Syslog : Installer un serveur de trace

Le serveur de centralisation des fichiers de traces choisi est le serveur rsyslog basé sur le protocole syslog.

Autres ressources

- https://homputersecurity.com/2018/03/01/comment-mettre-en-place-un-serveur-syslog/

Pré-requis

Votre serveur Debian **REZOLAB** doit disposer d'un serveur **Apache** de **PHP5** et de **Mysql**.

Installation et configuration du serveur de traces

Installer rsyslog sur le serveur de trace

```
apt-get install rsyslog rsyslog-mysql
```

La configuration du paquet rsyslog-mysql va vous proposer de créer une base de données Mysql pour le serveur syslog. Acceptez, donnez le nom de la base et les utilisateurs de connexion à cette base de données (pour vous ici root, btssio).

Configuration du serveur rsylog en écoute sur le réseau Mettre en écoute sur le réseau le serveur rsyslog en dé-commentant les deux lignes suivantes dans son fichier de configuration “/etc/rsyslog.conf”

```
# provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
```

Relancez le serveur **rsyslog** par la commande “**service rsyslog retstart**”.

Vérifiez la mise en écoute sur le réseau par la commande **netstat -nl** et l'ouverture du **port 514**.

Installer et configurer le client syslog sur le serveur OpenERP

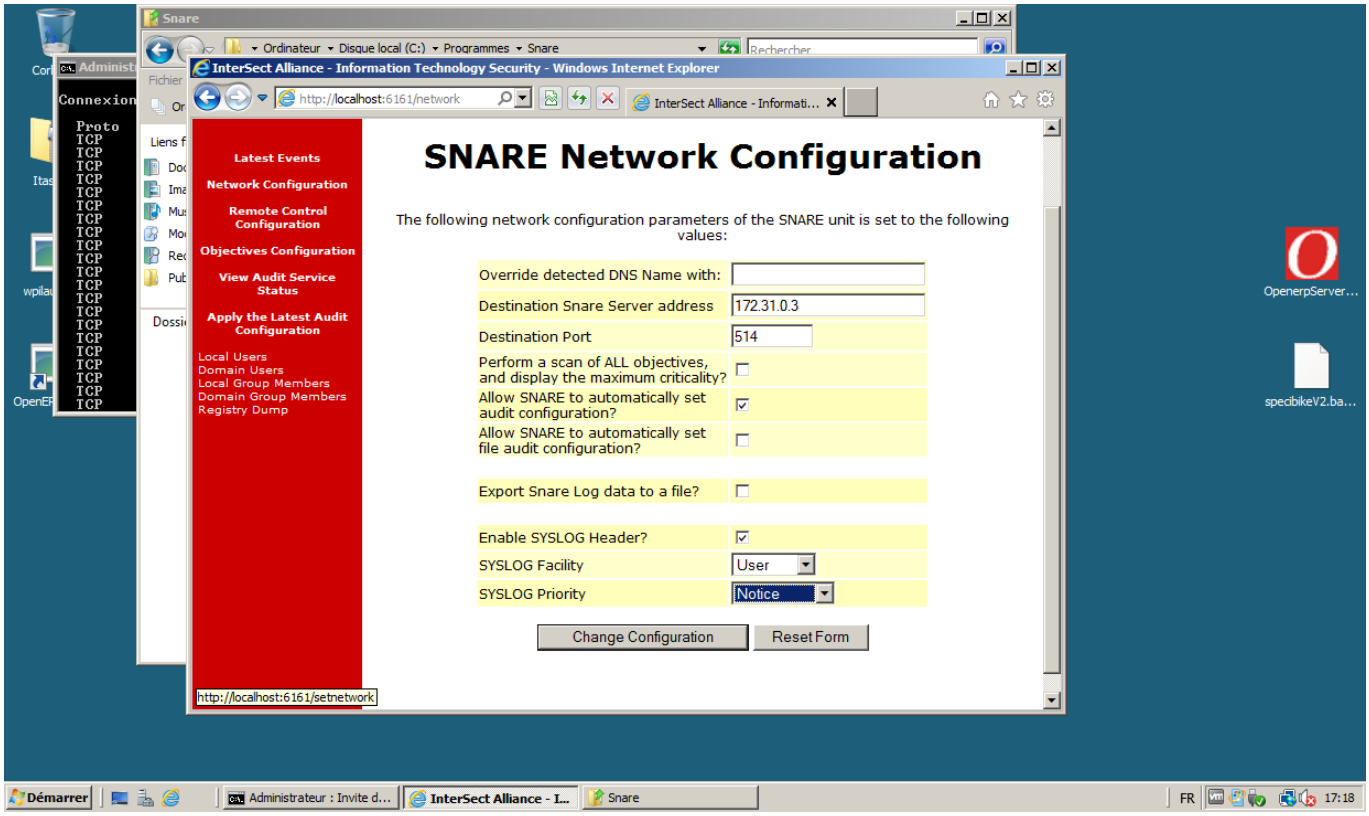
Malheureusement, Windows par lui-même ne peut pas envoyer les logs générés par l'observateur d'événements vers un serveur syslog. Un outil est requis pour cette fonction, c'est le logiciel **Snare**.

