Libriciel SCOP

Pré-requis Pastell

Version 5.0

Libriciel SCOP

Libriciel SCOP

Document

Auteur	Arnaud LAVIT	**Date de diffusion**	06/02/2026
Chef de Projet	Maxime REYROLLE	**N° de version**	5.0

Évolution du document

Version	Auteur	Nature des changements	Date
1.0	Arnaud LAVIT	Création du document pour la version 5.0	25/11/2025
1.1	Maxime Reyrolle	Ajout du dimensionnement lié à l'archivage	06/02/2026
1.2	Arnaud LAVIT	Ajout des pré-requis pour le glaneur SFTP	17/03/2026
1.3	Arnaud LAVIT	Ajout des pré-requis pour le SNI	19/03/2026
1.4	Arnaud LAVIT	Pré-requis CPU compatible x86-64-v3	17/08/2026

Licence

Ce document n'est pas libre de droits.

Ce manuel est publié sous la licence Creative Commons avec les particularités “Paternité – Partage à l'identique” (également connue sous l'acronyme CC BY-SA).

Détails de cette licence : Attribution - Partage dans les Mêmes Conditions 2.0 France



Libriciel SCOP

Table des matières

1 Présentation....4
2 Liste des systèmes d'exploitation supportés....5
2.1 CPU....5
2.2 Docker....5
2.3 Briques techniques....5
3 Dimensionnement et ressources....6
4 Communication réseau....8
5 Schéma d'architecture....9
6 URL....10
7 Briques techniques....11
7.1 Répertoires de travail....11
7.2 Glaneur SFTP....12
7.3 Prérequis en environnement avec reverse-proxy....12
7.4 Mail....12
7.5 Couplages annuaires, SSO....12
7.5.1 Capacités LDAP / ActiveDirectory....12
7.5.2 Capacités SSO....12
8 Navigateurs compatibles....14
9 Systèmes d'exploitation compatibles....15
10 Accès à un compte privilégié....16
11 Accès aux bases de données....17
12 Certificats HTTPS....18
13 Limitations du logiciel....19

1 Présentation

Vous trouverez ci-dessous la liste de tous les éléments permettant la mise en œuvre du logiciel pastell.

2 Liste des systèmes d'exploitation supportés

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

OS	Statut	Commentaires
Ubuntu (version LTS en cours de support par l'editeur Canonical)	**Supporté**	OS de référence
RHEL 8.10	**Supporté**	Sous LICENCE
RHEL 9.6	**Supporté**	Sous LICENCE
RHEL 10.0	**Supporté**	Sous LICENCE
Rocky Linux 9.6	**Supporté**	
Rocky Linux 10.0	**Supporté**	

- Les OS DEBIAN ne sont pas supportés.
- Les versions non LTS d'Ubuntu Server ne sont pas supportées.
- Les distributions clones de RHEL autres que Rocky Linux ne sont pas supportées.

2.1 CPU

Il est nécessaire que votre CPU soit compatible x86-64-v3 (pour apporter la prise en charge des instructions SSE4.2)

2.2 Docker

La version 5.0 de Pastell est fournie sous forme de conteneur fonctionnant avec Docker Community Edition, qui seradéployé sur un serveur virtuel. L'outil **Docker Compose** est utilisé pour le déploiement.

- L'utilisation dans un environnement Docker Swarm existant n'est pas supportée.
- L'utilisation avec un orchestrateur Kubernetes (OpenShift, Tanzu) n'est pas supportée.

Les images Docker de nos produits ne peuvent pas être modifiées 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	version stable supportée par docker	Moteur Docker Community Edition
docker compose	version stable supportée par docker	Plugin docker compose

3 Dimensionnement et ressources

Le dimensionnement du disque peut se faire sur une partition unique ou sur plusieurs partitions, selon le choix del'exploitant technique.

Le formatage des partitions en **LVM** est fortement recommandé, car il permet d'augmenter l'espace disque à chaud.

