

SAE 5.Cyber.03 - R5.Cyber.11

Supervision d'un Service Web (Nginx)

Flavien Marchand

Sommaire

Sommaire	1
Filebeat	2
Les dashboards pour Nginx	3
[Filebeat Nginx] Overview ECS	3
[Filebeat Nginx] Access and error logs ECS	5

La supervision du service web Nginx a été effectuée sur un site web personnel hébergé sur mon serveur.

Filebeat

Après avoir installé Filebeat comme montré dans le [CR Installation Elastic](#) , activé le module nginx :

```
./filebeat modules enable nginx
```

Et ajouté cette conf dans modules.d/nginx.yml :

```
- module: nginx
  # Access logs
  access:
    enabled: true
    var.paths: ["/var/log/nginx/access.log*"]

  # Error logs
  error:
    enabled: true
    var.paths: ["/var/log/nginx/error.log*"]
```

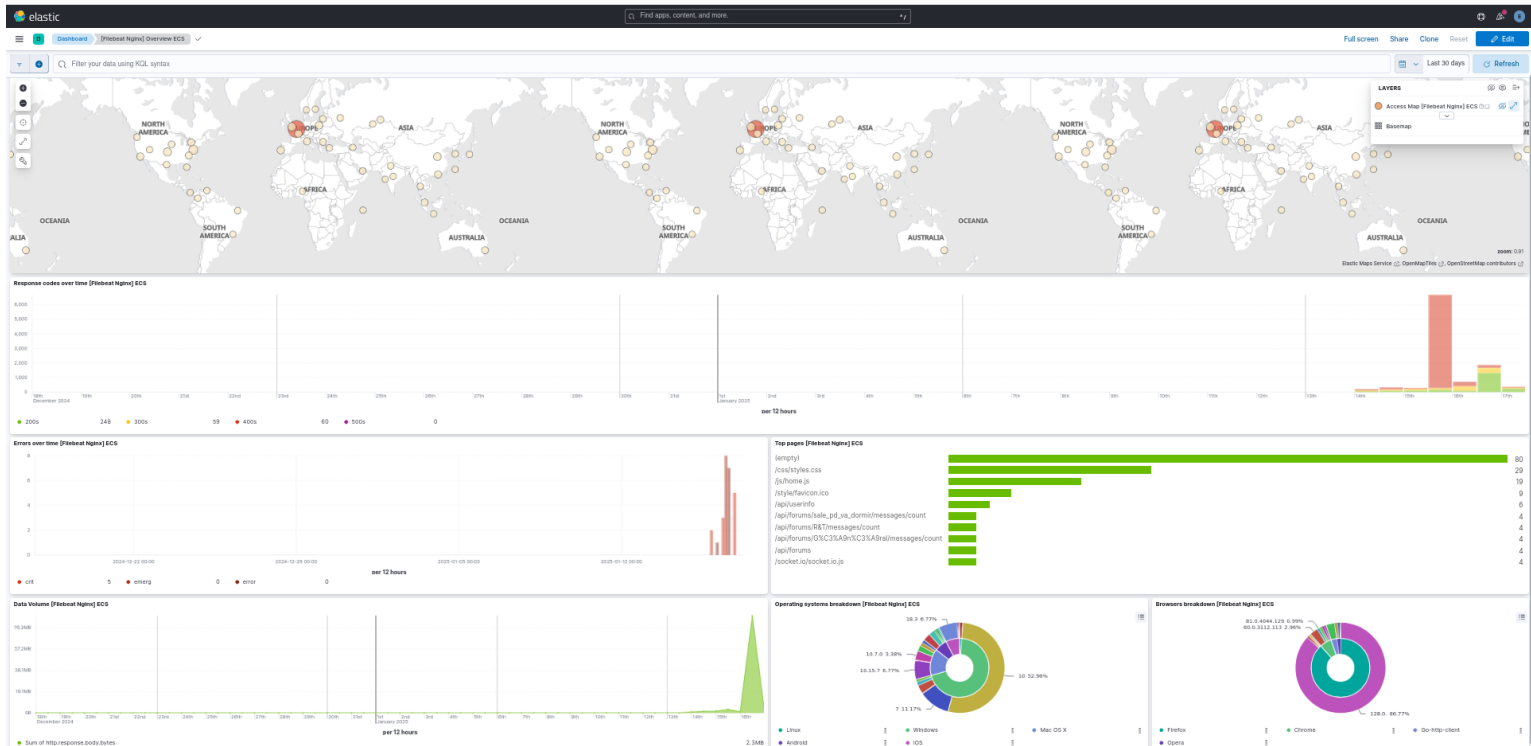
Une fois Filebeat lancé on obtient tous les dashboards de Filebeat :

