D R5.Cyber.

Modou Diop

RT3

4/ Compte rendu de supervision avec votre suite elastic d'équipement(s) Cisco **(SAE5.Cyber.03)**

Sommaire

INTRODUCTION

Le but de ce projet est de mettre en place une solution de supervision pour les équipements Cisco dans l'infrastructure réseau. En utilisant la suite Elastic (Elasticsearch, Logstash, Kibana), nous avons centralisé les logs et les métriques provenant des équipements Cisco afin d'assurer une gestion proactive des performances et de la sécurité réseau.

Ce rapport décrit les étapes de configuration, les métriques surveillées, ainsi que les tableaux de bord créés pour faciliter la gestion des équipements Cisco."

Configurer le switch pour envoyer les logs vers le serveur syslog

Apres quelques vérifications de réseau (port up/down, vlan...), on doit configurer le switch pour envoyer les logs vers l'adresse IP de notre machine virtuelle (192.168.1.2) avec la commande :

logging host 192.168.1.2

```
Switch(config)#int vlan 1
Switch(config-if)#ip add
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#do sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.1     YES manual up                    up
FastEthernet0/1        unassigned      YES unset  up                    up
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
```

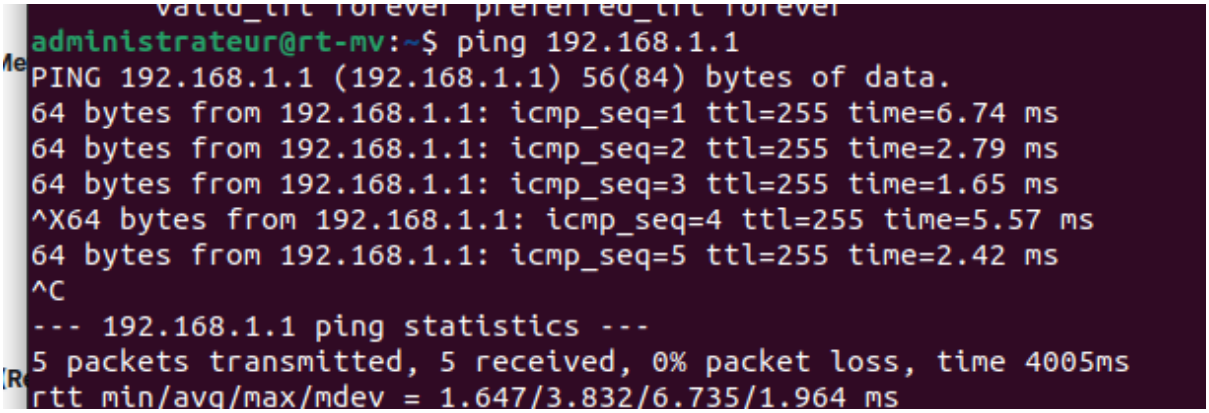
```
Switch(config-if)#do sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
10   VLAN0010                         active
```

```
Switch(config-if)#logging host 192.168.1.2
Switch(config)#exit
Switch#
*Mar  1 02:47:02.347: %SYS-5-CONFIG_I: Configured from console by console
Switch#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited, 0 flushes, 0 overru)
```

```
    Console logging: level debugging, 14 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 15 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    File logging: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 19 message lines logged
        Logging to 192.168.1.2  (udp port 514, audit disabled,
              link up),
              3 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
        Logging Source-Interface:       VRF Name:

Log Buffer (4096 bytes):
```

