refae

Pré-requis pour une installation de refae

Version 2.0

Libriciel SCOP

Libriciel SCOP

Document

Auteur	Antonio DA SILVA	**Date de diffusion**	15/05/2024
Chef de Projet	Florent VEYRES	**N° de version**	2.0

Évolution du document

Version	Auteur	Nature des changements	Date
1.0	Florent VEYRES	Création du document	05/10/2018
1.1	Florent VEYRES	Mise à jour poste client, distributions et briques techniques	22/03/2022
1.2	Florent VEYRES	Mise à jour version 1.1	20/04/2022
2.0	Antonio DA SILVA	Mise à jour version 2.0	15/05/2024
2.1	Antonio DA SILVA	Ajouts documentation	07/02/2025

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 Préambule....4
2 Liste des systèmes d'exploitation supportés....5
3 Ressources du système....6
  3.1 CPU et RAM....6
  3.2 Dimensionnement des disques....6
4 Accès à un compte privilégié....7
5 Ressources réseau....8
6 Docker....9
7 Briques techniques....10
8 Briques logicielles....11
9 Accès aux bases de données....12
10 Certificats HTTPS....13
11 Email....14
12 Connexion LDAP....15
13 Compatibilité des postes utilisateurs....16
  13.1 Navigateurs web....16
  13.2 Systèmes d'exploitation des postes utilisateurs....16
14 Capacités SSO....17

1 Préambule

Ce document détaille les éléments nécessaires à la mise en place manuelle du logiciel refae.Il est a destination des équipes d'administration système et réseaux des collectivités souhaitant installer refae.À noter qu'il ne mentionne pas les éléments afférents aux procédures de déploiement utilisées par les équipes d'installation de libriciel SCOP, et qu'il est recommandé qu'un atelier d'échange sur les prérequis de l'application ait lieu entre la collectivité et Libriciel SCOP.

2 Liste des systèmes d'exploitation supportés

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

OS	Statut	Commentaires
Ubuntu LTS x64 en cours de support par Canonical	**Oui**	**OS de référence**
RHEL maintenu par Red Hat	Oui	RHEL 7 non supporté. Versions majeures 8, 9 et 10, idéalement sur la dernière version mineure
Rocky Linux	Oui	Versions majeures 8, 9 et 10, idéalement sur la dernière version mineure.

- Les versions NON LTS d'Ubuntu Server ne sont pas supportées,
- Les autres versions clone de RHEL ne sont pas supportées, almalinux par exemple car c'est une distribution amont de RHEL.

Quelque soit la distribution choisie, celle-ci doit être basée sur un environnement serveur et ne pas contenir d'autre paquet que ceux fournis dans l'installation de base. En particulier, l'installation des composants graphiques (environnement de bureau, serveur X...) est proscrit.

3 Ressources du système

3.1 CPU et RAM

Ressource	Taille test	Taille production	Commentaires
CPU	1	2	Indicateur minimum
RAM	4 Go	8 Go	Indicateur minimum

Il est impératif que votre CPU soit compatible avec le jeu d'instructions x86_64-v2 pour que l'hébergement des données en stockage S3 local puisse fonctionner.

3.2 Dimensionnement des disques

Le dimensionnement disque peut être effectué tout en une même partition.Nous recommandons le formatage en **LVM** afin de pouvoir augmenter à chaud l'espace disque si nécessaire.

Partition	Taille test	Taille production	Commentaires
/	20 Go	20 Go	OS, images docker
/data	10 Go	10 Go	Fichiers, données applicatives, certificats, logs

NB : Ces valeurs sont des minima absolus de démarrage, et ne constituent pas des valeurs de confort en production dans tous les contextes d'utilisation.

NB : En cas de partition /var distincte de la partition racine, prévoir d'y provisionner 10Go supplémentaires afin de stocker les images docker dans /var/lib/docker.

4 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.

5 Ressources réseau

Voici la liste des ports utilisés en entrée et sortie:

Protocole	Port	Entrée	Sortie	Commentaires
HTTP	80 TCP	Oui	Oui	
HTTPS	443 TCP	Oui	Oui	
SMTP	25 TCP	Non	Oui	Généralement paramétré vers le relais SMTP local

Voici la liste des URLs utilisées depuis internet lors de la phase d'installation ou de mise à jour manuelle de l'application:

Ressource	Destination	Protocole	port TCP
Livrables	nexus.libriciel.fr	HTTPS	443
Images Docker Libriciel	registry.libriciel.fr	HTTPS	443
Images Docker Externes	hubdocker.libriciel.fr	HTTPS	443
livrables	*.libriciel.fr	HTTPS	443
Docker CE	download.docker.com	HTTPS	443

En phase d'exploitation, il faudra ouvrir l'accès en sortie vers https://allo.libriciel.fr afin d'assurer une remontée d'informationde la version de l'applicatif déployé vers nos services. L'unicité de l'instance est assurée par l'association d'un jeton généré parnotre infrastructure et défini dans une variable du fichier de contextualisation. Cette information nous permettra de communiquer ausujet des mises à jour critique à appliquer sur nos produits.

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

6 Docker

La version de ce logiciel est livrée sous forme de conteneurs fonctionnant sous Docker Community Edition qui seront déployés sur un serveur virtuel.

Docker Community édition sera 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'un registre dédié.

7 Briques techniques

Voici la liste des briques techniques installées directement sur le serveur.

Ces briques sont des prérequis, et seront déployées lors de l'installation, il est inutile de procéder à leur mise en place préalable.

