

R5.Cyber.

Modou Diop

RT3

3. compte rendu de supervision avec votre suite elastic d'un service web (Apache) (**SAE5.Cyber.03**)

Objectif :

- Mettre en place une surveillance des logs Apache à l'aide de Filebeat pour les centraliser dans l'écosystème Elastic (Elasticsearch, Kibana, etc.).

Rappel sur Apache	2
Installation et configuration	2
1. Activation du module Apache dans Filebeat	2
2. Configuration des chemins d'accès aux logs Apache	2
3. Test de la configuration	3
4. Redémarrage de Filebeat	3
5. Chargement des tableaux de bord Kibana	3
6. Vérification de tous les services	4
Supervision et analyse de notre suite elastic apache	4
1. Supervisions	4
2. Analyses	7

Rappel sur Apache

Apache, ou **Apache HTTP Server**, est un serveur web open-source populaire utilisé pour héberger des sites web

Installation et configuration

```
administrateur@rt-mv:~/Téléchargements$ sudo apt install apache2
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
apache2 est déjà la version la plus récente (2.4.52-1ubuntu4.12).
Le paquet suivant a été installé automatiquement et n'est plus nécessaire :
  dns-root-data
Veuillez utiliser « sudo apt autoremove » pour le supprimer.
0 mis à jour, 0 nouvellement installés, 0 à enlever et 4 non mis à jour.
administrateur@rt-mv:~/Téléchargements$
```

1. Activation du module Apache dans Filebeat

La commande `sudo filebeat modules enable apache` a permis d'activer le module Apache au sein de Filebeat, rendant ainsi l'agent capable de collecter et d'envoyer les logs Apache à Elasticsearch

```
administrateur@rt-mv:/etc/filebeat/modules.d$ sudo filebeat modules enable apache
Enabled apache
administrateur@rt-mv:/etc/filebeat/modules.d$ ls
activemq.yml.disabled  haproxy.yml.disabled  osquery.yml.disabled
apache.yml             ibmmq.yml.disabled    panw.yml.disabled
auditd.yml.disabled    icinga.yml.disabled    pensando.yml.disabled
awsfargate.yml.disabled  iis.yml.disabled      postgresql.yml.disabled
```

2. Configuration des chemins d'accès aux logs Apache

Le fichier de configuration `apache.yml` a été modifié pour spécifier les chemins exacts vers les fichiers de logs d'accès et d'erreurs d'Apache, ici les logs sont recherchés dans `/var/log/apache2/`.

```
administrateur@rt-mv: /etc/filebeat/modules.d
GNU nano 6.2 /etc/filebeat/modules.d/apache.yml
Module: apache
# Docs: https://www.elastic.co/guide/en/beats/filebeat/7.17/filebeat-module-apache.html

- module: apache
  # Access logs
  access:
    enabled: true

  # Set custom paths for the log files. If left empty,
  # Filebeat will choose the paths depending on your OS.
  var.paths: ["/var/log/apache2/access.log"]

  # Error logs
  error:
    enabled: true

  # Set custom paths for the log files. If left empty,
  # Filebeat will choose the paths depending on your OS.
  #var.paths:
  var.paths: ["/var/log/apache2/error.log"]
```

3. Test de la configuration

La commande `sudo filebeat test config` a été exécutée pour vérifier la validité de la configuration de Filebeat. Cela garantit que l'agent est prêt à fonctionner sans erreurs.

```
administrateur@rt-mv:/etc/filebeat/modules.d$ sudo nano /etc/filebeat/modules.d/apache.yml
administrateur@rt-mv:/etc/filebeat/modules.d$ sudo filebeat test config
Config OK
administrateur@rt-mv:/etc/filebeat/modules.d$ sudo systemctl restart filebeat
administrateur@rt-mv:/etc/filebeat/modules.d$ sudo filebeat setup --dashboards
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
```

4. Redémarrage de Filebeat

La commande `sudo systemctl restart filebeat` a redémarré le service Filebeat pour appliquer les modifications de configuration.

```
administrateur@rt-mv:/etc/filebeat/modules.d$ sudo systemctl restart filebeat
```