Snare développé par Alliance Interselect, est reconnu comme étant l'un des meilleurs outils gratuits pour cette fonction. C'est un logiciel open source disponible sous les termes de la licence GPL.

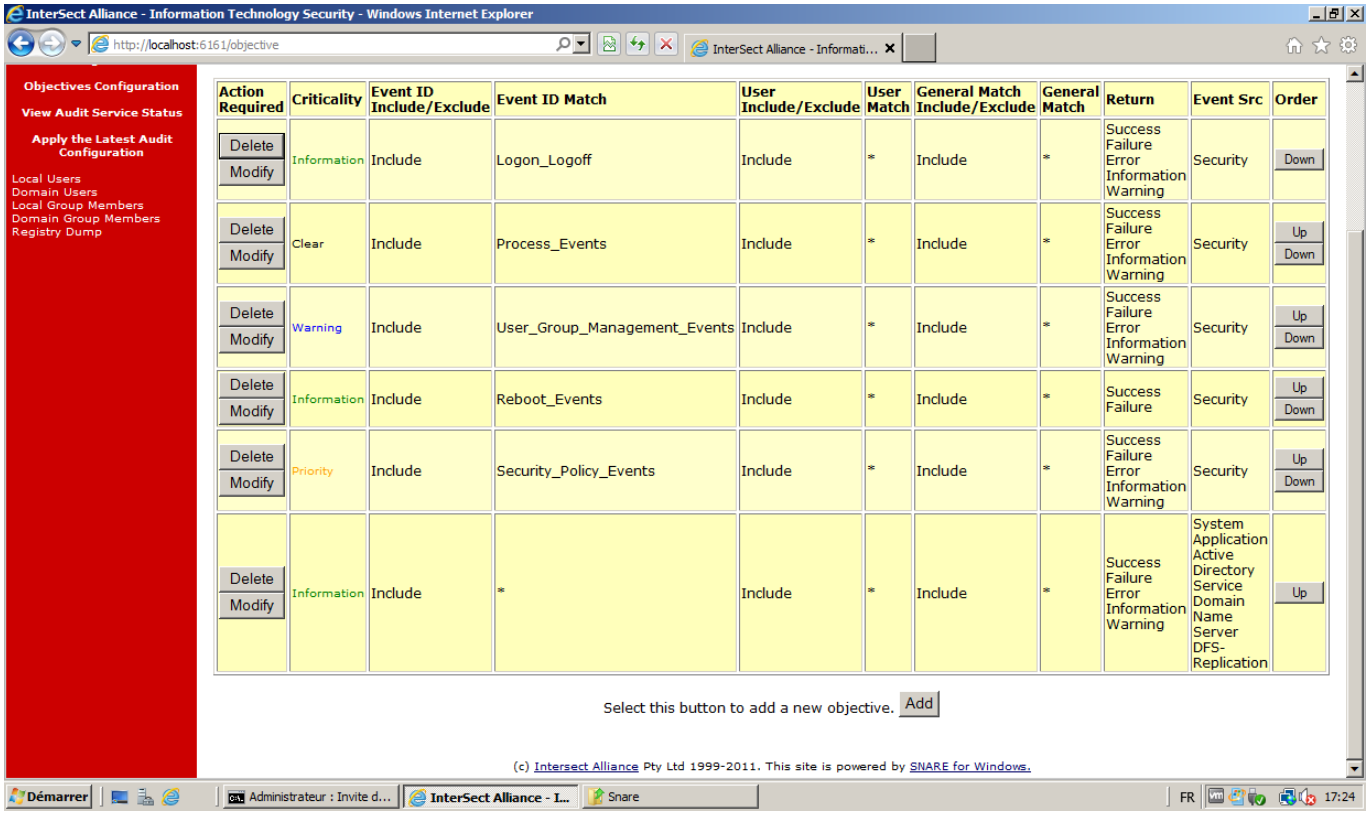
L'**agent Snare** peut être téléchargé sur le site web d'Interselect Alliance.
http://www.intersectalliance.com/projects/SnareWindows/index.html