Le tableau suivant présente des valeurs indicatives (susceptibles d'évoluer) :

Ressource	Ressources test	Ressources production	Commentaires
Disque système (racine)	30 Go	30 Go	Contiendra l'OS, les logs, les images docker
Disque de données (/data)	30 Go	80 Go	Contiendra la base de données, la configuration ainsi que les données de tous les composants
Espace "swap"	1 Go	1 Go	
CPU	2	2	
RAM	4 Go	4 Go	

Le dimensionnement de l'espace disque dépend très largement des types de flux traités par Pastell.

Les documents sont stockés dans le workspace : **/data/pastell/app/workspace**.

Pastell les conserve jusqu'à leur suppression éventuelle (purge).

Attention, le versement SAE peut être particulièrement consommateur de ressource disque en cas de transfert volumineux(vidéo par exemple).

Les données qui transitent seront stockées temporairement dans le répertoire **/data/pastell/app/tmp**

Pastell doit pouvoir :

- Dans le workspace : **/data/pastell/app/workspace**
  - Stocker la donnée source
  - Stocker l'archive créée
- Dans l'espace temporaire : **/data/pastell/app/tmp**
  - Copier la donnée source
  - Dézipper si nécessaire
  - Créer l'archive
  - Découper l'archive en morceaux (chunks) pour permettre l'envoi à asalae

L'espace temporaire n'est utilisé que pendant le traitement de l'archive, il est libéré une fois la génération etl'envoi au SAE terminé.

L'espace utilisé dans le workspace n'est pas libéré tant que le dossier n'est pas purgé (supprimé) de pastell.

Dans ce cas, et si les hypothèses suivantes sont vérifiées :

- les flux sont versés les uns après les autres et non en parallèle,
- les flux font un circuit complet : versement, acquittement, acceptation, purge dans la journée.

Alors, il convient de respecter les pré-requis suivants sur l'espace libre :

Taille totale de versement journalier	Taille minimum de l'espace temporaire : /data/pastell/app/tmp	Taille minimum du workspace : /data/pastell/app/workspace
1Go	20 Go	30 Go
5 Go	25 Go	30 Go
10 Go	40 Go	40 Go
20 Go	70 Go	70 Go
N Go	10 + 3xN Go	10 + 2xN Go

Si les dossiers ne sont pas purgés dans la journée, la taille du workspace devra être augmentée pour traiter de nouveauxtransferts.

Dans tous les cas, la taille du système de fichier contenant le répertoire temporaire doit présenter une placedisponible d'au moins trois fois le plus gros fichier versé sur Pastell.

Si le partitionnement choisi diffère de celui recommandé (deux partitions : une racine / et une partition /data/), ilest impératif de vérifier que le répertoire /var/lib/docker se trouve sur une partition disposant d’au moins 15 God’espace libre.

4 Communication réseau

Voici la liste des ports utilisés en entrée et sortie.

Protocole	Commentaires
HTTP port 80 TCP	redirection vers HTTPS
HTTPS port 443 TCP	Accès utilisateur et réception des flux (API)

Certaines ressources doivent être accessibles depuis internet.

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

Ressource	Destination	Protocole	port TCP
images docker	registry.libriciel.fr	HTTPS	443
images docker	hubdocker.libriciel.fr	HTTPS	443
livrables	nexus.libriciel.fr	HTTPS	443
livrables	ressources.libriciel.fr	HTTPS	443
livrables	curl.libriciel.fr	HTTPS	443
livrables	galaxy.ansible.com	HTTPS	443
livrables	download.docker.com	HTTPS	443

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

Source	Destination	Protocole	port TCP
Conteneurs	registry.libriciel.fr	HTTPS	443
Conteneurs	hubdocker.libriciel.fr	HTTPS	443
Conteneurs	allo.libriciel.fr	HTTPS	443

> La liste complète des éléments est décrite dans la documentation d'exploitation.

