pastell

Pré-requis pour un déploiement de Pastell v4.1

Version 4.1

Libriciel SCOP

Document

Auteur	Arnaud LAVIT	***Date de diffusion***	07/06/2024
Chef de projet	Maxime REYROLLE	***N° de version***	4.1

Évolution du document

Version	Auteur	Nature des changements	Date
1.0	Arnaud LAVIT	Création du document pour la version 4.1	07/06/2024
1.1	Arnaud LAVIT	Mise à jour liste OS supportés	03/07/2024
1.2	Arnaud LAVIT	Mise à jour liste urls utilisées	13/08/2024
1.3	Arnaud LAVIT	Mise à jour liste conteneurs et urls utilisées	15/10/2024

Licence

Table des matières

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 supportés.

OS	Statut	Commentaires
Ubuntu (version LTS en cours de support par l'editeur Canonical)	**Supporté**	OS de référence
RHEL 8	**Supporté**	Sous LICENCE

- 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.

2.1. Docker

La version 4.1 de pastell est livrée sous forme de conteneur fonctionnant sous Docker community edition qui sera déployé sur 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	version stable suportée par docker	Moteur Docker Community Edition
docker compose	version stable suportée par docker	Plugin docker compose

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*Ces valeurs peuvent être amenées à 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 */data/*.

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

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

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.

Les données qui transitent seront stockées dans un répertoire de type tmpfs. (potentiellement dans /data)

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

Taille totale de versement journalier	**Taille minimum du système de fichier tmpfs**	**Taille minimum du système de fichier /data**
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 + 3xN Go

Pour les versements supérieurs à 20 Go, une étude complémentaire pourrait-être envisagée en fonction de la volumétrie supplémentaire.

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

En cas de partitionnement différent de celui proposé ici (2 partitions : une racine / et une `/data/`), il est nécessaire de vérifier que le répertoire `/var/lib/docker` soit sur une partition qui contient au moins 10 Go de 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	*.libriciel.fr	HTTPS	443
DOCKER	download.docker.com	HTTPS	443

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

Source	Destination	Protocole	port TCP
Tâche planifiée (entretien LiberSign)	libersign.libriciel.fr	HTTPS	443
Tâche planifiée (entretien validca)	validca.libriciel.fr	HTTPS	443
Conteneurs	registry.libriciel.fr	HTTPS	443
Conteneurs	hubdocker.libriciel.fr	HTTPS	443
Conteneurs	sentry.libriciel.fr	HTTPS	443
Conteneurs	allo.libriciel.fr	HTTPS	443

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

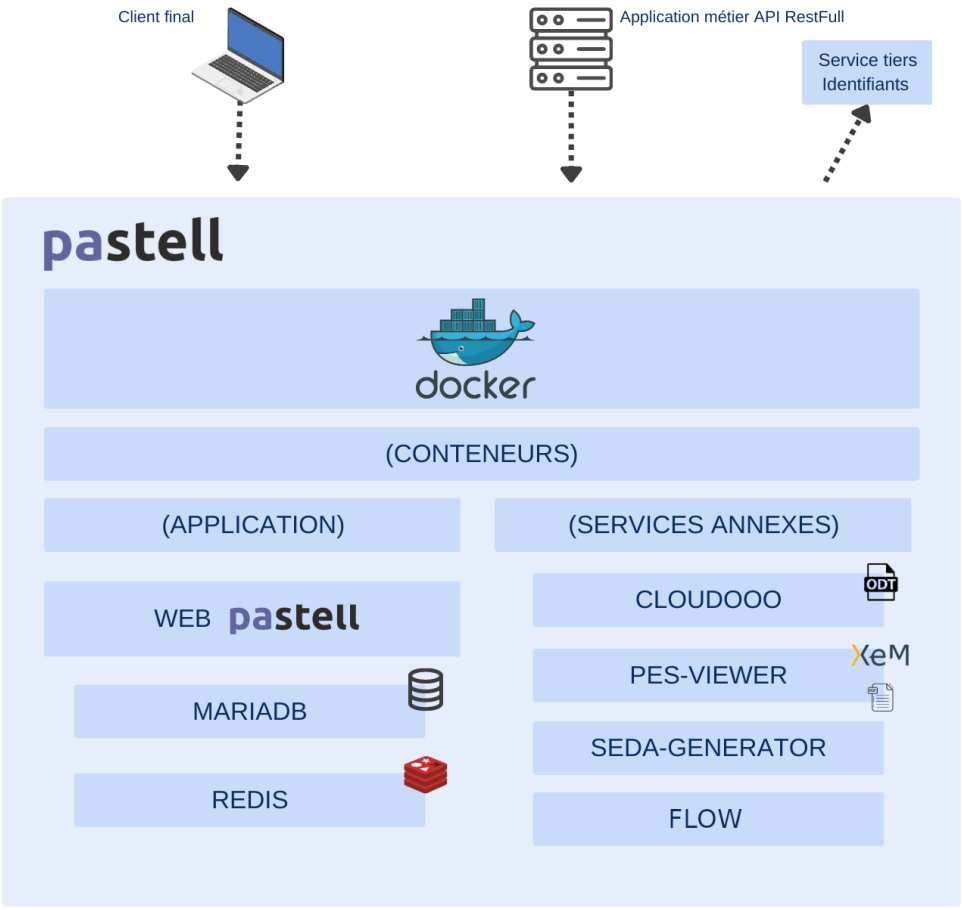
La version 4.1 de Pastell est compatible avec l'utilisation de proxy sortant.

