/20
25/

Prérequis Techniques Open-Prod 9.x

Société 1Life

Logiciel ERP

Créé par des industriels,
pour des industriels

Table des matières

Préambule

Ce document couvre les prérequis techniques relatifs aux différents environnements serveurs, aux aspects réseaux et télécoms, aux postes de travail et aux périphériques constituants le socle de fonctionnement d'une **version 9.x d'Open-Prod**. Il est disponible dans sa dernière version via ce lien public : https://www.1life.fr/documents-telechargeables

Le respect de ces prérequis techniques est essentiel au bon fonctionnement des solutions proposées par 1Life. La responsabilité de 1Life ne pourra être engagée en cas de dysfonctionnement de la solution lié à leur non-respect. Aucun support ne sera apporté s'ils ne sont pas respectés.

Ces prérequis sont applicables pour des environnements physiques (logiciels installés sur les machines de l'entreprise) comme pour des environnements hébergés à distance (logiciels installés sur des machines présentent sur d'autres sites de l'entreprise ou chez un prestataire externe).

L'installation d'une solution 1Life dans un environnement virtualisé (virtualisation de machines) est réalisée suivant les mêmes recommandations que pour un déploiement sur des machines physiques, s'effectue souvent de manière transparente car les ressources virtualisées sont présentées aux programmes d'installation ou aux applications de la même manière que s'il s'agissait de ressources physiques. Du fait des technologies mises en œuvre pour la virtualisation mais également de la consolidation qui amène souvent à mutualiser de nombreux serveurs virtuels sur un nombre réduit de machines physiques, les performances obtenues peuvent être moindres que celles proposées nativement par une configuration non virtualisée. L'évaluation des performances est donc à prendre en compte de manière prioritaire dans ce type de solution.

Dans le cas d'une utilisation commune avec d'autres applications que celles mentionnées dans ce document, le client doit s'assurer de respecter les préconisations communes à l'ensemble des offres proposées.

Toutes les préconisations présentées dans ce document de prérequis sont à mettre en relation avec l'éventuelle proposition de matériel ou de service d'hébergement construite lors de la phase d'avant-vente du projet (et dans ce cas systématiquement communiqué en complément). Cette proposition prend en compte toutes les caractéristiques techniques discutées avec les équipes avant-ventes système 1Life.

Nota :

- ✓ La gestion des sauvegardes est à la charge du Client en fonction des outils et des méthodes de sauvegarde utilisées par celui-ci. 1Life communique lors du déploiement tous les renseignements nécessaires concernant les données à sauvegarder et les précautions à prendre lors des procédures de sauvegardes/restaurations d'une base de données Open-Prod. 1Life préconise une sauvegarde totale des différents serveurs (base de données, applicatif, web…) avec tous les disques sans exception, ainsi que les fichiers de configuration Linux.
- ✓ L'installation concerne uniquement le déploiement de la partie applicative en lien avec Open-Prod, 1Life (myFAB) et ses modules connexes. Le déploiement ou paramétrage d'autres modules, fonctionnalités ou matériels sur cet environnement (intégration des environnements au domaine, antivirus, Firewall, obtention et installation certificat Https, connexion et paramétrage des imprimantes du réseau, routage, passerelle mail – SMTP, paramétrage NAS, sécurisation des environnements, etc.) est à réaliser directement par les équipes du client ou son prestataire informatique.
- ✓ La gestion, l'administration et le maintien en condition opérationnelle des différentes plateformes présentées dans ce document est de la seule responsabilité du Client ou de son prestataire informatique. 1Life intervient uniquement pour l'installation initiale des

applicatifs vendus sur cette plateforme lors de l'initialisation du projet et ce dans le cadre de la ou des prestations prévues à cet effet dans le contrat de vente.

- ✓ Par la suite, la mise à jour de version des produits Open-Prod, Jasper et 1Life (myFAB) sur les environnements sont à réaliser directement par les équipes du client ou son prestataire informatique via les procédures disponibles ici : https://docs.myFAB.fr/shelves/installation-et-mise-a-jour-environnement-open-prod-myFAB. Si besoin, une prestation d'accompagnement sur ces travaux au travers de la Tierce Maintenance Applicative (TMA) peut être proposée.

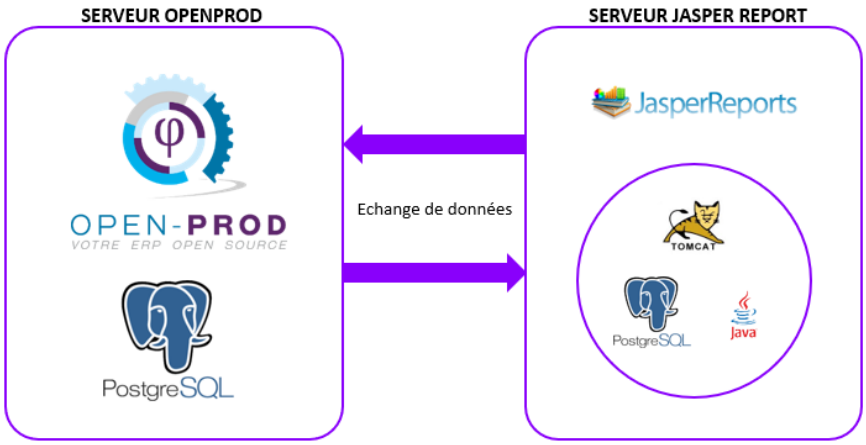
Architecture de la solution Open-Prod

L'infrastructure Open-Prod peut comporter :

- Un seul environnement serveur et cumuler le rôle de serveur Open-Prod et de serveur d'impression Jasper,
- Deux environnements serveurs distincts. L'un pour le serveur Open-Prod, le second dédié au serveur d'impression Jasper.

L'infrastructure sur un seul environnement est celle préconisée par défaut. L'infrastructure à deux environnements serveurs permet dans certains cas d'isoler et dédier des ressources spécifiques à la partie serveur d'impression, d'avoir deux environnements parfois moins couteux en hébergement (car individuellement moins puissant).