Installez l'outil en cliquant simplement sur l'exécutable Snare. Pour vous connecter à l'interface Web, utilisez le user **snare** et le mot de passe saisi au cours de l'installation.

Commencez par paramétrer l'**adresse du serveur rsyslog** (à adapter à votre serveur) et le port est (514) dans le menu **Network Configuration**.



Ensuite, paramétrez le **type de logs** qui sera envoyé vers le serveur. Par défaut, il y a déjà quelques règles préconfigurées. Conserver-les.



Sur le serveur rsyslog, vérifiez que les messages en provenance de votre OS Windows sont bien enregistrés dans le fichier **/var/log/syslog**.

Comment faire cette vérification ?

Configurez **vos serveurs** pour qu'ils remontent leur messages **syslog** vers votre serveur centralisé.

Installation et configuration du site web de consultation des fichiers de traces

Installez le site web de consultation centralisée des fichiers de trace

Téléchargez le package “**php-syslog-ng**” à l'adresse : http://www.webprk.net/var/files/php-syslog-ng-2.9.1r10_webprk.tar.gz

Décompressez l'archive et copiez le contenu du répertoire **html** dans le répertoire **/var/www**. Changez l'utilisateur et le groupe propriétaires du contenu du répertoire /var/www en “**www-data**” en utilisant la commande **chown**.

Quelle est la syntaxe de cette commande ?

Redirigez les messages du fichier de trace vers une base de données Mysql

Ouvrez le fichier **/etc/rsyslog.d/mysql.conf** dans un éditeur pour obtenir ceci :

```
### Configuration file for rsyslog-mysql
### Changes are preserved

$ModLoad ommysql
$template syslogNg," insert into logs(host,facility,priority,level,tag,datetime,program,msg) VALUES
('%HOSTNAME%', '%syslogfacility-text%', '%syslogpriority-text%', '%syslogseverity-text%', '%syslogtag%',
'%timereported:::date-mysql%', '%programname%', '%msg%')",SQL
*.* >localhost,syslog,root,root;syslogNg
```

Le template explique comment rediriger les messages du fichier de trace **syslog** dans la base de données **mysql** créée au moment de l'installation du paquet **rsyslog-mysql**.

La dernière ligne indique où se situe le serveur Mysql (localhost), comment s'appelle la base de données à peupler (syslog), comment s'y connecter (root, root).

Redémarrez le serveur rsyslog et vérifiez en faisant une requête SQL sur la base “syslog”, table “logs” que votre table est bien peuplée des messages du fichier syslog de trace.

Quelle est la requête permettant de faire cette vérification ?

