



Pré-requis pour un déploiement

Version 4.1.x

Document

Auteur	Sébastien Picard	Date de diffusion	31/10/2025
Chef de Projet	Arnaud AUZOLAT	N° de version	4.1.x

Évolution du document

Version	Auteur	Nature des changements	Date
1.0	Sébastien PICARD	Nouvelle version	31/10/2025

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](#)



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 Bureautique client.....	16
14 Authentification boîte mail OAuth2.....	17

1 Préambule

Ce document détaille les éléments nécessaires à la mise en place manuelle du logiciel WebGFC.

Il est a destination des équipes d'administration système et réseaux des collectivités souhaitant installer WebGFC.

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. Version mineure à jour nécessaire: 8.10 et 9.5 à l'heure actuelle.

- 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.

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	Commentaire
Nombre de cores de CPU	2	Indicateur minimum
RAM	6Go	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

Il est recommandé de partitionner le système hôte en deux partition distinctes, dont une partition montée sur /data/ qui servira à héberger les données de l'application.

Nous recommandons le formatage en **LVM** afin de pouvoir augmenter à chaud l'espace disque si nécessaire.

Partition	Taille	Commentaire
/	50 Go	OS, images docker
/data	150Go	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'information de la version de l'appliquatif déployé vers nos services. L'unicité de l'instance est assurée par l'association d'un jeton généré par notre infrastructure et défini dans une variable du fichier de contextualisation. Cette information nous permettra de communiquer au sujet 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 webgfc.

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.

Webgfc ne supporte pas de base de données externalisée. En effet, la base de données ne contenant qu'une petite partie des métadonnées, 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 minimales des briques logicielles pour webgfc 4.1.X :

Origine Image Docker	Composant	Version	Fonction
Image Libriciel Scop	webgfc-symfony-fpm	4.1.0	fpm
Image Libriciel Scop	webgfc-symfony-fpm-consumer	4.1.0	consumer d'exécution des tâches
Image Libriciel Scop	webgfc-nginx	4.1.0	front
Image Libriciel Scop	workflow	2.2.15	gestion des circuits
Image Libriciel Scop	gfc-redis-subscriber	1.0.1	souscription redis
Image Libriciel Scop	cloudooo	24.8.7-PDFA	Service de conversion odt/PDF
Image Libriciel Scop	webgfc/webgfc-db	4.1.0	base de données
Image Libriciel Scop	libriciel-feedback	2.0.1	retour d'information à libriciel
Image Libriciel Scop	flow	1.5.1	fusion documentaire
Image Officielle	minio/minio	RELEASE.2025-07-23T15-54-02Z	Service S3
Image Officielle	mcuadros/ofelia	v0.3.19	ordonnancement des traitements
Image Officielle	redis	6.2.20-alpine	Service Redis

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 patches, 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 pourrions 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 plateforme ne sera pas opérationnelle à 100% pour la production. Certaines parties pourraient également ne pas être 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 administrateur 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 serveur SMTP, vers des adresses 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 Bureautique client

WebGFC requiert également l'utilisation d'un outil bureautique manipulant correctement le format ODT.

Toutes les versions LibreOffice sont compatibles avec le format ODT v1.2. Nous conseillons de manière générale d'utiliser la dernière version qualifiée par nos équipes.

Composant	Version	Support	Commentaires
LibreOffice	> 5.0	Supporté	L'utilisation de la dernière version au long cycle de test (anciennement "Stable" ou "Still") supportée par The Document Foundation (LibreOffice 25.2.6 en date du 08/10/2025) est recommandée
LibreOffice	=< 5.0	Non supporté	
Microsoft Office	Toutes	Non supporté	Libriciel ne fournit pas de support en cas d'utilisation de MS Word (toutes versions) (*)

(*) source : [Différences entre le format Texte OpenDocument \(.odt\) et le format Word \(.docx\)](#)

NB : MSOffice et LibreOffice cohabitent parfaitement sur un même poste de travail. MSOffice peut être utilisé comme outil bureautique standard, LibreOffice peut être considéré comme l'outil bureautique dédié à l'utilisation de WebGFC.

14 Authentification boîte mail OAuth2

Depuis le 01 Octobre 2022, Microsoft a changé les paramètres d'authentification de leur service cloud et n'autorise plus l'authentification dite "basique" (cf. <https://techcommunity.microsoft.com/t5/exchange-team-blog/basic-authentication-deprecation-in-exchange-online-september/ba-p/3609437>).

Dans le cas où le système de messagerie utilisé par la collectivité est un Microsoft Exchange online / Office365, il est donc nécessaire de prendre en compte cette information. Les mails ne pourront plus être remontés par l'application webgfc car l'authentification "basique" ne sera plus opérationnelle.

Il sera nécessaire de nous fournir un "client_id" et un "client_secret" générés depuis votre Azure AD.

Libriciel SCOP ne pourra en aucun cas intervenir sur l'Azure AD de la collectivité, cette action sort du cadre du support.

Autres sources :

- Authentifier une connexion IMAP, POP ou SMTP à l'aide d' [OAuth](#)
- Configurer une application cliente pour accéder à une API web : [API WEB](#)