# Pré-requis pour une installation de i-Parapheur

**Version 4.6**

Libriciel SCOP

## Document

| | | | |
|---|---|---|---|
| ***Auteur*** | Lukas HAMEURY | ***Date de diffusion*** | 30/08/2019 |
| ***Chef de projet*** | Stéphane VAST | ***N° de version*** | 4.6 |

## Évolution du document

| Version | Auteur | Nature des changements | Date |
|---|---|---|---|
| 1.0 | Lukas HAMEURY | Rédaction du document | 13/07/2018 |
| 1.1 | Lukas HAMEURY | Mise à jour du document selon version 4.6.4 | 24/01/2019 |
| 1.2 | Stéphane VAST | précisions sur BDD MariaDB ou MySQL | 11/03/2019 |
| 1.3 | Lukas HAMEURY | fin du support Ubuntu 14.04 | 29/04/2019 |
| 1.4 | Lukas HAMEURY | Mise à jour du document selon version 4.6.6 | 30/08/2019 |

## Licence

# Table des matières

# 1. PRÉSENTATION

## 1.1. Objectifs

Ce manuel décrit succinctement les pré-requis à l'installation d'un serveur i-Parapheur v4.6 sur un système d'exploitation GNU/Linux. Il s'adresse aux administrateurs techniques et systèmes de celui-ci.

## 1.2. Étendue

Outre les composants et ressources de base, on y parle également certificats électroniques pour connexions HTTPS serveur.

> Attention toutefois, l'installation est une opération relativement complexe; ce n'est pas un "setup.exe" en mode graphique. Elle réclame de nombreuses dépendances logicielles, et des compétences confirmées en administration système GNU/Linux.

# 2. LISTE DES SYSTÈMES D'EXPLOITATION SUPPORTÉS

Seules les versions de systèmes d'exploitation présents ci-dessous sont considérées.
Seuls les systèmes 64 bits sont supportables.

> NB: les versions NON LTS d'Ubuntu Server ne sont pas supportées.

| OS serveur 64bit | Statut | Commentaires |
|---|---|---|
| Ubuntu 12.04 LTS | `Obsolète` | non supporté. |
| Ubuntu 14.04 LTS | `Obsolète` | non supporté. |
| Ubuntu 16.04 LTS | *Supporté* | préférer version 18.04 |
| Ubuntu 18.04 LTS | **Supporté** | OS de référence fortement conseillé |
| Debian 7 | `Obsolète` | non supporté. |
| Debian 8 (Jessie) | *Supporté* | préférer Debian 9 |
| Debian 9 (Stretch) | **Supporté** | |
| CentOS / RHEL 5 ou 6 | `Obsolète` | non supporté. |
| CentOS / RHEL 7 | **Supporté** | |
| Oracle Linux 5 ou 6 | `Obsolète` | non supporté. |
| Oracle Linux 7 | *Supporté* | préférer l'original RHEL7 |
| SLES 11 SP2 | `Non qualifié` | donc non supporté. |

> *Remarque* : L'installation sur un serveur GNU/Linux 32bits n'est pas supportée. Système opérateur 64 bits obligatoire

L'installation a été validée sur la plate-forme de référence **Ubuntu 18.04 Server LTS**, Debian 9 (dernière version stable à ce jour).
Le parapheur électronique i-Parapheur peut également être installé sur d'autres systèmes d'exploitation de la même famille GNU/Linux : Fedora, Mageia Server, Gentoo, SUSE... sous réserve que les pré-requis logiciels ci-dessous soient respectés, et sous réserve de validation par les équipes techniques de Libriciel SCOP.

**Attention** : RHEL ou CentOS version 5 ne sont plus supportés, à cause de la dépendance OpenSSL trop ancienne (et présentant des failles de sécurité).
RHEL ou CentOS version 6 ne sont plus supportés, à cause de dysfonctionnements applicatifs importants et de la dépendance Python (2.6) trop ancienne.

# 3. DIMENSIONNEMENT ET RESSOURCES

Le dimensionnement disque peut être effectué tout en une même partition, ou plusieurs selon le choix assumé de l'exploitant technique.
Le formatage des partitions en **LVM** est fortement conseillé afin de pouvoir augmenter à chaud l'espace disque.

