Installer le logiciel.

Extraire l'archive dans un endroit adéquat, `/var/www/OSSEC-WUI` ou `/var/www/html/OSSEC-WUI` sont de bons endroits !
Votre serveur web doit être muni de PHP 7, les versions précédentes fonctionnaient avec PHP 5 mais je ne peux plus faire de test avec PHP 5 qui est réputé "en fin de vie".
Les extensions PHP suivantes sont obligatoires:
php7 curl
php7 json
pho7 mbstring
php7 mysql
php7 xml
L'installation devrait fonctionner avec Postgresql mais je ne l'ai pas testé.
Dans un premier temps on installe le logiciel sans authentification.

Connexion avec la base de données.
La connection de la base de données est définie dans le fichier "db_ossec.php":

```
...
if ( ! defined('DB_USER_O') )
     {    define ('DB_USER_O', 'User name');
          define ('DB_PASSWORD_O', 'Password');
          define ('DB_HOST_O', 'IP Address');
          define ('DB_NAME_O', 'Database name');
          define ('DB_TYPE_O', 'running');
#         define ('DB_TYPE_O', 'history');
     }
....
```

La constante "DB_TYPE_O" est utilisée pour définir le "type" de l'installation:
"running" pour la base de données alimentée directement par Ossec.
"history" pour la base de données "history".

L'utilisation standard est le mode "running" avec une seule base de données.
Adaptation des paramètres fonctionnels.
Certains paramètres sont stockés dans le fichier "config.php".
Vous pouvez ajuster certaines fonctions, par exemple:
- $google_api_key = string
Utilisé pour accéder aux cartes (pour l'inspection IP), en obtenir un nouveau car c'est le mien!
- $glb_indexgraphlogarithmic = "true"
Vous pouvez utiliser "false", mais "true" donne souvent une meilleure visibilité ...
- $glb_autorefresh = integer (seconds)
Self explanatory.

Quelques valeurs "par défaut" utilisées pour la première utilisation de "index.php" par exemple
- $glb_level = 1 .. 15
Niveau par défaut au démarrage :
- $glb_hours = 1..144
Nombre d'heures affichées :
- $glb-graphbreakdown = (source|path|level|rule_id)
Mode utilisé pour le graphe "index.php"

Certaines valeurs à utiliser pour définir la hauteur de certains graphiques, il peut être utile pour les écrans plutôt petits:
- $glb_height_index = 380;
Pour le graphe de "index.php".
- $glb_height_detail = 300;
Pour le graphe « detail ».
- $glb_height_stat_rules = 500;
Pour les statistiques par règle.
- $glb_height_stat_level = 500;
Pour les statistiques par niveau.
- $glb_height_mass_left = 600;
  $glb_height_mass_right_high = 300;

$glb_height_mass_right_low = 300;
Pour ajustement de la taille des trois graphes de massmonitoring.

Regardez dans ce fichier pour voir d'autres paramètres.

Deux modes de fonctionnement sont disponibles.
Le mode standard s'appelle "running" et utilise directement la base de données ossec.
Vous pouvez diviser les données entre deux bases de données:
- le "running" alimenté par Ossec.
- l'historique est alimenté par toutes les alertes supprimées de la base de données "running".
La méthode est efficace, vous supprimez les alertes de "running" lorsque les alertes sont traitées, mais toutes les alertes supprimées sont insérées dans la base de données "history" pour des besoins statistiques et d'autres raisons.
Ainsi, la partie "running" est plutôt petite et il est donc rapide d’inspecter les données, mais toutes les informations restent dans l'historique.

Pour la base de données historique, vous devez:
- créer une nouvelle base de données
- donner des droits au propriétaire de la base de données en cours d'exécution pour l'insérer dans cette nouvelle base.
- créer un nouvel utilisateur avec insertion / suppression / sélection / mise à jour sur la nouvelle base (ou utiliser l'utilisateur standard avec suffisamment de droits sur la nouvelle base de données.Le nouvel utilisateur doit, au moins, avoir le droit de sélectionner dans la base de données en cours.
- créer une table "alerte" dans la nouvelle base
- créer des vues de base donnant accès aux autres tables de l'utilisateur en cours d'exécution.
Exemple: créer une catégorie de vue en sélectionnant * from running.category;
- ajouter un déclencheur sur le "running" du récit en cours pour insérer les lignes supprimées dans la table d'alerte de l'historique.
Les modèles de toutes les actions sont fournis dans le répertoire SQL.

Pour le logiciel, vous devez créer un nouveau répertoire près de / var / www / OSSEC-WUI, par exemple / var / www / OSSEC-WUI-HIS ... et créer des liens.
cd OSSEC-WUI-HIS
ln -s ../OSSEC-WUI/* ./
rm db_ossec.php
rm config.php
cp ../OSSEC-WUI/db_ossec.php ./
cp ../OSSEC-WUI/config.php./
Vous pouvez donc accéder à la base de données historique avec le mode "historique".

```
if ( ! defined('DB_USER_O') )
     {    define ('DB_USER_O', 'User name');
          define ('DB_PASSWORD_O', 'Password');
          define ('DB_HOST_O', 'IP Address');
          define ('DB_NAME_O', 'History Database name');
#         define ('DB_TYPE_O', 'running');
          define ('DB_TYPE_O', 'history');
     }
```

Ppour finir ajustez certains paramètres dans le fichier config.php selon vos besoins.

Par défaut le mode authentifié n'est pas activé.

Pour l'activer il suffit de « linker » amilogged.php_auth to amilogged.php et de consulter documentation « AUTH_INIT ».

Et c'est tout.