Dashboards			
Search...		Recently updated ▾	Tags ▾ Create dashboard
☐ Name, description, tags	Last updated ▾		Actions
☐ [Filebeat Salesforce] Setup Audit Trail Dashboard SetupAuditTrail EventLogFile Data beats	2 days ago		✎ 🔍
☐ [Filebeat Salesforce] Logout Dashboard Logout EventLogFile Data beats	2 days ago		✎ 🔍
☐ [Filebeat Salesforce] Apex Dashboard Apex EventLogFile Data beats	2 days ago		✎ 🔍
☐ [Filebeat Salesforce] Login Dashboard Login EventLogFile Data beats	2 days ago		✎ 🔍
☐ [Filebeat Suricata] Events Overview Overview of the Suricata events dashboard.	2 days ago		✎ 🔍
☐ [Filebeat Suricata] Alert Overview Overview of the Suricata Alerts dashboard.	2 days ago		✎ 🔍
☐ [Filebeat Netflow] Top-N Flows Top N network flows	2 days ago		✎ 🔍
☐ [Filebeat Netflow] Traffic Analysis Netflow traffic analysis	2 days ago		✎ 🔍
☐ [Filebeat Netflow] Overview Overview of Netflow	2 days ago		✎ 🔍
☐ [Filebeat Netflow] Geo Location Netflow geo location	2 days ago		✎ 🔍
☐ [Filebeat Netflow] Flow records Netflow flow records	2 days ago		✎ 🔍
☐ [Filebeat Netflow] Flow Exporters Netflow exporters	2 days ago		✎ 🔍
☐ [Filebeat Netflow] Conversation Partners Netflow conversation partners	2 days ago		✎ 🔍
☐ [Filebeat Netflow] Autonomous Systems Autonomous systems Netflow	2 days ago		✎ 🔍
☐ [Filebeat Icinga] Main Log ECS Filebeat Icinga module dashboard for the main log files	2 days ago		✎ 🔍
☐ [Filebeat PostgreSQL] Query Duration Overview ECS Dashboard for analyzing the query durations of the Filebeat PostgreSQL module	2 days ago		✎ 🔍

