**Graylog**

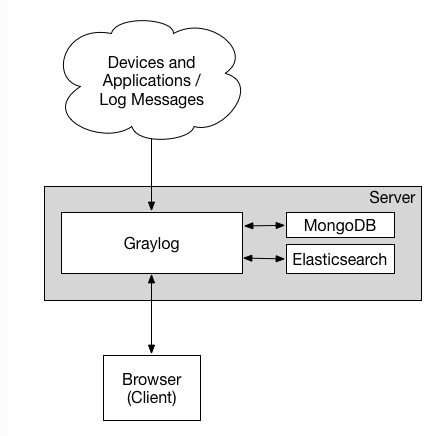
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **DESC** | | | | |
| Gestionnaire/Monitoring logs | | | | |
| **FILES** | | | | |
| /etc/ | graylog/ | server/ | server.conf | Configuration |
| /var/ | log/ | graylog-server/ | server.log | Logs |
| **QUICK START** | | | | |
|  | | | | |

**Généralités :**

* Graylog utilise :
  + MongDB pour stocker la configuration
  + Elasticsearch pour stocker les données

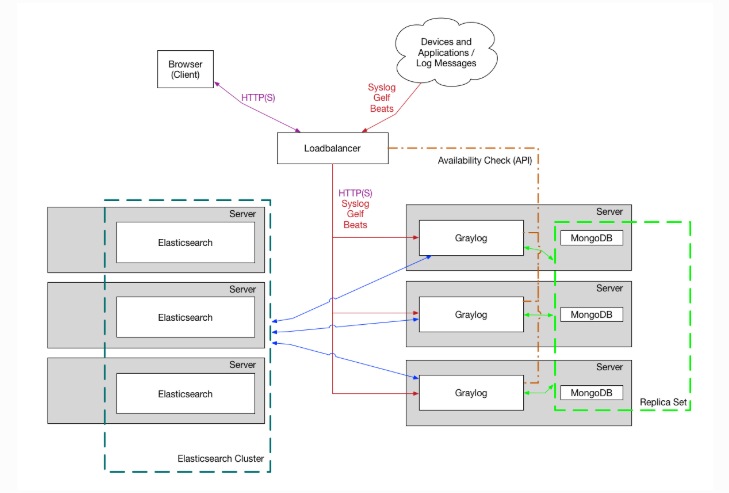
**Fonctionnement**

* 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** | |
|  |  |
| **OBLIGATOIRE** | |
|  |  |
|  |  |
| **SECURITE** | |
|  |  |
|  |  |
|  |  |