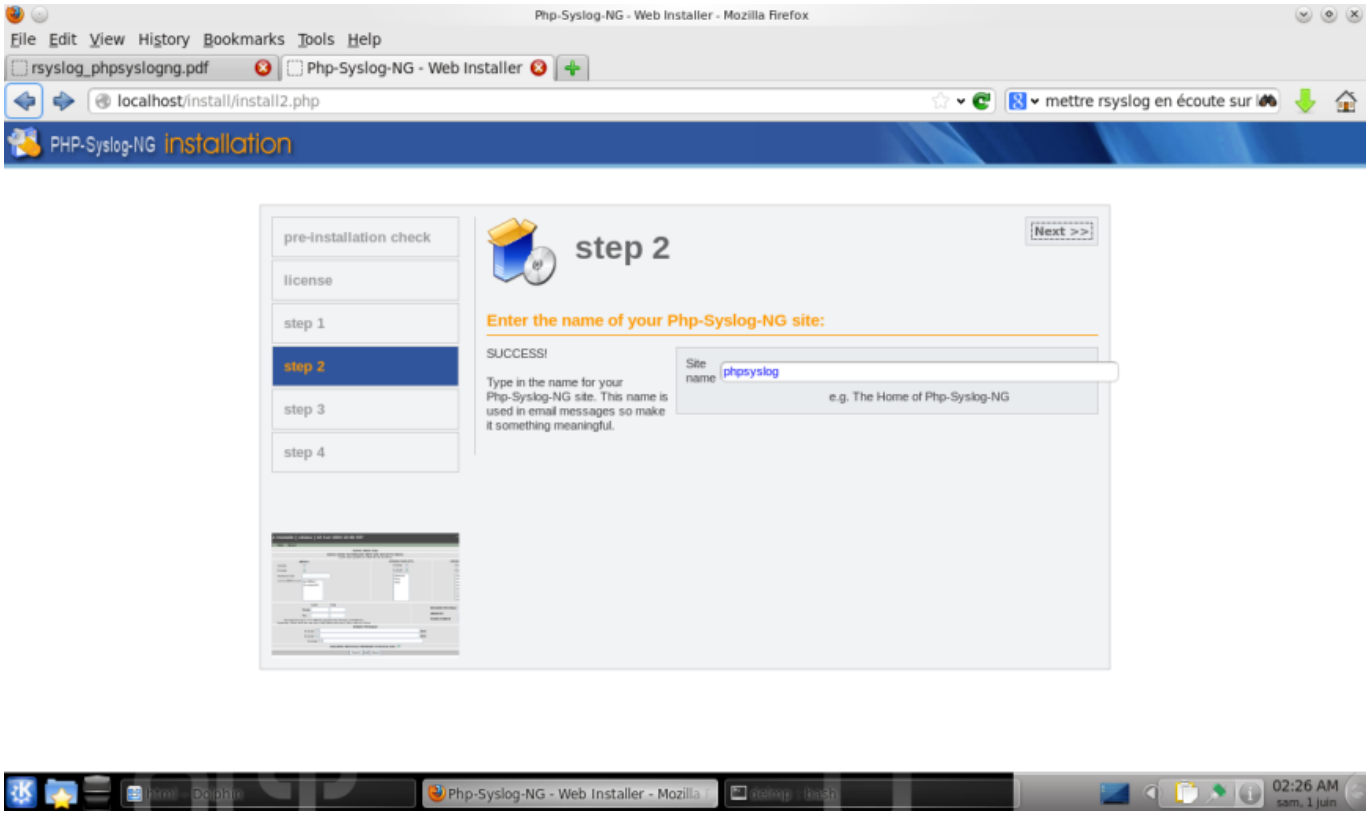
Quel est l'intérêt de basculer les fichiers de trace dans un serveur Mysql ?