Deux environnements serveur



Mono environnement serveur

Configuration environnement Open-Prod Server

1. Open-Prod

La configuration matérielle pour la partie Open-Prod Server dépend du nombre d'utilisateurs concurrents. Si cet environnement accueille également le serveur d'impression Jasper ajouter simplement 4 Go de RAM complémentaires aux prérequis indiqués ci-dessous pour cumuler les deux rôles (Open-Prod + Jasper).

Composants	Nombre d'utilisateurs			
	Moins de 10	Moins de 20	Entre 20 et 60	> 60
Processeur	>= à 3Ghz 4 cœurs [1]	>= à 3Ghz 6 cœurs [1]	>= à 3Ghz 8 cœurs [1]	Nous consulter lors de la phase d'avant-vente
Système d'exploitation 64 bits	Linux Ubuntu Server 22.04 LTS [2]			
Langue	Jeu de caractère fr_FR.UTF-8			
Mémoire Ram	8 Go	16 Go	32 Go	
Stockage	100 Go SAS HDD 15K tpm ou SSD en RAID [3]	200 Go SAS HDD 15K tpm ou SSD en RAID [3]	> 200 Go SAS HDD 15K tpm ou SSD en RAID [3]	
Carte Réseau	1 Gb/s [4]			
	Base de données [7]			
Moteur de base de données **64 bits**	PostgreSQL 14			
Classement	fr_FR.UTF-8			
	Environnement			
Accès Internet	Oui (obligatoire) [5]			
Navigateur Internet	Oui			
Outil prise en main distante	Oui [6]			

[1] A augmenter selon étude (système d'exploitation, nombre d'utilisateurs, nombre de bases de données utilisées…). Il est obligatoire de dédier cet environnement à la solution 1Life pour éviter les conflits suivants :

- Incompatibilité entre les différents choix de paramétrage des bases
- Non maîtrise des performances liées à la charge induite par une autre application
- Evolutions de versions de bases de données pouvant intervenir à des moments différents
- Procédures de maintenances hétérogènes (par exemple les sauvegardes)

[2] Par défaut seule une version Ubuntu Server 22.04 LTS de base est requise. D'autres éléments seront déployés en complément lors de l'installation des produits Open-Prod et 1Life.

[3] Disques des environnements serveurs connectés en SAS : SSD, HDD 10K ou 15K Tours avec des débits disques mesurés sur les environnements serveur au minimum à 400 Mb/s.

[4] Cartes réseaux et switch reliant les environnements serveurs correctement réglés pour fonctionner dans les conditions optimums de leurs capacités (Idéalement pour un réseau physique, 1 Gbits). Latence réseau correcte comprise entre 1 et 10ms (et vérifiée via un ping entre la partie client et la partie environnement applicatif, puis entre l'environnement applicatif et l'environnement bases de données).

[5] Lors de l'installation de l'application, un accès total de l'environnement à Internet (sans filtrage ou proxy) est obligatoire pour pouvoir télécharger les fichiers d'installation, de mise à jour de l'application et permettre le support de la plateforme. Par la suite un filtrage est possible selon les services utilisés mais un accès permanent à l'API pour contrôler la sérialisation des produits est obligatoire via l'URL https://tracker.open-prod.org/ et https://seria.myfab.fr/.

[6] Lors de l'installation un accès distant complet (niveau administrateur) à l'environnement est impératif (VPN, TeamViewer, Anydesk, etc.). Par la suite le maintien de ce type accès est fortement conseillé pour être accompagné plus efficacement à distance par notre service déploiement et support (dans ce cas l'accès est à activer ponctuellement, uniquement sur demande de 1Life).
[7] La base de données est déployée par 1Life lors de l'installation d'Open-Prod.

Seule une version Ubuntu Server 22.04 LTS de base (sans modules complémentaires proposés par l'installateur Ubuntu en fin de processus) est requise pour chaque environnement. Les éléments « système » ci-dessous (paquets) seront déployés en complément des produits myFAB par 1Life lors de l'installation. Si d'autres versions de ces composants sont souhaitées, ils peuvent être déployés par vos soins en amont de l'installation après consultation et validation de notre équipe technique.

/!\ Aucun serveur web ou système de base de données ne doit être présent sur l'environnement mis à disposition lors de l'installation. Ces composants vont être déployés via l'installation d'Open-Prod. Le service applicatif Open-Prod va obligatoirement être déployé sur le même environnement que le service de base de données.

Composants complémentaires au système d'exploitation, à Open-Prod et Jasper Server pouvant être déployés par 1Life lors de l'installation :

	Paquet standard Open-Prod - myFAB	Port(s) utilisé(s)
Gestionnaire des impressions	CUPS	631
Gestionnaire de partage de fichiers	Samba	139 ou 445
Gestion des scripts	PHP 8.0	(na)
PgAdmin avec Apache	(Version web)	80
NGINX		80 / 443

2. Environnement optionnel dédié au serveur d'impression Jasper

Dans le cas du choix de deux environnements serveur distincts. L'un pour le serveur Open-Prod (cf. § IV.1) et le second dédié au serveur d'impression Jasper, la configuration pour l'environnement dédié au serveur d'impression Jasper est à minima :

Composants	Caractéristiques
Processeur	>= à 3Ghz 2 cœurs [1]
Système d'exploitation 64 bits	Linux Ubuntu Server 22.04 [2]
Langue	Jeu de caractère fr_FR.UTF-8
Mémoire Ram	4 Go
Stockage	20 Go SAS HDD 15K tpm ou SSD en RAID [3]
Carte Réseau	1 Gb/s [4]
	Base de données [7]
Moteur de base de données 64 bits	PostgreSQL intégrée (bundle Jasper)
Classement	fr_FR.UTF-8
	Documents et report
Moteur de report [5]	JasperReport 7
	Environnement
Accès Internet	Oui (obligatoire) [5]
Navigateur Internet	Oui
Outil prise en main distante	Oui [6]

[1] A augmenter selon étude (système d'exploitation, nombre d'utilisateurs, nombre de bases de données utilisées…). Il est obligatoire de dédier cet environnement à la solution 1Life pour éviter les conflits suivants :

- Incompatibilité entre les différents choix de paramétrage des bases
- Non maîtrise des performances liées à la charge induite par une autre application
- Evolutions de versions de bases de données pouvant intervenir à des moments différents
- Procédures de maintenances hétérogènes (par exemple les sauvegardes)

[2] Par défaut seule une version Ubuntu Server 22.04 LTS de base est requise.