5. Chargement des tableaux de bord Kibana

La commande `sudo filebeat setup --dashboards` a chargé les tableaux de bord Kibana préconfigurés pour la visualisation des données Apache. Cela permet d'avoir une interface graphique pour analyser les logs.

```
administrateur@rt-mv:/etc/filebeat/modules.d$ sudo filebeat setup --dashboards
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
```

6. Vérification de tous les services

```
● filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.
   Loaded: loaded (/lib/systemd/system/filebeat.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2025-01-24 16:36:00 CET; 28min ago
     Docs: https://www.elastic.co/beats/filebeat
    Main PID: 41897 (filebeat)
      Tasks: 9 (limit: 2878)
     Memory: 32.5M
        CPU: 3.163s
    CGroup: /system.slice/filebeat.service
           └─41897 /usr/share/filebeat/bin/filebeat --environment systemd -c /etc/filebeat/fil

janv. 24 17:00:05 rt-mv filebeat[41897]: 2025-01-24T17:00:05.413+0100      INFO      [monito>
janv. 24 17:00:35 rt-mv filebeat[41897]: 2025-01-24T17:00:35.471+0100      INFO      [monito>
janv. 24 17:01:05 rt-mv filebeat[41897]: 2025-01-24T17:01:05.417+0100      INFO      [monito>
janv. 24 17:01:35 rt-mv filebeat[41897]: 2025-01-24T17:01:35.424+0100      INFO      [monito>
janv. 24 17:02:05 rt-mv filebeat[41897]: 2025-01-24T17:02:05.465+0100      INFO      [monito>
janv. 24 17:02:35 rt-mv filebeat[41897]: 2025-01-24T17:02:35.448+0100      INFO      [monito>
janv. 24 17:03:05 rt-mv filebeat[41897]: 2025-01-24T17:03:05.424+0100      INFO      [monito>

● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2025-01-24 16:27:11 CET; 37min ago
     Docs: https://www.elastic.co
    Main PID: 41209 (node)
      Tasks: 11 (limit: 2878)
     Memory: 205.0M
        CPU: 1min 5.811s
    CGroup: /system.slice/kibana.service
           └─41209 /usr/share/kibana/bin/./node/bin/node /usr/share/kibana/bin/./src/cli/dis

janv. 24 16:27:11 rt-mv systemd[1]: Started Kibana.
janv. 24 16:27:11 rt-mv kibana[41209]: Kibana is currently running with legacy OpenSSL providers

● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2025-01-24 16:55:26 CET; 9min ago
     Docs: https://httpd.apache.org/docs/2.4/
    Main PID: 42910 (apache2)
      Tasks: 55 (limit: 2878)
     Memory: 4.1M
        CPU: 59ms
    CGroup: /system.slice/apache2.service
           └─42910 /usr/sbin/apache2 -k start
              └─42911 /usr/sbin/apache2 -k start
                 └─42912 /usr/sbin/apache2 -k start
```

Supervision et analyse de notre suite elastic apache

Nous allons maintenant voir et analyser le tableau de bord Kibana configuré pour visualiser les données collectées par Filebeat à partir des logs Apache.

