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

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$
```

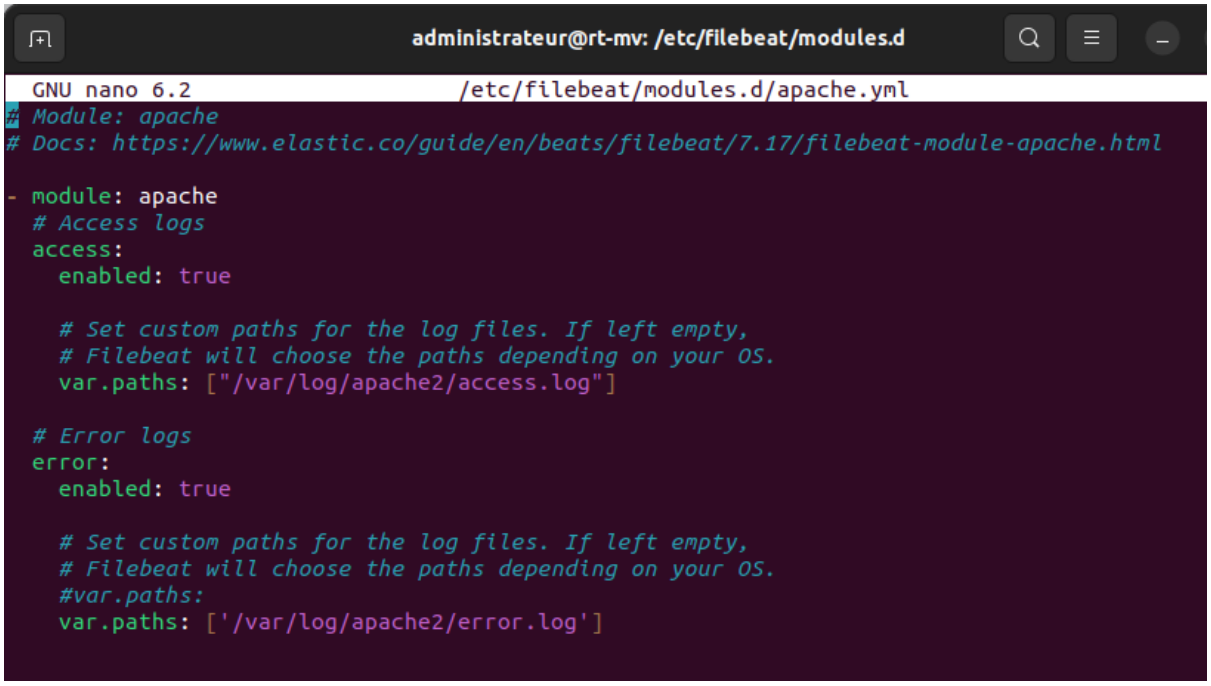
1. Activation du module Apache dans Filebeat

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
```

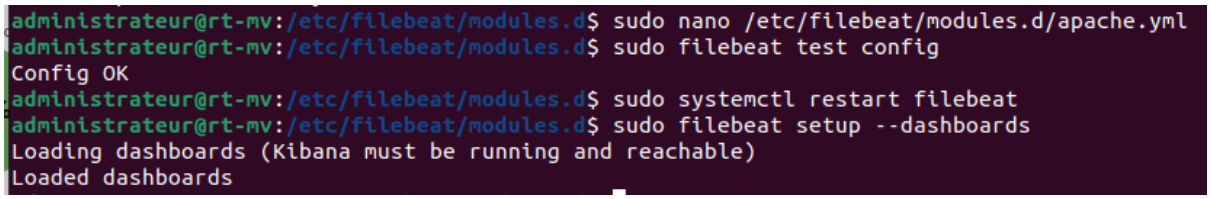
2. Configuration des chemins d'accès aux logs Apache

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/`.



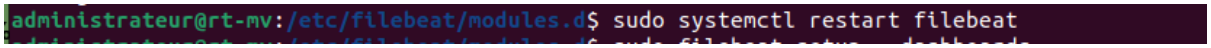
3. Test de la configuration

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.