Le tableau suivant donne des valeurs indicatives :

| Ressource | Quantité | Commentaires |
|---|---|---|
| Espace disque système (racine) | ~20 Go | L'espace disque non-swap peut être réuni en une seule partition de 80 Go minimum |
| Espace disque "data" | Tests: >40 Go<br>Prod: > 100 Go | Pour `/opt`, cet espace est à moduler (ie. à augmenter)<br>en fonction de l'objectif de volumétrie ciblé. |
| Espace "swap" | > 3 Go | On a toujours besoin d'un peu de `swap` ... |
| CPU 64 bits | 2 à 32 | **Indicateur minimum**, à augmenter si besoin |
| Quantité RAM | > 5 Go | Indicateur minimum, augmenter selon le besoin |

Explications détaillées :

- **CPU** : 64 bit, dual-core minimum: naturellement, plus de ressources il y a, mieux c'est. Avec 4,8, 12 coeurs ou davantage, l'application sera naturellement plus réactive et fluide.
- **Mémoire** : 5 Go de **RAM minimum** pour le serveur. En effet il faut compter 3,5 Go de RAM minimum libres pour le moteur d'application (i-Parapheur + LibreOffice + MySQL + frontal web + GhostScript) seul, 1Go de plus pour le service de "visionneuse Xemelios". Et ce, hors système d'exploitation qui consomme aussi des ressources. Davantage de RAM aidera également l'application. Provisionner 1Go de RAM supplémentaire en cas d'installation de LiberValid sur ce serveur.

Si 30 utilisateurs simultanés ou 300 utilisateurs occasionnels (ce sont des MINIMA !) :

- Minimum RAM : 4 Go pour l'application, soit 5 à 6 Go pour la machine virtuelle
- Minimum CPU : 64 bit, 2x server-class CPU (ou 2xDual-core)

Si 100 utilisateurs simultanés ou 1000 utilisateurs occasionnels :

- Minimum RAM : 5 Go pour l'application, soit 6 à 7 Go pour la machine virtuelle
- Minimum CPU : 64 bit, 4x server-class CPU (ou 6xDual-core)

Selon la charge et/ou la qualité de service attendues, il est possible de répartir les composants sur différentes machines, ou monter le système en cluster, sur la base d'architecture cluster d'Alfresco. (NB : la mise en cluster n'est pas supportée par les équipes techniques Libriciel SCOP).

> *NB :*
> • Prévoir un minimum de 40Go d'espace disque libre 'data' en mode "expérimentation".
> Pour une utilisation en production, prévoir un minimum de **200Go** de disque pour les données, et 40Go pour la base de données.
> • Les valeurs de consommation mémoire sont des minima absolus de démarrage, et ne constituent pas des valeurs de confort ni de production. En effet, i-Parapheur s'appuie sur un moteur de GED Alfresco Community (et ses nombreuses dépendances) qui est un gros consommateur de ressources à lui tout seul.
> Ne pas hésiter à gonfler ces valeurs tant au niveau RAM que CPU.

# 4. COMMUNICATION RÉSEAU / INTERNET

Voici la liste des ports utilisés en entrée et sortie.

Certains applicatifs doivent etres visibles depuis internet.

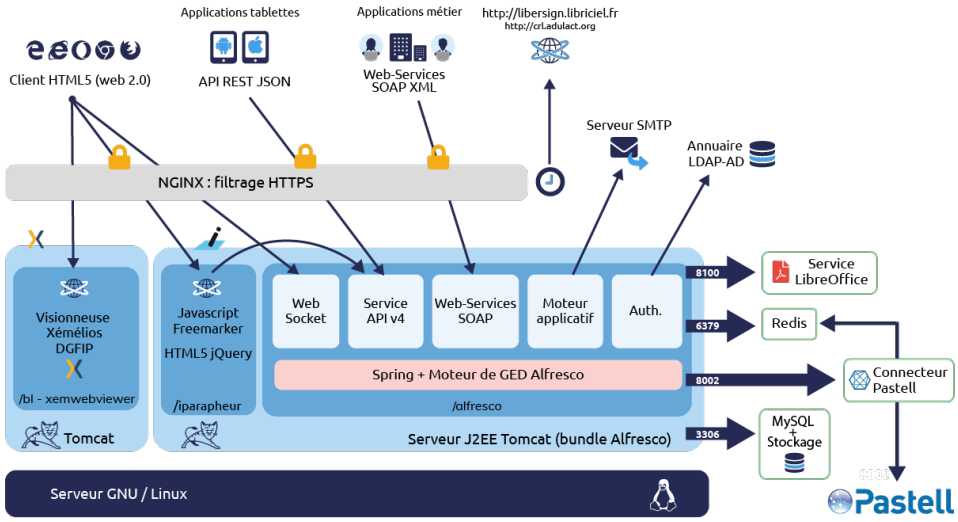
| Protocole | Entrée | Sortie | Commentaires |
|---|---|---|---|
| HTTPS (443 TCP) | Non | Oui | **validca.libriciel.fr** : récupération des AC et CRL RGS<br>(politique de sécurité applicative) |
| HTTPS (443 TCP) | Non | Oui | **libersign.libriciel.fr** : Mises-à-jour de LiberSign2<br>**Serveur pastell** : En cas de mise en place du connecteur Pastell |
| HTTPS (443 TCP) | Oui | Oui | En entrée: si usage extranet<br>En sortie: **www.s2low.org**<br>ou **s2low.formations.libriciel.fr**<br>Pour envoi des flux vers le TDT |
| SMTP (25 TCP) | Non | Oui | Généralement paramétré vers le relais SMTP local |
| LDAP (389 TCP) | Non | Optionel | si couplage annuaire<br>pour synchronisation de comptes utilisateurs |