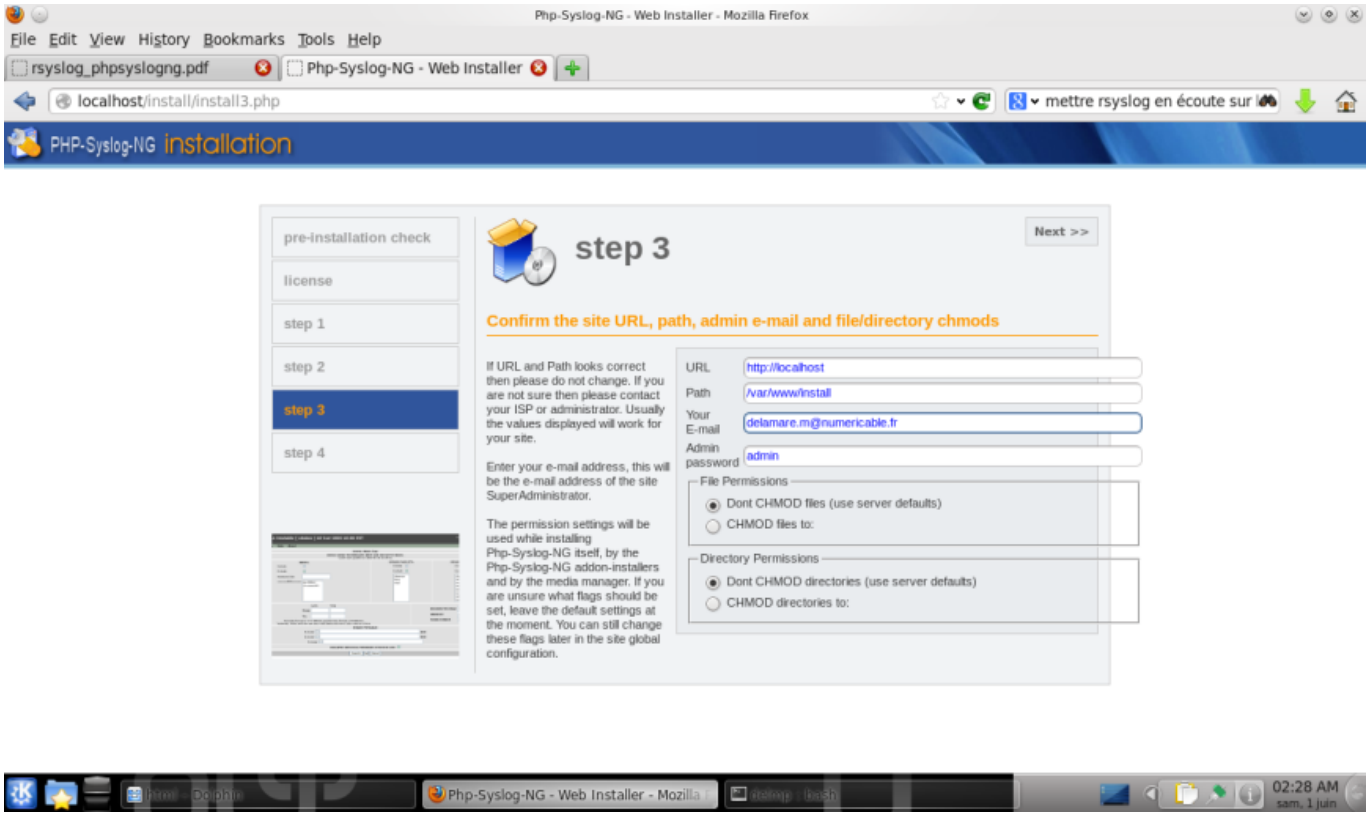
Configurez le site web

Dans un navigateur, tapez l'URL **localhost/install**. Vérifiez que les pré-requis sont corrects.

