

Stage en entreprise :

Version : 1.0

Horaires : 9h00—12h30 13h30-17h00

Sommaire :

Présentation de l'entreprise : Likinia	2
Likinia propose trois types de services :.....	2
Objectif du projet :	3
WinSyslog :	3
Syslog-NG :	4
Déplacement chez les clients :	4
Procédure d'installation des différents services mis en place :	5
Installation de Syslog-ng :	5
Installation d'un service SMTP (Simple Mail Transfer Protocole) :	6
Installation de Splunk :	9
Export des logs Windows :	10

Stage en entreprise :

Version : 1.0

Horaires : 9h00—12h30 13h30-17h00

Présentation de l'entreprise : Likinia

L'entreprise Likinia a été créée en 1996 et propose ses services en Ile de France et en Normandie. Elle s'adresse en particulier aux TPE (très petite entreprise) et aux PME (petite et moyenne entreprise). L'entreprise a notamment été récompensée par Microsoft comme étant l'entreprise la plus innovante autour des solutions office Pro en 2007.

Le siège de Likinia se situe à Paris néanmoins l'entreprise est aussi implantée à Iles où les solutions informatiques et les dépannages sont pris en charge. L'entreprise est composée de trois employés : deux techniciens et une assistante de direction.

Likinia propose trois types de services :

Infrastructures d'exploitations :

- Ingénierie système.
- Virtualisation des serveurs.
- Sécurité et disponibilité.

Solutions collaboratives :

- Portail d'entreprise.
- Gestion de documents.
- Processus métier : gérer dans le temps un ensemble d'activités corrélées et interactives (flux de travail, intégration avancée avec Microsoft Office...).

Solution de communications :

- Messagerie d'entreprise.
- Communications unifiées.
- Partage d'écran.
- Audio & vidéoconférence.

Elle propose également une intervention ponctuelle dans chaque entreprise, de la téléassistance logicielle, une assistance logicielle sur site, un support administration ainsi que des conseils et des tickets d'interventions. Les tickets d'interventions Likinia permettent aux entreprises de faire des économies sur les coûts des prestations, tout en bénéficiant d'un véritable service professionnel.

Stage en entreprise :

Version : 1.0

Horaires : 9h00—12h30 13h30-17h00

Objectif du projet :

S'informer et proposer une solution afin de mettre en place un service de stockage et de journalisation d'événements.

Recherche effectué pour la présentation de mes solutions à mon maître de stage :

Définition : Syslog est un protocole définissant un service de journaux d'événements d'un système informatique. C'est aussi le nom du format qui permet ces échanges.

Présentation : Syslog se compose d'une partie [cliente](#) et d'une partie [serveur](#). La partie cliente émet les informations sur le réseau, via le [port UDP](#) 514. Les serveurs collectent l'information et se chargent de créer les journaux.

L'intérêt de Syslog est donc de centraliser les journaux d'événements, permettant de repérer plus rapidement et efficacement les défaillances d'ordinateurs présents sur un réseau.

Il existe aussi un logiciel appelé *Syslog*, qui est responsable de la prise en charge des fichiers de journalisation du système. Ceci inclut aussi le démon klogd, responsable des messages émis par le noyau Linux.

WinSyslog : Comporte une version d'essai gratuit, un format professionnel d'environ 210€ et un format entreprise d'environ 759 €.

Ce logiciel fonctionne sous Windows et supporté par les serveurs suivants :

- Windows 2012 (R2)
- Windows 8
- Windows 7
- Windows 2008 (R2)
- Windows Vista
- Windows 2003 (R2)
- Windows XP
- Windows 2000

Fonctionnalité de WinSyslog :

- Recevoir les messages de la part d'un antivirus et/ou de la part de routeurs.
- Résolution des problèmes réseaux.
- conformer aux lois et politiques de l'entreprise en stockant les messages du journal dans des fichiers ou bases de données.
- Être alerté quand les conditions sont critiques.
- créer un référentiel central journal dans un environnement hétérogène.
- Fonctionne 24 heures sur 24 et 7 jours sur 7.

