Projet i-PARAPHEUR v4.1

Guide d'installation sur Ubuntu Server 12.04 LTS

Projet	**i-Parapheur**	Rédacteur	Stéphane VAST Chef Produit i-Parapheur stephane.vast@adullact-projet.coop		
Objet	**Guide d'installation du serveur i-Parapheur 4.1**				
Date	**27/09/2013**	Statut	Validé	Diffusé le	01/10/13

Destinataires pour validation :

Organisme	Nom	Fonction	Validé le
ADULLACT	Pascal KUCZYNSKI 04.67.65.05.88	Directeur Technique pascal.kuczynski@adullact.org	2/05/12
ADULLACT	Franck MEIGNEN	Administrateur Système	

Destinataire pour information :

Organisme	Nom	
ADULLACT	Pascal FEYDEL	Délégué Général de l'ADULLACT pascal.feydel@adullact.org

Sommaire

Contacts

Équipe projet : iparapheur@adullact-projet.coop
Site web : http://www.adullact-projet.coop/libriciels/iparapheur

Licence

1. Préambule à l'installation

Ce document vise à fournir un fil conducteur pour l'installation de l'application i-Parapheur. C'est un guide d'installation-type, à destination de techniciens expérimentés, à suivre et adapter selon l'environnement d'exploitation (système d'exploitation, contraintes réseau, etc.).

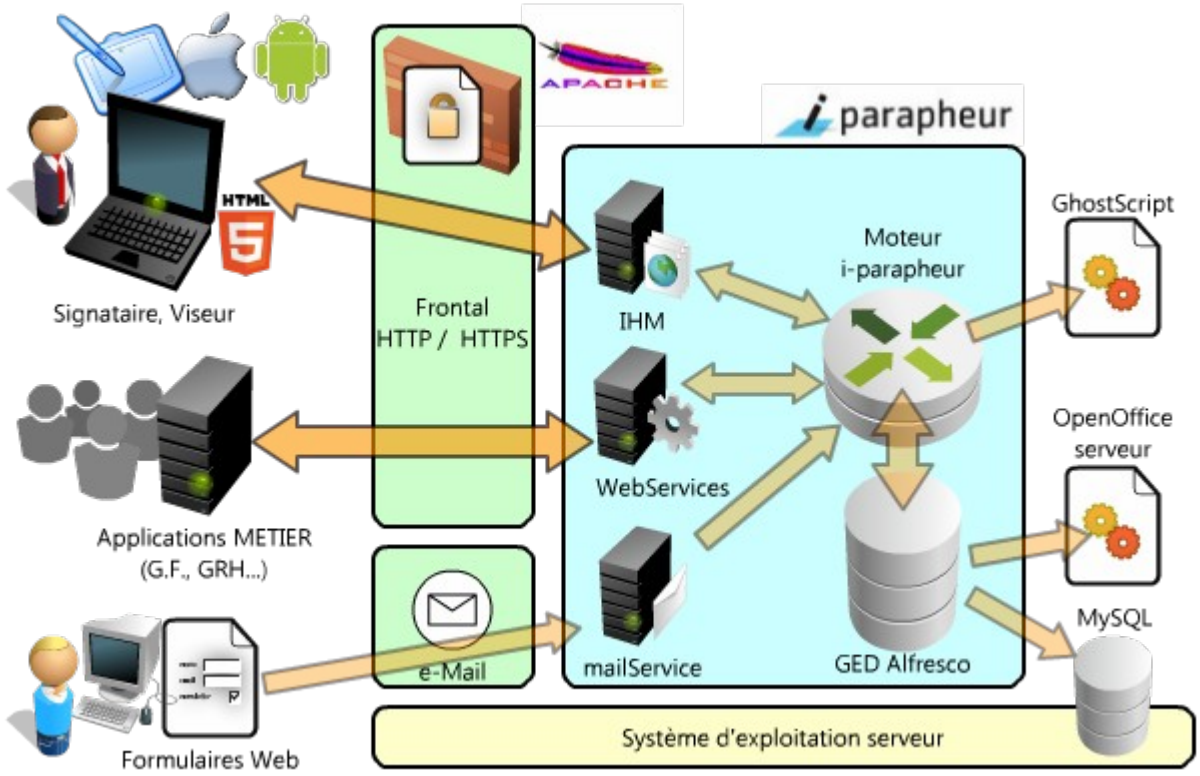
1.1. Contexte d'installation

Ce guide détaille l'installation sur plate-forme GNU/Linux en général, Ubuntu Server en particulier.

Quelques ressources Web ayant servi de base à cette procédure :

- http://wiki.alfresco.com/wiki/Installing_Alfresco_on_Ubuntu_7.10 (du 29 avr.2008)

1.2. Architecture logicielle serveur



L'installation du serveur réclame un certain nombre de pré-requis, autant de briques logicielles sur lesquelles va s'appuyer la solution i-Parapheur.

Quel que soit le système d'exploitation hôte, i-Parapheur a besoin des composants suivants :

- système d'exploitation 64bit, installé en Français, configuré avec encodage UTF-8,
- serveur de base de données MySQL 5.1 ou plus récent,
- Les polices de caractères standard de Microsoft pour aider à la production de PDFs,
- les utilitaires 'unzip', 'tar', 'GhostScript'
- serveur Web APACHE v2.2.17 ou mieux avec les modules SSL et PROXY_AJP, et donc OpenSSL
- accès à un serveur de messagerie SMTP, optionnellement une boite aux lettres POP3
- Alfresco 3.4.c Community (qui comprend SUN Java, ImageMagick, SwfTools, OpenOffice.org)

2. Pré-Requis logiciels – plate-forme GNU/Linux

L'installation a été validée sur la plate-forme **Ubuntu 12.04 Server LTS x64** (plate-forme supportée, et « support long terme » proposé par la société Canonical Ltd.), Debian Squeeze et supérieur.

Le parapheur électronique peut également être installé sur d'autres GNU/Linux : Fedora/ CentOS/ RedHat-ES, SUSE... sous réserve que les pré-requis logiciels soient respectés, ou sous réserve de validation par les équipes techniques de l'ADULLACT. L'installation sur serveur Microsoft™ n'est pas traitée dans ce document.
NB: Pendant l'installation, ***le serveur doit-être connecté*** sur un réseau relié à Internet afin de récupérer et installer les dernières mises-à-jour des composants logiciels disponibles.

2.1. Système opérateur – installation de Ubuntu Server

Localisation **FR**
Attribuer un nom de machine (pas de '_' dans le nom) :
exemple : iparapheur
Sélection de logiciels: choisir *OpenSSH server*

Exemple de partitionnement (HD de 300Go) :
/ 30G
swap 2G
/opt 200G <--- *ici sera l'entrepôt*
/var 70G <--- *ici sera la Base de Données*

NB : Les binaires d'installation seront déposés par convention dans **`/opt/_install`** .

2.2. Configuration du système Ubuntu, connecté à Internet

Vérifier et mettre à jour les dépôts (repository) de logiciels avec les privilèges administrateur:

```
$ sudo -s
#root > vi /etc/apt/sources.list
```

Commenter en préfixant avec le caractère '#' la ligne spécifiant le chemin du CD-ROM :

```
deb cdrom:[Ubuntu-Server 12.04 _Precise Pangolin_ - ...]/ precise main restricted
```

et s'assurer de la présence des dépôts *universe* et *multiverse* (normalement déjà activés):

```
deb     http://archive.ubuntu.com/ubuntu/ precise main restricted universe multiverse
deb-src http://archive.ubuntu.com/ubuntu/ precise main restricted universe multiverse
deb     http://archive.ubuntu.com/ubuntu/ precise-updates main restricted universe multiverse
deb-src http://archive.ubuntu.com/ubuntu/ precise-updates main restricted universe multiverse
deb     http://archive.ubuntu.com/ubuntu/ precise-security main restricted universe multiverse
deb-src http://archive.ubuntu.com/ubuntu/ precise-security main restricted universe multiverse
```

(ajouter le ou les dépôts manquants)

Debian : activer les repos 'main' 'contrib', 'non-free' .
Pour le dépôt 'backports' (pour OOo) nouvelle ligne :
deb http://backports.debian.org/debian-backports/ \ squeeze-backports main contrib non-free
, puis : apt-get install debian-backports-keyring

Mise à jour du système :

```
#root > apt-get update
#root > apt-get -s dist-upgrade     # Simulation
#root > apt-get dist-upgrade        # Mise à jour
```

NB: Éléments de confort (éditeur de texte, complétion) :

```
#root > apt-get install vim-nox      # coloration syntaxique dans vi
#root > vi /etc/bash.bashrc          # pour régler la complétion automatique
```

NB: en cas de mise à jour du kernel ('linux-image....'), rebooter:

```
#root > reboot
```

2.3. Installation des pré-requis logiciels

Base de données MySQL (sauf si il existe un service externalisé) :

```
#root > apt-get install mysql-server
```

Quelques outils nécessaires :

```
#root > apt-get install ntp xfonts-base psmisc unzip
#root > apt-get install ghostscript gsfonts
```

Si RedHat/CentOS: installer composants xorg-x11-fonts-Type1 libXext
Voir annexe pour procédure d'installation des polices TTF Microsoft.

OPTION: Polices de caractères TTF standard Microsoft™ (pour la transformation de documents):

```
#root > apt-get install ttf-mscorefonts-installer x-ttcidfont-conf
```

OPTION: JAVA: installer le JDK6 depuis le site java.com de Oracle (NB : java est livré avec Alfresco) :

```
#root > mkdir /opt/java ; cd /opt/java ; chmod +x /opt/_install/jdk-6u43-linux-x64.bin
#root > /opt/_install/jdk-6u43-linux-x64.bin
```

Vérifier que cette version est bien reconnue:

```
#root > java -version
```

Sinon, régler le problème avec '**update-alternatives**'

```
#root > update-alternatives --install "/usr/bin/java" "java" "/opt/java/jdk1.6.0_43/bin/java" 1
```

Puis ajouter si nécessaire la ligne suivante dans **/etc/profile** :

```
export LC_ALL=fr_FR.UTF-8
```

Il est important que s'assurer que c'est la version Oracle/SUN de JAVA qui sera utilisée.

