R5.Cyber.11

Modou Diop

RT3

2/ Compte rendu de supervision elastic d'une machine Ubuntu **(SAE5.Cyber.03)**

Pour cette partie Filebeat est l'outil clé pour la **supervision d'une machine Ubuntu** dans le cadre de notre projet.

C’est quoi Filebeat

Filebeat est un outil de collecte de logs léger qui fait partie de la suite Elastic Stack. Son rôle principal est de lire et d'envoyer des fichiers de logs à des destinations comme :

- **Elasticsearch** pour indexer et rechercher les données,
- **Logstash** pour un traitement et une transformation supplémentaire,

Filebeat agit comme une "sonde" qui surveille les fichiers logs et transmet les nouvelles entrées dès qu'elles apparaissent.

Pourquoi utiliser Filebeat ?

Dans notre projet, Filebeat est utilisé pour ingérer des logs des services déployés :

- Notre projet implique la configuration de services comme Elasticsearch, Kibana ou Logstash, Filebeat peut superviser leurs fichiers de logs et les intégrer dans la plateforme Elastic pour :
    - **Suivre la performance et la disponibilité** des services,
    - **Détecter les erreurs** ou comportements anormaux rapidement.

Filebeat est conçu pour collecter et centraliser les fichiers logs d'une machine. Ces logs contiennent des informations cruciales pour la supervision, comme :

- Les **erreurs système** ou d'application.
- Les **connexions SSH** (tentatives de connexion réussies ou échouées).
- Les **changements d'état des services**.
- Toute activité suspecte ou anormale.

En configurant Filebeat sur une machine Ubuntu, je peux surveiller en temps réel tous ces événements et les transmettre à Elasticsearch pour une analyse approfondie via Kibana.

Installation et configuration de Filebeat

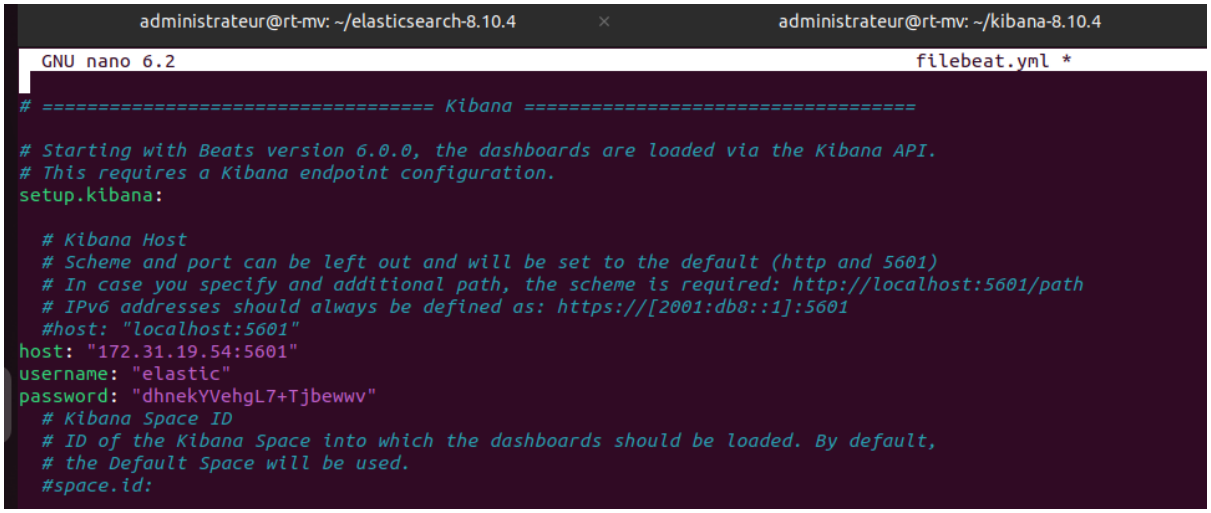
Configuration de Kibana (setup.kibana) :

Le bloc setup.kibana est utilisé pour intégrer Filebeat à Kibana.