Stage en entreprise :

Version : 1.0

Horaires : 9h00—12h30 13h30-17h00

Lien externe : <http://winsyslog.com/en/>

Syslog-NG : Logiciel Open Source fonctionne sous Debian, Mac OS, Ubuntu...

Côté serveur : L'application syslog-ng est un serveur syslog hautes performances proposant des services de traitement des journaux sophistiqués et un accès de base de données direct.

- Fonction flexible de filtrage et de tri des messages.
- Analyse et réécriture des messages.
- Classification des messages.
- Gestion de charges extrêmes.
- Accès direct à la base de données.
- Prise en charge des protocoles IPv4 et IPv6.

Côté client :

L'application syslog-ng a pour tâche principale d'assurer un transfert des journaux à la fois sécurisé et fiable.

- Journalisation sécurisée avec (SSL/TLS)*
- Transfert fiable des messages
- Prise en charge des protocoles syslog standard
- Collecte des messages locaux

*Le SSL (Secure Socket Layer) / TLS (Transport Layer Security) est le protocole de sécurité le plus répandu qui crée un canal sécurisé entre deux machines communiquant sur Internet ou un réseau interne. Dans notre société centrée sur un Internet vulnérable, le SSL est généralement utilisé lorsqu'un navigateur doit se connecter de manière sécurisée à un serveur web.

Tuto Ubuntu : <http://www.lolokai.com/blog/2012/04/25/installation-dun-serveur-syslog-sous-ubuntu-11-10/>

Déplacement chez les clients :

L'entreprise Likinia a 7 entreprises clientes. Je suis allé chez Activ Dynamique afin d'installer une imprimante Oki le mardi 24 Mai. J'ai également été à la Cop le jeudi 26 Mai afin de régler un problème sur un switch Cisco. Enfin le mercredi 1^{er} juin je suis allé dans l'entreprise Dumas Auvray pour installer une imprimante et chez Ofosec pour un problème de bruit dans la salle serveur. Tous mes déplacements ont eu pour but d'observer ainsi que de comprendre l'implantation

Stage en entreprise :

Version : 1.0

Horaires : 9h00—12h30 13h30-17h00

Procédure d'installation des différents services mis en place :

Installation de Syslog-ng :

Date du début des recherches jusqu'à la mise en place complète du service : 23/05/16 au 27/05/16

```
dubois@dubois-VirtualBox:~$ sudo apt-get install syslog-ng
```

Il faut se rendre dans le fichier syslog-ng afin de configurer le serveur :

```
dubois@dubois-VirtualBox:~$ sudo nano /etc/default/syslog-ng
```

```
# If a variable is not set here, then the corresponding
# parameter will not be changed.
# If a variables is set, then every invocation of
# syslog-ng's init script will set them using dmesg.

# log level of messages which should go to console
# see syslog(3) for details
#
CONSOLE_LOG_LEVEL=1

# Command line options to syslog-ng
#SYSLOGNG_OPTS="--no-caps"
```

Pour activer le serveur il faut enlever le « # » devant CONSOLE_LOG_LEVEL=1

Il n'y a plus qu'à relancer le service.

```
sudo service syslog-ng restart
```

Afin d'améliorer l'utilisation de ses données pour l'utilisateur j'ai choisie de mettre en place une interface web s'appelant LogAnalyser.

Pour l'installer il suffit de faire :

```
root@OCS:/home/likinia# apt-get install loganalyser
```

Il ne reste plus qu'à se connecter sur un navigateur web comme suit et de suivre l'installateur :

<http://Adresse.IP.du.serveur/LogAnalyser>

Cette solution comportant quelques contraintes et également des problèmes d'archives des événements, nous avons décidé de ne pas la garder. Nous pouvons également noter que Syslog-ng comporte pratiquement plus de communauté et il est donc difficile de trouver des informations utiles pour régler une panne éventuelle.