2.4. Installation d'un serveur de courrier électronique

Cette étape est nécessaire **en l'absence** d'un serveur de messagerie directement exploitable:

```
#root > apt-get install postfix bsd-mailx
```

Type de configuration : *Local uniquement*

Vérifier le nom de domaine dans **/etc/mailname** , puis redémarrer postfix:

```
#root > /etc/init.d/postfix reload
```

OPTION: si utilisation du 'Email-Service' de i-parapheur pour l'injection de formulaires, il faut installer un serveur POP3 (voir http://doc.ubuntu-fr.org/pop pour les détails la configuration):

```
#root > apt-get install dovecot-common dovecot-pop3d
```

Éditer le fichier de configuration **/etc/dovecot/dovecot.conf**, et modifier les lignes:

```
protocols = pop3
mail_location = mbox:~/mail:INBOX=/var/mail/%u:INDEX=MEMORY
```

Remarque : Sur Debian , c'est le MTA exim qui est installé par défaut. Voir :
http://jerome.colombet.free.fr/?2010/05/28/103--debian-configurer-exim4-vers-un-relais

2.5. Installation du serveur Web Apache2

Sur RedHat4 : up2date -i httpd
Sur RedHat5 : yum install httpd

Composant logiciel nécessaire pour traiter les connexions sécurisées.
L'installation se fait avec la ligne suivante :

```
#root > apt-get install apache2 ca-certificates
```

Remarque pour Debian : il est possible pour Debian 5 (Lenny) ou 6 (Squeeze) de forcer l'installation d'une version plus récente pour Apache, en configurant APT (pinning de repository).

```
#root > apt-get install -t unstable openssl apache2
```

Remarque pour RedHat/CentOS : Apache est requis dans sa version la plus récente possible (v2.2.17 ou plus récent pour bénéficier de toutes les optimisations de paramétrage). Ces versions récentes ne sont pas fournies en standard par les distributions RedHat et CentOS (la version 5.x ne fournit que Apache 2.2.3 en standard!). Un contournement possible consiste à utiliser un dépôt logiciel alternatif :

- http://pkgs.org/centos-5-rhel-5/centalt-x86_64/
- ou autre...

Si RedHat 5.4 32bits (au 14/08/2011): la source est http://pkgs.org/centos-5-rhel-5/centalt-i386/

- httpd-2.2.22-1.el5.i386.rpm
- httpd-tools-2.2.22-1.el5.i386.rpm
- mod_ssl-2.2.22-1.el5.i386.rpm
- apr-util-ldap-1.3.9-1.el5.i386.rpm
- apr-util-1.3.9-1.el5.i386.rpm

Si RedHat 5.7 64bits (au 28/03/2012, les versions peuvent évoluer) :

- apr-util-1.3.9-1.el5.x86_64.rpm
- apr-util-ldap-1.3.9-1.el5.x86_64.rpm
- httpd-2.2.22-1.el5.x86_64.rpm
- httpd-tools-2.2.22-1.el5.x86_64.rpm
- mod_ssl-2.2.22-1.el5.x86_64.rpm

(installer le dernier 'centalt-release' depuis http://centos.alt.ru/repository/centos/5/x86_64/)
rpm -Uvh centalt-release*rpm, puis yum install httpd mod_ssl

Ressources : http://www.howtoforge.com/perfect-server-centos-5.7-x86_64-ispconfig-3

3. Installation et configuration du serveur Web Apache2

3.1. Activation des modules Apache2

Visualiser les modules actifs, et ajouter au besoin SSL et proxy_AJP :

```
#root > ls -l /etc/apache2/mods-enabled/          # Vérifier que le mod_ssl est présent.
#root > a2enmod ssl
#root > a2enmod proxy_ajp
```

Sur Debian : ajouter dans /etc/apache2/ports.conf : Listen 443

Sur une centos 4.4 ou RedHat : Placer les vhost dans /etc/http/conf.d/*.conf

3.2. Configuration des hôtes virtuels HTTP et HTTPS

L'architecture impose un paramétrage fin du serveur Web, au niveau du transfert des requêtes entre le poste de travail et le serveur i-parapheur, ainsi que sur la gestion des accès par certificat.

```
#root > cd /etc/apache2
#root > cp /opt/_install/confs/parapheur* sites-available        # (copie des modèles de vhost)
#root > a2ensite parapheur                                      # (activation du vhost HTTP)
#root > a2ensite parapheur.ssl                                  # (activation du vhost HTTPS)
```

Dans les fichiers 'vhost' nommés par exemple « parapheur » et « parapheur.ssl », adapter les adresses IP, email, noms FQDN du serveur (dans cet exemple : iparapheur.ma-collectivite.fr), chemin d'accès selon le contexte d'installation : respectivement les directives « VirtualHost », « ServerAdmin », « ServerName », voire « Directory » « Alias ».

Ci-après, un exemple pour le fichier de VirtualHost nommé « parapheur » :

ATTENTION : Ce sont des valeurs données à titre d'exemple

```
<VirtualHost 1.2.3.4:80>
        ServerAdmin webmaster@ma-collectivite.fr
        ServerName iparapheur.ma-collectivite.fr
        DocumentRoot "/var/www/parapheur"

        LogLevel info
        ErrorLog /var/log/apache2/iparapheur_error.log
        CustomLog /var/log/apache2/iparapheur_access.log combined

        <Directory /var/www/parapheur>
                Allow from all
        </Directory>
        <Directory /opt/iParapheur/tomcat/webapps/alfresco/images>
                Allow from all
        </Directory>
        <Directory /opt/iParapheur/tomcat/webapps/alfresco/css>
                Allow from all
        </Directory>
        <Directory /opt/iParapheur/tomcat/webapps/alfresco/scripts>
                Allow from all
        </Directory>
        Alias /alfresco/images /opt/iParapheur/tomcat/webapps/alfresco/images
        Alias /alfresco/css /opt/iParapheur/tomcat/webapps/alfresco/css
        Alias /alfresco/scripts /opt/iParapheur/tomcat/webapps/alfresco/scripts

        <Proxy *>
                order deny,allow
                allow from all
        </Proxy>

        <Location /bl-xemwebviewer>
                ProxyPass  ajp://localhost:9009/bl-xemwebviewer
        </Location>
        <Location /iparapheur>
                ProxyPassMatch  ajp://localhost
        </Location>
        <Location /alfresco/wcservice/>
                ProxyPassMatch  ajp://localhost
        </Location>
        <Location /alfresco/service/>
                ProxyPassMatch  ajp://localhost
        </Location>
        <Location /alfresco/wcs/>
                ProxyPassMatch  ajp://localhost
        </Location>
        <Location /alfresco/d/>
```

```
                ProxyPassMatch  ajp://localhost
        </Location>
        <Location /alfresco/navigate/>
                ProxyPassMatch  ajp://localhost
        </Location>
        <LocationMatch /alfresco$>
                ProxyPassMatch  ajp://localhost
        </LocationMatch>
        <LocationMatch /alfresco/(?!images|css|scripts)>
                ProxyPassMatch  ajp://localhost
        </LocationMatch>
</VirtualHost>
```

Exemples de VirtualHost « parapheur.ssl » (testé sous Ubuntu 10.04 LTS) :

ATTENTION : Ce sont des valeurs données à titre d'exemple

```
<VirtualHost 1.2.3.4:443>
        ServerAdmin webmaster@ma-collectivite.fr
        ServerName iparapheur.ma-collectivite.fr
        DocumentRoot "/var/www/parapheurssl"

        SSLEngine on
        SSLSessionCacheTimeout 300
        SSLCipherSuite RSA:!SSLv2:!RC2:!DES:!EXP:!eNULL
        SSLCertificateKeyFile /etc/apache2/ssl/apache-priv-key.pem
        SSLCertificateFile  /etc/apache2/ssl/apache-cert.pem
        SSLCARevocationPath  /etc/apache2/ssl/validca
        SSLCACertificatePath /etc/apache2/ssl/validca
        SSLVerifyClient require
        SSLVerifyDepth 10
        SSLOptions +StdEnvVars
        SSLInsecureRenegotiation on

        LogLevel info
        ErrorLog /var/log/apache2/iparapheur_ssl_error.log
        CustomLog /var/log/apache2/iparapheur_ssl_access.log combined

        <Location "/ws-iparapheur-no-mtom">
                SSLVerifyDepth 2
                SSLOptions +ExportCertData
                Allow from all
                ProxyPass  ajp://localhost/alfresco/ws-iparapheur-no-mtom
        </Location>
        <Location "/ws-iparapheur">
        #       SSLRenegBufferSize 20000000
                SSLVerifyDepth 2
                SSLOptions +ExportCertData
                Allow from all
                ProxyPass  ajp://localhost/alfresco/ws-iparapheur
        </Location>
        <Location "/alfresco">
                SSLVerifyDepth 2
                SSLOptions +ExportCertData
                Allow from all
                ProxyPassMatch  ajp://localhost/alfresco
        </Location>
        BrowserMatch "MSIE [2-6]" nokeepalive ssl-unclean-shutdown downgrade-1.0 force-response-1.0
        BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown
</VirtualHost>
```

Dans le répertoire **/etc/apache2/ssl/** déposer le script **recup_crl.sh** qui téléchargera périodiquement la liste des autorités de certification reconnues par la plate-forme (dans un sous-répertoire *validca*):

```
#root > mkdir /etc/apache2/ssl; cd /etc/apache2/ssl/
#root > cp /opt/_install/confs/recup_crl.sh . ; chmod +x recup_crl.sh
#root > ./recup_crl.sh /etc/apache2/ssl
```

Dans le répertoire **/etc/apache2/ssl/** , installer le certificat SSL du serveur web Apache (2 fichiers : un certificat X509, et une clé RSA). Celui-ci aura été acquis au préalable auprès d'une autorité de certification compétente, ou à défaut auprès d'une AC de moindre confiance (locale et auto-signée, cf. Annexe).