> NB: Pendant l'installation, le serveur doit être connecté à internet (flux sortants full HTTP + HTTPS, sans proxy) afin de récupérer et installer les dernières mises-à-jour des composants logiciels nécessaires.

# 5. SCHÉMA D'ARCHITECTURE

Le schéma d'architecture montre en substance les briques logicielles utilisées.

Ces briques peuvent être réparties sur différentes machines, nous conseillons de regrouper toutes ces briques dans un même serveur.




L'application i-Parapheur peut être exploitée en réseau local, ou être utilisée pour la réception de flux provenant d'Internet.

L'accès utilisateur à i-Parapheur s'effectue principalement par navigateur, une URL en domaine ou sous-domaine dédié sera nécessaire, par exemple : **iparapheur.mondomaine.fr**.

Dans le cas d'un accès nécessaire depuis l'extérieur, seront nécessaires :

- Une URL en domaine ou sous-domaine public
- L'accès au port 443 HTTPS devra être ouvert depuis l'extérieur du réseau et routé correctement vers le serveur (ex : NAT, reverse proxy).

> *Remarque* : À chaque instance de i-Parapheur (ex: test, qualification, production) doit être provisionnée sa propre machine.

# 6. BRIQUES TECHNIQUES

Voici la liste des briques techniques qui supportent l'application.

Ces briques sont des pré-requis, et seront déployées à l'installation; inutile de procéder à leur mise en place préalablement à l'intervention planifiée d'un technicien Libriciel SCOP.

| Composant | Version | Commentaires |
|---|---|---|
| MariaDB<br>ou MySQL | 10 (MariaDB)<br>5.1 à 5.7 (MySQL) | par défaut sur le même hôte que l'application |
| NginX | > 1.8 | points d'entrée HTTP/HTTPS.<br>Prévoir certificats TLS serveur |
| LibreOffice | 4.2.8 à 5.4 | Génération des aperçus, et fichiers PDF |
| Alfresco Community | 3.4.c | socle technique à usage dédié et exclusif |
| JAVA JDK | 1.8_u171 | En support du serveur d'application web |
| Python | 2.7 | pour procédures d'exploitation |
| Redis | > 3.0 | Pour fonctionnement avec le connecteur Pastell |

*Cas MariaDB ou MySQL* : il est évidemment possible de déporter l'hébergement de la base de données sur une plate-forme tierce (cas de serveur mutualisant la ressource pour diverses applications), sous réserve que les pré-requis suivants d'allocation de ressources soient respectés:

- plafond autorisé de 350 connexions simultanées à la base de données
- `ping` applicatif entre i-Parapheur et le serveur BDD**inférieur à 2ms**,
- adaptation de la procédure de backup applicative pour sauvegardes cohérentes
- accès à procédure d'optimisation régulière des indexes (mysql-check)
- et diverses adaptations de configuration sur paramètres "innodb", etc. (voir manuel d'installation pour les détails)

> Autres moteurs de base de donnée : i-Parapheur v4.xx n'est pas conçu ni qualifié pour tourner sur les moteurs PostgreSQL, MS SQL-server ni Oracle.
> Seuls MariaDB et MySQL sont supportés, dans les versions précisées ci-dessus.

