**Graylog**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **DESC** | | | | |
| Gestionnaire/Monitoring logs | | | | |
| **FILES** | | | | |
| /etc/ | graylog/ | server/ | server.conf | Configuration |
|  |  |  | Log4j2.xml | Logging configuration |
|  | Default/ | Graylog-server | JVM settings | |
| /var/ | log/ | graylog-server/ | server.log | Logs |
|  | Lib/ | Graylog-server/ | journal | Message journal files |
| **QUICK START** | | | | |
| * Configuration server.conf * Configuration elasticsearch.yml   + Cluster.name : graylog   + Network.host :   + http.port : 9200 * Configuration Graylog webserver basique :   + Configurer un Input   + Utiliser un extractor pour parser le message entrant * Configuration Graylog webserver avancée:   + Crée des streams avec indices différents pour chaque log différents | | | | |

**Généralités :**

* Graylog utilise :
  + MongDB pour stocker la configuration
  + Elasticsearch pour stocker les données
  + Graylog-server avec serveur web intégré si besoin
  + Collector-sidecar si besoin de rapatrier des fichiers vers Graylog
* Graylog Marketplace pour les add-ons.
* Mot de passe root uniquement définit dans la configuration
* Inspection de la base ES par l’onglet search, puis transformation en widgets directement dans l’onglet Dashboard
* Web Interface et collector-sidecar communiquent avec Graylog-server via la REST API
* Sécurité :
  + Utiliser TLS
  + MongoDB et ES ne doivent pas écouter sur une interface publique
  + SELinux
* **Inputs -> extracteurs -> stream -> processing pipelines -> outputs**
* **Inputs :** 
  + Syslog
  + GELF
  + AWS
  + Beats via collector-sidecar
  + JSON
  + Netflow
  + Plain/Raw text
* **Extracteurs :** Parsing du message entrant
* **Stream :** routage des paquets entrants dans des catégories en temps réel et re-routés ou affectés à un set d’indices

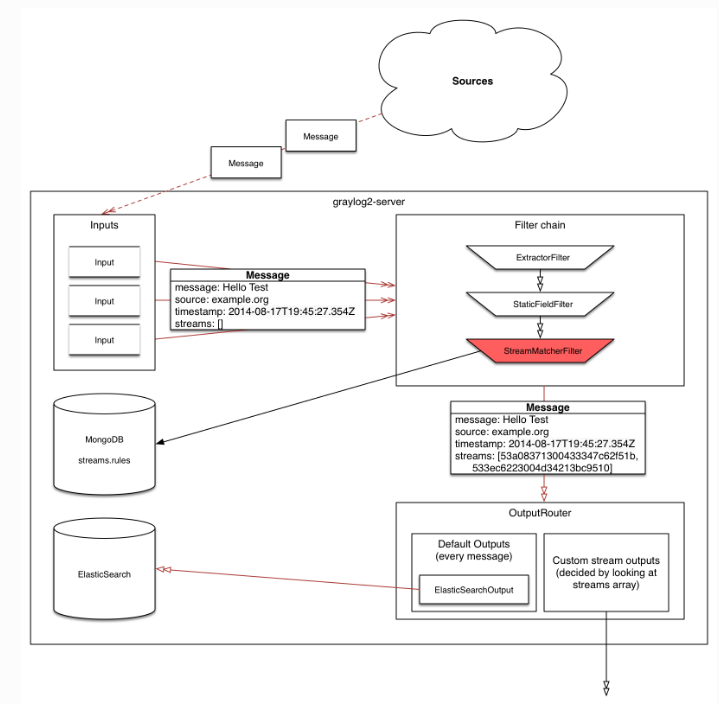
Le routing vers des streams s’effectue via des **règles** sur les messages entrants

On peut créer plusieurs stream en fonction de **conditions** (ex 1 stream d’alerting, un stream syslog, un stream d’alertes Suricata, un stream d’alertes Suricata de niveau 1…)

Chaque stream est affecté à un set d’indices.

Use case :

* Créer une liste de logins SSH failed et utilisation de quick values pour voir quel username ont été failed
* Autre



* **Outputs :** Pour forwarder des streams ailleurs
* **Alerting :** Basé sur les streams
  + Condition (Basé sur le nombre d’occurrences, le temps, le dépassement de seuils…)
  + Notification
* **Décorateurs :** Messages non modifiés en base mais modifiés à l’affichage
  + Modification de champs pour une meilleure visibilité
  + Combinaison de champs
  + Ajouts de champs aux messages

Les décorateurs sont composés de :

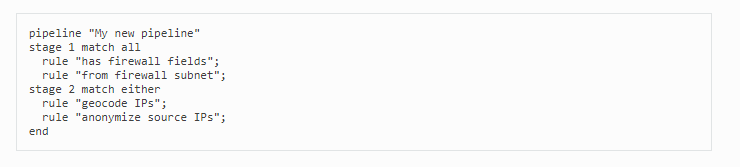
* Syslog severity mapper : Valeur numérique du level changé en phrase.
* Format string : Ajout d’un nouveau champ, qui peut contenir un ou plusieurs champs déjà existants, ainsi que du texte.
* Pipeline decorator
* Lookup table
* **Pipeline :** Basé sur les streams

Etablissement de règles ou série de règles sur des logs : enrichissement ou modification de logs.