Il permet de charger des tableaux de bord prédéfinis (**dashboards**) pour visualiser facilement les données collectées et d'assurer que les données envoyées par Filebeat sont accessibles dans Kibana via une interface utilisateur.

sudo nano /etc/filebeat/filebeat.yml

Dans /etc/filebeat/filebeat.yml :



```
administrateur@rt-mv: ~/elasticsearch-8.10.4        administrateur@rt-mv: ~/kibana-8.10.4
 GNU nano 6.2                                                    filebeat.yml *
# ---------------------------- Elasticsearch Output ----------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["https://172.31.19.54:9200"]
  username: "elastic"
  password: "dhnekYVehgL7+Tjbewwv"
  ssl:
    enable: true
    ca_trusted_fingerprint: 9666e2755a2c2aeef31b66cfc22245fe2bc0440bc431cc88f00a06005d70eb13

  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  #username: "elastic"
  #password: "changeme"
```

Grâce à cette configuration, tu pourras afficher les logs collectés par Filebeat directement dans Kibana sous forme de graphiques ou de tableaux de bord, facilitant ainsi la supervision de ta machine Ubuntu.

Ensuite activer le module **system** de Filebeat. Ce module est conçu pour collecter des journaux spécifiques avec la commande **`sudo filebeat modules enable system`**

Puis lister tous les modules disponibles pour Filebeat et leur état avec la commande **sudo filebeat modules list.**

```
Fichier  Édition  Affichage  Rechercher  Terminal  Onglets  Aide
administrateur@rt-mv: ~/elasticsearch-8.10.4        administrateur@rt-mv: ~/kibana-8.10.4
administrateur@rt-mv:~/filebeat-8.10.4-linux-x86_64$ sudo filebeat modules enable system
[sudo] Mot de passe de administrateur :
Module system is already enabled
administrateur@rt-mv:~/filebeat-8.10.4-linux-x86_64$ ./filebeat modules list
Enabled:

Disabled:
activemq
apache
auditd
aws
awsfargate
azure
barracuda
bluecoat
cef
checkpoint
```

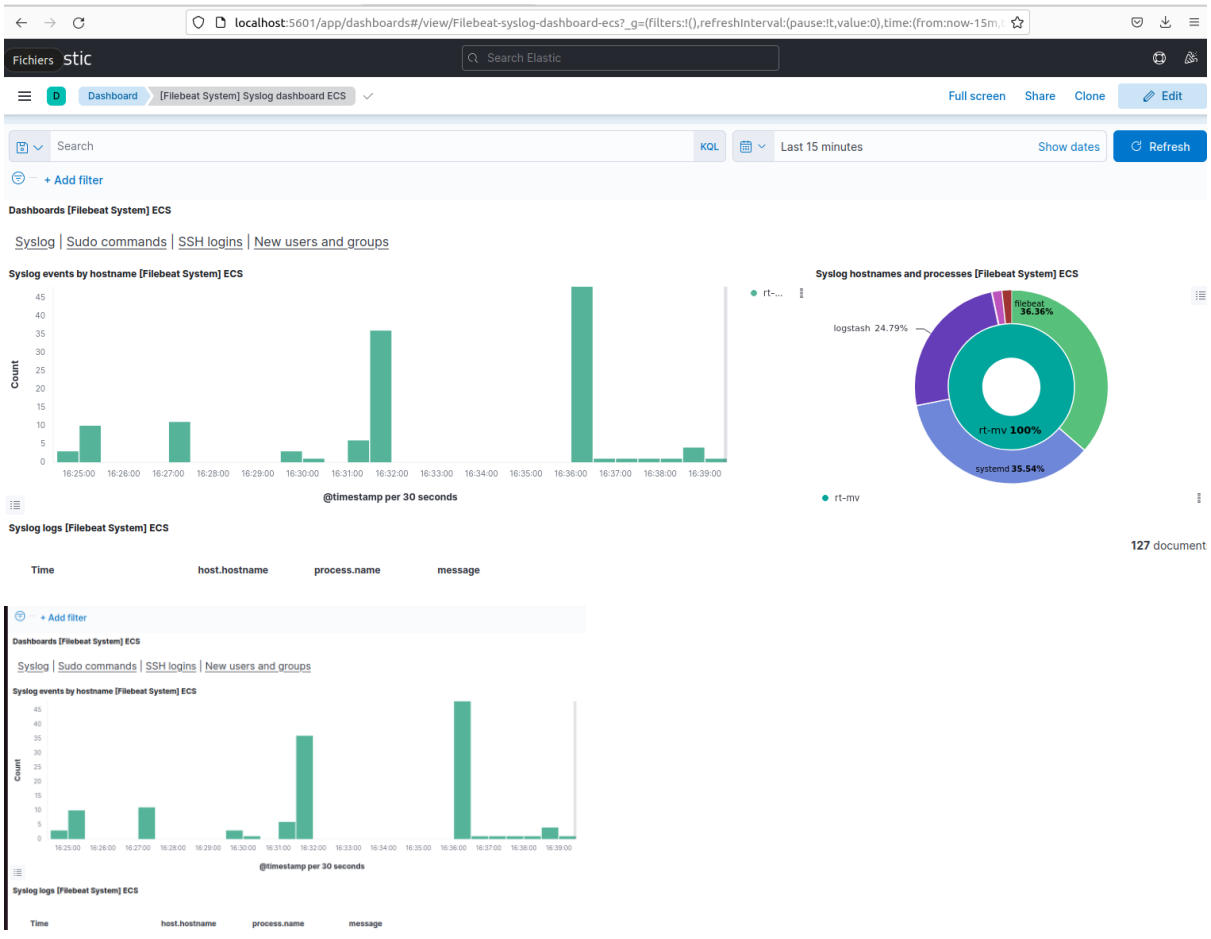
```
administrateur@rt-mv:~/Téléchargements$ sudo filebeat setup --pipelines --modules system
administrateur@rt-mv:~/Téléchargements$ sudo filebeat setup --index-management -E output.logstash.enabled=false -E 'output.elasticsearch.hosts=["localhost:9200"]'
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite: true` for enabling.

Index setup finished.
administrateur@rt-mv:~/Téléchargements$ sudo filebeat setup -E output.logstash.enabled=false -E output.elasticsearch.hosts=['localhost:9200'] -E setup.kibana.host=loca
host:5601
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite: true` for enabling.

Index setup finished.
  Aide g dashboards (Kibana must be running and reachable)
Loaded dashboards
Setting up ML using setup --machine-learning is going to be removed in 8.0.0. Please use the ML app instead.
See more: https://www.elastic.co/guide/en/machine-learning/current/index.html
It is not possble to load ML jobs into an Elasticsearch 8.0.0 or newer using the Beat.
Loaded machine learning job configurations
Loaded Ingest pipelines
administrateur@rt-mv:~/Téléchargements$ sudo systemctl start filebeat
```

