iparapheur

Prérequis pour une installation d'iparapheur en version 5.2

Version 5.2

Libriciel SCOP

Document

Auteur	Romain DE FILIPPIS	***Date de diffusion***	09/12/24
Chef de projet	Adrien BRICCHI	***N° de version***	5.2

Évolution du document

Version	Auteur	Nature des changements	Date
1.0	Romain DE FILIPPIS	Création du document.	09/12/24

Licence

Table des matières

1. PRÉSENTATION

1.1. Objectifs

Ce manuel décrit succinctement les pré-requis à l'installation d'un serveur iparapheur version 5.2 sur un système d'exploitation GNU/Linux.

2. LISTE DES SYSTÈMES D'EXPLOITATION SUPPORTÉS

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

OS	Statut	Commentaires
Ubuntu LTS en cours de support par L'éditeur Canonical	**Supporté**	OS de référence, préconisé, version serveur sans interface graphique
RHEL 8	**Supporté**	Sous LICENCE, version serveur sans interface graphique

- Les OS DEBIAN ne sont pas supportées.
- Les versions NON LTS d'Ubuntu Server ne sont pas supportées.
- Les versions clone de RHEL ne sont pas supportées.
- Les versions serveur sans interface graphique sont à favoriser.

2.1. CPU

Il est nécessaire que votre CPU soit compatible x86-64-v2 (pour apporter la prise en charge des instructions SSE4.2)

2.2. Docker

La version 5.2 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.

2.3. 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	27.1.x	Moteur Docker Community Edition
docker compose	2.29.x	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 (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

4.1.2. Phase d'instalation

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

Ressource	Destination	Protocole	Port TCP
Deploiement	*.libriciel.fr	HTTPS	HTTPS
ressources	ressources.libriciel.fr	HTTPS	443
Deploiement	deploiement.libriciel.fr	HTTPS	443
Deploiement	mattermost.libriciel.fr	HTTPS	443
Deploiement	nexus.libriciel.fr	HTTPS	443
Deploiement	curl.libriciel.fr	HTTPS	443
Deploiement	bootstrap.pypa.io	HTTPS	443
Deploiement	packagecloud.io	HTTPS	443
Docker CE	download.docker.com	HTTPS	443
OS	fr.archive.ubuntu.com	HTTPS	443

4.1.3. Contexte RHEL et depot satelitte

Dans le cas où vous souhaiteriez utiliser un `dépôt satellite` il est important d'ajouter plusieurs dépôt dont le `dépôt Docker` et le `dépôt EPEL` (Extra Packages for Enterprise Linux) qui sert pour l'installation de Prometheus Node Exporter avec l'outil de gestion de paquets "dnf".

Prometheus Node Exporter est installé par un fichier `rpm` téléchargé sur `packagecloud.io` si ce flux est ouvert, vous n'avez pas besoin d'ajouter le `dépôt EPEL` à votre `dépôt satellite`.

4.1.4. Phase de production

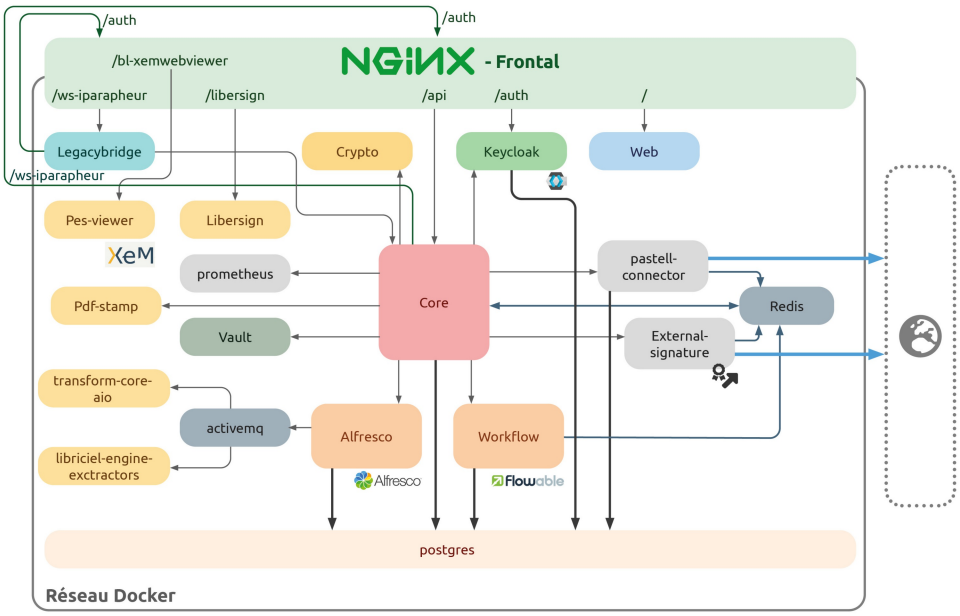
Voici la liste des URL utilisées depuis internet dans la phase de RUN (production) :

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

> Pour utiliser les connecteurs de signature externe (Yousign, Universign...), il faut ouvrir les urls en lien avec ceux-ci.

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.domaine.invalid**.

