

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 rsyslog 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 restart**".

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**.

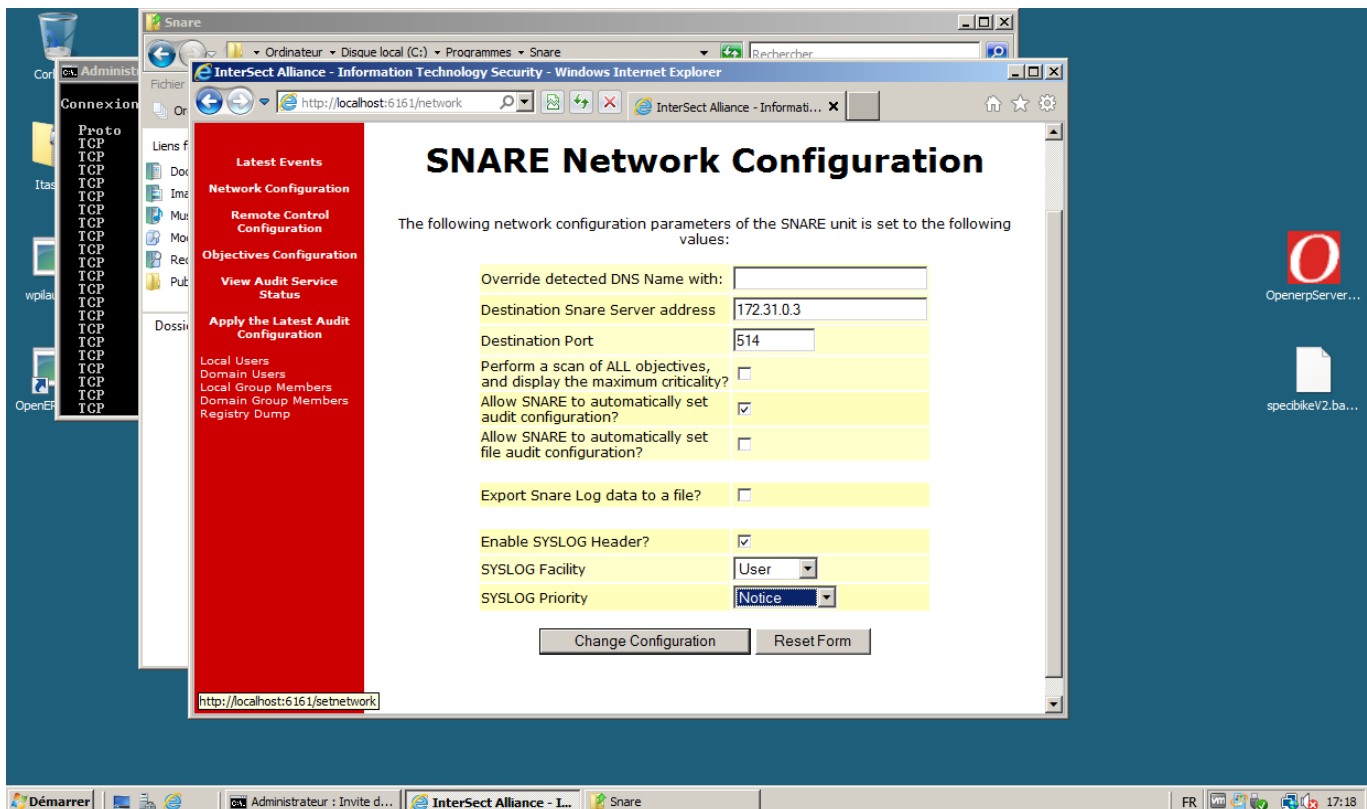
Snare développé par Alliance Interselect, est reconnu comme étant l'un des meilleurs outils gratuits pour cette fonction. C'est un logiciel open source disponible sous les termes de la licence GPL.

L'**agent Snare** peut être téléchargé sur le site web d'Interselect Alliance.