Composant	Version	Commentaires
docker-ce	version stable supportée par docker	Moteur Docker Community Edition
docker compose	version stable supportée par docker	Plugin docker compose

8 Briques logicielles

Voici la liste des briques logicielles constituant versae.

Ces briques seront déployées à l'installation, il est inutile de procéder à leur mise en place préalable.Toutes ces briques doivent être regroupées dans un même serveur.

refae ne supporte pas de base de données externalisée. En effet, la base de données ne contenant qu'une petite partie des metadonnées, il n'y a aucune plus value à l'externaliser (ou les autres briques), ce qui peut au contraire entraîner un risque d'intégrité des données en cas de restauration.

Versions des briques logicielles :

Composant	Source	Version
refae	Image Docker officielle	2.0.x
PHP	Image Docker officielle	8.3.x
APACHE	Image Docker officielle	2.4.x
Postgres	Image Docker officielle	16.3.x
Async	Image Docker officielle	2.0
Mercure	Image Docker officielle	0.15
Meilisearch	Image Docker officielle	1.6
LIBRICIEL-FEEDBACK	image docker développée et maintenue par libriciel	0.9.1

9 Accès aux bases de données

L’accès par une application tierce aux bases de données des logiciels Libriciel SCOP 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 SCOP 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, etc.) 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.

10 Certificats HTTPS

Afin de pouvoir utiliser les logiciels fournis par Libriciel SCOP, il sera nécessaire de mettre en place un certificat HTTPS, ainsi que la clé privée associée.

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).

Les prérequis techniques des certificats sont les suivants :

- Les certificats et la clé privée doivent être au format PEM.
- La clé privée ne doit pas être chiffrée.
- La clé privée doit avoir une longueur d'au moins 2048 bits (RSA-2048).

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

- L'acquisition et utilisation 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 fourni par Libriciel SCOP est accessible sur Internet.Libriciel SCOP n'est toutefois pas en mesure d'apporter de support sur la mise en place et l'utilisation des outils let's encrypt et certbot.
- L'utilisation de votre propre PKI si vous en gérez une. Nous déconseillons cependant l'utilisation d'une PKI externe non reconnue nativement par les navigateurs, systèmes d'exploitation et autres outils pouvant se connecter aux logiciels fournis par Libriciel SCOP.

Nous déconseillons également l'utilisation de certificats auto-signés.
L'utilisation 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 :

- Un certificat auto-signé sera généré, 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. Certaines parties pourraient également ne pas êtres opérationnelles y compris pour le test et la formation.

11 Email

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

- Une adresse mail liée au compte administrateur local:
  Un utilisateur administateur sera créé lors de l'installation, celui-ci doit être lié à une adresse email. Cette adresse pourra être utilisée en cas de réinitialisation du mot de passe du compte, ou bien pour la réception de notifications système.
- Une adresse mail émettrice:
  Lors de l'envoi d'un email, c'est cette adresse qui sera utilisée en tant qu'expéditrice. Cette adresse doit pouvoir être relayée par votre serveurs SMTP, vers des addresses internes et parfois externes à votre réseau local, selon votre cas d'usage de l'application. Elle n'a pas vocation à recevoir d'emails, et peut donc ne pas exister . Exemples : ne-pas-repondre@mairie-ville.fr, pastell@domaine.local

12 Connexion LDAP

Les éléments suivants seront nécessaires pour paramétrer la connexion LDAP de l'application:

- Le type de LDAP utilisé : Active Directory, openLDAP, lemonLDAP, etc.
- L'URL ou IP du serveur
- Le port utilisé. Généralement 389 pour le LDAP et 636 pour le LDAPS.
- Un compte utilisateur du LDAP habilité à requêter sur le serveur utilisé.
- Un groupe LDAP contenant les utilisateurs de l'application, qui sera utilisé par l'intermédiaire d'un filtre de recherche memberof. Exemple: (memberof=cn=monGroupe,ou=monOU,dc=monDC,dc=monDC).
- La base de recherche du DN des utilisateurs (exemple: "dc=mairie-ville,dc=fr")
- Dans le cadre de l'utilisation d'un LDAPS, le certificat SSL servi par le serveur LDAPS, afin qu'ils soit renseigné et vérifié dans l'application.

En cas d'utilisation de openLDAP ou autre fournisseur dont ce n'est pas le comportement par défaut, il est nécessaire que dans le LDAP, les utilisateurs aient l'attribut "memberof" renseigné avec le DN du groupe de sécurité utilisé par l'application.

13 Compatibilité des postes utilisateurs

13.1 Navigateurs web

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, etc.).

13.2 Systèmes d'exploitation des postes utilisateurs

Voici la liste des prérequis concernant les postes de travail des utilisateurs.

Système d'exploitation	Support	Commentaires
Windows 11	**Supporté**	**OS de référence**
Windows XP Vista, 7, 8, 8.1, 10	**Non Supportés**	Fin de support Microsoft le 14 octobre 2025
macOS / macOS X	**Non Supporté**	
Linux (Ubuntu, Debian, RedHat)	Supporté	

D'une manière générale, Libriciel maintient la compatibilité côté utilisateur 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 Windows sur les architectures Intel x86 et AMD64 et ne fonctionnent pas avec d'autres systèmes d'exploitation.

14 Capacités SSO

L'application refae peut être connectée avec certains systèmes de web-SSO:

- "Keycloak" : testé avec succès sur le protocole OpenID Connect Oauth2.

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