Mise en place database du mode « historique ».

Il est préférable de tout installer d'abord en mode non-authentifié.
Le but de cette installation est de pouvoir gérer au mieux les alertes, pour cela on dispose de deux modes d'opération :

Mode « running ».

Une gestion courante, les alertes, une fois "expliquées" (et éventuellement corrigées) sont supprimées de la table "alert" de la base "courante" et reportées automagiquement (trigger Mysql) dans la table "alert" d'une autre base.

Mode « history »

Cette autre base ne comporte que la table "alert", les autres "tables" sont remplacées par des vues vers les tables de la base "courante".

Installation du mode historique.

Base de données.

Il suffit de :

- Se connecter en "root".
- Se positionner dans le répertoire «doc/ HISTO ».
- Créer une nouvelle base "ossec_history"

```
mysql –user=root -p
..> CREATE DATABASE ossec_history CHARACTER SET = 'utf8' COLLATE = 'utf8_bin';
..> use ossec_history;
```

- - Donner les droits à l'utilisateur standard ossec sur cette base :

```
..> grant insert,select,update,select on ossec_history.* to 'ossec_user'@'localhost';
..> grant insert,select,update,select on ossec_history.* to
'ossec_user'@'ip_du_serveur_web';
```

- `- Créer une table "alert"`
  `..>` **`source CRE_HISTORY.sql`**

- `- Créer les vues adéquates`
  `..>` **`source CRE_VIEWS_HIS.sql`**

- `- installer le trigger sur la table "alert" de la base "courante".`
  `..>` **`use ossec_base;`**
  `..>` **`source CRE_TRIGGER_DEL_ALERT.sql`**

Logiciel.

Il faut :

- Créer un nouveau répertoire, par exemple « **`OSSEC_GUI-3.0-HIS`** ».
- Se rendre dans ce répertoire et y créer des liens vers le répertoire « principal ».
  `cd OSSEC-GUI-3.0-HIS`
  `ln -s ../OSSEC-GUI-3.0/* ./`
- Modifier le fichier « db_ossec.php » pour y mettre les caractéristiques de la base « historique » :
  `rm db_ossec.php`
  `cp ../OSSEC-GUI-3.0/db_ossec.php ./`
- `Editer le fichier « db_ossec.php pour y mettre les identifiants de pour DB_USER_O, DB_PASSWORD_O, DB_NAME_O sans oublier de passer DB_TYPE_O à la valeur « history ».`

Et c'est tout !

Pour vérifier le bon fonctionnement détruisez une ligne d'alerte dans l'application « running », celle-ci devrait apparaître instantanément dans la table « alert » de la base « ossec_history ».

N'oubliez pas de détruire (ou déplacer hors de l'arborescence WEB) le répertoire « doc » après usage.