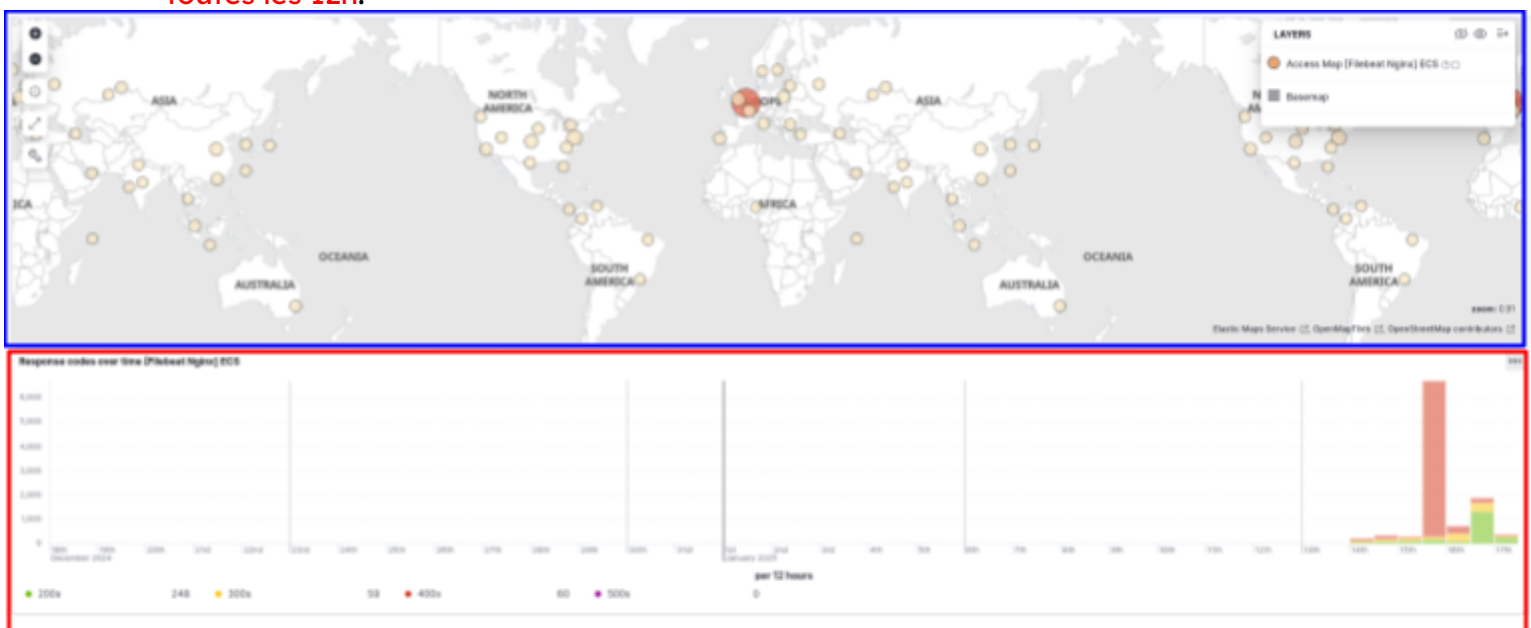
Les dashboards pour Nginx

[Filebeat Nginx] Overview ECS

On cherche nginx dans la barre de recherche et on sélectionne [\[Filebeat Nginx\] Overview ECS](#) :



Sur ce dashboard on peut voir la **localisation des connexions** qu'il y a eu sur notre site sur la map et le **nombre de requêtes par codes html (100, 200, 300, 400, 500) toutes les 12h.**



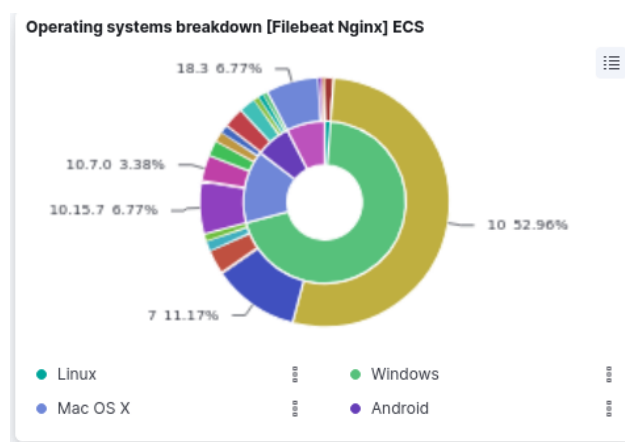
On y voit aussi le nombre d'erreur toutes les 12h et leur niveau de criticité (crit, emerg, error), on y voit aussi les "Top pages" donc les pages les plus visitées du site et leur nombre de visites.