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:1.26.1.0	nginx	Frontal web
registry.libriciel.fr:443/public/signature/ip-core:1.13.0	ip-core	Fait le lien entre tous les services
registry.libriciel.fr:443/public/signature/ip-web:1.11.1	web	Affichage du site
registry.libriciel.fr/public/signature/workflow:1.11.13	workflow	Gérer les circuits
registry.libriciel.fr:443/public/signature/pes-viewer:2.0.13	pes-viewer	Visionneuse XML
registry.libriciel.fr/public/signature/libersign:3.1.2	libersign	Applet de signature
registry.libriciel.fr/public/signature/crypto:3.1.7	crypto	Outil de signature
registry.libriciel.fr/public/signature/pdf-stamp:2.7.2	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:1.7.9	external-signature-connector	Brique pour la signature externe
registry.libriciel.fr/public/signature/legacy-bridge:1.6.3	legacy-bridge	Assure la rétro-compatibilité avec l'ancienne API en SOAP
registry.libriciel.fr:443/public/signature/ip-alfresco:23.2.1.0	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:2.47.1.3	prometheus	Gestions des métriques système des conteneurs
registry.libriciel.fr/public/signature/ip-vault:1.15.6.2	vault	Gestion des cachets serveurs
registry.libriciel.fr:443/public/signature/ip-activemq:5.16.7.0	alfresco-activemq	Sous-composant interne d'Alfresco
registry.libriciel.fr:443/public/signature/ip-postgresql:15.6.1	postgres	Base de données de l'application
registry.libriciel.fr:443/public/signature/ip-redis:6.2.14.1	redis	Gestion Cache
registry.libriciel.fr:443/public/signature/ip-keycloak:23.0.7.2	keycloak	Gérer les autorisations et les permissions
registry.libriciel.fr	postgres-periodic-tasks	Gestion de la base de données
registry.libriciel.fr:443/public/libriciel/ls-docker-cacerts:0.4.0	ca-certs	Gestion du truststore et des certificats

> Tous les conteneurs sont configurés pour démarrer au boot du serveur.

Tous les conteneurs peuvent être contrôlés via le composant `docker compose`.

6.1. Répertoires de travail

Voici les répertoires de travail nécessaires, ces derniers peuvent varier et être édités uniquement dans le fichier `.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. Certificats SSL pour service HTTPS

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

- un enregistrement dans le service DNS :
    - Accès web sur `iparapheur.domaine.invalid` ,
- d'acquérir le certificat électronique protégeant le nom FQDN*iparapheur.domaine.invalid*

8.2. Certificat HTTPS

Lors de l'installation iparapheur par Libriciel, un certificat auto signé est créé si aucun certificat n'a été fourni avant.

Les certificats sont définis par l'emplacement des variables `CERTIFICATE_FULLCHAIN_PATH` et `CERTIFICATE_PRIVKEY_PATH` présentes dans le `.env`, ainsi que dans un truststore pour que l'AC soit connue des différentes briques qui vont devoir communiquer.
Le chemin par défaut est `/data/iparapheur/certificate/ssl`

Vous avez la possibilité d'utiliser un certificat signé par une autorité de certification reconnue (Globalsign, Certinomis, Verisign ou autre), ou de générer vous-même votre certificat HTTPS depuis votre PKI.

Dans le second cas, il faudra un avertissement et une exception à ajouter au niveau du navigateur, et rajouter l'AC racine et intermédiaire dans le dossier `/data/iparapheur/certificate/local-cacerts/` pour qu'il soit ajouté automatiquement au truststore.

Les certificats doivent avoir le nommage suivant :

- `fullchain.pem` (Certificat racine, certificat intermédiaire, certificat server)
- `privkey.pem` (Clé privée)

8.3. Gestion du truststore et des certificats

Si vous souhaitez ajouter un certificat (dans le cas d'une connexion via LDAPS ou SSO), la prise en compte du certificat sera effective en ajoutant votre certificat au format (.crt) dans le dossier `/data/iparapheur/certificate/local-cacerts/` .

Un redémarrage sera nécessaire pour prendre en compte les nouveaux certificats.

```
cd /opt/iparapheur/current/
docker compose down -v && docker compose up -d
```

8.4. Couplages

8.4.1. Capacités LDAP/LDAPS (ActiveDirectory/OpenLDAP)

Il est possible de synchroniser l'application iparapheur avec les comptes utilisateurs gérés sur un annuaire de LDAP (OpenLDAP), ainsi que Microsoft ActiveDirectory.

Il est `obligatoire` conseillé de créer un groupe de sécurité spécifique afin de ne synchroniser que les comptes habilités à utiliser i-Parapheur.

Par exemple, on crée un groupe ayant pour DN `CN=iparapheur, OU=users, DC=libriciel, DC=fr` Pour lequel tous les utilisateurs à synchroniser seront membres.

> Il est `obligatoire` de nous fournir un `memberOf` (Filtre d'appartenance à un groupe spécifique).

Exemple :

`(memberOf=CN=Développeurs,OU=Groupes,DC=exemple,DC=com)`

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.

> Pour le cas du LDAP Sécurisé il est**obligatoire** de nous fournir le certificat de votre server LDAPS.

Lors de la planification, une fiche d'information vous est fournie, celle-ci doit être complétée pour permettre aux installateurs de mener à bien l'intervention.

> Il est important que le groupe LDAP avec lequel l'application sera couplée ne soit pas vide, et qu'il contienne au moins un utilisateur. (personne présente le jour de l'intervention) Vous pouvez aussi créer un compte et nous fournir le (login/mot de passe) si vous souhaitez que nous soyons autonomes sur les tests de connexion.

Pour les modalités techniques et commerciales d'un accompagnement à la mise en place, merci de contacter Libriciel SCOP.

8.4.2. Capacités SSO

L'application iparapheur peut être connecté avec tout système pleinement compatible OpenID Connect.

> L'interconnexion avec la brique Microsoft ADFS sous protocole OIDC Oauth 2 n'est pas fonctionnelle et non supporté.

Pour les modalités techniques et commerciales d'un accompagnement à la mise en place, merci de contacter Libriciel SCOP.

> Dans certains cas, il est nécessaire de nous fournir un certificat de votre server d'authentification, cela dépend de la configuration de celui-ci.