Une fois le certificat installé et dûment référencé dans le fichier VirtualHost « parapheur.ssl », vérifier que Apache fonctionne et écoute bien sur le port HTTPS (443):

```
#root > /etc/init.d/apache2 force-reload                    # ré-init. d'Apache
```

```
#root > netstat -antup | grep 443                    # doit donner un résultat
#root > cd /etc/apache2; rm sites-enabled/000-default    # un peu de ménage au besoin
```

Le script de mises-à-jour des CRL (listes des certificats révoqués) doit être appelé régulièrement (via CRON par exemple), voir annexe à ce propos.

OPTION: Cas des certificats pour Web-Services : Il faut constituer 2 magasins de certificat pour l'application cliente qui se connectera aux Web-Services i-Parapheur:

- un keyStore (contenant le certificat du client et sa partie privée), pour s'authentifier,
- un trustStore (contenant le certificat X509 du serveur) pour reconnaître le serveur.

Des outils tels que **Porte-Cle** (logiciel libre JAVA, version courante: 1.5) font cela très bien:
https://sourceforge.net/projects/portecle
Voir le manuel d'administration pour davantage d'informations concernant ce paramétrage.

3.3. Redirection automatique

Il s'agit de créer un fichier de redirection dans les répertoires déclarés comme « DocumentRoot » :

```
#root > cd /var/www; tar xzf /opt/_install/confs/var-www.tar.gz
#root > vim /var/www/parapheur/index.html
```

Adapter le fichier /var/www/parapheur/index.html (changer l'URL) :

```
<html>
  <head>
        <title>Redirection iParapheur</title>
        <meta http-equiv="refresh" content="1; URL=http://iparapheur.ma-collectivite.fr/alfresco">
  </head>
  <body></body>
</html>
```

Puis faire de même pour /var/www/parapheurssl/index.html (en redirigeant vers https...) :

```
#root > vim /var/www/parapheurssl/index.html
```

Adapter le fichier /var/www/parapheurssl/index.html (changer l'URL) :

```
<html>
  <head>
        <title>Redirection iParapheur</title>
        <meta http-equiv="refresh" content="1; URL=https://iparapheur.ma-collectivite.fr/alfresco">
  </head>
  <body></body>
</html>
```

NB : si usage de l'IHM v4, changer les fins des URLs en remplaçant /alfresco par /iparapheur

3.4. Remplacer Apache2 par Nginx ?

Il est possible d'utiliser Nginx à la place de Apache2, un exemple de fichier de configuration est disponible dans le paquet « confs.tar.gz ».
Nginx permettra notamment le déploiement pour l'accueil de connexions tablettes.

4. Composants i-Parapheur

4.1. Initialisation de la base de données de l'entrepôt

Tuning de MySQL : éditer le fichier /etc/mysql/my.cnf , et changer la variable suivante :

```
max_connections        = 360
```

Cela peut également être fait au run-time dans le client *mySQL* avec la commande :

```
set global max_connections=360;
```

La base de données va être initialisée avec la commande suivante :

```
#root > mysql -u root -psupersecret < /opt/_install/confs/mysql-init.sql
```

ATTENTION : mot de passe root défini à l'installation

NB : pour information, le contenu du fichier SQL :

```
create database alfresco default character set utf8 collate utf8_bin;
grant all on alfresco.* to 'alfresco'@'localhost' identified by 'alfresco' with grant option;
grant all on alfresco.* to 'alfresco'@'localhost.localdomain' identified by 'alfresco' with grant option;
```

4.2. Installation de Alfresco 3.4.c Community Edition

ATTENTION : La version requise est **3.4.c**, et non **3.3** ou autre !

Alfresco est téléchargeable sur http://sourceforge.net/projects/alfresco/files/ .
Dans ce manuel, l'installation est effectuée dans le répertoire **/opt/iParapheur** .
On procède ici à l'installation en mode console, ce qui autorise des déploiements en télé-intervention.

Ci-après un exemple avec le package d'installation Alfresco déposé dans **/opt/_install** :

```
#root > mkdir -p /opt/iParapheur; cd /opt/iParapheur
#root > chmod +x /opt/_install/alfresco-community-3.4.c-installer-linux-x64.bin
#root > /opt/_install/alfresco-community-3.4.c-installer-linux-x64.bin --mode text
Language Selection

Please select the installation language
[1] English - English
[2] French - Français
[3] Spanish - Español
[4] Italian - Italiano
[5] German - Deutsch
[6] Japanese - 日本語
Please choose an option [1] : 2
-------------------------------------------------------------------------------
Bienvenue dans l'assistant d'installation de Alfresco Community
-------------------------------------------------------------------------------
Sélectionnez des composants que vous désirez installer, décochez ceux que vous
ne voulez pas installer. Cliquez sur Suivant pour continuer.

MySQL : Y (Cannot be edited)
Java : Y (Cannot be edited)
Alfresco : Y (Cannot be edited)

SharePoint [Y/n] :n

Records Management [Y/n] :n

Web Quick Start [Y/n] :n

WCM Alfresco [Y/n] :n

Quickr Connector Support [Y/n] :n

OpenOffice [Y/n] :Y

Est-ce que la sélection est correcte ? [Y/n]: Y

-------------------------------------------------------------------------------
Type d'installation
[1] Facile - Installe les serveurs avec la configuration par défaut
[2] Avancé - Configure les ports du serveur et les propriétés de service
Merci de choisi une option. [1] : 2

-------------------------------------------------------------------------------
Dossier d'installation

Please choose a folder to install Alfresco Community.
Sélectionner un dossier [/opt/alfresco-3.4.c]: /opt/iParapheur
```

Les saisies au clavier sont indiquées en gras. Par exemple ici: choix d'installation en Français...

```
-------------------------------------------------------------------------------
Installation de la base de données

Veuillez sélectionner la configuration de base de données que vous souhaitez utiliser. Si vous
sélectionnez une base de données existante, vous devez configurer l'application Alfresco avant de
procéder à l'installation.

[1] Je souhaite utiliser la base de données MySQL groupée
[2] Je souhaite utiliser une base de données existante
Merci de choisi une option. [1] : 2

-------------------------------------------------------------------------------
Configuration de la base de données

URL JDBC [jdbc:mysql://localhost/alfresco]:
Pilote JDBC [org.gjt.mm.mysql.Driver]:
Nom de la base de données: [alfresco]:
Nom d'utilisateur []: alfresco

Mot de passe :
Saisir à nouveau :
-------------------------------------------------------------------------------
Configuration du port Tomcat

Veuillez saisir les paramètres de configuration Tomcat que vous souhaitez utiliser

Domaine du serveur Web : [127.0.0.1]: iparapheur.ma-collectivite.fr
Port de serveur Tomcat : [8080]:
Port d'arrêt Tomcat : [8005]:
Port SSL Tomcat [8443]:
Port AJP Tomcat : [8009]:

-------------------------------------------------------------------------------
Port FTP Alfresco

Please choose a port number to use for the integrated Alfresco FTP server.

Port : [21]: 2121

-------------------------------------------------------------------------------
Port RMI Alfresco

Please choose a port number for Alfresco to use to execute remote commands.

Port : [50500]:

-------------------------------------------------------------------------------
Admin Password

Veuillez indiquer un mot de passe afin d'utiliser le compte administrateur Alfresco

Mot de passe admin :
Répéter le mot de passe :
-------------------------------------------------------------------------------
Installer en tant que service

Si vous le souhaitez, vous pouvez enregistrer Alfresco Community en tant que service. Ainsi, le
démarrage s'exécutera automatiquement à chaque démarrage de la machine.

Installer Alfresco Community en tant que service ? [Y/n]: Y

-------------------------------------------------------------------------------
Port de serveur OpenOffice

Veuillez saisir le port que le serveur OpenOffice écoutera par défaut

Port de serveur OpenOffice [8100]:

-------------------------------------------------------------------------------
L'assistant d'installation est maintenant prêt à démarrer l'installation de
Alfresco Community sur votre ordinateur.

Voulez-vous continuer ? [Y/n]: Y

-------------------------------------------------------------------------------
Merci de patienter durant l'installation de Alfresco Community sur votre ordinateur.
 Installation en cours
 0% _____________ 50% _____________ 100%
 ########################################
-------------------------------------------------------------------------------
L'assistant vient de finir l'installation de Alfresco Community sur votre ordinateur.

Voir le fichier Lisezmoi ? [Y/n]: n
```

ATTENTION : ici on garde les valeurs par défaut.

ATTENTION : ici on garde les valeurs par défaut.