[3] Disques des environnements serveurs connectés en SAS : SSD, HDD 10K ou 15K Tours avec des débits disques mesurés sur les environnements serveur au minimum à 400 Mb/s.

[4] Cartes réseaux et switchs reliant les environnements serveurs correctement réglés pour fonctionner dans les conditions optimums de leurs capacités (Idéalement pour un réseau physique, 1 Gbits). Latence réseau correcte comprise entre 1 et 10ms (et vérifiée via un ping entre la partie client et la partie environnement applicatif, puis entre l'environnement applicatif et l'environnement bases de données).

[5] Lors de l'installation de l'application, un accès total de l'environnement à Internet (sans filtrage ou proxy) est obligatoire pour pouvoir télécharger les fichiers d'installation, de mise à jour de l'application et permettre le support de la plateforme. Par la suite un filtrage est possible selon les services utilisés mais un accès permanent à l'API pour contrôler la sérialisation des produits est obligatoire via l'URL https://tracker.open-prod.org/ et https://seria.myfab.fr/.

[6] Lors de l'installation un accès distant complet (niveau administrateur) à l'environnement est impératif (VPN, TeamViewer, Anydesk, etc.). Par la suite le maintien de ce type accès est fortement conseillé pour être accompagné plus efficacement à distance par notre service déploiement et support (dans ce cas l'accès est à activer ponctuellement, uniquement sur demande de 1Life).

[7] La base de données est déployée par 1Life lors de l'installation d'Open-Prod.

Par défaut seule une version Ubuntu Server 22.04 LTS de base (sans modules complémentaires proposés par l'installateur Ubuntu en fin de processus) est requise pour chaque environnement. Les éléments « système » ci-dessous (paquets) seront déployés en complément des produits myFAB par 1Life lors de l'installation. Si d'autres versions de ces composants sont souhaitées, ils peuvent être déployés par vos soins en amont de l'installation après validation de notre équipe technique.

/!\ Aucun serveur web ou système de base de données ne doit être présent sur l'environnement mis à disposition lors de l'installation. Ces composants vont être déployés lors de l'installation d'Open-Prod.

Composants complémentaires au système d'exploitation et Jasper Server pouvant être déployés par 1Life lors de l'installation :

	Paquet standard Open-Prod - myFAB	Port(s) utilisé(s)
Gestion des scripts	PHP 8.0	(na)
PgAdmin avec Apache	(Version web)	80

3. Stockage des documents - GED (Gestion Electronique des Documents)

Les documents attachés aux transactions de l'ERP peuvent être stockés localement sur l'environnement principal Open-Prod via la fonction Gestion Electronique des Documents (GED) native à l'ERP (à condition de prévoir un espace disque suffisant pour accueillir le volume des données sur cet environnement).

A défaut, un espace de stockage externe peut également être utilisé même si celui-ci est hébergé sur un autre type de plateforme (serveur Windows, Linux, NAS, etc.). Dans ce cas l'environnements de stockage doit être entièrement maitrisé par le client ou son prestataire (paramétrage, partage des dossiers, gestion des droits, adresse réseau, etc.) et savoir communiquer avec l'environnement Open-Prod sur le réseau commun (au travers du protocole de communication SMB ou NFS). Les débit et latences réseaux sont à mettre en adéquation avec l'usage et les volumes traités. Un paramétrage complémentaire de la plateforme Open-Prod est nécessaire pour accéder à ce type de ressource.

NOTA : quel que soit l'endroit de stockage des documents, la manipulation d'un document dans le filestore de la GED se réalise uniquement via l'application Open-Prod. Il n'est pas possible d'ajouter ou supprimer un document dans le filestore au travers d'un explorateur de fichiers (par exemple).

/!\ L'usage d'un stockage GED sur un environnement externe et / ou distant du serveur Open-Prod peut potentiellement fortement dégrader les temps de réponse du client web Open-Prod lors des manipulation de chargement / déchargement des documents dans l'application (fiche client, article, commande, etc.). Le temps de chargement / déchargement peut être très long si la taille des fichiers rangés en GED sont importants (plan CAO, vidéos, etc.). Dans ce cas privilégier un stockage des documents en local, sur le serveur Open-Prod (dans un filesystem distinct par exemple).

4. Mise en place connecteur Open-Prod avec Office 365 ou Google GMAIL

Le déploiement d'un connecteur Office 365 / Google GMAIL avec Open-Prod nécessite la publication de l'ERP sur le web public (mise en place d'une connexion de type SSL avec certificat publique, référencement DNS public de cet environnement, paramétrage du tenant Office 365 / GMAIL par le client, etc.). Se référer à la section des prérequis correspondant à la sécurité de l'accès aux environnements serveurs.

Configuration environnement Open-Prod Client

L'utilisation de l'application Open-Prod et des modules 1Life (myFAB) coté client se réalise au travers d'un simple navigateur Web.

Ce navigateur doit être conçu autour du moteur de rendu web Blink (de Google). D'autres navigateurs utilisant un moteur différent peuvent fonctionner mais le rendu visuel est souvent différent et peut parfois rendre l'application difficilement utilisable.

Nativement l'utilisation d'Open-Prod au travers d'un navigateur web utilise le port http 8068. Sur option, la sécurisation via du https peut être mise en place sur le serveur applicatif Open-Prod. Le navigateur web peut utiliser dans ce cas le port sécurisé 443 (en complément du port 8068). La sécurisation et les règles de trafics de flux sur le poste client sont donc à adapter en conséquence par le client ou son prestataire informatique (ouverture / blocage de ports, priorisation des flux, antivirus, etc.).