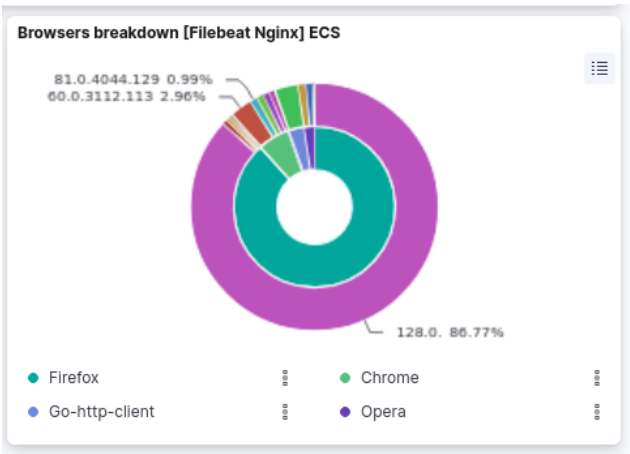
On voit aussi le "Data Volume" qui est le taux de données chargées sur le site toutes les 12h.



Les "Operating systems breakdown", donc tous les différents OS/systèmes d'exploitation avec lesquels les utilisateurs se sont connectés.

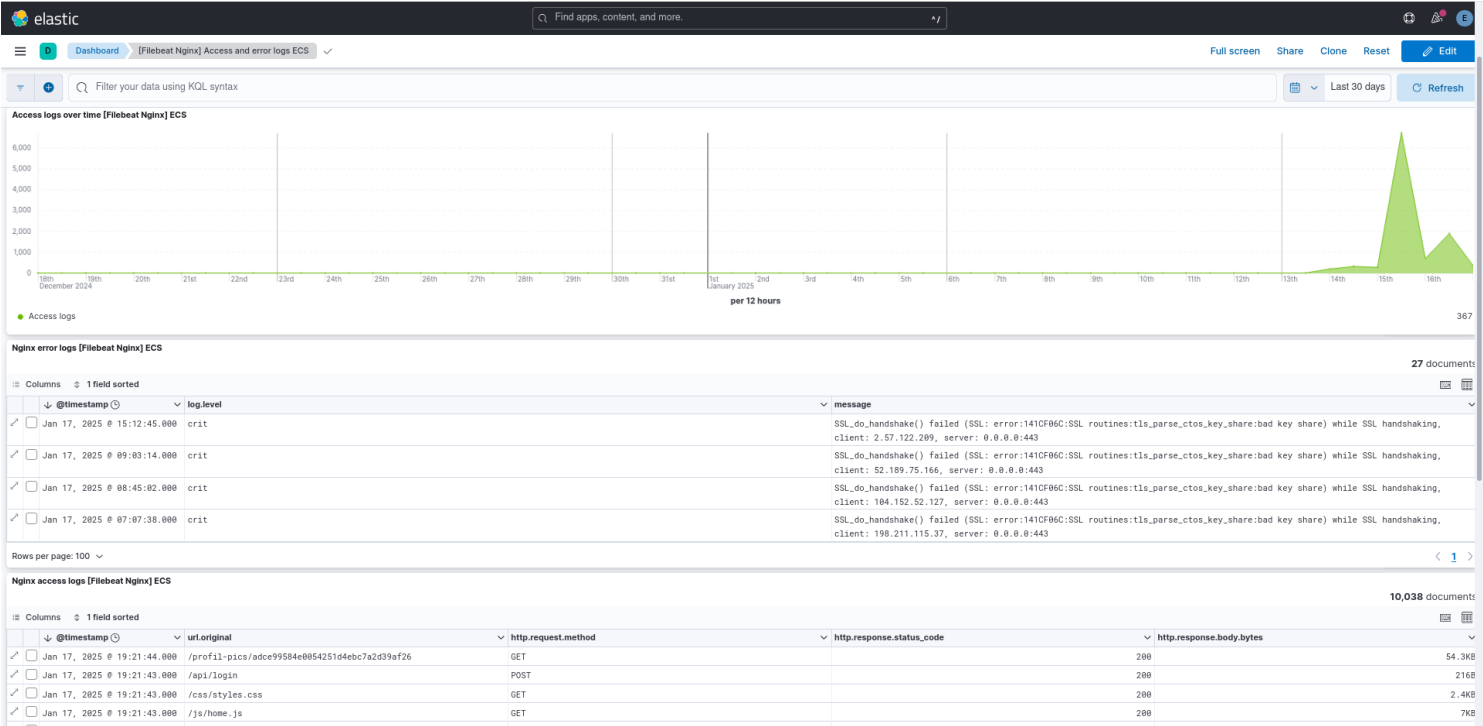


Et les “Browsers breakdown”, qui sont les différents navigateurs qui ont été utilisés pour se rendre sur le site.