Répertoire pour les traces applicatives : fichier nommé /var/log/alfresco/alfresco.log

```
#root > mkdir -p /var/log/alfresco/tomcat/logs ; mkdir -p /var/lib/alfresco/tmp
#root > rm -rf /opt/iParapheur/tomcat/logs
#root > ln -s /var/log/alfresco/tomcat/logs /opt/iParapheur/tomcat/logs
```

Permettre l'usage de Ghostscript par le WAR (exemple de localisation sur Ubuntu 12.04 LTS) :

```
#root > ln -s /usr/lib/libgs.so.9 /opt/iParapheur/common/lib/libgs.so
```

NB : si RedHat 6 : `ln -s /usr/lib64/libgs.so.8 /opt/iParapheur/common/lib/libgs.so`

4.3. Fichier de configuration 'alfresco-global.properties'

Ajouter les éléments de paramétrage i-Parapheur dans le fichier alfreso-global.properties :

```
#root > cd /opt/iParapheur/tomcat/shared/classes
#root > cat /opt/_install/confs/ADD-to_alfresco-global.properties >>alfresco-global.properties
```

Localisation de l'entrepôt (configuration de la base de données, emplacement de l'entrepôt):

```
#root > vi /opt/iParapheur/tomcat/shared/classes/alfresco-global.properties
```

Y vérifier les paramètres pour le stockage, la base de données, les divers chemins d'accès :

```
dir.root=/opt/iParapheur/alf_data

###  database connection properties
db.driver=org.gjt.mm.mysql.Driver
db.username=alfresco
db.password=alfresco
db.name=alfresco
db.url=jdbc:mysql://localhost/alfresco

ftp.enabled=false

### External executable locations
ooo.exe=/opt/iParapheur/openoffice/program/soffice.bin
ooo.enabled=false
img.root=/opt/iParapheur/common
img.dyn=${img.root}/lib
img.exe=${img.root}/bin/convert
swf.exe=/opt/iParapheur/common/bin/pdf2swf
jodconverter.enabled=true
jodconverter.officeHome=/opt/iParapheur/openoffice
jodconverter.portNumbers=8101
```

ATTENTION : Ce sont des valeurs données à titre d'exemple

Le copier-coller peut nuire à la santé du i-parapheur...

Et en particulier les lignes suivantes dédiées à i-Parapheur :

```
##
# Default properties used in i-parapheur
#-------------
db.pool.initial=100
db.pool.max=350
audit.enabled=true

# Renseigner l'url de base pour l'applet de signature (v3 only)
parapheur.signature.applet.url=http://iparapheur.ma-collectivite.fr/alfresco
## Modeles d'email : emetteur par defaut, et URL de base (sans http://)
parapheur.mail.from=ne-pas-repondre@ma-collectivite.fr
parapheur.mail.baseUrl=iparapheur.ma-collectivite.fr/iparapheur
# Modeles d'email : prefixe dans l'objet, par exemple [i-Parapheur]
parapheur.mail.objet.prefixe=[i-Parapheur]
parapheur.mail.targetVersion=4

## Proprietes pour generation PDF archive/impression
parapheur.archive.ttfVerdana.location=/opt/iParapheur/verdanai.ttf
parapheur.archive.iccprofile.location=/opt/iParapheur/srgb.profile
parapheur.archive.tamponActes.prefixe="Acquitté en PREFECTURE le:"

## parapheur.habillage (adullact|blex)
parapheur.habillage=adullact
## parapheur.ihm.document.uploadMaxSize :
# - 0 : taille illimitee (valeur par defaut)
# - n : taille limitee a 'n' (en mega-octets)
parapheur.ihm.document.uploadMaxSize=0

## (EXPERIMENTAL) Traitement par lot non bloquant (true|false)
parapheur.jobs.thread.enabled=false
```

ATTENTION : ce doit être cohérent avec les réglages de la Base de Données

```
75  ## Affichage d'apercu de dossier : parapheur.preview.enabled (true|false)
76  parapheur.preview.enabled=true
77  ## parapheur.tdts2low.statutjobinterval: periodicite de connection au TDT
78  #  30 : valeur par defaut (en minutes)
79  parapheur.tdts2low.statutjobinterval=30

80  ## parapheur.ws.getdossier : interaction Web-Services
81  parapheur.ws.getdossier.pdf.enabled=true
82  parapheur.ws.getdossier.pdf.docName="iParapheur_impression_dossier.pdf"

84  ## Generation des apercus bitmap pour client v4 (true|false)
85  parapheur.mobilepreview.enabled=true
86  ## Acces a GhostScript (attention au chemin celui-ci est system-dependant)
87  parapheur.ghostscript.path=/usr/bin/gs
88  parapheur.ghostscript.dpi=150

91  ## Valeur par defaut de la trigger cron
92  parapheur.notification.digest.cron=0 0 8 * * ?

94  ## Par defaut, i-Parapheur n'accepte pas les DOCX etc.
95  parapheur.document.openxml.accept=false

97  ## CDC Fast-Service
98  fastService.repeatintervalMinutes=30
99  fastService.startDelayMinutes=40
```

4.4. Fichier de configuration TOMCAT 'server.xml'

Par défaut le connecteur AJP13 est activé mais mal configuré.

```
#root > vi /opt/iParapheur/tomcat/conf/server.xml                    (activer connecteur AJP13:8009)
```

Ligne 90 : la ligne sur le connecteur AJP13, et vérifier que son paramétrage est de la forme :

```
<Connector port="8009"  enableLookups="false" protocol="AJP/1.3"
           URIEncoding="UTF-8" connectionTimeout="600000" redirectPort="8443" />
```

4.5. Script de lancement/arrêt TOMCAT : 'ctl.sh' (tuning JVM)

Le script installé est nécessaire mais son contenu est insuffisant pour les besoins i-parapheur.

```
#root > vi /opt/iParapheur/tomcat/scripts/ctl.sh                    (vérifier les chemins)
```

Recommandations pour le script « ctl.sh », à adapter selon le contexte (chemins d'accès, etc.) :

ATTENTION : Ce sont des valeurs données à titre d'exemple

```
2   export LANG=fr_FR.UTF-8

6   CATALINA_PID=/var/run/parapheur.pid

13  export JAVA_OPTS='-XX:MaxPermSize=512m -Xms1536m -Xmx1536m -Xss1024k -XX:PermSize=64m -XX:NewSize=256m
-Dfile.encoding=UTF-8          -Djava.io.tmpdir=/var/lib/alfresco/tmp          -Dalfresco.home=/opt/iParapheur
-Dcom.sun.management.jmxremote'

26  export JAVA_OPTS='-XX:MaxPermSize=512m -Xms1536m -Xmx1536m -Xss1024k -XX:PermSize=64m -XX:NewSize=256m
-Dfile.encoding=UTF-8          -Djava.io.tmpdir=/var/lib/alfresco/tmp          -Dalfresco.home=/opt/iParapheur
-Dcom.sun.management.jmxremote'

32    $TOMCAT_BINDIR/shutdown.sh 9 -force
```

4.6. Personnalisation du fichier WAR de alfresco

Injection du fichier AMP (Alfresco Module Package) de i-Parapheur, dans le WAR Alfresco de base :

```
#root > cp /opt/_install/iParapheur-vX.Y.Z/iParapheur-vX.Y.Z_nnnnn.amp  /opt/iParapheur/amps/
#root > cd /opt/iParapheur
#root > bin/apply_amps.sh

This script will apply all the AMPs in amps and amps-share to the alfresco.war and share.war files
in tomcat/webapps
Press control-c to stop this script . . .
Press any other key to continue . . .

Module 'parapheur' installed in 'tomcat/webapps/alfresco.war'
   -    Title:        i-Parapheur ADULLACT
   -    Version:      3.4
   -    Install Date: Mon Dec 24 15:55:34 CET 2012
   -    Desription:   Parapheur electronique ADULLACT
```

```
No modules are installed in this WAR file
No modules are installed in this WAR file
About to clean out tomcat/webapps/alfresco and share directories and temporary files...
Press control-c to stop this script . . .
Press any other key to continue . . .

Cleaning temporary Alfresco files from Tomcat...
```

Dépaquetage du fichier WAR résultant dans le sous-répertoire 'alfresco', pour sa configuration :

```
#root > cd /opt/iParapheur/tomcat/webapps ; mkdir alfresco ; chmod 755 alfresco ; cd alfresco
#root > /opt/iParapheur/java/bin/jar -xf ../alfresco.war
#root > rm -f WEB-INF/lib/bcprov-jdk15*  WEB-INF/lib/bcmail-jdk15*
#root > rm -f WEB-INF/lib/asm-3.1.jar  WEB-INF/lib/cglib-2.2.jar
#root > rm -f WEB-INF/lib/geronimo-servlet_2.4_spec-1.1.1.jar  WEB-INF/lib/servlet-api-2.4.jar
```

Désactivation de la web-app inutile 'share', externalisation de log4j.properties :

```
#root > cd /opt/iParapheur/tomcat/webapps ; mv share.war share.war.inutile
#root > cd /opt/iParapheur/tomcat/webapps/alfresco/WEB-INF/classes
#root > cp log4j.properties ../../../../shared/classes/alfresco/extension/custom-log4j.properties
```

Renseigner l'emplacement du fichier de log applicative :

```
#root > vi /opt/iParapheur/tomcat/shared/classes/alfresco/extension/custom-log4j.properties

      16  log4j.appender.File.File=/var/log/alfresco/alfresco.log
```

4.7. Connecteur Web-Services

Configuration des URLs du fichier WSDL (remplacement des noms FQDN par défaut pour les connecteurs Web-Services) :

```
#root > cd /opt/iParapheur ; cp /opt/_install/confs/custom-wsdl.sh .
#root > ./custom-wsdl.sh  iparapheur.ma-collectivite.fr
```

Ce script va remplacer les URLs des services par celle donnée en paramètre, en fin de fichier:

```
<soap:address location="https://iparapheur.ma-collectivite.fr:443/ws-iparapheur" />
<soap:address location="https://iparapheur.ma-collectivite.fr:443/ws-iparapheur-no-mtom" />
```

Pour information : contenu du script

```
#!/bin/bash
sedpattern="s/iparapheur.demonstrations.adullact.org/$1/g"
sed  -i $sedpattern  tomcat/webapps/alfresco/WEB-INF/wsdl/iparapheur.wsdl
```

