Create database for the « history » mode.

The purpose off this installation is to be ablemanage the alerts in a better mode and for that it offers two modes off operation :

« Running » mode.

A current management, the alerts, once "explained" (and possibly corrected) are removed from the "alert" table of the "current" database and automagically reported (Mysql trigger) in the "alert" table of another database.

« History » mode.

This other database contains only the "alert" table, the other "tables" are replaced by views to the tables of the "running" database.

Installing the history mode.

Database.

- Log in as "root" (or another "DBA" user).

```
cd …./doc/HISTO
```

- Create a new base "ossec_history"

```
create database ossec_history character set = 'utf8' collate = 'utf8_bin';
use ossec_history;
```

- Give the rights to the standard user ossec on this basis:

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

- Create an "alert" table

```
source CRE_HISTORY.sql
```

- Create the appropriate views

```
source CRE_VIEWS_HIS.sql
```

- Install the trigger on the "alert" table of the "current" database.

```
use ossec_base;
source CRE_TRIGGER_DEL_ALERT.sql
```

Software.

- Create a new directory in /var/www/html, for example « **OSSEC_GUI-3.0-HIS** ».
- Go into that new directory and make links to the “main” directory.

  ```
  cd OSSEC-GUI-3.0-HIS
  ln -s ../OSSEC-GUI-3.0/* ./
  ```

- Remove the db_”ossec.php” file

  ```
  rm db_ossec.php
  cp ../OSSEC-GUI-3.0/db_ossec.php ./
  ```

- Edit the file « db_ossec.php and put the “good” values DB_USER_O, DB_PASSWORD_O, DB_NAME_O, do not forget to set DB_TYPE_O to « history ».
- Il you are using authentication you can do the same operation for the “db_auth.php” file if the credentials and database are different.

And that's all !