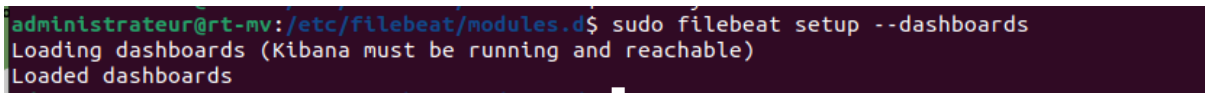
4. Redémarrage de Filebeat

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

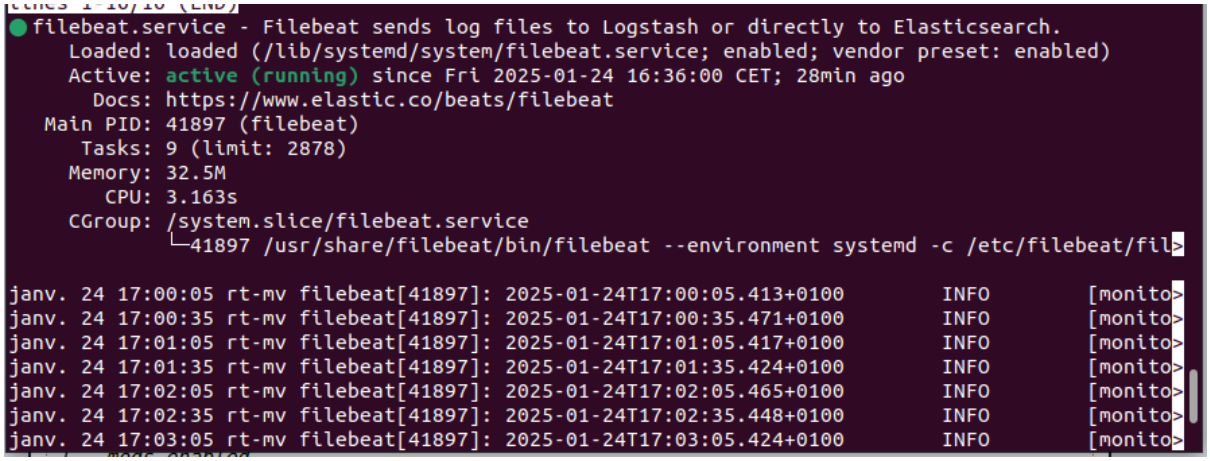


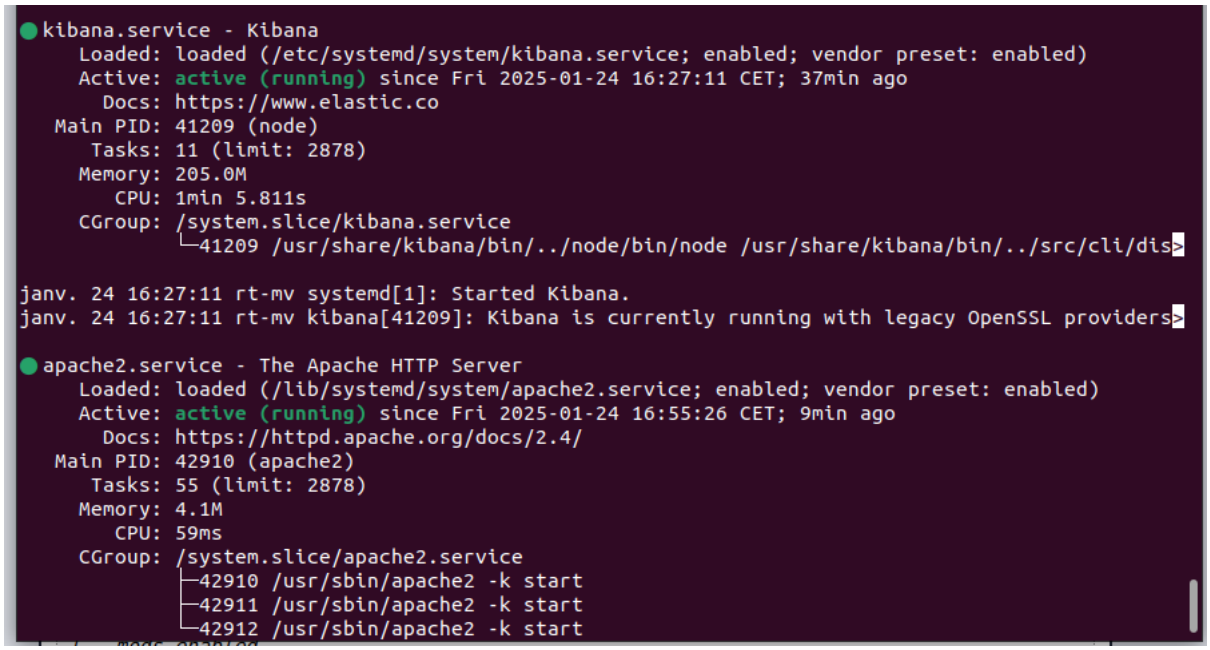
5. Chargement des tableaux de bord Kibana