Sur PC

Navigateurs web compatibles sur PC :

Composants	Caractéristiques
Navigateur Web	Tous navigateurs basés sur le moteur Open Source Blink de Google
Navigateurs compatibles (non exhaustif) :	Chromium browser (Linux, Mac, Windows)
	Google Chrome (Linux, Mac, Windows)
	Microsoft Edge (depuis la version 80.0.361.111)
	Opera (depuis la version 1520)

Sur dispositif mobile

Dans certains cas, l'application Open-Prod peut être utilisée sur des appareils mobiles (smartphone, tablette, terminal code barre) via un navigateur Web ou bien via une application web native (application Android en .apk).

Pour un usage via un navigateur web, celui-ci doit être compatible avec le moteur de rendu web Blink (de Google) identique aux caractéristiques pour PC présentées ci-dessus. Utiliser les pages de l'application prévues spécifiquement pour cet usage (responsive design et adapté pour des tailles d'écrans de 6 à 12 pouces).

Pour un usage via une application web native (.apk), seul le système Android est pris en charge. Ces applications web sont adaptées pour un usage sur des écrans de 6 à 12 pouces (selon le fonctionnel) et requiert un système Android et composant WebView minimum.

Dispositif mobile sous Android :

Composants	Minimum	Recommandé
Matériel		
Unité centrale	Processeur 1,8 Ghz	
Système d'exploitation	Android 8 (1)	
Langue	FR ou EN	
Mémoire RAM	4 GB RAM	
Mémoire Flash	16 GB	
Carte Réseau	WIFI 802.11 a/g(2)	WIFI 802.11 a/g/n(2)
SIM		Nano SIM ou eSIM + VPN
Ecran	Couleur HD 6 pouces (3) 1280 x 720	
Clavier physique (4)		47 ou 50 touches
Lecteur code barre		2D compatible 1D (5)
Accessoires	Avec socle de rechargement (6)	Avec socle de rechargement (6) Poignée ou « gun »
Logiciels		
Android WebView	Version 112 (7)	

(1) Le système d'exploitation Android installé sur le matériel doit permettre l'installation de fichiers APK externes.

(2) Les applications fonctionnent uniquement en mode « connecté » via connexion Wifi ou 4/5G. Un débit réseau minimum de 54 Mbit/s est à supporter. L'utilisation d'une connexion 4G ou 5G en remplacement du Wifi est possible au travers de l'utilisation d'un VPN d'entreprise connecté au réseau local. Dans ce cas le terminal doit être compatible pour les réseaux mobiles et un client VPN pour ce matériel doit être disponible.

(3) Un écran minimum est requis pour les saisies de transaction de stock code barre / radio. Sinon la taille de l'écran dépend de l'usage applicatif à couvrir.

(4) Un clavier physique permet sur de petits écrans la saisie de données sans interaction graphique diminuant la zone de lecture.

(5) L'usage du code barre dans les applications est un plus. Son utilisation est à adapter selon les contextes. Le format 2D est à privilégier car il offre plus de possibilités dans l'avenir et améliore la lecture des codes-barres 1D.

(6) L'utilisation d'un puit de rechargement pour les terminaux code barre est obligatoire. Le chargement des appareils terminaux code barre par simple cordon USB n'est pas assez fiable en milieu industriel pour recharger correctement et de manière pérenne les terminaux mobiles.

(7) Les APK Open-Prod pour Android utilisent le composant Android Google WebView pour fonctionner. Selon les versions d'Android, il est également possible de paramétrer l'utilisation du moteur Google Chrome à la place de WebView. La version de WebView et / ou de Chrome indiquée est celle utilisée avec la dernière version Open-Prod diffusée au moment de la rédaction des prérequis. Attention, cette version peut évoluer dans le temps, ce composant Android doit pouvoir être mis à jour pour éventuellement faire fonctionner une nouvelle version des APK Open-Prod.

Configuration environnement « bac à sable » de test

Les tests (de tous les niveaux) sur une application sont très rarement (dans l'idéal jamais) effectués directement sur l'environnement de production. Toutes modifications de version logicielle et / ou de paramétrage peut entrainer des effets de bords sur les flux implémentés au sein de l'ERP. Pour limiter ce genre de problèmes 1Life préconise l'utilisation d'un environnement de test (bac à sable).

Les tests de non-régression sont à réaliser sur un environnement de test étanche et doivent permettre de vérifier à minima que les fonctionnalités principales ou « critiques » du système d'information sont toujours disponibles après une montée de version ou une évolution de paramétrage.

La configuration matérielle pour un environnement de « test fonctionnel » (hors test de charge, multi utilisateurs) est à minima :

Composants	A minima
Processeur	>= à 3Ghz 2 cœurs (1)
Système d'exploitation 64 bits	Linux Ubuntu Server 22.04 LTS (2)
Langue	Jeu de caractère fr_FR.UTF-8
Mémoire Ram	8 Go
Stockage	100 Go HDD 7,5K tpm ou SSD (3)
Carte Réseau	1 Gb/s (4)
	Base de données (7)
Moteur de base de données 64 bits	PostgreSQL 14
Classement	fr_FR.UTF-8
	Environnement
Accès Internet	Oui (obligatoire) (5)
Navigateur Internet	Oui
Outil prise en main distante	Oui (6)

(1) A augmenter selon étude (nombre d'utilisateurs de test, nombre de bases de données utilisées, nombre de traitements automatisé, nombre de reports Jasper, etc.).
(2) Par défaut seule une version Ubuntu Server 22.04 LTS de base est requise. Par défaut les fonctions Open-Prod Server et Jasper Server seront mutualisées sur cet environnement.
(3) Disques des environnements serveurs connectés avec des débits disques mesurés sur les environnements serveur au minimum à 100 Mb/s. Taille du disque en fonction du nombre et de la volumétrie des bases de données et des fichiers GED.
(4) Cartes réseaux et switchs reliant les environnements serveurs correctement réglés pour fonctionner dans les conditions optimums de leurs capacités (Idéalement pour un réseau physique, 1 Gbits). Latence réseau correcte comprise entre 1 et 10ms (et vérifiée via un ping entre la partie client et la partie environnement applicatif, puis entre l'environnement applicatif et l'environnement bases de données).
(5) Lors de l'installation de l'application, un accès total de l'environnement à Internet (sans filtrage ou proxy) est obligatoire pour pouvoir télécharger les fichiers d'installation, de mise à jour de l'application et permettre le support de la plateforme.