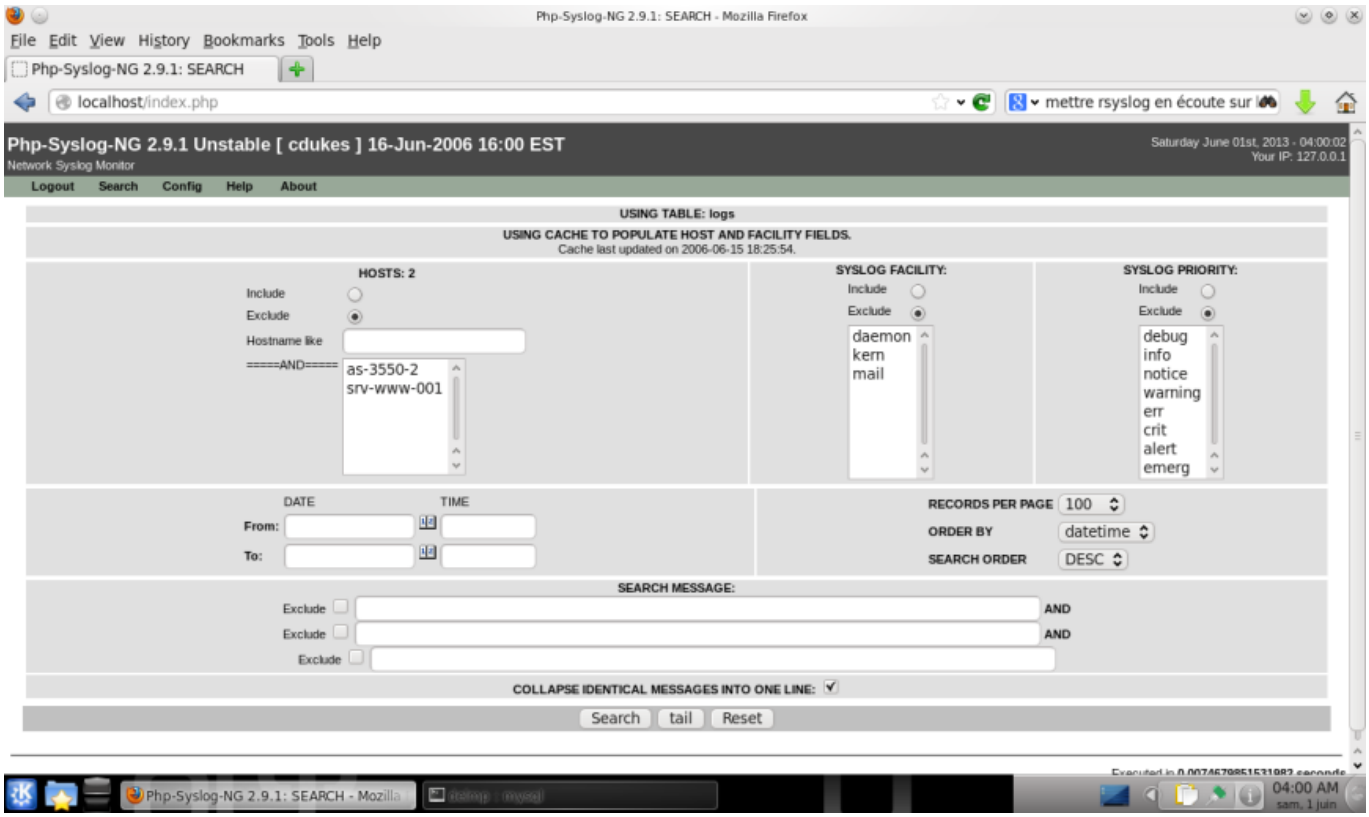
Puis configurez votre site :