Configurer Filebeat pour récupérer les logs syslog

D'abord un ping pour s'assurer qu'on est bien sur le réseau



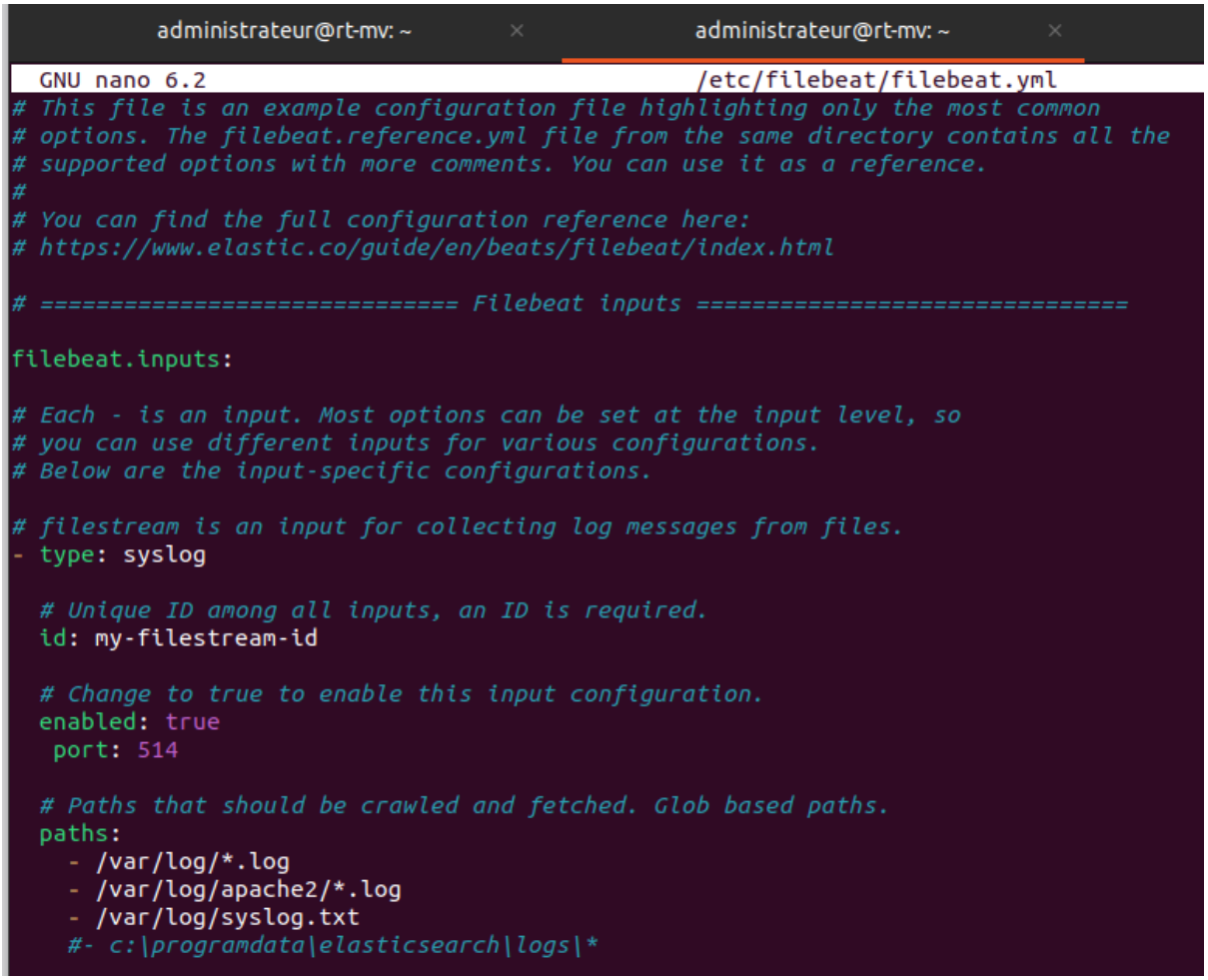
Apres sur la machine virtuelle, pour ponsulter les Logs et les Métriques dans Kibana

il faut :

Ouvrir le fichier de configuration de Filebeat :