4.8. Déploiement du WAR « iparapheur »

Copie du fichier WAR de iparapheur dans le répertoire des webapps de TOMCAT :

```
#root > cd /opt/_install/iParapheur-vX.Y.Z
#root > cp *.war /opt/iParapheur/tomcat/webapps/iparapheur.war
#root > cp deployWarIparapheur.sh /opt/iParapheur/
#root > cd /opt/iParapheur/tomcat/webapps ; mkdir iparapheur
#root > cd /opt/iParapheur
#root > ./deployWarIparapheur.sh
```

4.9. Fichier de configuration 'iparapheur-global.properties'

Paramétrage, à partir d'un fichier d'exemple fourni :

```
#root > cd /opt/iParapheur/tomcat/shared/classes
#root > cp /opt/_install/confs/iparapheur-global.properties .
#root > vi /opt/iParapheur/tomcat/shared/classes/iparapheur-global.properties
```

Y adapter notamment le paramètre pour l'accès à LiberSign (attention, l'URL se termine en alfresco) :

```
  8  parapheur.signature.applet.url=http://iparapheur.ma-collectivite.fr/alfresco
```

Exemple de fichier :

```
#####################################################################
#   Parametrage i-Parapheur  (webapp iparapheur.war)                #
#                                                                   #
#                            copyleft 2013 - Adullact-Projet        #
#####################################################################

#################################
# URL de localisation de l'applet de signature LiberSign (se termine par alfresco car pointe sur v3)
parapheur.signature.applet.url=http://iparapheur.ma-collectivite.fr/alfresco

#################################
## Preferences utilisateur     ##
# Affichage des onglets dans les options
parapheur.ihm.options.password.show=true
parapheur.ihm.options.theme.show=true
parapheur.ihm.options.signature.show=true
parapheur.ihm.options.langue.show=true

#################################
## Bas de page                 ##
# URL du lien bas de page
parapheur.ihm.contact.support.url=http://www.adullact-projet.coop/
# Texte du lien bas de page
parapheur.ihm.contact.support.text=Support technique

#################################
## Themes de l'interface       ##
# Dossier des themes
parapheur.ihm.themes.directory=/var/www/themes
# Themes disponibles
parapheur.ihm.themes.disponibles=tenant1/rose,default

#################################
## Visibilite des dossiers     ##
# Visibilité par défaut de la collectivite principale (racine)
parapheur.ihm.creerdossier.visibilite.defaut=group
# Visibilité par défaut par tenant
parapheur.ihm.creerdossier.visibilite.defaut.tenant={"tenant1":"confidentiel"}
# Visibilités disponibles à la création (public|group|confidentiel)
parapheur.ihm.creerdossier.visibilite.valeurs=public,group,confidentiel
```

4.10. Divers réglages finaux

La génération des calques pour les visuels d'impression nécessite les fichiers suivants :

```
root > cd /opt/_install/confs ; cp srgb.profile verdanai.ttf /opt/iParapheur/
```

NB : certains messages sont mal traduits par Alfresco. Leur correction peut se faire en éditant le fichier de langue FR :

```
root > vim tomcat/webapps/alfresco/WEB-INF/classes/alfresco/messages/webclient_fr_FR.properties
       (ligne 852)
```

Un réglage sur le script de contrôle alfresco.sh (mentions surlignées à ajouter en début du fichier) :

```
#!/bin/sh

ulimit -Hn 16384
ulimit -Sn 16384

# Disabling SELinux if enabled
if [ -f "/usr/sbin/getenforce" ] && [ `id -u` = 0 ] ; then
    selinux_status=`/usr/sbin/getenforce`
    /usr/sbin/setenforce 0 2> /dev/null
fi

INSTALLDIR=/opt/iParapheur
cd $INSTALLDIR
```

Activer le script de contrôle pour OpenOffice.org :

```
root > cd /opt/iParapheur/openoffice/scripts ; mv openofficectl.sh ctl.sh
```

OPTION Configuration en mode multi-collectivité :
Si nécessaire, l'application i-Parapheur peut fonctionner en « colocation » de collectivité, grâce à l'activation du mode « multi-tenancy » d'Alfresco.
L'activation de ce mode s'effectue avec les manipulations suivantes :

```
#root > cd /opt/iParapheur/tomcat/shared/classes/alfresco/extension/mt
#root > mv  mt-context.xml.sample  mt-context.xml
#root > mv  mt-admin-context.xml.sample  mt-admin-context.xml
#root > mv  mt-contentstore-context.xml.sample  mt-contentstore-context.xml
```

Se référer au manuel d'administration (i-Parapheur_v3.2_Admin-multiCollectivite_v1.2.pdf) disponible sur le magasin ADULLACT pour l'exploitation de cette fonctionnalité.
La colocation (multi-tenancy) est limitée arbitrairement à 99 collectivités maximum par l'engineering Alfresco. Il est possible d'outrepasser cette limitation en modifiant certains paramètres internes (en particulier la gestion de la taille du cache[1]).
En cas de dépassement de ce maximum, il est recommandé de mettre en place plusieurs serveurs, et répartir les collectivités « locataires » sur ces différentes instances.

1 Voir l'article http://wiki.alfresco.com/wiki/MT .

4.11. Validation de l'installation

Après démarrage de l'application (voir le chapitre suivant pour la commande de démarrage) ou reboot du serveur, les manipulations suivantes permettent de s'assurer que l'installation s'est bien déroulée.

NB : un premier démarrage peut prendre jusqu'à 5 minutes selon la puissance des ressources allouées au serveur. Les démarrages suivants sont plus rapides (de 45 à 100 secondes).

Rappel : La vérification du bon démarrage de Tomcat peut se faire en examinant les traces 'catalina' :

```
#root > tail -f /var/log/alfresco/tomcat/logs/catalina.out
```

Un serveur fonctionnel enregistre dans ces traces ce message « *INFO: Server startup in xxxx ms* ».
Si ce message n'apparaît pas, contrôler l'activité CPU du processus Java de TOMCAT (par exemple avec la commande 'top') : en effet, le serveur peut ne pas avoir fini de démarrer.
Dans le cas contraire (activité nulle), les traces 'catalina' sont assez verbeuses, et font rapidement état du problème de démarrage.

OPTION Redémarrage du serveur :
Pour vérifier que les services sont bien actifs: **`reboot`** puis login, '**`sudo -s`**'. Chacune des commandes suivantes doit donner un résultat.

```
#root > ps aux | grep -i office
#root > ps aux | grep -i tomcat
#root > ps aux | grep -i mysql
```

4.11.1. Contrôle des services réseau

La commande suivante liste les ports réseau ouverts en écoute (prêts à servir) :

```
root > netstat -antup | grep LISTEN
```

Les lignes intéressantes, respectivement pour Apache, MySQL, OpenOffice.org, et i-Parapheur :

```
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      1599/apache2
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      1599/apache2
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      1353/mysqld
tcp        0      0 127.0.0.1:8100          0.0.0.0:*               LISTEN      5715/soffice.bin
tcp6       0      0 127.0.0.1:50500         :::*                    LISTEN      5627/java
tcp6       0      0 127.0.0.1:8005          :::*                    LISTEN      5627/java
tcp6       0      0 :::8009                 :::*                    LISTEN      5627/java
tcp6       0      0 :::50508                :::*                    LISTEN      5627/java
tcp6       0      0 :::35183                :::*                    LISTEN      5627/java
tcp6       0      0 :::8080                 :::*                    LISTEN      5627/java
tcp6       0      0 :::35800                :::*                    LISTEN      5627/java
```

4.11.2. Contrôle des accès Web HTTP et HTTPS

Pré-requis : un navigateur Web sur un poste avec accès au serveur.

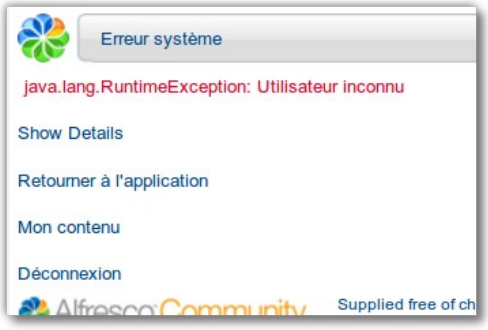
Figures : écran de connexion administrateur (test 1)

écran de connexion utilisateur (tests 2 & 3)

Dans un navigateur web, les URLs du tableau ci-après (personnaliser le nom de domaine selon le nom du serveur) doivent donner un écran de connexion ci-dessus :

N°	URL	Partie testée
1	http://iparapheur.ma-collectivite.fr:8080/alfresco/	Serveur TOMCAT Java en direct. Si KO, revoir l'installation en chapitre 4. Si OK : en profiter pour se connecter en admin , y définir son certificat de connexion.
2	http://iparapheur.ma-collectivite.fr/iparapheur/	Si N° 1 OK, pour valider l'installation du serveur Apache (chapitre 3).
3	http://iparapheur.ma-collectivite.fr	Si N° 2 OK, pour valider la redirection HTTP

Si les tests précédents sont concluants, tester l'accès HTTPS sur:
https://iparapheur.ma-collectivite.fr .
Pré-requis : un certificat client exploitable par le navigateur.



- Le navigateur doit réclamer un certificat client
- Sur sélection puis validation d'un certificat client, le message d'erreur suivant apparaît (« java.lang.RuntimeException: Utilisateur inconnu ») : c'est parfaitement logique et normal.
- Sur sélection du certificat client associé au compte 'admin' (voir test 1), la connexion doit permettre l'accès à la Console d'administration.

Remarque : si erreur 117 en HTTPS, mettre à jour les condensats des AC d'apache :

```
root > cd /etc/apache2/ssl
root > c_rehash /etc/apache2/ssl/validca
```

Penser également alors à inclure cette commande dans le script recup_crl.sh (voir tâches planifiées).
NB : Si installation sur RHEL/CentOS, la commande « c_rehash » est fourni par le composant logiciel optionnel « **openssl-perl** » :

```
root > yum install openssl-perl

( yum install ./perl-WWW-Curl-4.09-3.el6.x86_64.rpm ./openssl-perl-1.0.0-27.el6_4.2.x86_64.rpm )
```

Concernant la partie Web-Services, se référer au manuel administrateur pour la constitution des keystores à utiliser dans le logiciel métier (client du i-Parapheur).

