iparapheur

Pré-requis pour une installation de iparapheur

Version 5.1

Libriciel SCOP

Document

Auteur	Franck MEIGNEN	***Date de diffusion***	28/06/2022
Chef de projet	Adrien BRICCHI	***N° de version***	5.1

Évolution du document

Version	Auteur	Nature des changements	Date
1.0	Franck MEIGNEN	Création du document selon la version 5.0	28/06/2022
1.1	Sebastien PICARD	Changement du schéma d'architecture logicielle et correction coquilles	25/08/2022
2.0	Axel CHEVRIER	Changement de la version du parapheur pour la 5.1	23/01/24
2.1	Adrien BRICCHI	Correction de typos	09/02/24

Licence

Table des matières

1. PRÉSENTATION

1.1. Objectifs

Ce manuel décrit succinctement les pré-requis à l'installation d'un serveur iparapheur version 5.1 sur un système d'exploitation GNU/Linux.

2. LISTE DES SYSTÈMES D'EXPLOITATION SUPPORTÉS

Seules les versions des systèmes d'exploitation présents ci-dessous sont supportées.

OS serveur 64bit	Statut	Commentaires
Ubuntu 22.04 LTS Server	**Supporté**	OS de référence, préconisé, version serveur sans interface graphique
RedHat 8 (RHEL 8)	**Supporté**	Sous LICENCE, version serveur sans interface graphique

2.1. Docker

La version 5.1 d'iparapheur est livrée sous forme de conteneur docker fonctionnant sous Docker et fonctionnant sous un serveur virtuel.

Docker Community édition est utilisé avec le composant `docker-compose`.

- L'utilisation sous environnement SWARM existant n'est pas supporté,
- L'utilisation sous orchestrateur Kubernetes (OpenSHIFT/ TANZU) n'est pas supporté.

Les images Docker de nos produits ne sont pas modifiables et proviennent d'une registry dédiée.

2.2. Briques techniques

Voici la liste des briques techniques.

Ces briques sont des pré-requis, et seront déployées à l'installation, inutile de procéder à leur mise en place.

Composant	Version	Commentaires
Docker CE	20.x	Moteur Docker Community Edition
docker compose	2.61	commande de pilotage des conteneurs docker

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	Ressources test	Ressources production	Commentaires
Disque système (racine)	50 Go	100 Go	Contiendra l'OS, les logs, les images docker
Disque de données (/data)	50 Go	100 Go	Contiendra la base de données, la configuration ainsi que les données de tous les composants
CPU	4	6	
RAM	12 Go	16 Go	

Ces indicateurs conseillés peuvent être amenés à être revus à la hausse selon le contexte d'exploitation.

Explications détaillées :

- **CPU** : 4 cœurs minimum. Avec 6, 8, 12 cœurs ou davantage, l'application sera plus réactive et fluide.
- **Mémoire** :
  - 16 Go de **RAM minimum** pour le serveur,
  - Certains services peuvent être coupés (Matomo+MariaDB, Pastell-connector...) sur une instance de test n'exploitant pas les fonctionnalités associées. Cela permet de réduire l'empreinte mémoire.

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

- Minimum RAM : 4 Go pour l'application, soit 16 Go pour la machine virtuelle,
- Minimum CPU : 4 cœurs.

Si 100 utilisateurs simultanés ou 1000 utilisateurs occasionnels :

- Minimum RAM : 6 Go pour l'application, soit 20 Go pour la machine virtuelle,
- Minimum CPU : 8-10 cœurs.

L'architecture N-tiers répartie sur plusieurs serveurs n'est pas supportée.

4. COMMUNICATION RÉSEAU

4.1. Tableau de flux réseau

Voici la liste des ports utilisés en entrée et sortie.