La version 5.0 de Pastell est compatible avec l'utilisation de proxy sortant.

5 Schéma d'architecture

Le schéma d'architecture décrit les briques logicielles utilisées.

Ces briques sont présentes sur un seul et même serveur.

Pastell peut être utilisé dans un réseau local, ou être utilisé pour la réception de flux provenant d'Internet.

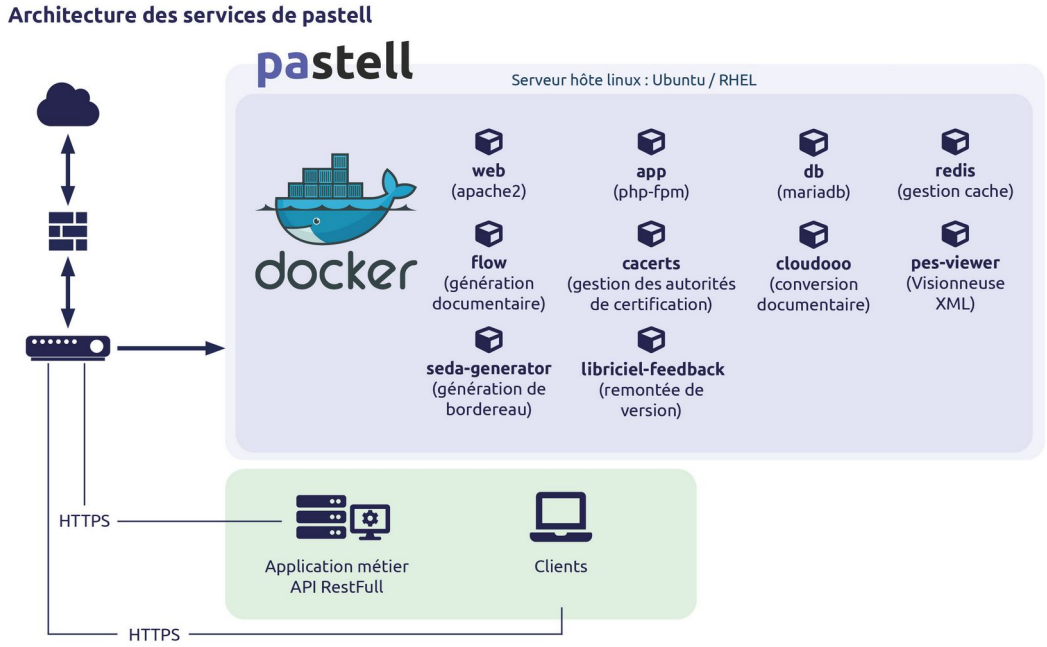


schéma d'architecture de la plateforme

6 URL

L’accès à Pastell se fait via un navigateur. Une URL dédiée sous forme de domaine ou de sous-domaine est nécessaire, parexemple : **pastell.mondomaine.fr**.

Pour un accès depuis l’extérieur du réseau :

L’URL doit être publique.

Les ports 80 (HTTP) et 443 (HTTPS) doivent être ouverts depuis l’extérieur (via NAT, reverse proxy, etc.).

Remarque : Il est recommandé de ne pas installer plusieurs instances de Pastell (ex : test, prod) sur un même serveur.

Une URL dédiée est également nécessaire pour la fonction de mail sécurisé, par exemple : **pastell-mailsec.mondomaine.fr**.

7 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	version stable supportée par docker	
docker compose plugin	version stable supportée par docker	

Briques logicielles :

Composant	Version	Commentaires
PHP	8.4.x	Image Docker
APACHE	2.4.x	Image Docker
MariaDB	11.4.x	Image Docker
REDIS	8.2.x	Image Docker
SEDA-GENERATOR		Image Docker
CLOUDOOO		Image Docker
PES-VIEWER		Image Docker
CA-CERTS		Image Docker
FLOW		Image Docker
LIBRICIEL-FEEDBACK		Image Docker

7.1 Répertoires de travail

Point de montage hôte	Commentaire
/opt/pastell/	Contient les fichiers de configurations propres au contexte d'exploitation
/data/	Contient les données et configurations
/data/pastell/web/certificates/	contient les certificats
/var/lib/docker	contient les images docker

Le fichier **/opt/pastell/current/.env** contient les directives de configuration.