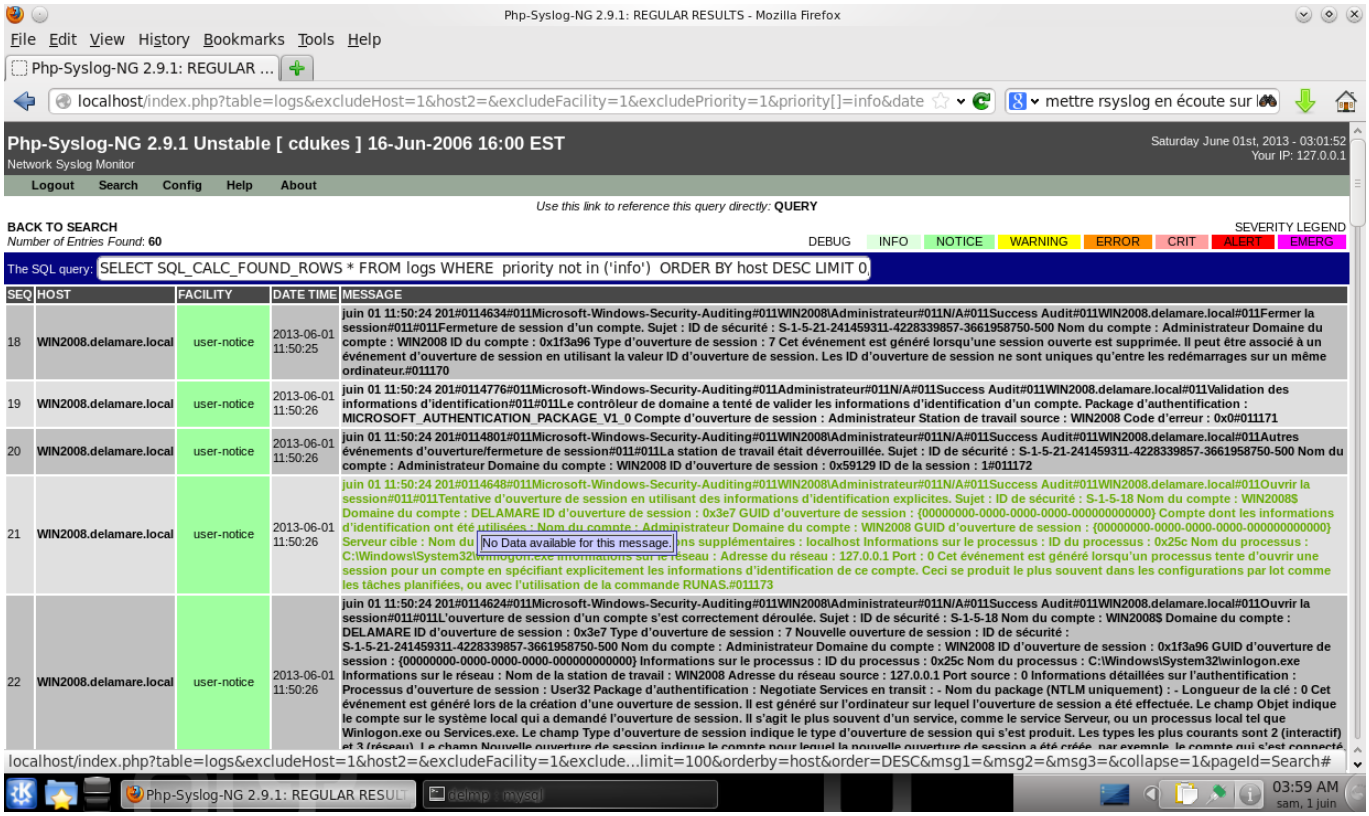

Php-Syslog-NG - Web Installer - Mozilla Firefox
File Edit View History Bookmarks Tools Help
rsyslog_phpsyslogng.pdf
Php-Syslog-NG - Web Installer
localhost/install/install1.php
mettre rsyslog en écoute sur
PHP-Syslog-NG installation
pre-installation check
license
step 1
step 2
step 3
step 4
step 1
Next >>
MySQL database configuration:
Setting up Php-Syslog-NG to run on your server involves 4 simple steps...
Please enter the hostname of the server Php-Syslog-NG is to be installed on.
Enter the MySQL username, password and database name you wish to use with Php-Syslog-NG.
Enter the table name prefix (if any) to be used by this Php-Syslog-NG instance and select what to do in case there are existing tables from former installations.
Host Name
localhost
This is usually 'localhost'
MySQL User Name
root
Enter a valid username such as 'root' or a username given by your server administrator.
MySQL Password
For site security using a password for the mysql account is mandatory
Verify MySQL Password
Retype password for verification
MySQL Database Name
syslog
Some hosts only allow a certain DB name per site. If this is the case, set that name here and use the Prefix option below.
MySQL Port
3306
Specify the port which MySQL is running on (Default is 3306)
MySQL Table Prefix
Do NOT use 'old_' since this is used for backup tables
Syslog User Name
sysloguser
This user is used to access the SQL (read) data on the backend, there's probably no need to change it from the default (sysloguser)
Syslog User Password
For site security using a password for the mysql account is mandatory
Php-Syslog-NG - Web Installer - Mozilla
02:24 AM
sam. 1 juin


Php-Syslog-NG - Web Installer - Mozilla Firefox
File Edit View History Bookmarks Tools Help
rsyslog_phpsyslogng.pdf
Php-Syslog-NG - Web Installer
localhost/install/install2.php
mettre rsyslog en écoute sur
PHP-Syslog-NG installation
pre-installation check
license
step 1
step 2
step 3
step 4
step 2
Next >>
Enter the name of your Php-Syslog-NG site:
SUCCESS!
Type in the name for your Php-Syslog-NG site. This name is used in email messages so make it something meaningful.
Site name
phpsyslog
e.g. The Home of Php-Syslog-NG
Php-Syslog-NG - Web Installer - Mozilla
02:26 AM
sam. 1 juin



Utiliser le service Web





From:
/ - **Les cours du BTS SIO**

Permanent link:
/doku.php/sisr3/syslog_05

Last update: **2018/12/17 11:37**