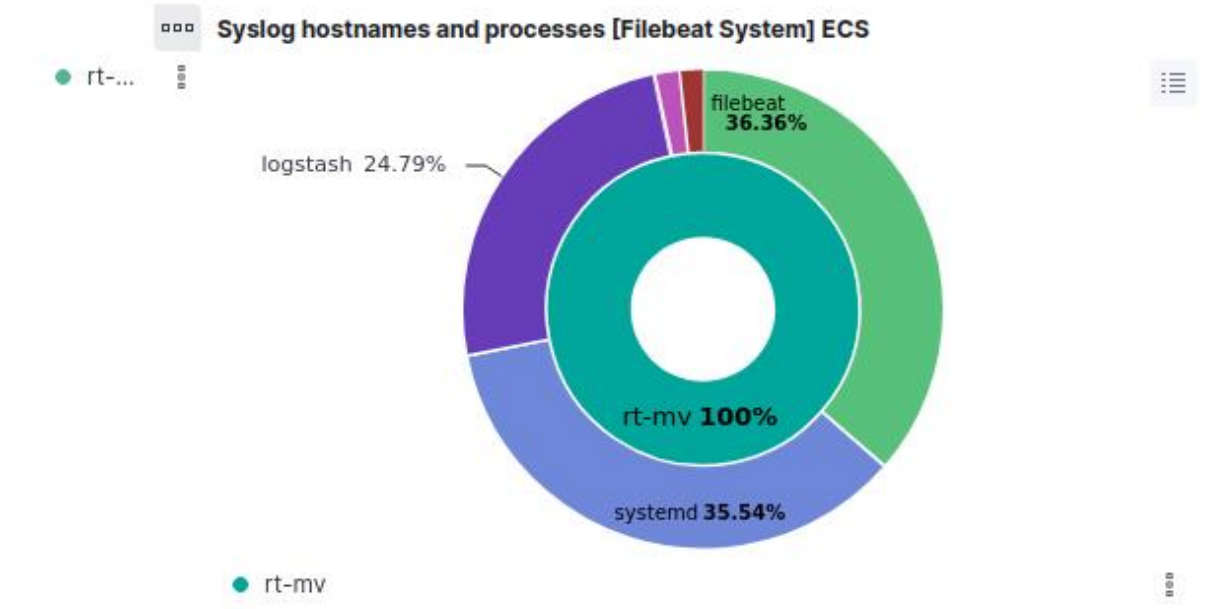
Cette commande configure les pipelines nécessaires dans Elasticsearch pour interpréter et traiter correctement les données collectées par le module **system**. Elle prépare également les tableaux de bord prédéfinis pour Kibana.

```
administrateur@rt-mv:~/Téléchargements$ sudo systemctl enable filebeat
Synchronizing state of filebeat.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable filebeat
Created symlink /etc/systemd/system/multi-user.target.wants/filebeat.service → /lib/systemd/system/filebeat.service.
administrateur@rt-mv:~/Téléchargements$ curl -XGET 'http://localhost:9200/filebeat-*/_search?pretty'
{
  "took" : 63,
  "timed_out" : false,
  "_shards" : {
    "total" : 2,
    "successful" : 2,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 0,
      "relation" : "eq"
    },
```