5. Guide rapide d'Exploitation

5.1. Commandes de lancement /arrêt de i-Parapheur

```
#root > /etc/init.d/alfresco start
```

NB : La toute première fois, le lancement va initialiser les données i-Parapheur dans la base de données et le système de fichiers (alf_data) ; ce processus est relativement long (2 à 5 minutes).
La vérification du bon démarrage de Tomcat peut se faire en examinant les traces 'catalina' :

```
#root > tail -f /var/log/alfresco/tomcat/logs/catalina.out
```

Un serveur fonctionnel enregistre dans les traces ce message « *INFO: Server startup in xxxx ms* ».

Arrêt de iParapheur :

```
#root > /etc/init.d/alfresco stop
```

5.2. Cas de serveur SMTP externe

Pour configurer les notifications par mail auprès des acteurs de i-Parapheur.

```
#root > vi /opt/iParapheur/tomcat/shared/classes/alfresco-global.properties
```

Les paramètres de connexion SMTP suivants sont disponibles (ajouter en fin de fichier) :

```
#
# Outbound Email Configuration
#-----------------------------
mail.host=monSMTPjoliQuiMarche.ma-collectivite.fr
mail.port=25
mail.username=anonymous
mail.password=
mail.encoding=UTF-8
mail.from.default=ne-pas-repondre-SVP@ma-collectivite.org
mail.smtp.auth=false
```

ATTENTION : Ce sont des valeurs données à titre d'exemple

Adapter selon contexte.

5.3. Exemple de mise en place de procédure de sauvegardes

Copie du script de sauvegarde dans le répertoire d'installation :

```
#root > cp /opt/_install/confs/backup_parapheur.sh /opt/iParapheur/
#root > cp /opt/_install/confs/send_backup.sh /opt/iParapheur/bin
#root > chmod +x /opt/iParapheur/bin/send_backup.sh /opt/iParapheur/backup_parapheur.sh
```

Régler le CRON afin que la procédure s'exécute tous les jours à 3h05 du matin (dans cet exemple) :

```
#root > crontab -e
```

Les backups DOIVENT se faire à froid (application arrêtée), voir l'exemple de lignes pour CRON :

```
MAILTO=''
0 0 * * * /etc/apache2/ssl/recup_crl.sh /etc/apache2/ssl && /etc/init.d/apache2 restart >/dev/null 2>&1
5 3 * * * /etc/init.d/alfresco stop  >/dev/null 2>&1
15 3 * * * /usr/bin/killall -q -e -g -s 9 /opt/iParapheur/java/bin/java >/dev/null 2>&1
16 3 * * * /usr/bin/killall -q -e -s 9 /opt/iParapheur/openoffice/program/soffice.bin >/dev/null 2>&1
18 3 * * * /bin/rm -f /var/run/parapheur.pid  >/dev/null 2>&1
19 3 * * * /usr/sbin/ntpdate ntp.ubuntu.com pool.ntp.org  >/dev/null 2>&1
20 3 * * * /opt/iParapheur/backup_parapheur.sh  >/dev/null 2>&1
45 3 * * * /etc/init.d/alfresco start >/dev/null 2>&1
```

Explication : La 1ère ligne met à jour les ACs et CRLs pour Apache ; puis arrêt de l'application. Enfin, une commande de mise à jour de l'heure système, et lancement du script de backup, avant redémarrage de l'application.

Enfin, éditer le fichier *send_backup.sh* pour régler les paramètres de serveur distant (FTP ou CIFS).

5.4. Procédure de restauration d'une sauvegarde

- le fichier *alfresco-global.properties* doit être modifié temporairement: positionner le paramètre
  `index.recovery.mode=FULL`
- Arrêter l'application i-Parapheur (voir procédure ci-dessous)
- Exécuter le script *restore_parapheur.sh* dans le répertoire */opt/iParapheur/bin*
- Effacer le répertoire /opt/iParapheur/alf_data/lucene-indexes

- Renommer /opt/iParapheur/alf_data/backup-lucene-indexes
  en /opt/iParapheur/alf_data/lucene-indexes
- Relancer l'application
- après démarrage, remettre le paramètre `index.recovery.mode=AUTO`

5.5. Monitoring du serveur

Il convient de surveiller le service, pourquoi pas avec des sondes de type Nagios sur :

- OpenOffice.org, TOMCAT, Apache/Nginx,
- consommation CPU
- consommation RAM
- occupation disque.

Exemple pour la consommation disque (si absence de sonde) :
Avec un script BASH très simple nommé /opt/iParapheur/espace.sh :

```
#!/bin/bash
# version 1.0.0 par Stephane VAST
df -h | mail -s "Espace disque sur mon serveur maCollectivite.fr" exploitation@maCollectivite.fr
```

Ce script appelé régulièrement par CRON :

```
0 8 * * 1 /opt/iParapheur/espace.sh >/dev/null 2>&1
```

5.6. Procédure de mise à jour mineure

Cela ne concerne QUE des mises-à-jour dites « mineures » (3.2.x à 3.2.y par exemple). Elle ne fonctionne pas pour une mise à jour depuis une version 3.0.xx (car changement de socle Alfresco).

Dans le package tar.gz sont livrés un script *iparaph-updateAMP.sh* , et un guide *LISEZ-MOI.txt* :

```
#root > cp /opt/_install/confs/iparaph-updateAMP.sh /opt/iParapheur
```

Lire le fichier LISEZ-MOI.txt : il précise les opérations à effectuer, selon l'écart de versions de produit.

NB : pour l'exécution du script *custom-wsdl.sh* (voir § 4.6 sur le connecteur Web-Services) :

```
#root > cd /opt/iParapheur
#root > ./custom-wsdl.sh  iparapheur.ma-collectivite.fr
```

Cas de mise à jour depuis Ubuntu 10.04 : le passage vers Ubuntu 12.04 se fait assez simplement :

```
#root > apt-get update
#root > apt-get dist-upgrade                        # éventuel reboot si mise-à-jour du kernel
#root > apt-get install update-manager-core
#root > vi /etc/update-manager/release-upgrades     # positionner :  Prompt=lts
#root > do-release-upgrade
```

NB : depuis la version 3.4 et plus, il y a une dépendance sur GhostScript, qui se résout ainsi :
- installer les paquets GhostScript et gsfonts (voir au début du manuel d'install)
- le lien symbolique vers common/lib/libgs.so :

```
#root > ln -s /usr/lib/libgs.so.9 /opt/iParapheur/common/lib/libgs.so
```

5.7. Mises-à-jour des CRL

Opération nécessaire pour avoir un contrôle efficace de validité des certificats, les listes des certificats révoqués par AC peuvent être mises-à-jour toutes les nuits (voir CRON aux chapitres précédents). Voici le script **`/etc/apache2/ssl/recup_crl.sh`**

```
#!/bin/bash
# version 1.0.1 par Stephane VAST

DIR=$1
cd $DIR

if [ -e $DIR/validca.tgz ]
then
        rm $DIR/validca.tgz
fi

if [ -e /tmp/validca.md5sum ]
then
        rm /tmp/validca.md5sum
fi

/usr/bin/wget --no-proxy -q http://crl.adullact.org/validca.tgz

cd /tmp
/usr/bin/wget --no-proxy -q http://crl.adullact.org/validca.md5sum

MD5=`md5sum $DIR/validca.tgz | awk '{print $1}'`
echo $MD5
if [ -z "$MD5" ]
then
        echo "CALCUL MD5 IMPOSSIBLE: TELECHARGEMENT AVORTE?";
        exit;
fi

if [ $MD5 != `cat /tmp/validca.md5sum` ]
then
        echo "PROBLEME MD5SUM DIFFERENT DE CELUI TELECHARGE";
        exit;
fi

if [ -e $DIR/validca-old ]
then
        rm -r $DIR/validca-old
fi

if [ -e $DIR/validca ]
then
        mv $DIR/validca $DIR/validca-old
fi

cd $DIR
tar -xzf $DIR/validca.tgz
```

6. Annexe : Trucs & astuces

6.1. I-Parapheur derrière un serveur proxy

L'accès à Internet peut être filtré par un serveur mandataire (proxy), variable d'environnement :

```
http_proxy="http://<username>:<pwd>@<ip>:<port>"       #pour les scripts d'installation
HTTP_PROXY="http://<username>:<pwd>@<ip>:<port>"
```

i-Parapheur en a besoin pour la connexion au TdT, et éventuellement pour le serveur horodateur.
Éditer le fichier `/opt/iParapheur/alfresco.sh` et ajouter à la clause JAVA_OPTS par exemple:

```
-Dhttp.proxyHost=proxy.mydomain.com -Dhttp.proxyPort=8080 -Dhttp.nonProxyHosts=192.168.0.*|10.1.*
```

Dans cet exemple le proxy est 'proxy.mydomain.com' sur le port '8080', en précisant que l'accès aux sous-réseaux 192.168.0.0/24 et 10.1.0.0/16 se fait sans passer par le proxy.