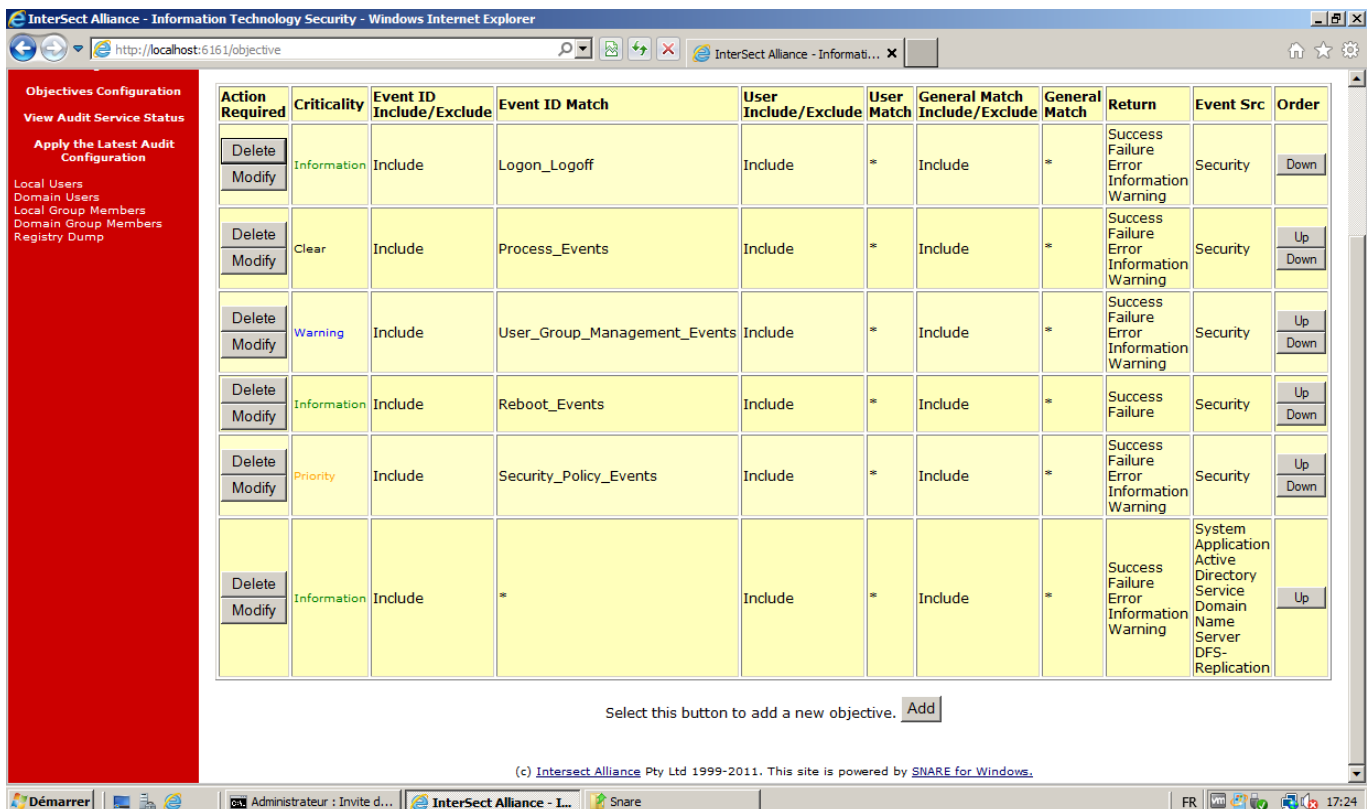
<http://www.interselectalliance.com/projects/SnareWindows/index.html>

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 ?

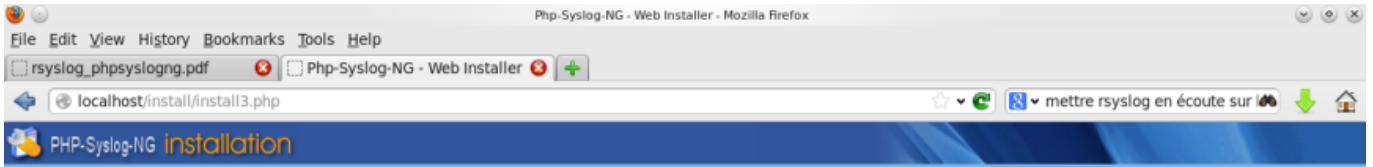
Configurez le site web

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

Puis configurez votre site :