Supervision et analyse de la machine Ubuntu

Sur l'interface, nous avons un tableau de bord dans Kibana à partir des logs collectés par Filebeat et montrent une supervision fonctionnelle et bien configurée.





127 documents

Syslog logs [Filebeat System] ECS

127 documents

	Time	host.hostname	process.name	message
›	Jan 24, 2025 @ 16:39:05.000	rt-mv	filebeat	2025-01-24T16:39:05.468+0100#011INFO#011[monitoring]#011log/log.go:184#011Non-zero metrics in the last 30s#011{"monitoring": {"metrics": {"beat":{"cgroup":{"memory":{"mem":{"usage":{"bytes":-14589952}}}},"cpu":{"system":{"ticks":370,"time":{"ms":58}},"total":{"ticks":1270,"time":{"ms":107},"value":1270},"user":{"ticks":900,"time":{"ms":49}}},"handles":{"limit":{"hard":524288,"soft":524288},"open":15},"info":{"ephemeral_id":"05b690b8-e13f-46fb-80f1-2326a9bcb5c3","uptime":{"ms":183325},"version":"7.17.27"},"memstats":{"gc_next":25711088,"memory_alloc":12533424,"memory_total":18828270
›	Jan 24, 2025 @ 16:38:50.000	rt-mv	rtkit-daemon	message repeated 7 times: [Supervising 7 threads of 4 processes of 1 users.]
›	Jan 24, 2025 @ 16:38:47.000	rt-mv	rtkit-daemon	Supervising 7 threads of 4 processes of 1 users.
›	Jan 24, 2025 @ 16:38:35.000	rt-mv	filebeat	2025-01-24T16:38:35.448+0100#011INFO#011[monitoring]#011log/log.go:184#011Non-zero metrics in the last 30s#011{"monitoring": {"metrics": {"beat":{"cgroup":{"memory":{"mem":{"usage":{"bytes":-9388032}}}},"cpu":{"system":{"ticks":320,"time":{"ms":20}},"total":{"ticks":1170,"time":{"ms":35},"value":1170},"user":{"ticks":850,"time":{"ms":15}}},"handles":{"limit":{"hard":524288,"soft":524288},"open":15},"info":{"ephemeral_id":"05b690b8-e13f-46fb-80f1-2326a9bcb5c3","uptime":{"ms":153300},"version":"7.17.27"},"memstats":{"gc_next":23116248,"memory_alloc":14887144,"memory_total":183319712,"rss":48803840},"runtime":{"goroutines":58}},"filebeat":{"events":{"added":1,"done":1},"harvester":{"open_files":4,"running":4}},"libbeat":{"config":{"module":{"running":1}},"output":{"events":{"acked":1,"active":0 "batches":1 "total":1} "read":{"bytes":6} "write":{"bytes":1191}} "pipeline":{"clients":2 "events":{"active":0 "published":1 "tota
›	Jan 24, 2025 @ 16:38:30.000	rt-mv	gnome-shell	libinput error: event6 - VirtualBox mouse integration: client bug: event processing lagging behind by 87ms, your system is too slow
›	Jan 24, 2025 @ 16:38:05.000	rt-mv	filebeat	2025-01-24T16:38:05.427+0100#011INFO#011[monitoring]#011log/log.go:184#011Non-zero metrics in the last 30s#011{"monitoring": {"metrics": {"beat":{"cgroup":{"memory":{"mem":{"usage":{"bytes":-2510848}}}},"cpu":{"system":{"ticks":300,"time":{"ms":42}},"total":{"ticks":1130,"time":{"ms":50},"value":1130},"user":{"ticks":830,"time":{"ms":8}}},"handles":{"limit":{"hard":524288,"soft":524288},"open":1