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.



6. Vérification de tous les services





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.

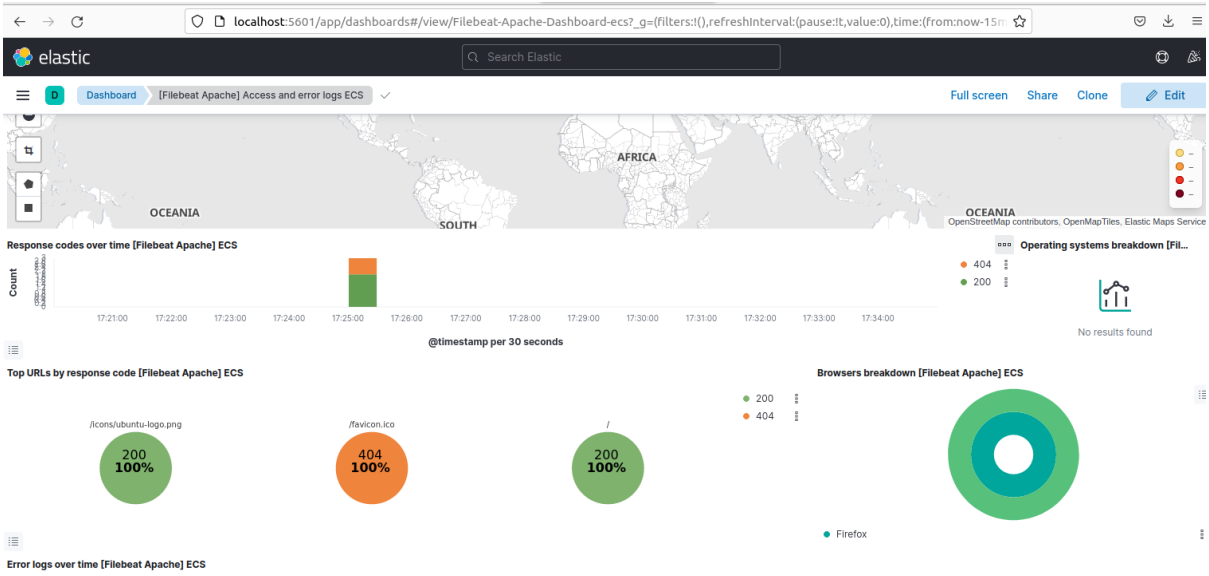
Ce tableau de bord offre une vue d'ensemble de l'activité de votre serveur web.