2 sortes de pipeline :

* Pipeline decorator, non persistants (qui ont besoin d’un processing pipeline non affecté à un stream)
* Processing pipeline affecté à un stream, persistant

Basé sur les règles Drools : conditions suivis d’une liste d’actions



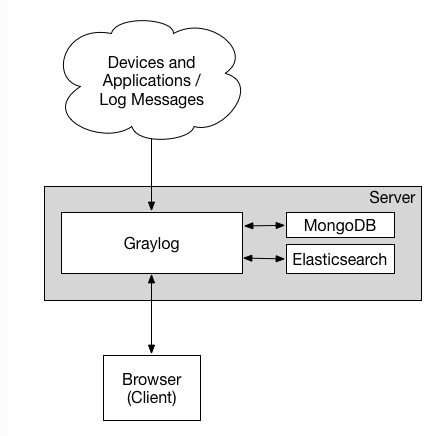


$message.dst\_ip -> accès aux champs du message

**Corrélations ?**

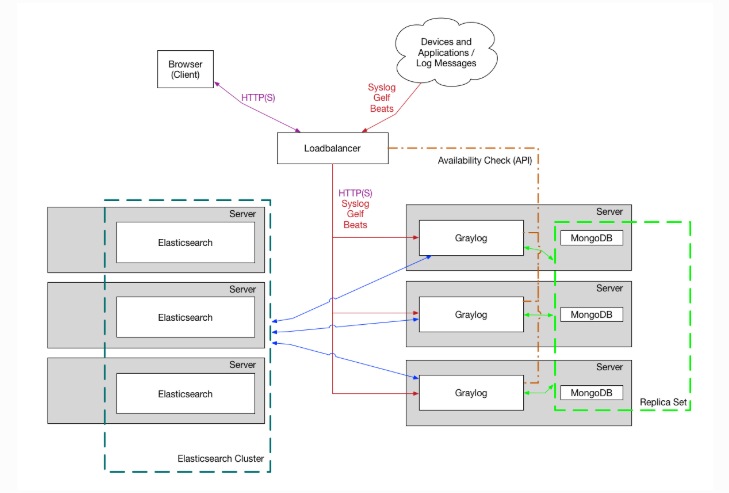
**Fonctionnement**

* Basique :

****

* Multi-node simple :
  + Elasticsearch, MongoDB et graylog-server sur leur host respectif
  + Elasticsearch d’un côté, MongoDB et graylog-server de l’autre
* Multi-node complexe :

High availability, Elasticsearch et MongoDB sont clustérisés.



**Fichier de configuration :**

|  |  |  |
| --- | --- | --- |
| **Directive** | **Comments** | |
| **GENERALE** | | |
| **Is\_master** | Un seul maitre Graylog-server si cluster  Ce maitre va exécuter des actions de maintenances périodiques | |
| **Node\_id\_file= <path>** | Fichier contenant l’ID de ce nœud Graylog | |
| **Root\_username** | Nom du root | |
| **Rules\_files = <path>** | Drools rule file (rewriting des messages entrants) | |
| **Dashboard\_widget\_default\_cache\_time** | Délai de rafraîchissement des widgets par défaut | |
| **Allow\_highlighting** | Autorise le highligh des résultats lors d’une recherche Graylog, mais consomme beaucoup de ressources | |
| **STREAM** | | |
| **Stream\_processing\_timeout** | Renvoie une faute si un la durée de match d’un stream excède cette valeur | |
| **Stream\_processing\_max\_faults** | Désactivation du stream si le nombre de fautes dépasse cette valeur | |
| **OBLIGATOIRE** | | |
| **Password\_secret=<secret>** | Utilisé pour le chiffrement et le salage  Min 64 caractères  Utilisé le même pour tous les nœuds  pwgen –N 1 –s 96 | |
| **Root\_password\_sha2** | Mot de passe root  Echo –n <password> | shasum –a 256  Echo –n <password> | sha256sum | |
| **Rest\_listen\_uri** | Doit être atteignable par les autres nœuds Graylog-server ainsi que par les collecteurs s’ils sont utilisés  @IP interne de Graylog  127.0.0.1 :9000/api/  **Mais mettre en publique si besoin du web server ?** | |
| **Rest\_transport\_uri** | @IP publique de Graylog  192.168.1.1 :9000/api/ | |
| **Web\_enable** |  | |
| **Web\_listen\_uri** | @IP interne de Graylog  127.0.0.1 :9000/  **Mais mettre en publique si besoin du web server ?** | |
| **Web\_endpoint\_uri** |  | |
| **Elasticsearch\_hosts** | Liste de nœuds ES ou Graylog va se connecter | |
| **Mongodb\_uri** | Connection à MongoDB | |
| **Root\_timezone= <TZ>** |  | |
| **SECURITE** | | |
| **REST** | **Rest\_enable\_tls** | HTTPS pour la REST API |
| **Rest\_tls\_cert\_file** | Certificat X509 |
| **Rest\_tls\_key\_file** | Clef privée |
| **Rest\_tls\_key\_password** | Passphrase protégeant la clef privée |
| **Web** | **web\_enable\_tls** |  |
| **web\_tls\_cert\_file** |  |
| **web\_tls\_key\_file** |  |
| **web\_tls\_key\_password** |  |
| **Email** | Voir partie correspondante | |

**Syntaxe de la recherche :**

|  |  |
| --- | --- |
| **Directive** | **Comments** |
| (ssh login) | Inclut le terme ssh ou login |
| "ssh login" | Inclut le term exact ssh login |
| \_exists : |  |
| /REGEX/ |  |
| NOT AND OR |  |
| ? \* | Globbing (doit être activé dans la configuration) |
| > | < | <= | >= |  |