The screenshot shows the 'step 1' configuration screen for MySQL database setup. On the left, a sidebar lists 'pre-Installation check', 'license', 'step 1' (highlighted), 'step 2', 'step 3', and 'step 4'. The main content area is titled 'step 1 MySQL database configuration:'. It includes instructions: '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.', and '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.' The form fields are: Host Name (localhost), MySQL User Name (root), MySQL Password (masked with dots), Verify MySQL Password (masked with dots), MySQL Database Name (syslog), MySQL Port (3306), MySQL Table Prefix (empty), Syslog User Name (sysloguser), and Syslog User Password (masked with dots). A 'Next >>' button is in the top right.

The screenshot shows the 'step 2' configuration screen. The sidebar highlights 'step 2'. The main content area is titled 'step 2 Enter the name of your Php-Syslog-NG site:'. It includes instructions: 'Type in the name for your Php-Syslog-NG site. This name is used in email messages so make it something meaningful.' and a 'SUCCESS!' message. The form field 'Site name' contains 'phpsyslog' and has a tooltip that says 'e.g. The Home of Php-Syslog-NG'. A 'Next >>' button is in the top right.



pre-installation check

license

step 1

step 2

step 3

step 4

step 3

Confirm the site URL, path, admin e-mail and file/directory chmods

If URL and Path looks correct then please do not change. If you are not sure then please contact your ISP or administrator. Usually the values displayed will work for your site.

Enter your e-mail address, this will be the e-mail address of the site SuperAdministrator.

The permission settings will be used while installing Php-Syslog-NG itself, by the Php-Syslog-NG add-on-installers and by the media manager. If you are unsure what flags should be set, leave the default settings at the moment. You can still change these flags later in the site global configuration.

URL:

Path:

Your E-mail:

Admin password:

File Permissions

Dont CHMOD files (use server defaults)

CHMOD files to:

Directory Permissions

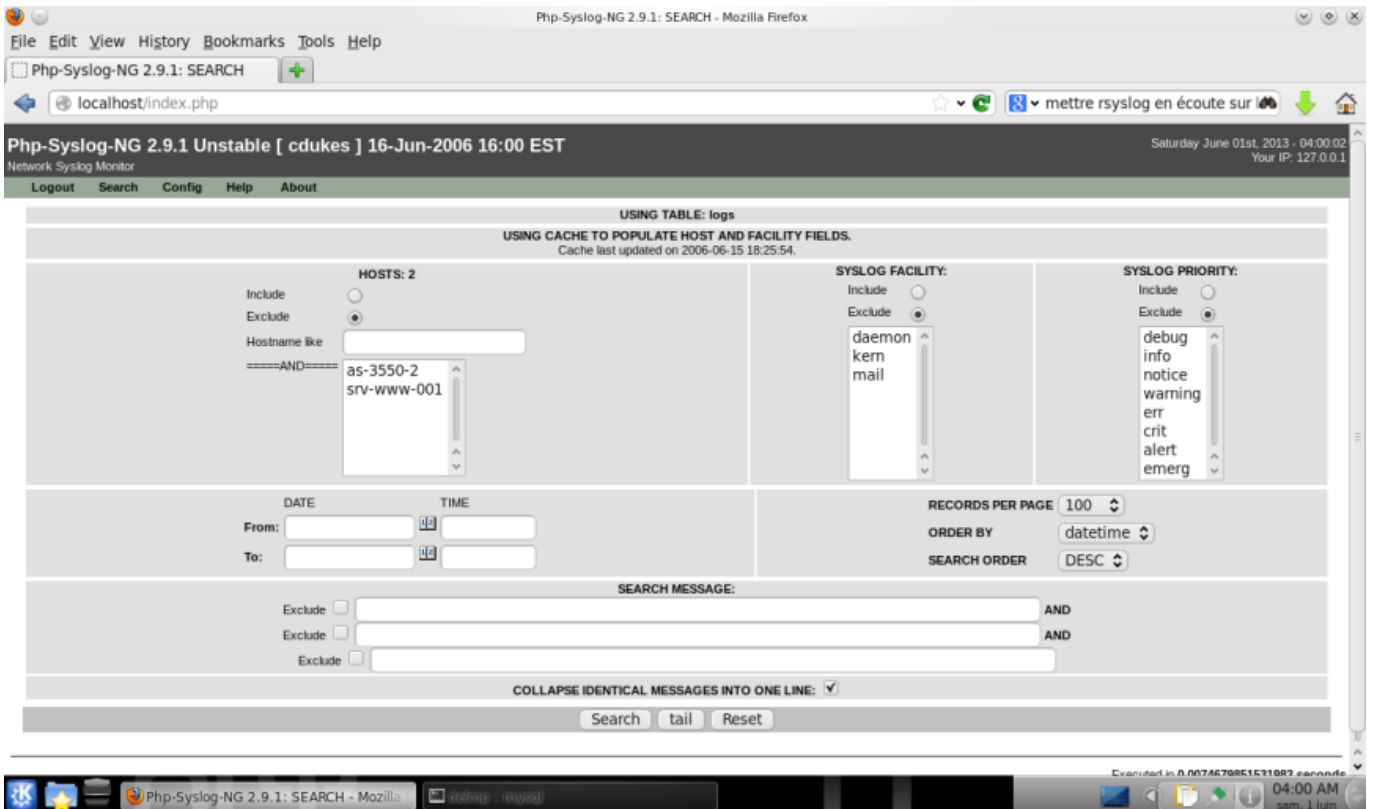
Dont CHMOD directories (use server defaults)