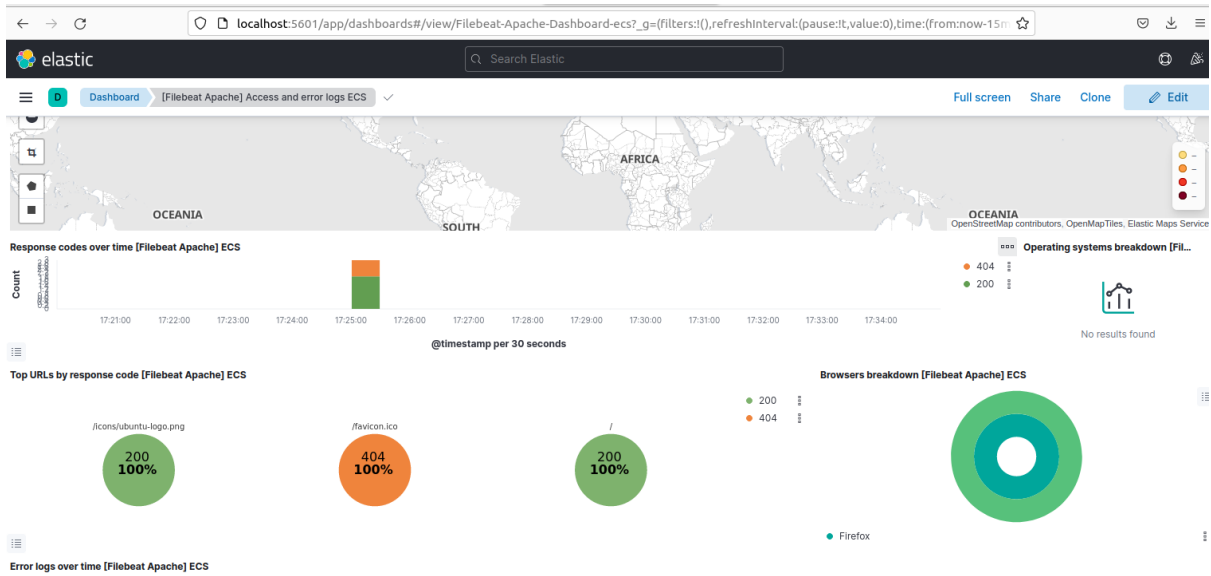
Ce tableau de bord offre une vue d'ensemble de l'activité de votre serveur web.

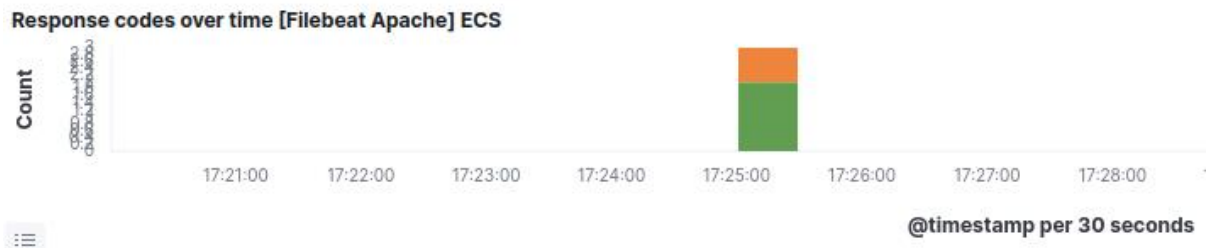
1. Supervisions

Les principaux éléments visualisés sont :

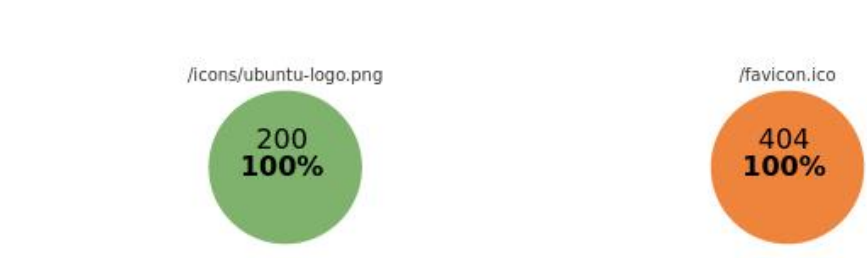
- **Carte géographique:** Elle permet de visualiser la répartition géographique des requêtes reçues par votre serveur.
- **Graphiques temporels:** Ils montrent l'évolution dans le temps des codes de réponse HTTP (200, 404, etc.), du nombre de requêtes par seconde et de la répartition des navigateurs utilisés.

- **Camembert:** Il indique la répartition des navigateurs utilisés pour accéder à votre site.

