utilisateur admin@gmail.com à atteint son nombre maximal de tentative de connexion !
Jan 22 06:48:28 debian cybersecurite_app: Le compte admin@gmail.com a été débloquenté !

root@debian:/var/log# tail -10 syslog
Jan 22 06:44:16 debian cybersecurite_app: L'utilisateur admin@gmail.com à atteint son nombre maximal de tentative de connexion !
Jan 22 06:44:46 debian cybersecurite_app: Le compte admin@gmail.com a été débloquenté !
Jan 22 06:46:43 debian cybersecurite_app: il y a eu 1 tentative de connexion au compte admin@gmail.com
Jan 22 06:46:43 debian cybersecurite_app: il y a eu 1 tentative de connexion au compte admin@gmail.com
Jan 22 06:47:52 debian cybersecurite_app: il y a eu 1 tentative de connexion au compte admin@gmail.com
Jan 22 06:47:54 debian cybersecurite_app: il y a eu 2 tentative de connexion au compte admin@gmail.com
Jan 22 06:47:55 debian cybersecurite_app: il y a eu 3 tentative de connexion au compte admin@gmail.com
Jan 22 06:47:57 debian cybersecurite_app: il y a eu 4 tentative de connexion au compte admin@gmail.com
Jan 22 06:47:57 debian cybersecurite_app: L'utilisateur admin@gmail.com à atteint son nombre maximal de tentative de connexion !
Jan 22 06:48:28 debian cybersecurite_app: Le compte admin@gmail.com a été débloquenté !
root@debian:/var/log#
```