Anomalies identifiées :

1. **Erreur d'intégration de la souris VirtualBox:**
    a. **Message:** "Isbinput error: eventfd VirtualBox mouse integration: client bug: event processing lagging behind by 87ms, your system is too slow"
    b. **Interprétation:** Ce message indique clairement un problème avec l'intégration de la souris VirtualBox dans votre système.
2. **Fluctuations importantes des métriques:**

a. **Message:** "Non-zero metrics in the last 30s"
b. **Interprétation:** Bien que ce message indique simplement qu'il y a eu des changements dans les métriques, des fluctuations importantes et répétées

pourraient signaler un problème sous-jacent, comme une fuite de mémoire ou une charge élevée sur le processeur.

1. Syslog Events by Hostname

Graphique des événements Syslog par intervalle de temps :

Description :
Ce graphique illustre le volume d'événements Syslog enregistrés toutes les 30 secondes sur le système.

Données visibles :
L'hôte principal générant ces événements est nommé `rt-mv`.
On observe des variations dans l'intensité des logs, avec des pics (par exemple, vers 16:36:00).

Interprétation :

Les pics indiquent des périodes d'activité élevée du système ou des événements significatifs. Ces événements peuvent inclure :

- **Connexions SSH ou sudo** (commandes administratives).
- **Changements système critiques** (exemple : démarrage/arrêt de services via `systemd`).
- **Activité utilisateur** ou activité d'applications (exemple : `logstash` collectant les journaux).

À surveiller :

Si ces pics sont inattendus ou se répètent sans raison, ils peuvent indiquer un problème (exemple : tentatives de connexion non autorisées ou surcharge système).

2. Syslog Hostnames and Processes (Diagramme circulaire)

Répartition des processus générant des logs :

- **Description :** Ce diagramme montre les principaux processus ayant émis des logs sur le système supervisé (`rt-mv`).

  processus identifiés :

  - **Logstash (24.37%)** : Collecte et traitement des journaux.
  - **Systemd (35.84%)** : Gère les services et le démarrage/arrêt du système.
  - Autres processus mineurs (restent dans les 39.79%).

Interprétation :

Une grande part des événements est liée à `systemd`, ce qui est normal pour un système en fonctionnement. Cela peut inclure des redémarrages de services ou des journaux de gestion.
La présence de `logstash` confirme que mon pipeline de collecte des données fonctionne bien.

À surveiller :

Des processus inhabituels dans cette liste pourraient signaler des logiciels indésirables ou des activités anormales.
Si `systemd` génère trop d'événements, cela peut indiquer des services instables ou en boucle de redémarrage.

3. Syslog Logs Table (Journal détaillé)

Données détaillées des logs :

Description : Cette table fournit des informations précises sur chaque événement Syslog.

Interprétation :

Cette vue est essentielle pour enquêter sur des problèmes spécifiques :

Identifier les erreurs critiques (exemple : un service qui ne démarre pas).
Suivre les commandes `sudo` ou les tentatives de connexion SSH.
Analyser les logs liés à des processus-clés comme `systemd`.