Le fichier **/opt/pastell/current/compose.yaml** est remplacé à chaque mise à jour de l'application ; il ne doit donc pasêtre modifié.

7.2 Glaneur SFTP

Le glaneur SFTP peut se connecter à un serveur SFTP distant sans contrainte particulière sur le système de fichiers utilisé côté distant. En revanche, lorsque le service est hébergé sur le même serveur que pastell, seuls les systèmes de fichiers locaux de type extFS et XFS sont supportés. Les systèmes de fichiers réseau tels que CIFS ou NFS ne sont pas compatibles dans ce cas, y compris lorsqu'ils sont montés localement et exposés comme des répertoires standards.

7.3 Prérequis en environnement avec reverse-proxy

Dans un contexte où l'application est exposée derrière un reverse-proxy (Nginx, Apache, Traefik, HAProxy, etc.), la gestion du SNI (Server Name Indication) doit être correctement activée et configurée côté reverse-proxy.

Le SNI permet d'indiquer au serveur cible le nom d'hôte attendu lors de l'établissement de la connexion TLS. Sans cela, le serveur peut répondre avec un mauvais certificat ou refuser la requête.

7.4 Mail

Il est essentiel de renseigner plusieurs adresses e-mail nécessaires au bon fonctionnement de l'application.

Adresses pour les notifications système
Une ou plusieurs adresses doivent être renseignées afin de recevoir les notifications techniques (par exemple : tâchessuspendues).

Adresse e-mail du compte administrateur
Lors du premier démarrage de l'application, un utilisateur administrateur est automatiquement créé. Ce compte doitimpérativement être associé à une adresse e-mail valide, car il est impossible de créer un compte sans e-mail.Cette adresse doit être fonctionnelle : la récupération du mot de passe s'effectue uniquement via la fonction Mot depasse oublié, qui envoie la procédure de réinitialisation sur l'adresse liée au compte.

Adresse e-mail émettrice
Selon la configuration de votre serveur SMTP, certaines adresses peuvent ne pas être autorisées. Il est donc nécessairede nous fournir une adressee-mail valide et capable d'émettre depuis votre serveur SMTP. Toutes les communications envoyées par l'application utiliseront cette adresse.Exemple: **ne-pas-repondre@domain.invalid**.

7.5 Couplages annuaires, SSO

7.5.1 Capacités LDAP / ActiveDirectory

Il est possible de synchroniser l'application Pastell avec les comptes utilisateurs présents dans un annuaire LDAP (OpenLDAP) ou Microsoft Active Directory.

Si un tel annuaire existe déjà, son organisation doit être connue de l'exploitant et communiquée au préalable. Celapermet de configurer correctement le lien avec Pastell afin que les comptes utilisateurs enregistrés dans l'annuairepuissent être importés et reconnus par l'application.

7.5.2 Capacités SSO

L'application Pastell peut être intégrée avec tout système entièrement compatible OpenID Connect.

Elle peut également être connectée à certains systèmes de Web-SSO, notamment :

- Apereo CAS (anciennement Jasig CAS) : prise en charge des protocoles CAS v2 et v3, avec utilisation obligatoire duProxy Granting Ticket (PGT).À noter : le protocole CAS v1 n’est pas supporté.La version du serveur CAS importe peu, tant que la version du protocole est conforme.
- Keycloak : intégration validée avec succès via le protocole OpenID Connect / OAuth2.
- LemonLDAP::NG.

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

8 Navigateurs compatibles

Les logiciels produits par Libriciel SCOP sont développés principalementpour 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 logicielsproduits 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.