CHMOD directories to:

Next >>



Utiliser le service Web



Php-Syslog-NG 2.9.1: REGULAR RESULTS - Mozilla Firefox

File Edit View History Bookmarks Tools Help

localhost/index.php?table=logs&excludeHost=1&host2=&excludeFacility=1&excludePriority=1&priority[]=info&date

Php-Syslog-NG 2.9.1 Unstable [cdukes] 16-Jun-2006 16:00 EST Saturday June 01st, 2013 - 03:01:52 Your IP: 127.0.0.1

Logout Search Config Help About

Use this link to reference this query directly: QUERY

BACK TO SEARCH Number of Entries Found: 60

DEBUG INFO NOTICE WARNING ERROR CRIT ALERT EMERG SEVERITY LEGEND

The SQL query: SELECT SQL_CALC_FOUND_ROWS * FROM logs WHERE priority not in ('info') ORDER BY host DESC LIMIT 0

| SEQ | HOST | FACILITY | DATE TIME | MESSAGE |
|-----|------------------------|-------------|---------------------|--|
| 18 | WIN2008.delamare.local | user-notice | 2013-06-01 11:50:25 | juin 01 11:50:24 201#0114634#011Microsoft-Windows-Security-Auditing#011WIN2008\Administrateur#011N/A#011Success Audit#011WIN2008.delamare.local#011Fermer la session#011#011Fermeture de session d'un compte. Sujet : ID de sécurité : S-1-5-21-241459311-4228339857-3661958750-500 Nom du compte : Administrateur Domaine du compte : WIN2008 ID du compte : 0x1f3a96 Type d'ouverture de session : 7 Cet événement est généré lorsqu'une session ouverte est supprimée. Il peut être associé à un événement d'ouverture de session en utilisant la valeur ID d'ouverture de session. Les ID d'ouverture de session ne sont uniques qu'entre les redémarrages sur un même ordinateur.#011170 |
| 19 | WIN2008.delamare.local | user-notice | 2013-06-01 11:50:26 | juin 01 11:50:24 201#0114776#011Microsoft-Windows-Security-Auditing#011Administrateur#011N/A#011Success Audit#011WIN2008.delamare.local#011Validation des informations d'identification#011#011Le contrôleur de domaine a tenté de valider les informations d'identification d'un compte. Package d'authentification : MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Compte d'ouverture de session : Administrateur Station de travail source : WIN2008 Code d'erreur : 0x0#011171 |
| 20 | WIN2008.delamare.local | user-notice | 2013-06-01 11:50:26 | juin 01 11:50:24 201#0114801#011Microsoft-Windows-Security-Auditing#011WIN2008\Administrateur#011N/A#011Success Audit#011WIN2008.delamare.local#011Autres événements d'ouverture/fermeture de session#011#011La station de travail était déverrouillée. Sujet : ID de sécurité : S-1-5-21-241459311-4228339857-3661958750-500 Nom du compte : Administrateur Domaine du compte : WIN2008 ID d'ouverture de session : 0x59129 ID de la session : 1#011172 |