À surveiller :

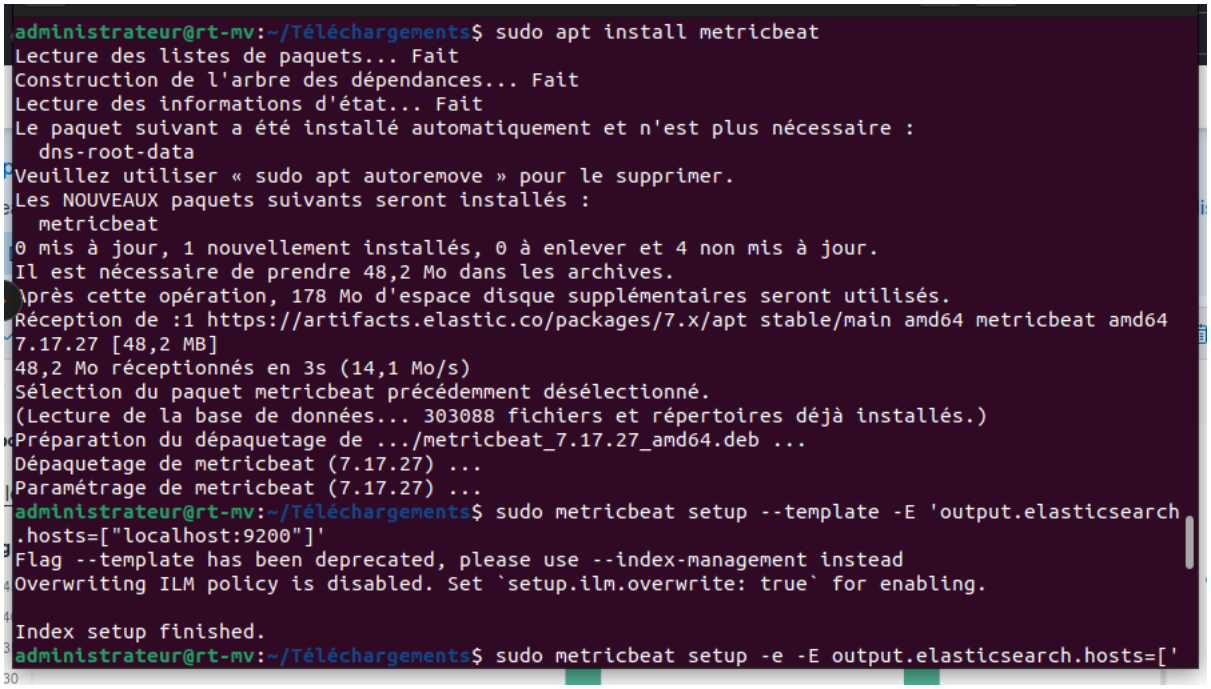
Les erreurs ou avertissements récurrents dans les messages.
Les logs inattendus ou générés par des processus inconnus.