Par la suite un filtrage est possible selon les services utilisés mais un accès permanent à l'API pour contrôler la sérialisation des produits est obligatoire via l'URL https://tracker.open-prod.org/ et https://seria.myfab.fr/.

(6) Lors de l'installation un accès distant complet (niveau administrateur) à l'environnement est impératif (VPN, TeamViewer, Anydesk, etc.). Par la suite le maintien de ce type accès est fortement conseillé pour être accompagné plus efficacement à distance par notre service déploiement et support (dans ce cas l'accès est à activer ponctuellement, uniquement sur demande de 1Life).

(7) La base de données est déployée par 1Life lors de l'installation d'Open-Prod.

Imprimantes

Il existe deux manières d'imprimer un document dans Open-Prod (l'une et l'autre peuvent être complémentaires selon les besoins) :

- L'impression en différée : le document est généré au format PDF depuis le serveur Jasper, puis l'utilisateur le télécharge sur son poste de travail (via son navigateur web). Dans ce cas, la tâche d'impression est gérée par le système d'exploitation du poste client (souvent Windows) et exploite les imprimantes déclarées en local sur le poste client.
- L'impression en direct : le document est imprimé directement sur une imprimante du réseau depuis l'ERP (édition d'une étiquette d'expédition ou de colisage par exemple). L'impression de documents en direct depuis l'ERP n'est possible que si les serveurs d'Open-Prod, Jasper, CUPS (serveur d'impression) et les imprimantes sont connectés ensemble sur un même réseau et si les imprimantes de ce réseau sont déclarées dans le serveur d'impression Linux (CUPS).

Dans le cas des impressions en direct, les éditions sont générées par le serveur d'impression Jasper puis soumises aux imprimantes par le gestionnaire d'impression Linux déployé sur l'environnement Open-Prod (gestionnaire d'impression nommé CUPS). L'imprimante doit obligatoirement être compatible avec un serveur d'impression Linux CUPS, comporter une interface RJ45 ou Wifi native, être accessible directement par le réseau (sans utilisation de connecteurs USB ou autres interfaces).

Le serveur d'impression Linux (CUPS) est compatible avec les imprimantes ayant fait l'objet d'une validation sous Linux. D'une manière générale, la qualité du support d'une imprimante sous Linux dépend essentiellement du bon vouloir du constructeur de l'imprimante.

Pour connaitre la compatibilité du matériel d'impression avec la plateforme Linux se référer aux données du constructeur de ce matériel. Si ces données ne sont pas disponibles, consulter le site https://openprinting.org/printers. Le site affiche la liste des imprimantes compatible sous Linux sans driver particuliers.

La validation, le branchement et le paramétrage des imprimantes sur l'environnement client et en lien avec Linux sous CUPS est de la seule responsabilité des équipes du client ou de son prestataire informatique.

ATTENTION : Dans le cas d'une installation en SaaS ou en hébergement, par défaut, seule l'impression différée est disponible. Les documents imprimés normalement « en sortie direct » sur une imprimante sont à traiter en impression différée. Si une impression en direct est souhaitée, la plateforme SaaS ou d'hébergement doit être connectée au réseau ou se trouve physiquement les imprimantes (via un VPN par exemple).

Réseau

L'ensemble des solutions proposées par 1Life(myFAB) sont à mettre en communication avec le reste du système d'information de l'entreprise. Des interconnections sont parfois à réaliser entre un ou plusieurs réseaux différents (architecture multisites, environnements hébergés, impression, etc.). La mise en œuvre de solutions de routage, de réseaux privés virtuels ou toutes autres solutions d'interconnexions est à réaliser directement par les équipes du client ou celles de son prestataire informatique.

Composants	Minimum	Recommandé
Protocole de communication	TCP/IP « IPv4 » (1) (2)	
Téléassistance 1Life (Windows et Linux) (3)	https://www.teamviewer.com/fr/telecharger/	
Accès Internet pour le téléchargement des correctifs applicatifs Open-Prod - myFAB	Téléchargeables sur Git depuis ligne de commande myhelp	
Réseau local (LAN)	100 Mb/s	1 Gb/s - 10 Gb/s
Réseau local (Wi-Fi)	Norme 802.11n/ac/ad	Norme 802.11ax
Accès Internet « fixes »	ADSL (4)	SDSL / Fibre (4)
Accès Internet mobiles	4G (4)	Wi-Fi (4)

(1) Le protocole TCP/IP « V6 » peut également être présent.
(2) Selon votre infrastructure et votre niveau de sécurité, des ajouts « d'exceptions » sur votre navigateur Internet ou des évolutions de paramètres sur vos routeurs ou vos serveurs proxy peuvent être nécessaires.
(3) La téléassistance 1Life a lieu obligatoirement via Internet avec la solution TeamViewer. Si un autre outil de prise en main distant est souhaité c'est au client d'en assurer le cout de licence (prévoir une licence complète pour les équipes 1life).
(4) Ces recommandations sont données à titre d'information. En fonction de l'usage et des attentes en termes de performances nos services peuvent étudier avec vous l'offre la mieux adaptée à votre solution.