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.



architecture de l'application

6. URL

L'accès à Pastell s'effectue par navigateur, une URL en domaine ou sous-domaine dédié sera nécessaire, ex **pastell.mondomaine.fr**.

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

- Une URL en domaine ou sous-domaine public.
- L'accès aux ports 80 HTTP et 443 HTTPS devront être ouverts depuis l'extérieur du réseau (ex : NAT, reverse proxy).

> *Remarque* : Plusieurs instances de Pastell (ex: test, prod) ne doivent pas être installées sur un même serveur.

Une URL dédiée sera nécessaire pour la fonction de mail sécurisé, ex **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 suportée par docker	
docker compose plugin	version stable suportée par docker	

Briques logicielles :

Composant	Version	Commentaires
pastell	4.1.x	Image Docker
PHP	8.1.x	Contenu dans l'image pastell
APACHE	2.4.x	Contenu dans l'image pastell
MariaDB	10.11.x	Image Docker
REDIS		Image Docker
SEDA-GENERATOR		Image Docker
CLOUDOOO		Image Docker
PES-VIEWER		Image Docker
FLOW		Image Docker
LIBRICIEL-FEEDBACK		Image Docker

7.1. Répertoires de travail

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

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

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
`/opt/pastell/`	Contient les fichiers de configurations propres au contexte d'exploitation
`/data/`	Contient les données et configurations
`/data/pastell/certificates/ssl`	contient les certificats
`/var/lib/docker`	contient les images docker

7.2. Mail

Il est important de renseigner plusieurs adresses mail qui sont nécessaires au bon fonctionnement de l'application.

- Une ou plusieurs adresses sur lesquelles les notifications système seront envoyé (Exemple : tâche suspendue) (Exemple : admin@domaine.local).
- Une adresse mail du compte admin Un utilisateur admin sera créé lors du premier démarrage de l'application, celui-ci doit obligatoirement être lié à un mail, car un compte ne peut pas être créé sans mail. Il est important qu'elle soit valide, car la récupération du mot de passe ne peut être effectuée qu'avec la fonction "mot de passe oublié" qui envoie une procédure de changement de mot de passe au mail du compte avec lequel il est associé (Exemple : admin@domaine.local).
- une adresse mail émettrice, selon la configuration de votre serveur SMTP, il se peut que certaines adresses mail ne soient pas acceptées, c'est pour cela qu'il faut nous fournir une adresse mail valide qui puisse émettre des mails depuis votre SMTP. Dès qu'un mail sera envoyé, c'est cette adresse qui sera utilisée. (Exemple : ne-pas-repondre@mairie-ville.fr, info@domaine.local)

7.3. Couplages annuaires, SSO

7.3.1. Capacités LDAP / ActiveDirectory

Il est possible de synchroniser l'application pastell 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 pastell. Ceci afin que les comptes d'utilisateurs inscrits dans l'annuaire soient importés et connus de pastell.

7.3.2. Capacités SSO

L'application pastell 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. Peu importe la version du serveur CAS, du moment que la version de protocole est respectée.
- "Keycloak" : testé avec succès sur 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.

7.4. 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 pastell, effectuer les backups

8. NAVIGATEURS COMPATIBLES

Les logiciels produits par Libriciel SCOP sont développés principalement pourGoogle 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.

9. SYSTÈMES D'EXPLOITATION COMPATIBLES

D'une manière générale, Libriciel assure la compatibilité côté client avec la plupart des systèmes d'exploitations 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 Windows sur les architectures Intel x86 et AMD 64 et ne fonctionnent pas avec d'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