4.1.1. Flux entrants

Protocole	Commentaire
HTTP port 80 TCP	Redirection vers HTTPS
HTTPS port 443 TCP	Accès utilisateur et réception des flux depuis les applications métier

Voici la liste des URL utilisées depuis internet pour la phase d'installation :

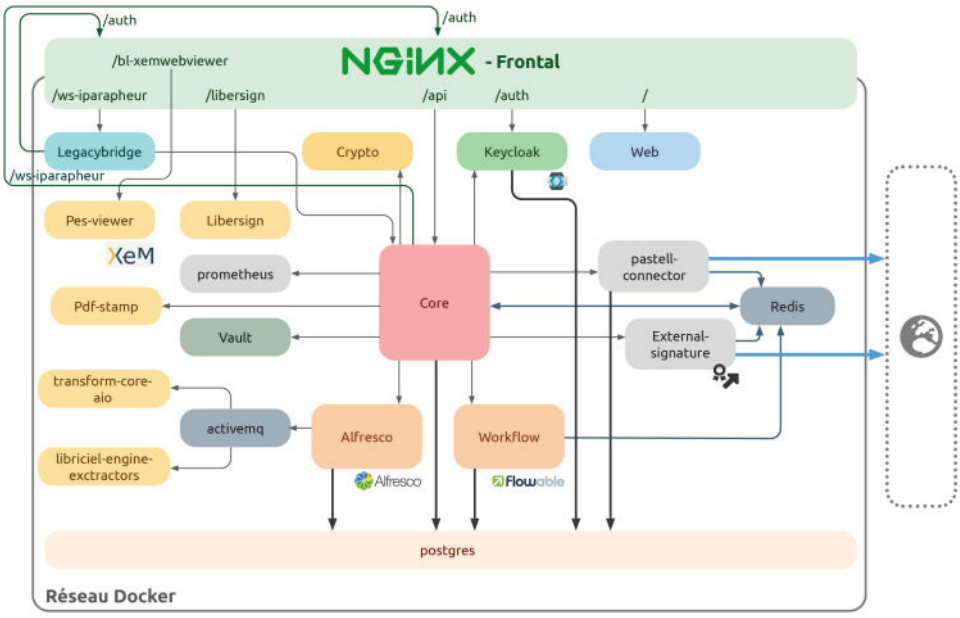
Ressource	Destination	Protocole	Port TCP
OS	ressources.libriciel.fr	HTTPS	443
OS	bootstrap.pypa.io	HTTPS	443
OS	download.docker.com	HTTPS	443
OS	omnitruck.chef.io	HTTPS	443
OS	deploiement.libriciel.fr	HTTPS	443
OS	rubygems.org	HTTPS	443

Voici la liste des URL utilisées depuis internet dans la phase de RUN (production) :

Ressource	Destination	Protocole	Port TCP
conteneurs	Service de messagerie	SMTP	25
conteneurs	Annuaire AD / LDAP	LDAP	389 / 636
conteneurs	SSO OPENID	OIDC Oauth2	443
conteneurs	Site libersign.libriciel.fr	HTTPS	443
conteneurs	Site validca.libriciel.fr	HTTPS	443
conteneurs	Site update.libriciel.fr	HTTPS	443
conteneurs	Site registry.libriciel.fr	HTTPS	443
conteneurs	Site hubdocker.libriciel.fr	HTTPS	443
conteneurs	Site sentry.libriciel.fr	HTTPS	443

5. SCHÉMA D'ARCHITECTURE

Le schéma d'architecture décrit les briques logicielles utilisées.



architecture de l'application

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

L'accès utilisateur à iparapheur 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* : Chaque instance d'iparapheur (ex : test, qualification, production) doit être hébergée sur sa propre machine.

6. BRIQUES TECHNIQUES

Voici la liste des conteneurs Docker utilisés.

