**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 :   + Configurer un Input   + Utiliser un extractor pour parser le message entrant | | | | |

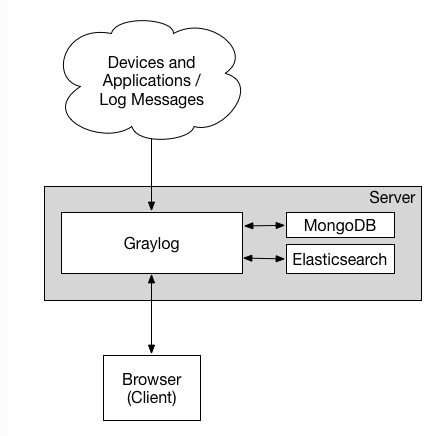
**Généralités :**

* Graylog utilise :
  + MongDB pour stocker la configuration
  + Elasticsearch pour stocker les données
* Graylog Marketplace pour les add-ons.
* Mot de passe root uniquement définit dans la configuration
* Stream : Les logs entrants sont affectés à un stream et peuvent être re-routés
* Inspection de la base ES par l’onglet search, puis transformation en widgets directement dans l’onglet Dashboard
* Inputs :
  + Syslog
  + GELF
  + AWS
  + Beats via collector-sidecar
  + JSON
  + Netflow
  + Plain/Raw text
* Alerting
  + Condition
  + Notification
* Pipeline : Etablissement de règles ou série de règles sur des logs : enrichissement ou modification de logs.

**Corrélations ?**

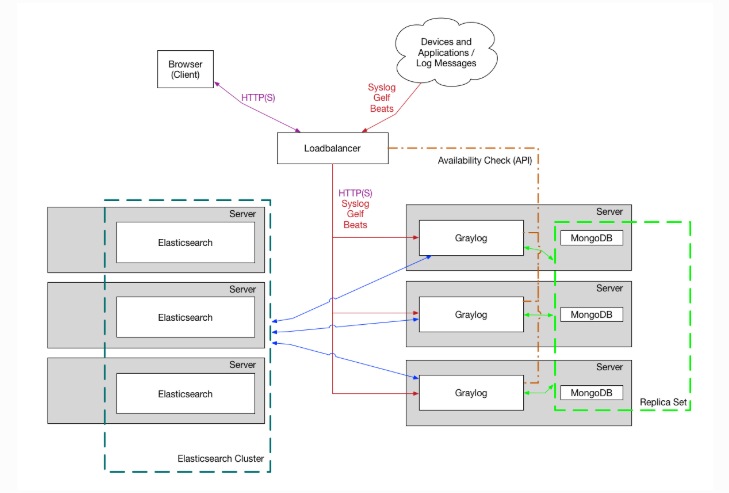
**Fonctionnement**

* 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 |
| **Root\_username** | Nom du root |
| **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\_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 |
| **SECURITE** | |
|  |  |
|  |  |
|  |  |

**Syntaxe de la recherche :**

|  |  |
| --- | --- |
| **Directive** | **Comments** |
|  |  |