Dimensionnement des accès

Le dimensionnement des accès à la solution Open-Prod dépend de plusieurs critères :

- L'utilisation de la solution Open-Prod sur l'environnement client (simple consultation d'une fiche, import / export de données, chargement d'un document en GED, etc.)
- L'utilisation actuelle du lien télécom du client
- Les utilisations annexes de l'accès Internet en dehors de la solution Open-Prod (web, messagerie, VPN, transfert de fichiers, etc…)

Consommation sur la partie cliente :

Pour une installation On Premise (client et serveur sur un même réseau local). Une bande passante moyenne de 500-800 Kbits/s par utilisateur est à envisager.

Pour une installation avec un serveur hébergé (client sur un réseau local et serveur distant hébergé). La bande passante consommée d'un client est identique à celle consommée en On Premise. Une

attention particulière est à apporter sur le flux web de l'ERP (application critique) afin qu'il soit éventuellement priorisé par rapport aux autres flux internet de l'entreprise.

La latence entre les clients et l'environnement serveur doit être inférieure à 100 millisecondes pour éviter tout problème. Les meilleures performances seront obtenues si la latence est inférieure à 50 millisecondes.

L'importance de la cybersécurité pour les PME

L'Importance de la Cybersécurité pour les PME

Dans un monde de plus en plus connecté, la cybersécurité est devenue une priorité incontournable pour toutes les entreprises, y compris les petites et moyennes entreprises (PME). Souvent perçues comme des cibles moins attractives pour les cybercriminels, les PME sous-estiment parfois l'importance d'investir dans des mesures de cybersécurité robustes. Pourtant, ces entreprises représentent une part significative de l'économie et sont exposées à divers risques liés aux cyberattaques. Les petites et moyennes entreprises (PME) doivent notamment accorder une attention particulière à la protection de l'accès externe à leurs systèmes d'information. Cette précaution est essentielle pour garantir la sécurité des données sensibles et assurer la continuité des opérations.

Pourquoi la Cybersécurité est Cruciale pour les PME

1. Protection des Données Sensibles : Les informations sensibles, telles que les données clients, les informations financières et les secrets commerciaux, peuvent être des cibles privilégiées pour les hackers. Protéger ces actifs est fondamental pour assurer la pérennité de l'entreprise
2. Prévention des Cyberattaques : Les cyberattaques, comme les ransomwares et le phishing, peuvent paralyser les opérations d'une PME. En 2024, près de 40 % des attaques de ransomware ont visé des TPE/PME, mettant en péril leur activité quotidienne
3. Réduction des Risques Financiers : Le coût moyen d'une cyberattaque pour une PME est estimé entre 10.000€ et 50.000 € en Europe. Une attaque peut entraîner des pertes financières importantes et nuire à la réputation de l'entreprise

Mesures de Cybersécurité Essentielles

1. Formation des Employés : Jusqu'à 90 % des cyberattaques sont liées à une erreur humaine. Former le personnel sur les bonnes pratiques en matière de cybersécurité est primordial pour réduire les risques
2. Authentification Multi facteurs (MFA) : Mettre en place une authentification à plusieurs facteurs ajoute une couche de sécurité supplémentaire pour protéger les accès sensibles
3. Sauvegardes Régulières : Assurez-vous que toutes vos données critiques soient sauvegardées régulièrement sur un système sécurisé et hors ligne. En cas d'attaque, ces sauvegardes permettent une restauration rapide
4. Pare-feu et Antivirus Avancés : Un pare-feu bien configuré et un antivirus avancé constituent une première ligne de défense efficace contre les cyberattaques

Consulter le Site de l'ANSSI

Pour renforcer votre cybersécurité, il est essentiel de consulter les ressources et les recommandations de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). L'ANSSI est l'autorité nationale en matière de sécurité et de défense des systèmes d'information en France. Elle offre des conseils, des outils et des formations pour aider les entreprises à se protéger contre les cybermenaces

Visitez le site de l'ANSSI pour en savoir plus sur les meilleures pratiques en matière de cybersécurité et pour accéder à des ressources précieuses suivez ce lien : https://cyber.gouv.fr/. Notamment des recommandations concernant les TPE/PME sous https://cyber.gouv.fr/publications/la-cybersecurite-pour-les-tpepme-en-treize-questions.

Sécurité de l'accès aux environnements serveurs

L'installation d'Open-Prod sur l'environnement mis à disposition par le client n'active par défaut aucun protocole de sécurité complémentaire sur le système d'exploitation ou bien l'infrastructure réseau (pare feu, chiffrage SSL, chiffrage disque, restriction d'accès sur des ports ou des IP, etc.). Il revient donc au client ou à son prestataire informatique de sécuriser l'environnement Open-Prod à la hauteur des risques auxquels il va être potentiellement exposé. 1Life ne pourra être tenu responsable d'un défaut de sécurisation de l'environnement et de son usage.

Recommandations au niveau du Système d'exploitation Linux et couche réseau :

Cryptage des flux via SSL

La connexion à un environnement accessible au travers du web public doit à minima être sécurisé via le chiffrage du flux par le protocole SSL (https). La mise en place de ce chiffrage nécessite :

- L'usage d'un certificat à générer / acheter auprès d'une autorité reconnue,
- La déclaration de l'environnement exposé auprès de son gestionnaire de DNS

Une documentation technique concernant la mise en œuvre de la sécurisation des flux via le protocole SSL sur l'environnement Open-Prod est disponible. L'équipe 1Life peut accompagner si besoin cette mise en place (sur la base d'une prestation complémentaire).