Image Docker	Nom du conteneur	Fonction
registry.libriciel.fr:443/public/signature/ip-nginx:1.24.0.3	nginx	Frontal web
registry.libriciel.fr:443/public/signature/ip-core:1.10.7	ip-core	Fait le lien entre tous les services
registry.libriciel.fr:443/public/signature/ip-web:1.9.7	web	Affichage du site
registry.libriciel.fr/public/signature/workflow:1.10.3	workflow	Gérer les circuits
registry.libriciel.fr:443/public/signature/pes-viewer:2.0.9	pes-viewer	Visionneuse XML
registry.libriciel.fr/public/signature/libersign:3.1.0	libersign	Applet de signature
registry.libriciel.fr/public/signature/crypto:3.0.12	crypto	Outil de signature
registry.libriciel.fr/public/signature/pdf-stamp:2.6.4	pdf-stamps	Worker d'envoi des notifications mail
registry.libriciel.fr/public/signature/iparapheur-connector:1.3.11	iparapheur-connector	Connecteur iparapheur (mails sécurisés)
registry.libriciel.fr/public/signature/external-signature-connector:1.7.2	external-signature-connector	Brique pour la signature externe
registry.libriciel.fr/public/signature/legacy-bridge:1.5.22	legacy-bridge	Assure la rétro-compatibilité avec l'ancienne API en SOAP
registry.libriciel.fr:443/public/signature/ip-alfresco:23.1.0.0	alfresco	Stocker les données
registry.libriciel.fr:443/public/signature/alfresco-transform-core-aio:3.1.1.0	alfresco-transform-core-aio	Sous-composant d'Alfresco, en charge de la transformation des documents en PDF
registry.libriciel.fr:443/public/signature/ip-alfresco-transform-extractors:1.3.1	libriciel-engine-extractors	Sous-composant d'Alfresco, en charge de l'extraction des données des documents
registry.libriciel.fr/public/signature/ip-prometheus:2.47.1.1	prometheus	Gestions des métriques système des conteneurs
registry.libriciel.fr/public/signature/ip-vault:1.7.10.3	vault	Gestion des cachets serveurs
hubdocker.libriciel.fr/alfresco/alfresco-activemq:5.16.5-jre11-rockylinux8	alfresco-activemq	Sous-composant interne d'Alfresco
hubdocker.libriciel.fr/postgres:15.4	postgres	Base de données de l'application
hubdocker.libriciel.fr/redis:6.2.12-alpine	redis	Gestion Cache
hubquayio.libriciel.fr/keycloak/keycloak:21.1.2.0	keycloak	Gérer les autorisations et les permissions

6.1. Répertoires de travail

Voici les répertoires de travail nécessaires, ces derniers peuvent varier et être édités uniquement dans le fichie `.env`.

Le fichier `docker-compose.yml` est un template qui sera remplacé régulièrement pour la mise à jour de patch, il ne doit pas être modifié.

Point de montage hôte	Commentaire
`/data`	Contient les données et configurations

6.2. Autres points notables

L'opération d'installation nécessite des droits d'administrateur (root) afin :

- D'installer les packages de distribution GNU/Linux correspondant aux pré-requis, ainsi que l'application,
- De configurer et relancer les services docker,
- De mettre à jour périodiquement la politique de sécurité HTTPS,
- De lancer/arrêter l'application iparapheur, effectuer les sauvegardes.

7. POSTE CLIENT

L'application iparapheur est développée dans le respect des standards du web (standard W3C), et nécessite les particularités suivantes :

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

7.1. Navigateurs compatibles

Les logiciels produits par Libriciel SCOP sont développés principalement pour Google Chrome et Mozilla Firefox.

Libriciel SCOP assure la compatibilité de tous ces logiciels avec :

- La dernière version stable de Google Chrome,
- La dernière version de Mozilla Firefox,
- Les versions ESR de Mozilla Firefox maintenues par Mozilla.

Bien que développés pour les standards du web, le fonctionnement et l'affichage des logiciels produits par Libriciel SCOP ne sont pas garantis :

- Sur d'autres versions de Google Chrome (beta, canary) ou Mozilla Firefox (ESR non-maintenues, anciennes versions),
- Sur d'autres navigateurs (Microsoft Internet Explorer, Microsoft Edge, Apple Safari, Opera...),
- Sur les technologies de bureau à distance (Citrix XenApp, Citrix XenDesktop, Microsoft RDS, Microsoft Terminal Server...), en particulier pour les fonctionnalités de signature électronique.

7.2. Systèmes d'exploitation compatibles

D'une manière générale, Libriciel assure la compatibilité côté client avec la plupart des systèmes d'exploitation grand-public maintenus par leurs distributeurs et permettant de faire fonctionner les navigateurs compatibles.

Néanmoins, le fonctionnement et l'affichage des logiciels produits par Libriciel SCOP ne sont garantis que sur les versions du système Microsoft Windows maintenues par Microsoft à destination des postes clients.

En particulier, les outils de signature (Libersign) ne sont développés que pour Microsoft Windows sur les architectures Intel-x86 et AMD-64, et ne fonctionnent pas avec d'autres systèmes d'exploitations.

Les systèmes d'exploitation suivants sont non supportés, car hors du support de Microsoft : Windows XP, Vista, Windows 7 et 8.