## 6.1. Points du serveur impactés

Installer le i-Parapheur nécessite d'intervenir sur l'arborescence GNU/Linux:

- `/opt/` pour y déposer l'application i-Parapheur. Sinon, possibilité d'installer un lien symbolique de /opt/iParapheur -> [dir]/iParapheur
- `/etc/profile` pour configurer les variables d'environnement JAVA_HOME, et LC_ALL
- `/etc/nginx/` pour configurer les hôtes virtuels (modes HTTP, HTTPS et autorités de certification de confiance pour les certificats)
- `/tmp/` de taille respectable (5 Go minimum), pour effectuer les opérations courantes d'installation et d'usage.
- `/var/log/` pour y déposer les logs applicatives de Tomcat et Alfresco
- `/var/lib/` (alfresco/tmp/) pour y déposer des fichiers temporaires d'Alfresco
- `/etc/init.d/` pour y installer le script de démarrage de i-parapheur, en qualité de service autonome.
- `/etc/systemd/system` pour y installer le script de démarrage des modules Connecteur Pastell et Pes-viewer

## 6.2. Autres points notables

Cette opération d'installation nécessite également des droits d'administrateur (root) afin de:

- installer les packages de distribution GNU/Linux correspondant aux pré-requis, ainsi que l'application
- configurer et relancer les services HTTP-HTTPS, MySQL, Postfix, CRON
- mettre à jour périodiquement la politique de sécurité HTTPS
- lancer/arrêter l'application i-Parapheur, effectuer les backups

> Notes : L'installation sur plate-forme serveur Microsoft Windows est théoriquement possible, mais cela reste non supporté à ce jour par l'équipe technique Libriciel SCOP: en particulier, le paramétrage HTTPS/TLS avec authentification forte par certificat y est délicat, en outre l'exécution de GhostScript n'y est pas thread-safe (donc dangereux et inexploitable en production).
> L'utilisation d'autres systèmes de base de données libres ou propriétaires (PostgreSQL, Oracle,...) n'est pas qualifiée ni supportée par Libriciel SCOP.

# 7. POSTE CLIENT

L'application i-Parapheur est développé dans le respect des standards du web (standard W3C), et nécessite les particularités suivantes :

- Activation de JavaScript,
- Acceptation des cookies de session,

> *NB* : Le port HTTPS (TCP 443) doit être ouvert entre le serveur et les postes clients.

## 7.1. Navigateurs et systèmes compatibles

La solution i-Parapheur est utilisé avec succès sur les environnements suivants:

- Systèmes opérateurs supportés de Microsoft: Windows 7, Windows 8.1, Windows 10.
- Si navigateurs Microsoft Internet Explorer : Seul IE-11 est supportable officiellement, à cause de la politique de support de la société Microsoft.
  Nous recommandons la version la plus récente possible (IE-10, IE-11).
- Navigateurs Mozilla Firefox (recommandé en version la plus récente, ou ESR supporté par Mozilla),
- Navigateurs Google Chrome ou Chromium
- Navigateur Microsoft Edge (hors opérations de signature électronique)

## 7.2. Signature électronique sur poste PC Windows

L'outil de signature (LiberSign) s'adapte selon le navigateur utilisé:

- Pour Mozilla Firefox , Google Chrome ou Opera: une extension de navigateur est utilisée, avec un "logiciel compagnon".
- Le logiciel compagnon est installé dans le répertoire utilisateur, normalement accessible sans droit administrateur.
- Remarque pour les postes sous contrainte (avec GPO ou restriction de droit de type Citrix): le poste utilisateur doit avoir accès au répertoire `%LOCALAPPDATA%` , directement utilisé par l'extension LiberSign
- Pour Microsoft Internet Explorer: déploiement du plugin Java à jour, pour permettre la signature électronique. En l'absence de "magasin d'extensions", le recours au système d'applets JAVA reste obligatoire pour le moment.

L'usage de certains serveurs mandataires (proxy HTTP et HTTPS) peut gêner le bon fonctionnement des applets Java de signature électronique.

*Cas particulier* : avec le navigateur Edge , sur Windows 10, le plugin "Sun/Oracle JAVA" n'est pas disponible. Il n'y a pas d'extension LiberSign non plus.
En effet, la technologie d'extensions pour Edge n'est assez pas mature ni complète (à l'écriture de ce document, mai.2017). Il n'est pas possible de signer électroniquement avec ce navigateur pour le moment. Les travaux sont en cours.

## 7.3. Signature électronique sur poste Apple macbook (macOS), ou Linux

**La signature électronique sur les ordinateurs Apple macOS n'est pas supportée.**

Seule la plateforme Microsoft est supportée pour les opérations de signature électronique.