En cas de proxy authentifiant (utilisateur « username », et mot de passe « supersecret »), ajouter :

```
-Dhttp.proxyUser=username  -Dhttp.proxyPassword=supersecret
```

Cas très particulier de proxy MS ISA Server 2004 « sécurisé » : il utilise une authentification NTLM via le domaine, nom de machine, login, mot de passe ! Installer NTLM Authorization Proxy Server :

```
#root > apt-get install ntlmaps
```

Éditer le fichier `/etc/ntlmaps/server.cfg` et positionner les champs suivants :

```
Dans [GENERAL]
LISTEN_PORT: 5865                    #port du proxy local
PARENT_PROXY: proxy.nom.de.domaine   #le proxy ISA de la collectivité
PARENT_PROXY_PORT: port              #port du proxy ISA de la collectivité
ALLOW_EXTERNAL_CLIENTS: 0            #1 pour permettre des connections par cet intermédiaire.
Dans [NTLM_AUTH]
NT_HOSTNAME: Ma_Machine              #nom de la machine connue sur le domaine (Windows)
NT_DOMAIN: Domaine_NT                #le nom de domaine NT de la collectivité
USER: c_est_moi                      #le nom de connexion dans le domaine NT
PASSWORD: mon_mot_de_passe           #le mot de passe correspondant sur le domaine NT
LM_PART:1                            #
NT_PART:1                            #
NTLM_FLAGS: 07820000                 #
#root > /etc/init.d/ntlmaps restart
#root > export http_proxy=http://localhost:5865
```

Éditer le fichier `/opt/iParapheur/alfresco.sh` et régler ajuster le proxy sur localhost:5865.

Autre piste : Voir le logiciel « cntlm » à utiliser en remplacement de ntlmaps ?

6.2. Paramétrage avancé du connecteur Web-Services

L'accès à aux Web-services i-Parapheur est doublement sécurisé par **MCA + Basic**: *certificat client* d'authentification HTTPS, et identifiant *login/password* vers i-Parapheur. Il est aussi possible de faire automatiquement intervenir le champ 'CN' du certificat dans le login présenté à i-Parapheur : le compte créé dans i-Parapheur devra alors être de la forme '`<CN>.<login>`'. La syntaxe du séparateur (ici le caractère '.' par défaut) est également paramétrable.

Ce réglage se fait dans le fichier :
`/opt/iParapheur/tomcat/webapps/alfresco/WEB-INF/applicationAcegi.xml`

Aller à la section **`bean id="x509AndBasicAuthenticationProcessingFilter"`** et adapter la valeur de la propriété **`dealWithCertificate`** selon le comportement souhaité: `false` ou `true`.

NOTE : L'utilisation des WebServices iParapheur a été expérimentée avec succès avec des clients JAVA (avec JAX-WS), C++ (avec gSOAP), PHP (avec WSO2 wsf-php), C#, NatStar.
Dans le cas de wsf-PHP, il y a un bug de double requête dans la librairie AXIS2/C HTTP embarquée. Le correctif est disponible sous forme de patch à l'URL suivante :
https://issues.apache.org/jira/browse/AXIS2C-1244 .

6.3. Installation des « swftools » sur RedHat, Debian, Ubuntu10.10 …

Inutile depuis l'installeur alfresco 3.4 : le composant logiciel « swftools » (qui fournit l'utilitaire **pdf2swf**) n'est pas disponible dans les dépôts RedHat, ni Ubuntu 10.10 (*swftools is broken by design, that's why it's not in the repositories anymore*), l'installation se fait par compilation des sources...

Pour Suse SLES 10 : https://tpeelen.wordpress.com/2010/04/27/installing-swftools-suse-10/
Pour RedHat :

```
#root >  yum install zlib-devel libjpeg-devel giflib-devel freetype-devel gcc gcc-c++ make
```

Pour Ubuntu 10.10 :

```
#root >  apt-get install build-essential libgif-dev libjpeg-dev zlib1g-dev libfreetype6-dev
```

Puis dérouler les commandes :

```
#root >  wget http://www.swftools.org/swftools-0.9.1.tar.gz
#root >  tar xzf swftools-0.9.1.tar.gz
#root >  cd swftools-0.9.1
#root >  ./configure --disable-lame
#root >  make && make install
```

L'outil exécutable « pdf2swf » est accessible dans **/usr/local/bin** , le chemin d'accès pour i-parapheur est à renseigner dans '**alfresco-global.properties**'. Éditer le fichier :

```
#root > vi /opt/iParapheur/tomcat/shared/classes/alfresco-global.properties
```

Dans la zone « External executable locations » (vers la ligne 32), localiser le paramètre 'swf.exe' (généralement ligne 38) et le positionner de la façon suivante :

```
32  ### External executable locations
33  ooo.exe=/opt/iParapheur/openoffice/program/soffice.bin
34  ooo.enabled=true
35  img.root=/opt/iParapheur/common
36  img.dyn=${img.root}/lib
37  img.exe=${img.root}/bin/convert
38  swf.exe=/usr/local/bin/pdf2swf
```

Chemin d'accès complet à pdf2swf

NB : une anomalie dans l'installeur Alfresco 3.4.c pour système GNU/Linux 32bits justifie d'installer le composant swftools de cette façon. Cette anomalie n'est pas présente sur l'installeur Alfresco pour GNU/Linux 64bits, recommandé.

6.4. Installation des Polices TTF standard Microsoft sur Red-Hat/CentOS...

Sans paquet RPM fournissant ces polices de caractère, télécharger et constituer ce paquet « à la main », avec une connexion Internet opérationnelle !
Toujours en mode super-utilisateur, se placer dans le répertoire de travail, installer les pré-requis et télécharger le projet depuis le site SourceForge.net :

```
#root >  mkdir -p /opt/_install/msttcorefonts && cd /opt/_install/msttcorefonts
#root >  yum install wget cabextract rpm-build chkfontpath ttmkfdir
#root >  wget http://corefonts.sourceforge.net/msttcorefonts-2.0-1.spec
```

Construction et installation du paquet RPM (exemple de chemin sur CentOS 5) :

```
#root >  rpmbuild -ba msttcorefonts-2.0-1.spec
#root >  rpm -ivh /usr/src/redhat/RPMS/noarch/msttcorefonts-2.0.1.noarch.rpm
#root >  /sbin/service xfs reload
```

NB: CentOS6 : https://oimon.wordpress.com/2011/09/05/msttcorefonts-on-rhel6-centos-6-sl6/
Pas de XFS à redémarrer.
En cas de souci, voir le site du projet : http://corefonts.sourceforge.net/

Astuce : D'éventuelles fontes 'particulières' peuvent être définies en les copiant dans le répertoire :
/opt/iParapheur/openoffice/basis3.2/share/fonts/truetype/ (adapter selon contexte d'installation)

D'une manière générale, ajouter des polices au système suffit avec :

```
#root > mkdir -p /usr/share/fonts/truetype/mesjoliesfontes
#root > cp /tmp/fonts/*.ttf /usr/share/fonts/truetype/mesjoliesfontes/
#root > fc-cache -f -v
```

Pour les polices Office2007 (Calibri,...) :
http://www.oooninja.com/2008/01/calibri-linux-vista-fonts-download.html

6.5. Service OpenOffice.org en écoute sur un port particulier

Lorsque l'on choisit un port différent du port par défaut (8100), Alfresco n'honore pas cette configuration. Il faut modifier la définition du bean suivante (dans tomcat/webapps/alfresco) :

WEB-INF/classes/alfresco/subsystems/OOoDirect/default/openoffice-transform-context.xml

Remplacer à la ligne 58 :

```
<bean id="openOfficeConnection" class="net.sf.jooreports.openoffice.connection.SocketOpenOfficeConnection"/>
```

par :

```
<bean id="openOfficeConnection" class="net.sf.jooreports.openoffice.connection.SocketOpenOfficeConnection">
    <constructor-arg>
        <value>${ooo.port}</value>
    </constructor-arg>
</bean>
```

6.6. Remplacer le service OpenOffice.org par LibreOffice 3.6 ou 4.0

Le bundle « alfresco 3.4.c » livre par défaut une version assez ancienne d'OOo, qui fonctionne bien pour les opérations courantes (HTML, ODT,...). LibreOffice offre de meilleurs filtres pour gérer certains formats de fichier fermés (.DOC .DOCX et autres).

Cas LibreOffice 4.0 :

- Sur Ubuntu12.04, ajouter au préalable les packages **libcups2** et **libfontconfig1** .

```
#root >  apt-get install libcups2 libfontconfig1
```

- Télécharger la version sur http://download.documentfoundation.org/libreoffice/stable/

```
#root >  wget http://download.documentfoundation.org/libreoffice/stable/4.0.5/deb/x86_64/LibreOffice_4.0.5_Linux_x86-64_deb.tar.gz
```

- NB : Après installation, l'application doit se lancer avec la commande (une seule ligne!) :

```
/opt/libreoffice4.0/program/soffice.bin --norestore --nodefault --nologo --headless  \
  --nofirststartwizard --accept="socket,host=localhost,port=8100;urp;StarOffice.ServiceManager"
```

- Les commandes suivantes permettent de remplacer OOo par LibreOffice :

```
#root > cd /opt/iParapheur/openoffice/scripts
#root > cp openoffice_ctl.sh ctl.sh
#root > cd .. ; mv scripts ../ooscripts
#root > rm -rf *
#root > cp -a /opt/libreoffice4.0/* ./
#root > mv ../ooscripts ./scripts
```

- Adapter le script de lancement /opt/iParapheur/openoffice/scripts/ctl.sh :

```
SOFFICE="$SOFFICEBIN --headless --nodefault --nofirststartwizard --nolockcheck --nologo --norestore
--invisible --accept=socket,host=0,port=8100,tcpNoDelay=1;urp"
```

6.7. Couplage avec annuaire LDAP, ressources diverses

Voir la littérature sur Internet, notamment concernant le couplage « alfresco - ldap »:

- http://wiki.alfresco.com/wiki/Alfresco_Authentication_Subsystems
- http://wiki.alfresco.com/wiki/The_Synchronization_Subsystem
- http://www.ochounos.com/#blog/6

D'autres sources d'inspiration pour faciliter l'installation :

- http://howtoforge.org/how-to-install-alfresco-community-3.3-on-ubuntu-server-10.04-lucid-lynx
- http://blog.mycroes.nl/2010/04/installing-alfresco-33-on-ubuntu-lucid.html

6.8. Certificats électroniques, autorité de certification et openSSL

Le i-parapheur s'appuie fortement sur l'usage de certificats électroniques pour sécuriser les communications, produire des signatures numériques, etc.
Ces certificats sont à acquérir auprès d'une autorité de certification présumée fiable pour l'exploitant. La force probante des connexions et des signatures est directement liée au niveau de confiance accordé aux certificats utilisés.