Types de certificats SSL à utiliser selon l'usage :

	Prix	Garantie	Contraintes	Usage
Certificat SSL Auto signé (Privé)	Gratuit	Cryptage du flux	Alerte de sécurité systématique sur le navigateur. Non utilisable pour communiquer avec d'autres services web (O365, services.gouv.fr, etc.)	Suffisant pour simplement sécuriser les échanges entre le serveur et le client
Certificat SSL DV Gratuit (Public)	Gratuit	Cryptage du flux + contrôle domaine	Doit s'appuyer sur un nom de domaine (avoir un nom pour cette machine dans son domaine et l'inscrire dans son DNS) Doit être renouvelé tous les 3 mois (processus automatique mais à surveiller) Le port 80 doit rester ouvert pour le renouvellement automatique du certificat Peut ne pas être reconnu par certains navigateurs (= alerte de sécurité)	Suffisant pour sécuriser les échanges entre le serveur et le client et consommer des services web (O365, télédéclaration, etc.)
Certificat SSL DV ou OV payant (Public)	Payant (prix selon type et caractéristiques)	Cryptage du flux + contrôle domaine + contrôle identité	Certificat payant Doit être renouvelé tous les 1 à 3 ans selon le certificat (processus à réaliser manuellement)	Type de certificat à utiliser par défaut. Couvre l'ensemble des besoins pour un prix modique en général

Usage d'un VPN

La connexion à un environnement accessible en nomadisme au travers du web public doit idéalement être réalisée au travers d'une connexion sécurisée via un VPN. La mise en place de cette connexion est à réaliser par le client ou son prestataire informatique spécifiquement pour Open-Prod ou en complément d'un VPN déjà existant dans l'entreprise (prise en compte des règles de routage pour Open-Prod).

Filtrage des ports TCP/IP

Les ports TCP/IP des environnements Open-Prod en flux entrants doivent être ouverts à minima (uniquement ceux à utiliser pour le fonctionnement de l'applicatif) et filtrés de manière à autoriser uniquement les classes d'adresses IP qui peuvent s'y connecter. Ce filtrage est à réaliser par le client ou son prestataire informatique directement sur l'environnement ou le réseau hébergeant le ou les serveurs Linux.

Configuration du filtrage des flux entrants sur un environnement hébergé (cas le plus sécurisé), hors présence d'un VPN qui véhiculerait les flux ci-dessous :

				Liste des filtrages IP à mettre en place		
Port	**Protocol**	**Service**	**Description du service associé**	**Règle**	**Obligatoire / optionnel**	**Environnement concerné**
22	TCP	SSH	Administration Linux	Listes IP autorisées en entrée	Obligatoire	Open-Prod / Jasper
8068	TCP	HTTP	Accès Open-Prod non sécurisé	Listes IP autorisées en entrée	Obligatoire si pas de SSL	Open-Prod
443	TCP	HTTPS	Accès Open-Prod sécurisé (si SSL)	Listes IP autorisées en entrée	Obligatoire si SSL	Open-Prod
8080	TCP	HTTP	Accès administration Jasper	Listes IP autorisées en entrée	Obligatoire si Jasper Studio distant	Jasper
5432	TCP	Postgre SQL	Accès bases de données (Jasper studio, BI, etc.)	Listes IP autorisées en entrée	Obligatoire si Jasper Studio distant, Pgadmin distant, BI distant)	Open-Prod
80	TCP	Pgadmin	Administration du serveur bases de données (PostgreSQL)	Listes IP autorisées en entrée	Obligatoire si Pgadmin (installé sur serveur)	Open-Prod
3389	TCP	RDP	Accès au bureau à distance	Listes IP autorisées en entrée	Optionnel	Open-Prod / Jasper

NOTA : La liste des IP autorisées en entrée est constituée à minima des adresses IP client (publique ou privée), des adresses IP 1Life (accès externe consultant et / ou support) et ce en fonction des protocoles d'accès ouverts.

Les ports TCP/IP des environnements Open-Prod en flux sortant ne doivent pas être filtrés (au moins pour l'installation) sous peine de bloquer le processus d'installation d'Open-Prod puis d'utilisation d'autres services. Une fois l'installation réalisée, la politique de filtrage des flux sortants peut être éventuellement activée en tenant compte des différents services utilisés (http, https, FTP, DNS, sites web banque, etc.). Un accès permanent à l'API pour contrôler la sérialisation des produits via l'URL https://tracker.open-prod.org/ et https://seria.myfab.fr/ est obligatoire.

L'ensemble de ces filtrages est à réaliser par le client ou son prestataire informatique directement sur l'environnement Linux ou bien sur l'infrastructure de la plateforme d'hébergement de l'environnement.

Recommandations au niveau de l'ERP :

Un certain nombre de modules sont disponibles au sein de l'ERP et de son serveur applicatif afin d'augmenter la sécurité d'accès à Open-Prod :

- Limitation des tentatives de connexions,
- Chiffrement des mots de passe,
- Politique de sécurité des mots de passe,
- Authentification via ldap,
- Two-Factor autentication (TOTP)
- SSO – Oauth2
- SSO OpenID Connect
- Etc.

Ils peuvent être activés directement dans Open-Prod après l'installation de l'ERP. Certains modules sont en lien avec des couches applicatives et / ou réseaux complémentaires à l'ERP. Se rapprocher de l'équipe avant-vente technique 1life pour plus d'informations.

Obligations et recommandations pour la sécurité d'accès aux environnements Open-Prod

La sécurisation de votre environnement applicatif ERP est une priorité essentielle et relève de votre responsabilité. Elle nécessite une approche multicouche couvrant l'ensemble des aspects, de l'infrastructure réseau à l'application elle-même.

Vous trouverez ci-dessous une liste des principaux mécanismes de sécurité à mettre en place, qu'ils soient recommandés ou obligatoires, sur ces différentes couches (liste non exhaustive).

Nos équipes techniques sont à votre disposition en phase d'avant-vente pour vous accompagner dans l'analyse de ces éléments et leur adaptation à vos besoins fonctionnels et techniques.

1. Sécurité du serveur et du système d'exploitation (environnement Linux)

- Appliquer les mises à jour et correctifs de sécurité Linux régulièrement - [obligatoire].
- Automatiser les redémarrages de sécurité (unattended-upgrades) - [obligatoire].
- Désactiver les services Linux inutiles - [obligatoire]
- Mettre en place des règles strictes de permissions des fichiers et des utilisateurs - [obligatoire]
- Activer les logs d'audit système et applicatif Linux - [obligatoire].
- Restreindre l'accès SSH avec des clés plutôt que des mots de passe - [recommandé].
- Désactiver l'accès root direct et modifier le port SSH - [recommandé].
- Configurer le pare-feu logiciel local de l'environnement (iptables, nftables, UFW) - [recommandé].
- Utiliser l'authentification forte en administration (MFA/2FA) - [recommandé].
- Centraliser les logs avec ELK Stack, Graylog ou Splunk - [recommandé].
- Utiliser un système logiciel ou matériel de détection des intrusions (IDS/IPS) - [recommandé].