Stage en entreprise :

Version : 1.0

Horaires : 9h00—12h30 13h30-17h00

Installation d'un service SMTP (Simple Mail Transfer Protocole) :

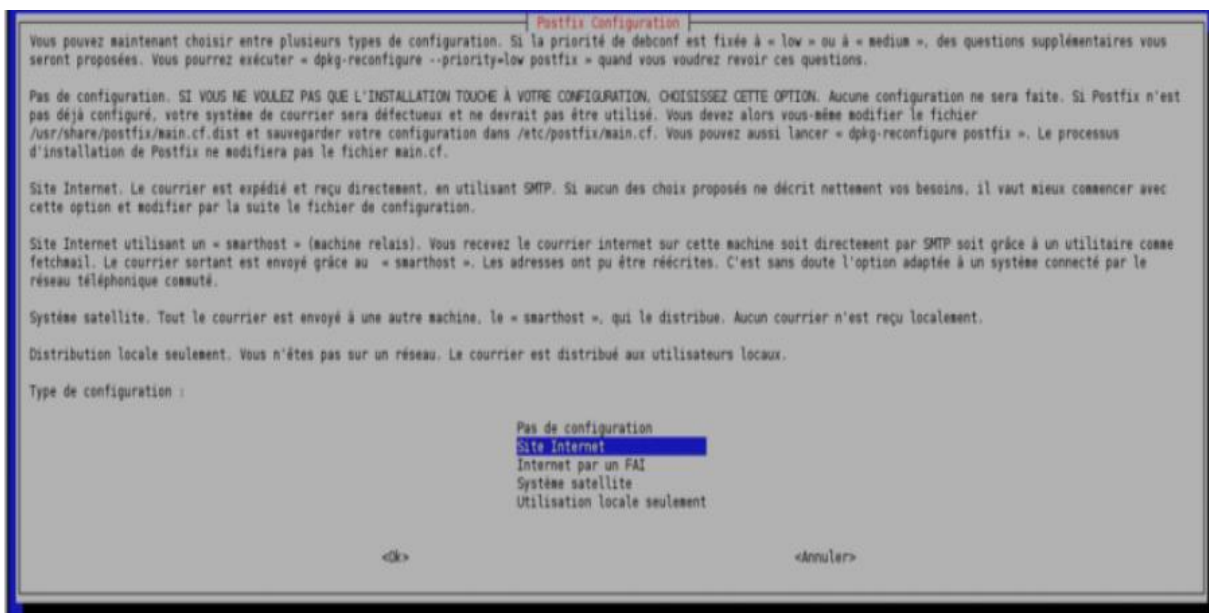
Date du début des recherches jusqu'à la mise en place complète du service : 30/05/16 au 2/06/16

Objectif : Mettre en place un service mail afin de récupérer tous les messages d'alertes provenant d'Arcserv.

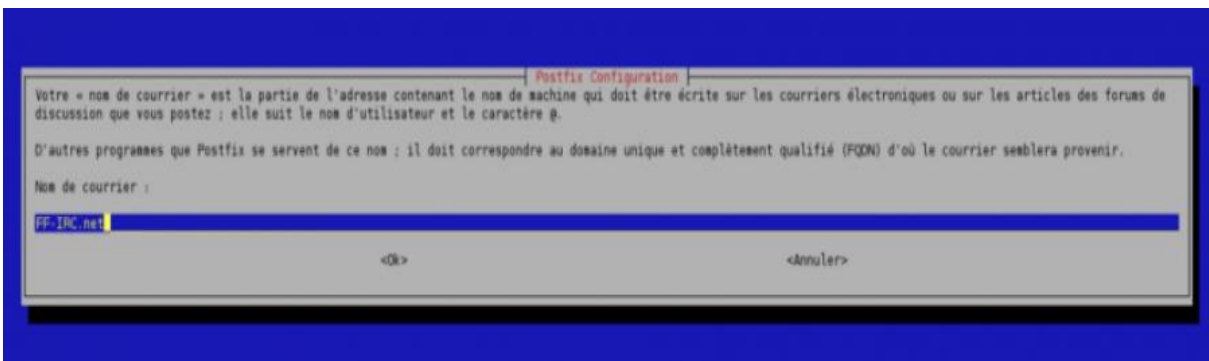
Pour installer Postfix il suffit de taper la commande suivante :

```
root@OCS:/home/likinia# apt-get install postfix postfixadmin
```

Postfixadmin est l'interface web de Postfix.