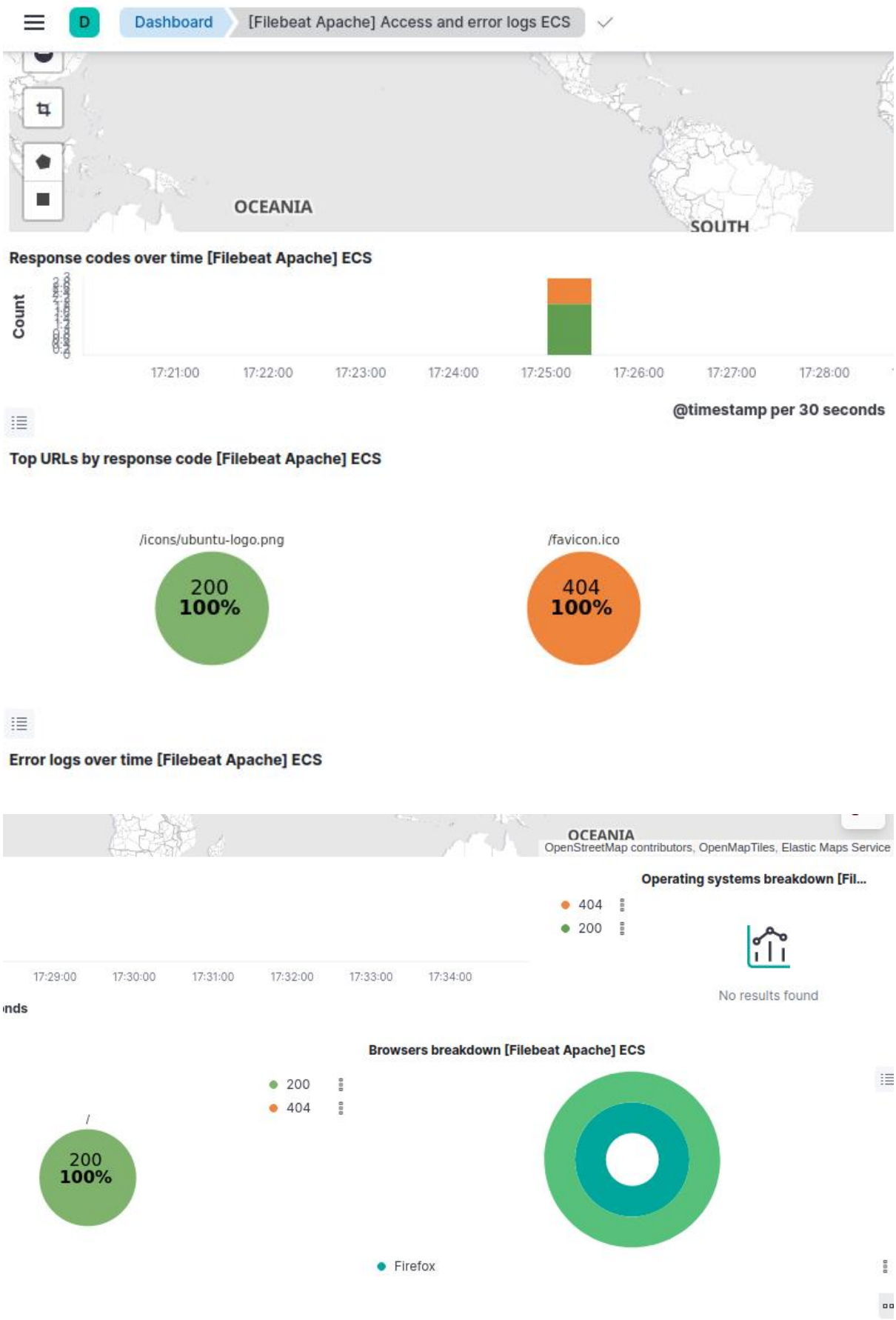
1. Supervisions

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.




D
Dashboard
[Filebeat Apache] Access and error logs ECS
OCEANIA
SOUTH
Response codes over time [Filebeat Apache] ECS
Count
17:21:00
17:22:00
17:23:00
17:24:00
17:25:00
17:26:00
17:27:00
17:28:00
@timestamp per 30 seconds
Top URLs by response code [Filebeat Apache] ECS
/icons/ubuntu-logo.png
200
100%
/favicon.ico
404
100%
Error logs over time [Filebeat Apache] ECS
OCEANIA
OpenStreetMap contributors, OpenMapTiles, Elastic Maps Service
Operating systems breakdown [Fil...
404
200
17:29:00
17:30:00
17:31:00
17:32:00
17:33:00
17:34:00
No results found
Browsers breakdown [Filebeat Apache] ECS
200
404
/
200
100%
Firefox

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.