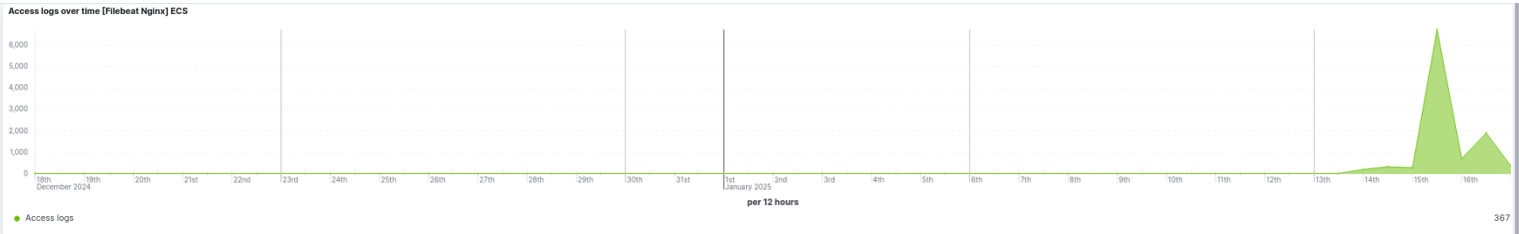


[Filebeat Nginx] Access and error logs ECS

Le dashboard [Filebeat Nginx] Access and error logs ECS permet d’avoir plus de détails sur les access logs et error logs de nginx :



Sur ce dashboard on voit donc un graphique du nombre d’access logs à travers le temps :



Les error logs de nginx, qui montrent la date, le niveau de criticité et le message d’erreur :

Nginx error logs [Filebeat Nginx] ECS					27 documents
Columns 1 field sorted					
	@timestamp	log.level	message		
☒	Jan 17, 2025 @ 15:12:45.000	crit	SSL_do_handshake() failed (SSL: error:141CF86C:SSL routines:tls_parse_ctos_key_share:bad key share) while SSL handshaking, client: 2.57.122.209, server: 0.0.0.0:443		
☒	Jan 17, 2025 @ 09:03:14.000	crit	SSL_do_handshake() failed (SSL: error:141CF86C:SSL routines:tls_parse_ctos_key_share:bad key share) while SSL handshaking, client: 52.189.75.166, server: 0.0.0.0:443		
☒	Jan 17, 2025 @ 08:45:02.000	crit	SSL_do_handshake() failed (SSL: error:141CF86C:SSL routines:tls_parse_ctos_key_share:bad key share) while SSL handshaking, client: 104.152.52.127, server: 0.0.0.0:443		
☒	Jan 17, 2025 @ 07:07:38.000	crit	SSL_do_handshake() failed (SSL: error:141CF86C:SSL routines:tls_parse_ctos_key_share:bad key share) while SSL handshaking, client: 198.211.115.37, server: 0.0.0.0:443		

Puis les access logs, qui montrent la date, l’url auquel l’utilisateur à tenter de se connecter, la méthode de requête (Get, Post), le code de réponse html (100, 200, 300, 400, 500) et le taux de données chargées pour afficher cette page :

Nginx access logs [Filebeat Nginx] ECS					10,038 documents
Columns 1 field sorted					
	@timestamp	url.original	http.request.method	http.response.status_code	http.response.body.bytes
☒	Jan 17, 2025 @ 19:21:44.000	/profil-pics/adce99584e085425104ebc7a2d39af26	GET	200	54.3KB
☒	Jan 17, 2025 @ 19:21:43.000	/api/login	POST	200	216B
☒	Jan 17, 2025 @ 19:21:43.000	/css/styles.css	GET	200	2.4KB
☒	Jan 17, 2025 @ 19:21:43.000	/js/home.js	GET	200	7KB