7.3. Signature électronique sur poste PC Windows

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

- Pour Mozilla Firefox, Google Chrome, Microsoft Edge, ou Opera : pas "d'applet JAVA", car une extension de navigateur est utilisée, en liaison 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.

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. La version sortie en janvier 2020 dénommée "Edge (Chromium)" permet l'installation des extensions du Chrome-web-store. Avec l'extension Libersign du Chrome-web-store, il devient possible de signer électroniquement avec ce navigateur.

7.4. 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. Sur les matériels Apple, seule la virtualisation Windows permet de signer électroniquement : par exemple, avec "VMware Fusion" ou "Parallels".

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.

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 iparapheur. 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 iparapheur) ne supporte pas les connexions de type SNI, par exemple :

- Si usage en poste client de WindowsXP et Internet-Explorer (configuration non supportée 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 iparapheur 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 :

- deux enregistrements dans le service DNS :
  - Accès web sur `iparapheur.dom.local` ,
  - Accès web-services sur `secure-iparapheur.dom.local` (pour les applications métiers utilisant le `legacy-bridge`)
- d'acquérir le ou les certificat(s) électronique(s) protégeant les noms FQDN*iparapheur.dom.local* + *secure-iparapheur.dom.local*

8.3. Chiffrement HTTPS et sécurité TLS

Le protocole de sécurisation TLS a évolué dans sa version 1.3, voir la RFC8446. Cela donne les possibilités de sécurisation suivantes :

- SSLv2, SSLv3 : pas suffisamment robuste, abandonné pour iparapheur,
- TLS 1.0, TLS 1.1 : actifs par défaut, modifiable dans la configuration,
- TLS 1.2 : actif par défaut, modifiable dans la configuration,
- TLS 1.3 : inactif par défaut.

L'ANSSI recommande de prendre en charge la version "`TLS 1.3`". En particulier, dans son document de "Recommandations de sécurité relatives à TLS" :

- [R3] : Privilégier TLS 1.3 et accepter TLS 1.2,
- [R4] : Ne pas utiliser SSLv2, SSLv3, TLS 1.0 et TLS 1.1.

Cependant, ces recommandations ANSSI ne sont pas toujours adaptées à l'environnement d'exploitation et aux clients (navigateurs, applications métier) qui se connectent à iparapheur.

Client navigateur	**TLS 1**	**TLS 1.1**	**TLS 1.2**	**TLS 1.3**
InternetExplorer 11	oui	oui	oui	NON
Edge 12-18	oui	oui	oui	NON
Edge Chromium 79+	oui	oui	oui	oui
Chrome 70+	oui	oui	oui	oui
Firefox 63+	oui	oui	oui	oui

Technologie d'Application métier	**TLS 1.2**	**TLS 1.3**
.NET sur Windows Server	depuis 2008r2	non
OpenSSL stack	v1.0.1a et +	v1.1.1 et +
Java stack	1.7.0_u131 et +	Java 11

De nombreuses applications métier actuellement en production s'appuient sur des composants dans des versions antérieures à celles indiquées dans le tableau ci-dessus, donc inaptes aux recommandations concernant TLSv1.3 et/ou TLSv1.2 :

- Les applications basées sur "Axis 1.4" pour leurs web-services ne sont pas capables de tenir une négociation TLSv1.2, revenant en TLSv1. Exemple parmi d'autres, certaines versions de GFI-GECCO dialoguent avec iparapheur en "TLSv1", comme l'application KOLOK d'Arawak.

Ressources :

- TLS 1.2
- Can I use
- Site Microsoft
- La Chine bloque le HTTPS utilisant TLS 1.3 et ESNI

8.4. Couplages annuaires, SSO

8.4.1. Capacités LDAP / ActiveDirectory

Il est possible de synchroniser l'application iparapheur avec les comptes utilisateurs gérés sur 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 d'iparapheur.

8.4.2. Capacités SSO

L'application iparapheur 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). Peu importe la version du serveur CAS, du moment que la version de protocole est respectée. À noter que le protocole CASv1 n'est pas supporté.
- "Keycloak" : testé avec succès sur le protocole OpenID Connect.
- "LemonLDAP::NG".

Se rapprocher de Libriciel SCOP pour les modalités techniques et commerciales d'accompagnement à la mise en place.