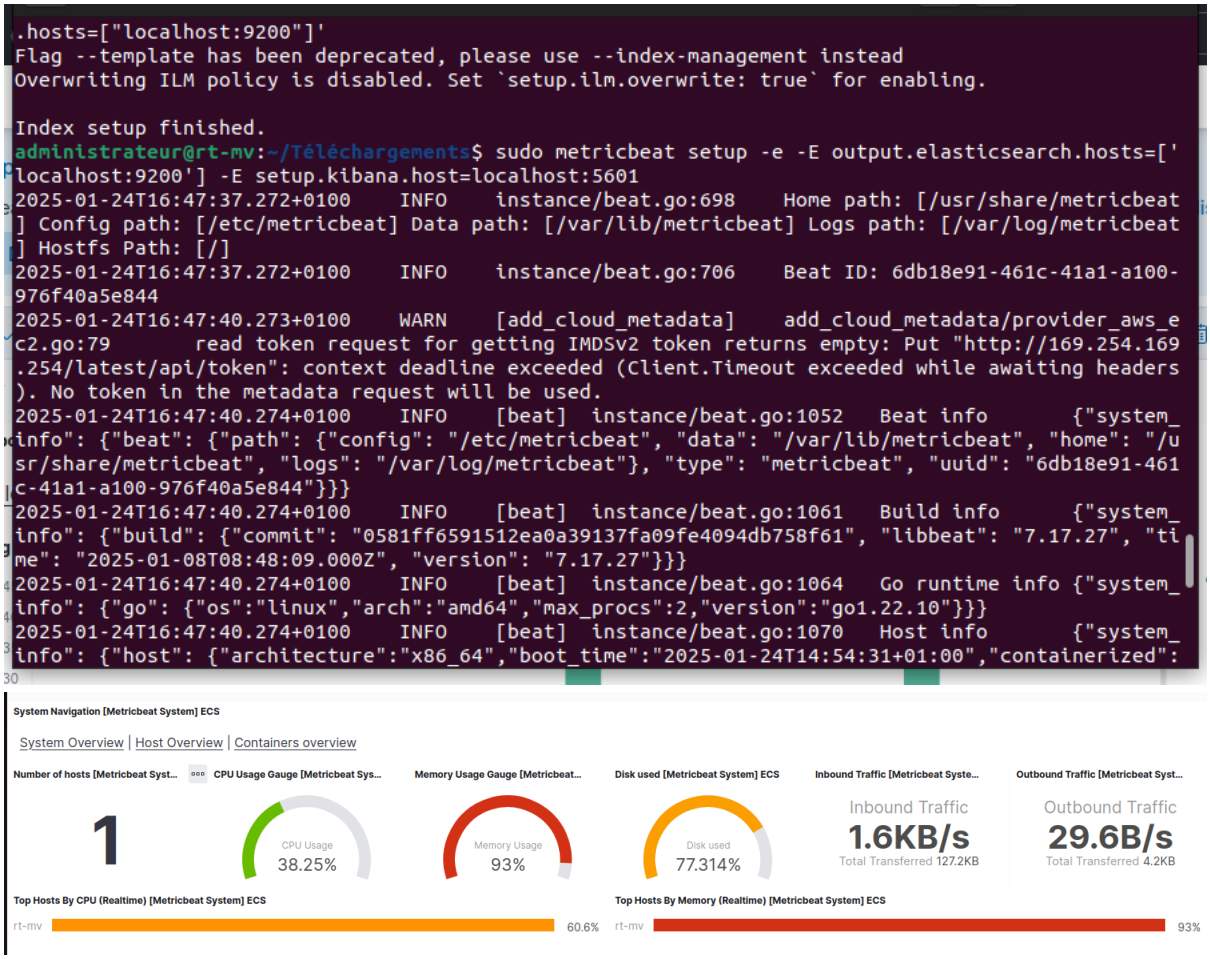
C’est quoi Metricbeat

Metricbeat est un agent léger qui collecte des métriques à partir de systèmes d'exploitation, de conteneurs, de bases de données et d'autres services, puis les envoie vers Elasticsearch (ou d'autres destinations comme Logstash). Ces métriques comprennent des données telles que :

- L’utilisation du CPU, de la RAM et du disque.
- Les statistiques réseau (débit, latence).
- Les métriques spécifiques aux services (par exemple : états des conteneurs Docker, métriques Apache, MySQL, etc.).

Installation et configuration de Metricbeat





Analyse de Metricbeat :

un tableau de bord généré par Metricbeat, un agent léger pour la collecte de métriques. Il fournit une vue instantanée de l'état de votre système ou de votre infrastructure.

Décomposition des indicateurs clés :

- **Nombre d'hôtes : 1**
  - Indique qu'un seul hôte est surveillé par Metricbeat.
- **Utilisation du CPU : 38,25%**
  - Le processeur est utilisé à moins de la moitié de sa capacité, ce qui suggère qu'il y a encore de la marge pour des charges de travail plus importantes.
- **Utilisation de la mémoire : 93%**
  - La mémoire est presque saturée. Il est important de surveiller de près l'évolution de cette métrique pour éviter des ralentissements ou des plantages dus à un manque de mémoire.
- **Disque utilisé : 77,314%**
  - L'espace disque est également presque plein. Il est recommandé de libérer de l'espace ou d'augmenter la capacité de stockage.
- **Trafic entrant : 1,6KB/s**

    - Le trafic entrant est faible, ce qui peut indiquer une activité réseau réduite.
- **Trafic sortant : 29,6GB/s**
    - Le trafic sortant est important, ce qui suggère que l'hôte est en train de transférer de grandes quantités de données vers d'autres systèmes.
- **Top hôtes par utilisation du CPU et de la mémoire**
    - Ces graphiques indiquent que l'hôte surveillé est celui qui consomme le plus de ressources CPU et mémoire.

Interprétation générale et recommandations :

Mémoire et disque presque saturés : Il est essentiel d'identifier les processus ou les applications qui consomment le plus de ressources et de prendre les mesures nécessaires pour les réduire ou les libérer. Cela peut impliquer de :

Arrêter des processus inutiles

Augmenter la capacité de mémoire

Libérer de l'espace disque en supprimant des fichiers inutiles

Optimiser les applications