Trouvez la section filebeat.inputs et activez la collecte des logs syslog en modifiant ou ajoutant la configuration suivante :

sudo nano /etc/filebeat/filebeat.yml



Démarrer Filebeat :

sudo systemctl start filebeat

sudo systemctl enable filebeat

Vérifier la réception des logs dans Elasticsearch

Explore les Logs

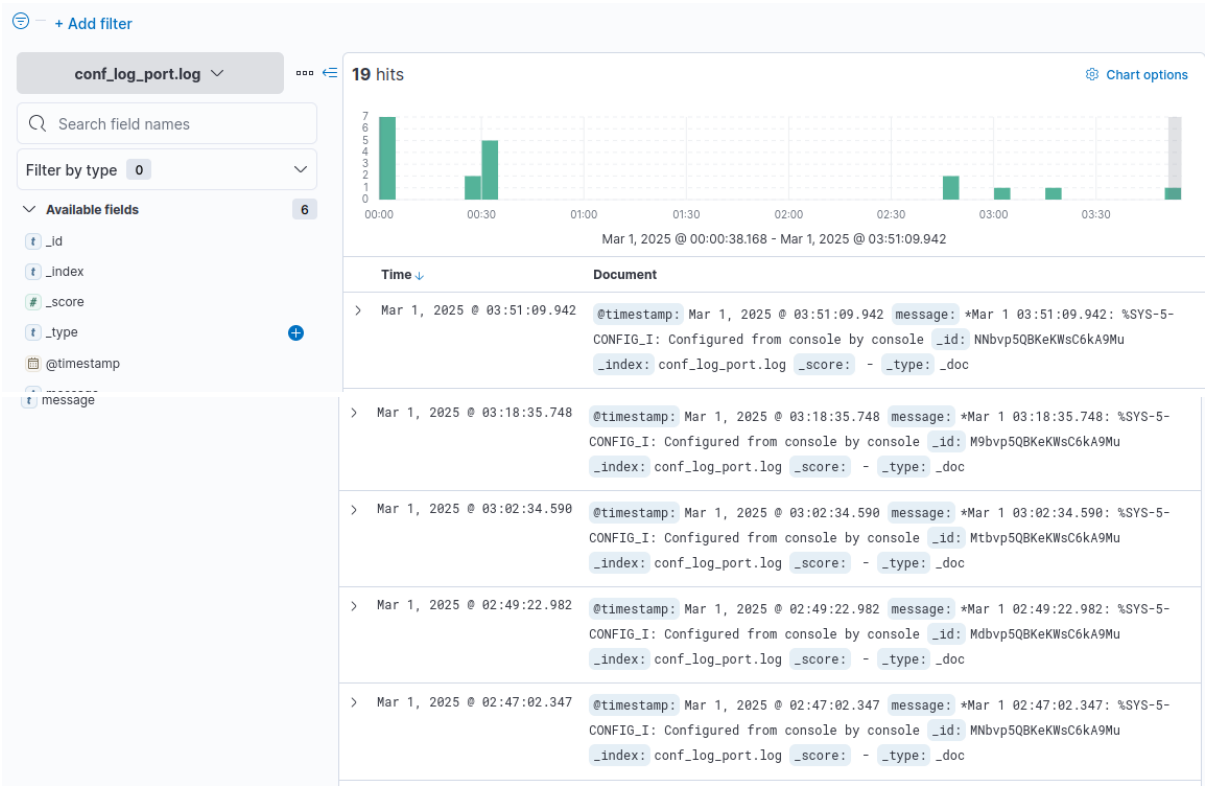
Avant d'explorer, Vérifier la configuration du serveur Syslog :

- Le serveur écoute bien sur le port 514 (UDP/TCP).
- Les logs du switch sont autorisés

Puis

Dans **Discover** pour explorer les données brutes des logs.