9 Systèmes d'exploitation compatibles

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

Néanmoins, le fonctionnement et l'affichage des logiciels produits par Libriciel SCOP ne sont garantisque 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 Windows sur les architectures Intel x86 et AMD 64 et ne fonctionnent pas avecd'autres systèmes d'exploitations.

10 Accès à un compte privilégié

Les installations nécessitent un accès à la machine avec un compte privilégié, généralement le compte root avec un UID à zéro.

Ce compte peut également être utilisé pour lancer des opérations le nécessitant comme allouer des ports privilégiés (80, 443).

L'absence d'accès à un compte privilégié rendra l'installation et l'utilisation du logiciel impossible.

11 Accès aux bases de données

L’accès par une application tierce aux bases de données des logiciels Libriciel est :

- interdit en mode écriture
- vivement déconseillé en accès lecture uniquement

Dans le cas où vous souhaiteriez brancher un outil sur les bases de données des logiciels, nous ne serons pas en mesure de prendre en charge au niveau de la maintenance les ralentissements que cela pourrait entraîner. Autrement dit, en cas de ralentissement de l'application, il serait nécessaire de débrancher vos outils de la base de données afin de voir si le problème persiste. Si tel n'était pas le cas, Libriciel n'apporterait aucune aide sur la résolution du problème.

Par ailleurs, le schéma des bases de données et plus généralement la définition de celles-ci (tables, vues, index, procédures stockées, ...) sont susceptibles d'évoluer à tout moment, y compris dans des patchs, voire dans le cas des hotfixes posés suite à une opération de maintenance.

12 Certificats HTTPS

Afin d'assurer un niveau de sécurité suffisant pour les installations hébergées par vos soins ("on premise") de nos logiciels, nous vous conseillons (dans l'ordre de préférence) :

- L'utilisation ou acquisition d'un certificat issu d'une autorité reconnue de confiance par les principaux navigateurs.
- La mise en place de certificat via let's encrypt (https://letsencrypt.org/fr/) uniquement si votre logiciel Libriciel SCOP est accessible sur Internet.Leur renouvellement pouvant être géré automatiquement, LIBRICIEL SCOP n'apporte aucun support sur ce composant.
- Vous pouvez également utiliser votre propre PKI si vous en gérez une.

Nous déconseillons l'utilisation d'une PKI externe non reconnue nativement par les navigateurs et autres systèmes d'exploitation.Nous déconseillons également l'utilisation de certificats auto-signés pour votre serveur web.La fourniture d'un certificat HTTPS est un pré-requis obligatoire à l'installation et utilisation de nos logiciels.

Si lors de l'installation, vous n'êtes pas en mesure d'en fournir un :

- Nous générerons un certificat auto-signé, valide un an.
- Celui-ci affichera une alerte de sécurité à chaque connexion par vos utilisateurs.
- Il ne permettra pas aux logiciels tiers (type Gestion financière) de se connecter nativement.

L'installation d'un tel certificat pourra être utilisée à des fins de formations et de tests, mais la plate-forme ne sera pas opérationnelle à 100% pour la production. Certaine partie pourrait également ne pas être opérationnelle y compris pour le test et la formation (exemple : connexion webdav).

Nous pourrons déployer dans le cadre de la prestation d'installation le certificat de votre choix (cf. les propositions ci-avant), dans le cas contraire, il vous faudra déployer le certificat adéquat par la suite (hors du cadre du support et de la maintenance)

13 Limitations du logiciel

Quelle que soit l'architecture, les valeurs suivantes sont considérées comme une utilisation hors-normes du produit et Libriciel ne pourra en garantir un fonctionnement correct.En fonction de l'architecture, il est possible que ces valeurs soient réduites.

- 2 millions de documents simultanés gérés dans la base de données
- 2 To de données maximum gérés par le workspace
- 20 millions de champs indexés
- 50 000 jobs maximums
- 10 000 entités