Choisir le type de configuration souhaité, pour notre cas « Site internet ».



Il faut rentrer le nom de courrier c'est-à-dire le nom de la machine qui va être écrit sur les courriers.

Il faut ensuite configurer les différents paramètres dans le fichier suivant :

Stage en entreprise :

Version : 1.0

Horaires : 9h00—12h30 13h30-17h00

```
root@OCS:/home/likinia# nano /etc/postfix/main.cf
```

```
# See /usr/share/postfix/main.cf.dist for a commented, more complete version
#
#
# Debian specific: Specifying a file name will cause the first
# line of that file to be used as the name. The Debian default
# is /etc/mailname.
#myorigin = /etc/mailname
#
smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
biff = no
#
# appending .domain is the MUA's job.
append_dot_mydomain = no
#
# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h
#
# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${queue_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${queue_directory}/smtp_scache
#
# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.
#
myhostname = mail.FF-IRC.net
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = FF-IRC.net, Nomdemachine.FF-IRC.net, localhost.FF-IRC.net, localhost
relayhost =
mynetworks = 127.0.0.0/8, 192.168.0.0/24
#mailbox_command = procmail -a "$EXTENSION"
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
home_mailbox = Maildir/
```

myhostname : c'est le nom de votre serveur de courriel, configuré dans les entrées MX, par défaut mail.domaine.net

mydestination : ceci est la concordance des domaines, remplacez Nomdemachine par votre nom de machine, et FF-IRC.net par votre domaine

mynetworks : permet de donner l'accès au serveur SMTP, en plus des 2 exemples, rajoutez votre IP extérieure si votre serveur n'est pas sur le même réseau que votre PC

home_mailbox = Maildir/ : Ceci est important ! Nous choisissons le format Maildir en accord avec le serveur IMAP ! Vous ne pourrez pas recevoir vos courriels par IMAP si cette ligne n'est pas ajoutée au fichier de configuration de Postfix !

Stage en entreprise :

Version : 1.0

Horaires : 9h00—12h30 13h30-17h00

Il ne reste plus qu'à accéder à l'interface web afin de créer un compte super admin à l'adresse suivante :

<http://Adresse.IP.du.serveur/postfixadmin/setup.php>

Puis à se connecter sur postfixadmin :

<http://Adresse.IP.du.serveur/postfixadmin>

Ce projet n'a finalement pas été implémenté sur le serveur de l'entreprise car postfix requiert un nom de domaine ou passer par un FAI (Fournisseur d'Accès Internet).

Stage en entreprise :

Version : 1.0

Horaires : 9h00—12h30 13h30-17h00

Installation de Splunk :

Date du début des recherches jusqu'à la mise en place complète du service : 03/06/16 au 08/06/16

Splunk est également un service de journalisation d'événement. Cependant la version d'essai n'est que de 60 jours et est bridé à 500Mo de log par jour.

Il faut télécharger un fichier compressé depuis le site internet de Splunk.

Lien externe : <https://www.splunk.com/>

Pour télécharger un fichier depuis Ubuntu il faut utiliser la commande wget puis le lien du fichier à télécharger.

Il faut maintenant décompresser le fichier comme suit :

```
root@OCS:/home/likinia# tar -xvzf splunk-6.4.1-debde650d26e-linux-2.6-amd64.deb
```

Maintenant il faut lancer l'installation avec la commande :

```
root@OCS:/home/likinia# cd tmp
```

Après l'installation, il ne reste plus qu'à démarrer Splunk :

```
root@OCS:/home/likinia# /opt/splunk/bin/splunk start
```

Désormais l'interface web est disponible :

http://nom_serveur_splunk:8000

Pour finir il faut créer un socket UDP à l'écoute sur le port 514 pour permettre à Splunk de recueillir les logs des serveurs ou machine.