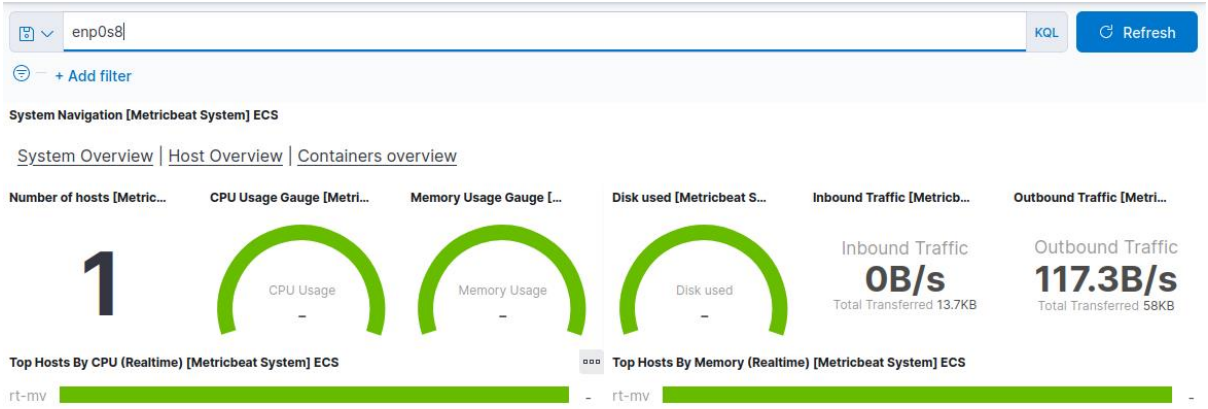
Utilise les filtres en haut de l'interface pour chercher des événements spécifiques comme ici pour voir les erreurs :



Analyser les logs dans Kibana

1. **Activité fréquente de configuration** :

   a. Les trois logs visibles dans l'extrait partagent le message principal `Configured from console by console`, indiquant que des modifications ont été appliquées à la configuration de l'équipement réseau (switch ou autre).
   b. Cela reflète une intervention manuelle (via console) par un administrateur réseau.
2. **Chronologie des événements** :
   a. Les événements se produisent en séquence :
      i. 03:02:34.590
      ii. 03:18:35.748
      iii. 03:51:09.942
   b. Cela montre des actions de configuration à intervalles réguliers.
3. **Indice de document** :
   a. Les logs sont indexés sous le type `conf_log_port.log`. Cela peut signifier que ces logs sont spécifiques à des modifications de configuration réseau (port de switch, VLAN, ou autre).
4. **Niveau d'information** :
   a. Le niveau %SYS-5 est un log de priorité moyenne (niveau 5 sur 8 selon la norme Syslog). Cela indique des événements non critiques mais informatifs, ici relatifs à la configuration.



- **Interface réseau filtrée : enp0s8**

  Ici nous avons appliqué un filtre pour afficher uniquement les données concernant l'interface réseau enp0s8.

- **Nombre de serveurs/hosts** : 1

  Seul un hôte est surveillé, indiqué par "Number of hosts: 1".

- **Trafic réseau** :

  Entrant (Inbound) : 0 B/s, avec un total de 13,7 Ko transférés.

Sortant (Outbound) : 117,3 B/s, avec un total de 58 Ko transférés.
L'interface réseau semble principalement transmettre des données sortantes.

- **Hosts principaux par utilisation :**

Le serveur rt-mv est actif et affiché comme étant en tête de l'utilisation (sans autre détail visible sur les graphes).

Pour pousser plus loin

Pour aller plus loin il est possible de :

Identifier les modifications spécifiques :

- Examinez les logs précédents ou suivants dans la chronologie pour voir quelles commandes ou changements exacts ont été appliqués. Cela peut inclure des activations/désactivations d'interfaces, des ajustements de VLAN, etc.

Rechercher des anomalies :

- Vérifie-s'il existe des erreurs ou alertes (niveaux Syslog supérieurs comme 3 ou 2) autour des mêmes horodatages. Par exemple, des logs de type `%LINK-3-UPDOWN` pourraient indiquer des interruptions réseau.

Relier à des actions utilisateur :

- Si vous avez des journaux d'accès ou d'authentification, croisez-les avec ces horodatages pour identifier quel administrateur a effectué les modifications.

Automatiser la surveillance :

- Configurez des alertes pour les niveaux de log critiques ou pour des modifications de configuration non planifiées.