|  |  |
| --- | --- |
| **CONF GRAYLOG SERVER** | |
| **Is\_master=true** | 1 master seulement si clusters de servers |
| **Node\_id\_file** | Path de l’ID de ce serveur |
| **Password\_secret** | Minimum 64 caractères : Le même pour tous les nœuds graylog.  Utilisé pour le mdp et salting.  Pwgen –n 1 –s 96 |
| **Root\_username** | Admin par défaut |
| **Root\_password\_sha2** | Echo –n <passwd> | shasum –a 256  Ne peut pas être changé autrement que dans ce fichier |
| **Root\_email** |  |
| **Plugin\_dir** |  |
| **Rest\_listen\_uri** | @adresse :port d’écoute du serveur REST API  Communication entre graylog serveur, serveur web…  @private address |
| **Rest\_transport\_uri** |  |
| **Rest\_enalble\_tls** |  |
| **Rest\_tls\_cert\_file** | Fichier de certificats X509 REST API |
| **Rest\_tls\_key\_file** | Clef privée REST API |
| **Rest\_tls\_key\_password** | Mdp pour unlocker la clef privée REST API |
| **Rest\_thread\_pool\_size** |  |
| **Trusted\_proxies** | Proxy |
| **CONF WEB SERVER** | |
| **Web\_enable** |  |
| **Web\_listen\_uri** | @d’écoute du REST API  @private address |
| **Web\_endpoint\_uri** | Par défaut rest\_transport\_uri.  @ public address |
| **Web\_enable\_tls** |  |
| **Web\_tls\_cert\_file** |  |
| **Web\_tls\_key\_file** |  |
| **Web\_tls\_key\_password** |  |
| **Web\_thread\_pool\_size** |  |
| **CONF ELASTIC SEARCH** | |
| **Elasticsearch\_hosts** | Graylog server se connectera dessus. |
| **Elasticsearch\_connect\_timeout** |  |
| **Elasticsearch\_socket\_timeout** |  |
| **Elasticsearch\_idle\_timeout** | -1 = infinity |
| **Elasticsearch\_max\_total\_connections** |  |
| **Elasticsearch\_discovery\_enabled** | Découverte de nœuds ES. |
| **CONF ELASTIC SEARCH - ROTATION** | |
| **Rotation\_strategy** | Count, size, time. |
| **Elasticsearch\_max\_docs\_**  **Per\_index** | A utiliser avec count, #documents maxi par index |
| **Elasticsearch\_max\_size\_**  **Per\_index** | A utiliser avec size. |
| **Elasticsearch\_max\_time\_**  **Per\_index** | A utiliser avec time. |
| **Elasticsearch\_max\_number\_**  **Of\_indices** |  |
| **Retention\_strategy** | Delete ou close (re-ouvrable plus tard) |
| **Elasticsearch\_disable\_version\_check** | Graylog check sir la version d’ES est compatible :  Laisser à true. |
| **No\_retention** | Désactive la rotation ES. |
| **Elasticsearch\_shards** | Un seul nœud ES : mettre 1. |
| **Autres confs performance…** |  |
|  |  |
| **MONGODB** | |
| **Mongodb\_uri** |  |
| **OPTS** | |
|  |  |
|  |  |
|  |  |
|  |  |
| **Comments :** | |