The screenshot shows the Splunk web interface for configuring a new UDP source. The breadcrumb navigation is 'splunk > Manager > Data Inputs > UDP > Add new'. The page title is 'Add new'. Under the 'Source' section, the 'UDP port *' is set to '514'. There is an empty 'Source name override' field with a note: 'If set, overrides the default source value for your UDP entry (host:port)'. Under the 'Source type' section, there is a note: 'Set sourcetype field for all events from this source.' The 'Set sourcetype' dropdown is set to 'From list', and the 'Select source type from list' dropdown is set to 'syslog'. A note below says: 'Select your source type from the list. If you don't see what you're looking for, you can find more source types in the Splunkbase apps browser or online at www.splunkbase.com.' At the bottom, there is a 'More settings' checkbox, a 'Cancel' button, and a 'Save' button.

Stage en entreprise :

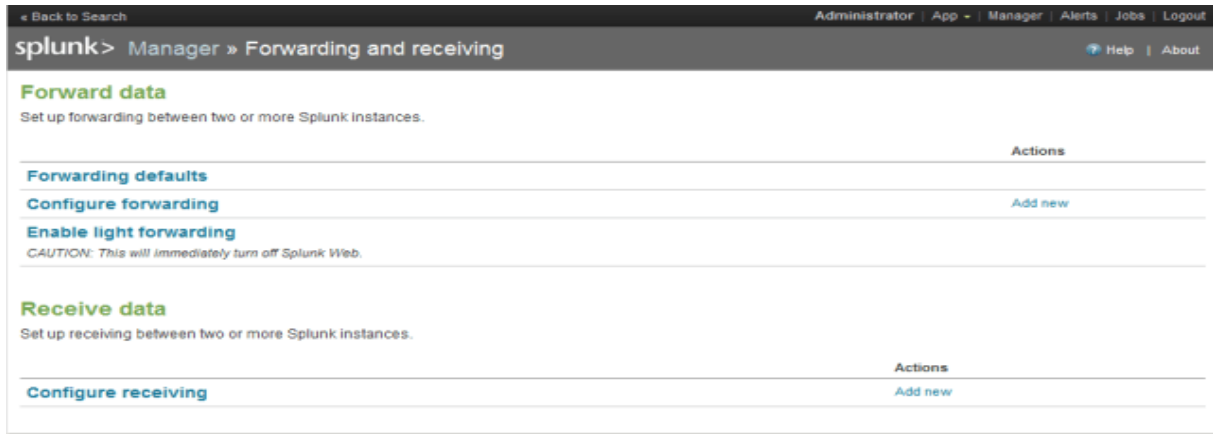
Version : 1.0

Horaires : 9h00—12h30 13h30-17h00

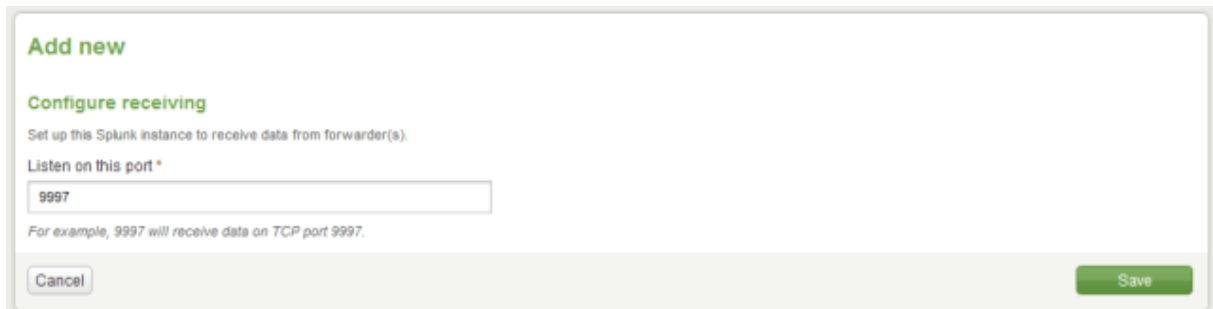
Pour vérifier que Splunk fonctionne bien nous pouvons regarder si il écoute bien sur le port 514 avec la commande : netstat -unlp

Export des logs Windows :

Il faut créer un socket Splunk dédié aux logs Windows



Indiquer le port d'écoute 9997 (TCP) puis sauvegarder :



Installer Splunk Universal Forwarder sur la machine cliente Windows.


Lancer l'installation.

Indiquer le nom du serveur Splunk ainsi que le port 9997 configuré plus haut.