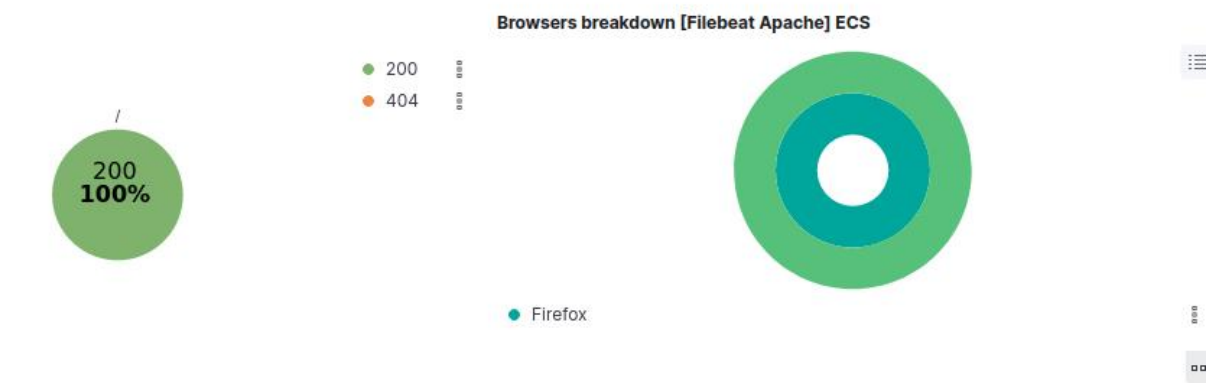
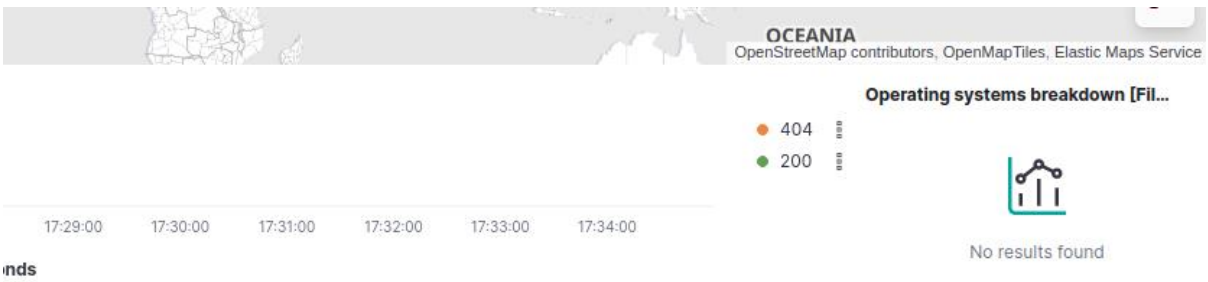




Top URLs by response code [Filebeat Apache] ECS



Error logs over time [Filebeat Apache] ECS



2. Analyses

1. Response codes over time [Filebeat Apache] ECS :

- a. Une visualisation des codes de réponse HTTP (200, 404) sur une période.
- b. On observe un pic pour les codes 200 et 404 à un moment donné (vers 17:25).

2. Top URLs by response code [Filebeat Apache] ECS :

- a. Une répartition des URL les plus sollicitées :
 - i. `/icons/ubuntu-logo.png` a un code de réponse **200 (100%)**.
 - ii. `/favicon.ico` a un code de réponse **404 (100%)**.

3. Browsers breakdown [Filebeat Apache] ECS :

- a. Un graphique circulaire montrant que tous les accès proviennent du navigateur **Firefox**.

4. Error logs over time [Filebeat Apache] ECS :

- a. Section vide, suggérant qu'aucune erreur critique n'a été détectée.

5. Operating systems breakdown [Filebeat Apache] ECS :

- a. Section vide, indiquant que l'information sur les systèmes d'exploitation n'a pas été collectée ou configurée.

En résumé, l'analyse montre principalement :

- Des requêtes réussies (**200**) et quelques erreurs (**404**).
- Firefox est le navigateur utilisé.