| 21 | WIN2008.delamare.local | user-notice | 2013-06-01 11:50:26 | juin 01 11:50:24 201#0114648#011Microsoft-Windows-Security-Auditing#011WIN2008\Administrateur#011N/A#011Success Audit#011WIN2008.delamare.local#011Ouvrir la session#011#011Tentative d'ouverture de session en utilisant des informations d'identification explicites. Sujet : ID de sécurité : S-1-5-18 Nom du compte : WIN2008S Domaine du compte : DELAMARE ID d'ouverture de session : 0x3e7 GUID d'ouverture de session : {00000000-0000-0000-0000-000000000000} Compte dont les informations d'identification ont été utilisées : Nom du compte : Administrateur Domaine du compte : WIN2008 GUID d'ouverture de session : {00000000-0000-0000-0000-000000000000} Serveur cible : Nom du [No Data available for this message] : Ins supplémentaires : localhost Informations sur le processus : ID du processus : 0x25c Nom du processus : C:\Windows\System32\winlogon.exe Informations sur le réseau : Adresse du réseau : 127.0.0.1 Port : 0 Cet événement est généré lorsqu'un processus tente d'ouvrir une session pour un compte en spécifiant explicitement les informations d'identification de ce compte. Ceci se produit le plus souvent dans les configurations par lot comme les tâches planifiées, ou avec l'utilisation de la commande RUNAS.#011173 |
| 22 | WIN2008.delamare.local | user-notice | 2013-06-01 11:50:26 | juin 01 11:50:24 201#0114624#011Microsoft-Windows-Security-Auditing#011WIN2008\Administrateur#011N/A#011Success Audit#011WIN2008.delamare.local#011Ouvrir la session#011#011L'ouverture de session d'un compte s'est correctement déroulée. Sujet : ID de sécurité : S-1-5-18 Nom du compte : WIN2008S Domaine du compte : DELAMARE ID d'ouverture de session : 0x3e7 Type d'ouverture de session : 7 Nouvelle ouverture de session : ID de sécurité : S-1-5-21-241459311-4228339857-3661958750-500 Nom du compte : Administrateur Domaine du compte : WIN2008 ID d'ouverture de session : 0x1f3a96 GUID d'ouverture de session : {00000000-0000-0000-0000-000000000000} Informations sur le processus : ID du processus : 0x25c Nom du processus : C:\Windows\System32\winlogon.exe Informations sur le réseau : Nom de la station de travail : WIN2008 Adresse du réseau source : 127.0.0.1 Port source : 0 Informations détaillées sur l'authentification : Processus d'ouverture de session : User32 Package d'authentification : Negotiate Services en transit : - Nom du package (NTLM uniquement) : - Longueur de la clé : 0 Cet événement est généré lors de la création d'une ouverture de session. Il est généré sur l'ordinateur sur lequel l'ouverture de session a été effectuée. Le champ Objet indique le compte sur le système local qui a demandé l'ouverture de session. Il s'agit le plus souvent d'un service, comme le service Serveur, ou un processus local tel que Winlogon.exe ou Services.exe. Le champ Type d'ouverture de session indique le type d'ouverture de session qui s'est produit. Les types les plus courants sont 2 (interactif) et 3 (réseau). Le champ Nouvelle ouverture de session indique le compte pour lequel la nouvelle ouverture de session a été créée, par exemple le compte qui s'est connecté |

localhost/index.php?table=logs&excludeHost=1&host2=&excludeFacility=1&exclude...limit=100&orderby=host&order=DESC&msg1=&msg2=&msg3=&collapse=1&pagelid=Search#

From: / - Les cours du BTS SIO

Permanent link: /doku.php/sir3/syslog_05

Last update: 2018/12/17 11:37

