

Create database for the « history » mode.

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

« Running » mode.

A current management, the alerts, once "explained" (and possibly corrected) are removed from the "alert" table of the "current" database and automatically 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).
- 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
```

And that's all !