Stage en entreprise :

Version : 1.0

Horaires : 9h00—12h30 13h30-17h00



Universal Forwarder - InstallShield Wizard

Specify Receiving Indexer
Please specify your receiving indexer

This step can be skipped if this information will be provided by a deployment server. If you have not specified a deployment server, you must specify a receiving indexer, otherwise this forwarder will do nothing. The port must be the port the indexer is listening on, not its management port.

Receiving indexer

Hostname or IP : Port :

Enter the hostname or IP of a receiving indexer, e.g. index.splunk.com

InstallShield

< Back Next > Cancel

Il est possible de chiffrer les échanges de logs entre les serveurs Windows et le serveur Splunk à l'aide des clés générées sur le serveur Splunk.



Universal Forwarder - InstallShield Wizard

Certificate Information
Optionally provide certificate information for verifying the identity of this machine

If the following certificate information is not provided, forwarded data will still be encrypted with the default Splunk certificate.

SSL Certificate (file containing public and private key pair)

Browse...

Certificate Password

Enter password

Confirm password

SSL Root CA (file containing the Root CA certificate to validate the server certificate)

Browse...

InstallShield

< Back Next > Cancel

Cocher la case Local si on ne veut que les logs de la machine. Sinon cocher l'autre case si l'on veut exporter les logs de Serveur Windows distant connu par la machine.

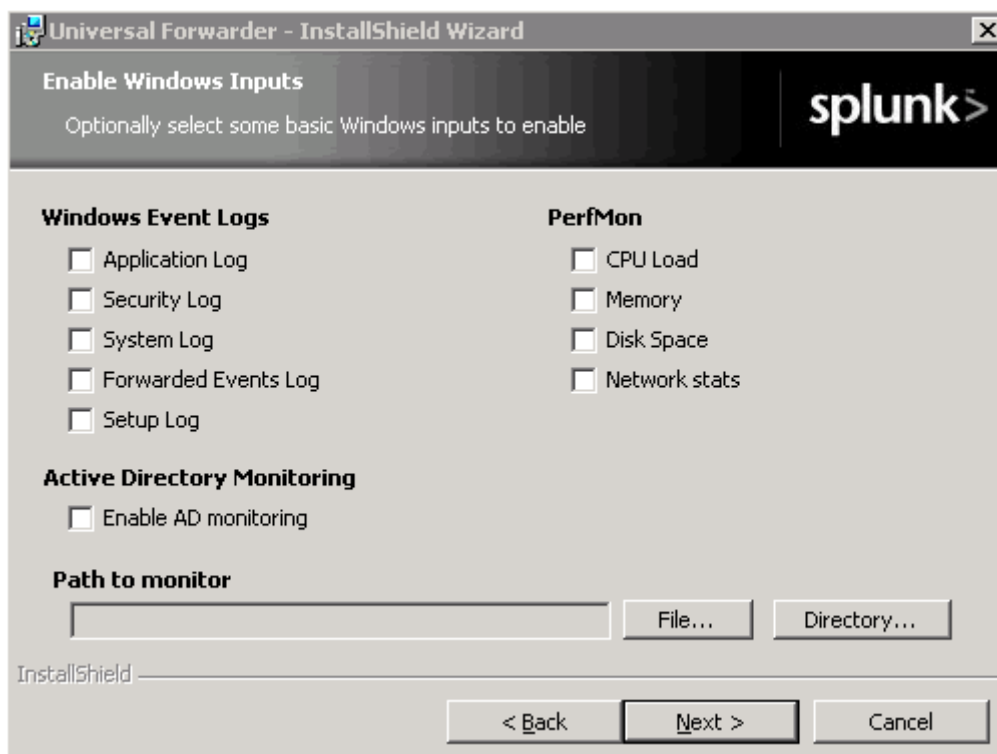
Stage en entreprise :

Version : 1.0

Horaires : 9h00—12h30 13h30-17h00



Dans cette fenêtre, il faut choisir les informations que l'on souhaite remonter au serveur Splunk :



L'installation est maintenant terminée il ne reste plus qu'à regarder si les logs sont affichés sur l'interface Web Splunk.