*NB* : Le support des certificats matériels (par exemple "RGS deux étoiles") sur Apple macOS nécessite un perpétuel re-développement, grâce aux changements incessants opérés par Apple dans la gestion des tokens USB.
Les experts de l'écosystème Apple sont bienvenus: vous pouvez contacter Libriciel SCOP, et contribuer à écrire du code libre compatible avec les nouvelles couches de sécurité cryptographiques pour chaque nouvelle version de macOS.

## 7.4. Cas des tablettes numériques (Android, iOS)

L'application i-Parapheur mettant en œuvre des fonctions de signature électronique, certains détails sont à noter sur tablette numérique:

- Apple i-Pad :
  - une application native est publiée et maintenue par Libriciel SCOP sur l'App Store (tm).
  - Elle permet toutes les opérations de consultation courante, annotations, visa/rejet.
  - En l'absence de support (USB, carte à puce) et de pilote pour certificat matériel (type RGS deux étoiles), il n'est réglementairement pas possible d'y signer électroniquement les flux Actes ou Helios.
- Android tablette (à partir de Google Android 4) :
  - une application native est publiée par Libriciel SCOP sur Google Play (tm).

    - Elle permet toutes les opérations de consultation courante, annotations, visa/rejet, ainsi que signature PKCS7 avec certificat logiciel.
    - En l'absence de support et de pilote pour certificat matériel (type RGS deux étoiles), il n'est pas possible d'y signer électroniquement les flux Actes ou Helios.
- Windows tablette type "Surface Pro" (processeur intel) :
    - En réalité c'est un PC déguisé en tablette numérique ! i-Parapheur y fonctionne comme sur un PC classique depuis un navigateur.
    - Se référer aux pré-requis classiques pour poste de travail client.
    - Il n'existe pas d'application "client lourd" pour Windows tablettes ni sur le "Windows Store".

# 8. ANNEXE - POUR L'ENVIRONNEMENT D'EXPLOITATION

## 8.1. Nombre d'adresses IP à réserver

Configuration HTTPS: la multiplicité des connexions entrantes et sortantes nécessite une (voire deux) adresses IPv4 dédiées à i-Parapheur. Pour éviter la multiplicité des adresses IP à réserver, la configuration serveur se repose sur le système SNI (ServerName Indication) dans les connexions HTTPS.
Il faut DEUX adresses IP si l'environnement métier se connectant avec i-Parapheur ne supporte pas les connexions de type SNI, par exemple:

- si usage en poste client de WindowsXP et Internet-Explorer (non supporté par Microsoft depuis jan.2016)
- si mise en SSO CAS, avec CAS ne supportant pas le SNI (si opéré avec tomcat6),
- si application tierce (par exemple opérée par tomcat6,...) ne supportant pas non plus le SNI

## 8.2. Certificats SSL pour service HTTPS

Les connexions i-Parapheur entrantes sont sécurisées par certificat électronique.
Pour chaque FQDN=*iparapheur.dom.local* (adapter naturellement le nom au besoin, il s'agit ici d'un exemple illustratif), il faut prévoir:

- 2 enregistrement dans le service DNS :
  - accès web sur `iparapheur.dom.local` ,
  - et web-services sur `secure-iparapheur.dom.local` (pour les applications métiers)
- Acquérir le ou les certificat(s) électronique(s) protégeant les noms FQDN*iparapheur.dom.local* + *secure-iparapheur.dom.local*
- Si usage de l'application tablette : prévoir 1 enregistrement supplémentaire dans le service DNS pou`m.iparapheur.dom.local`, et commander le certificat adéquat auprès de Libriciel SCOP.

## 8.3. Couplages annuaires, SSO

### 8.3.1. Capacités LDAP / ActiveDirectory

Il est possible de synchroniser l'application avec un annuaire de LDAP (OpenLDAP), ainsi que Microsoft ActiveDirectory. Si un tel annuaire est déjà en place, son organisation doit être connue de l'exploitant et avoir été communiquée au préalable, afin de créer le lien avec le parapheur. Ceci afin que les comptes d'utilisateurs inscrits dans l'annuaire soient importés et connus de i-Parapheur.

### 8.3.2. Capacités SSO

L'application i-Parapheur peut être connecté avec certains systèmes de web-SSO:

- "Apereo CAS" (ex- Jasig CAS): protocole v2 ou v3, avec usage nécessaire de PGT (proxy granting ticket). A noter que le protocole CASv1 n'est pas supporté.
- "LemonLDAP::NG".