OPTION: Si nécessaire, création d'une A.C. (autorité de certification, locale et auto-signée):

Éditer au préalable '**/usr/lib/ssl/openssl.cnf**' et décommenter au besoin la ligne 184 :

```
183 # This is typical in keyUsage for a client certificate.
184 keyUsage = nonRepudiation, digitalSignature, keyEncipherment
```

```
#root > cd /etc/apache2/ssl
#root > /usr/lib/ssl/misc/CA.pl -newca
```

```
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Herault
Locality Name (eg, city) []:Montpellier
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ADULLACT-PROJET
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:CA
Email Address []:
```

Déclaration de cette A.C. dans la liste des A.C. connues du serveur Web :

```
#root > cd /etc/apache2/ssl/validca/
```

Supprimer l'ancien lien symbolique pointant vers : ->cacert.pem

```
#root > cp -f ../demoCA/cacert.pem .
#root > openssl x509 -hash -in cacert.pem -noout          => exemple de résultat : 22f2539e
#root > ln -s cacert.pem 22f2539e.0
```

Création du certificat serveur pour Apache :

ATTENTION : Le **Common Name** correspond au **ServerName** de la machine!

```
#root > cd /etc/apache2/ssl
#root > /usr/lib/ssl/misc/CA.pl -newreq
#root > openssl  rsa -in newkey.pem  -out iparapheur-serveur-priv-key.pem
#root > /usr/lib/ssl/misc/CA.pl -sign
#root > cp newcert.pem iparapheur-serveur.pem
```

Création de certificat client (pour tests et/ou accès Web-services) :

```
#root > cd /etc/apache2/ssl
#root > /usr/lib/ssl/misc/CA.pl -newreq
#root > /usr/lib/ssl/misc/CA.pl -sign
#root > /usr/lib/ssl/misc/CA.pl -pkcs12 'Certificat de Monsieur X'
```

Enfin, renommer le certificat obtenu :

```
#root > mv newcert.p12  /le-chemin-qui-me-plait/le-nom-que-je-veux.p12
```

Astuce : Transformation d'un certificat PKCS12 en fichiers PEM X509 pour Apache

```
#root > openssl pkcs12 -in moncertificat.p12 -nocerts -nodes -out apache-priv-key.pem
#root > openssl pkcs12 -in moncertificat.p12 -clcerts -nokeys -out apache-cert.pem
```

Opération inverse: certificats de PEM → P12

```
#root > openssl pkcs12 -export -out moncertificat.p12 -inkey userkey.pem -in usercert.pem
```

autres astuces: réencoder un certificat de PEM → DER, vérifier une signature PKCS#7 sur PDF (cas ACTES)

```
#root > openssl x509 -outform der -in moncertificat.pem -out moncertificat.der    (PEM → DER)
#root > openssl smime -in masignature.p7s -inform PEM -binary -verify -content mondocument.pdf
 -CApath /chemin/du/validca -purpose any -out /dev/null
```

6.9. Module Apache « PROXY_AJP » indisponible

Se rabattre sur MOD_JK : http://wiki.apache.org/tomcat/FAQ/Connectors

```
#root > apt-get install libapache2-mod-jk
```

Activer le module jk: **Attention, Il faut mod_JK V.1.2.x**

```
#root > /etc/init.d/apache2 force-reload
#root > cp /tmp/FichiersCONF/apache/mod_jk.conf conf.d/
```

Sur une centos 4.4 ou RedHat :
Modifier le httpd.conf
Load jk_module modules/mod_jk.so
Placer le fichier mod_jk.so dans
/etc/httpd/modules/.

6.10. Problèmes de connexion Web-Services - CVE-2009-3555

Dans certains cas, l'interopérabilité entre application tierce et i-parapheur peut être compliquée lors de l'établissement de session SSL/TLS : l'erreur retournée étant une exception du style **SSLHandshakeException** assorti d'un message « SSL renegociation failure ».
A l'origine, la correction d'une vulnérabilité connue (CVE-2009-3555), et décrite aux l'URLs :

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2009-3555
http://java.sun.com/javase/javaseforbusiness/docs/TLSReadme.html

Une solution consiste à ajouter l'assertion suivante dans les JAVA_OPTS au lancement :

```
-Dsun.security.ssl.allowUnsafeRenegotiation=true
```

A noter également qu'un correctif distribué depuis la version *2.2.14-5ubuntu8.2* de **Apache** et la version *0.9.8k-7ubuntu8.1* de la **libssl** (distribution Ubuntu) permet de contourner également ce problème en cas d'impossibilité de patcher le client.
La libssl implémente (en backport de *openssl 0.9.8m*) la RFC5746[1].

Pour Apache (>2.2.15), il est possible de forcer l'usage vers l'ancien comportement avec une nouvelle directive à inclure dans la définition du VirtualHost : **SSLInsecureRenegotiation**

6.11. Problème « Too many open files »

Cela peut arriver, des exceptions dans les traces Alfresco, et le serveur d'application qui plante avec ce message : "too many open files". Cela peut arriver alors même que l'on croit avoir résolu les limites de fichier ouvrables par processus. Le wiki Alfresco a une réponse :

http://wiki.alfresco.com/wiki/Too_many_open_files

Parfois, elle peut s'avérer inefficace, même avec les paramètres système suivants :

```
$ ulimit -n
4096
$ ulimit -Hn
65536
```

La longue ligne de commande suivante peut révéler la réelle source du problème (une seule ligne!)[2]:

```
for pid in `pidof java`; do echo "$(< /proc/$pid/cmdline)"; egrep
'files|Limit' /proc/$pid/limits; echo "Currently open files: $(ls -1 /proc/
$pid/fd | wc -l)"; echo; done
```

Exemple de résultat :

```
Limit                     Soft Limit           Hard Limit           Units
Max open files            1024                 1024                 files
Currently open files: 142
```

Ceci montre que les paramètres système ne sont pas pris en compte.

Une solution de contournement est donnée sur les forums:
http://ubuntuforums.org/showthread.php?t=1583041 (confirmé par d'autres posts[3]), dans le script /etc/init.d/alfresco ajouter en début de fichier les instructions suivantes :

```
ulimit -Hn 16384
ulimit -Sn 16384
```

1 Voir http://tools.ietf.org/html/rfc5746
2 Source : https://forums.alfresco.com/en/viewtopic.php?f=14&t=40374&start=0
3 Voir http://www.jayway.com/2012/02/11/how-to-really-fix-the-too-many-open-files-problem-for-tomcat-in-ubuntu/

6.12. Problème de 'locale'

Problème de locale (ubuntu6.06) :

```
#root > vi /var/lib/locales/supported.d/local
Ne laisser que :  fr_FR@euro ISO-8859-15
                  fr_FR ISO-8859-15
Dans /etc/environment, vérifier que seules ces deux lignes sont présentes :
       LANG="fr_FR"            et     LANGUAGE="fr_FR"
#root > sudo dpkg-reconfigure locales
#root > reboot
```

6.13. Hôtes virtuels, SSL et SNI

Le but : utiliser un serveur Apache avec plusieurs hôtes virtuels (virtual hosts) HTTPS sur une seule adresse IP. Le *Server Name Indication*[1] (SNI) permet le support de plusieurs Virtual Host avec des certificats SSL différents.
Le problème des certificats sans SNI se présente dans le cas suivant : lorsque le client demande le certificat au serveur, il ne précise pas de nom de domaine au moment de la négociation SSL. Le serveur est ainsi incapable de savoir quel certificat envoyer en fonction du domaine. Comme un certificat est rattaché à un domaine bien précis, il était nécessaire de mettre en place un nouveau mécanisme d'échange.
Ce mécanisme implique une modification de la phase de négociation des échanges SSL et TLS. La modification est donc à réaliser côté client ET côté serveur. SNI est une extension à TLS.

Parmi les navigateurs, ceux qui supportent le SNI sont :
- Internet Explorer 7 ou + (sur Windows Vista et +, mais **pas WindowsXP même avec IE 8**)
- Mozilla Firefox 2.0 ou supérieur
- Opera 8.0 ou supérieur (le protocole TLS 1.1 doit être activé)
- Opera Mobile sur Android 10.1
- Google Chrome 6 ou supérieur (Windows, OS X 10.5.7 minimum)
- Safari 2.1 ou supérieur (Mac OS X 10.5.6 minimum)
- MobileSafari sur iOS 4.0 ou supérieur
- Android Honeycomb ou supérieur

Au niveau des serveurs, on trouve :
- Apache 2.2.12 ou supérieur en utilisant mod_ssl ou mod_gnutls
- Cherokee avec le support TLS compilé
- Les nouvelles versions de lighttpd 1.4.24 ou +, et 1.5.x
- Nginx avec le OpenSSL supportant le SNI
- Apache Tomcat sur Java7

Les bibliothèques (utilisable sur application client ou serveur) :
- Mozilla NSS client
- OpenSSL
  - 0.9.8f (sorti le 11/10/2007) - pas compilé par défaut, activé avec l'option '–enable-tlsext'
  - 0.9.8j (sorti le 07/01/2009) - compilé par défaut
- GNU TLS
- libcurl si SNI activé
- Python 3.2

NB : les plate-formes qui ne supportent pas SNI :
- Internet Explorer sur Windows XP
- Safari sur Windows XP
- Android 2.x
- Mozilla NSS serveur
- Python 2.x

1 Voir http://en.wikipedia.org/wiki/Server_Name_Indication