2. Sécurisation du réseau (routeur et reverse proxy)

- Configurer un pare-feu matériel (boitier de sécurité, routeur / firewall, etc.) - [obligatoire].
- Utiliser un VPN pour les connexions d'administration distante, inter-sites et nomades - [obligatoire].
- Filtrer les IP autorisées avec un pare-feu (deny all, allow specific) - [obligatoire].
- Mettre en place une segmentation réseau pour isoler les services critiques - [recommandé].
- Utiliser un proxy inverse (NGINX) pour protéger l'application - [recommandé].
- Mettre en place un monitoring avec des outils comme Fail2Ban - [recommandé].

- Configurer des alertes en cas d'activités suspectes - [recommandé].

3. Sécurisation des communications

- Activer **HTTPS avec TLS 1.2/1.3** - [obligatoire].
- Générer et renouveler les certificats SSL avec **Let's Encrypt** ou une autorité certifiée - [obligatoire].
- Fermer l'accès à l'ensemble des ports TCP/IP non essentiels - [obligatoire].
- Implémenter **HSTS (HTTP Strict Transport Security)** - [obligatoire].
- Désactiver les protocoles obsolètes (SSLv3, TLS 1.0, 1.1) - [recommandé].

4. Sécurisation des accès et authentification (applicatif ERP)

- Application des mises à jour et correctifs de versions régulièrement - [obligatoire].
- Politique de sécurité des mots de passe (longueur, complexité, fréquence) - [obligatoire, Cf. module ERP « Password Security »]
- Limitation des tentatives de connexions - [obligatoire, Cf. module ERP « Limiter les tentatives de connexion »]
- Chiffrement des mots de passe - [obligatoire, Cf. module ERP « Chiffrement des mot de passe»]
- Double authentification via TOTP (Two-Factor autentication), - [recommandé, Cf. module ERP « Authentification à 2 facteurs (TOTP)»]
- Authentification via une base de sécurité externe au travers de ldap / ldaps ou OpenID de Microsoft ou Google - [recommandé. Au travers d'un annuaire ldap / OpenID externe et du module ERP « Authentification via ldap » ou « SSO - OpenID Connect Authentication (OIDC)»]
- Personnaliser le système de gestion des accès interne à l'ERP - [recommandé, Cf. fonction ERP «Liste des contrôles d'accès»]

5. Sécurité des bases de données

- Ne pas utiliser l'utilisateur root pour les connexions applicatives - [obligatoire].
- Restreindre les accès en fonction des besoins (Principle of Least Privilege) - [obligatoire].
- Mettre en place des sauvegardes régulières et tester leur restauration - [obligatoire].
- Activer le logging et la surveillance des requêtes - [recommandé].

6. Sécurisation des environnements de delivery

- Séparer les environnements (dev, test, prod) – [obligatoire].
- Ne pas stocker les secrets en dur (utiliser Vault, AWS Secrets Manager) – [obligatoire].

Politique de mise à jour et de sauvegarde des environnements

Mise en place d'une politique globale de mise à jour

Afin de corriger des dysfonctionnements et/ou d'améliorer le support et la sécurité de ses produits, Canonical (éditeur de Linux Ubuntu), Objectif-Pi (Open-Prod), 1Life (myFAB) fournissent régulièrement des correctifs devant être appliqués sur les solutions concernées. 1Life préconise la mise en place systématique de l'ensemble de ces correctifs sur les environnements de test et de production. L'application de ces mises à jour est sous la responsabilité des équipes du client ou de son prestataire informatique. Ces mises à jour demandent souvent un redémarrage de l'environnement pour être appliquées. 1Life préconise de redémarrer l'ensemble des environnements à minima une fois par mois.

Le client ou son prestataire informatique sont invités à mettre en place une politique de mise à jour cohérente à la hauteur des risques auxquels ses environnements vont potentiellement être exposés

Sur l'ensemble de tous ces sujets, l'équipe avant-vente technique 1Life peut étudier avec le client final ou son prestataire informatique le contexte d'utilisation d'Open-Prod et le niveau de sécurisation à apporter pour les différents usages.

Information de support

Les différents produits (systèmes d'exploitation, moteurs de bases de données, produits bureautiques, …) cités dans ce document sont soumis à des conditions de support et particulièrement de « fin de support » de la part de leurs éditeurs respectifs.

Les dates de fin du support standard de ces produits et des informations plus détaillées et exhaustives sont disponibles auprès des éditeurs concernés (il est par exemple parfois possible au-delà de ces dates de support complet du produit, de disposer de correctifs de sécurité ou de certains autres correctifs via la souscription d'un contrat de support complémentaire et payant).

Cycle de Vie Ubuntu : https://doc.ubuntu-fr.org/lts

Pour bénéficier des dernières évolutions technologiques et du support de l'éditeur le cas échéant, il est important de prendre en compte ces cycles de vie et de réaliser une migration vers la plateforme la plus récente supportée par les diverses solutions métier.

Mise en place d'une politique globale de sauvegarde

La gestion des sauvegardes est à la charge du Client. Elle est à paramétrer en fonction des outils et des méthodes de sauvegarde déjà utilisées par celui-ci. 1Life communique lors du projet tous les renseignements nécessaires concernant les données à sauvegarder et les précautions à prendre lors des procédures de sauvegardes/restaurations d'une base de données Open-Prod. L'ensemble de ces informations sont disponibles ici : https://docs.myFAB.fr/books/3-gestion-des-sauvegardes-dopen-prod

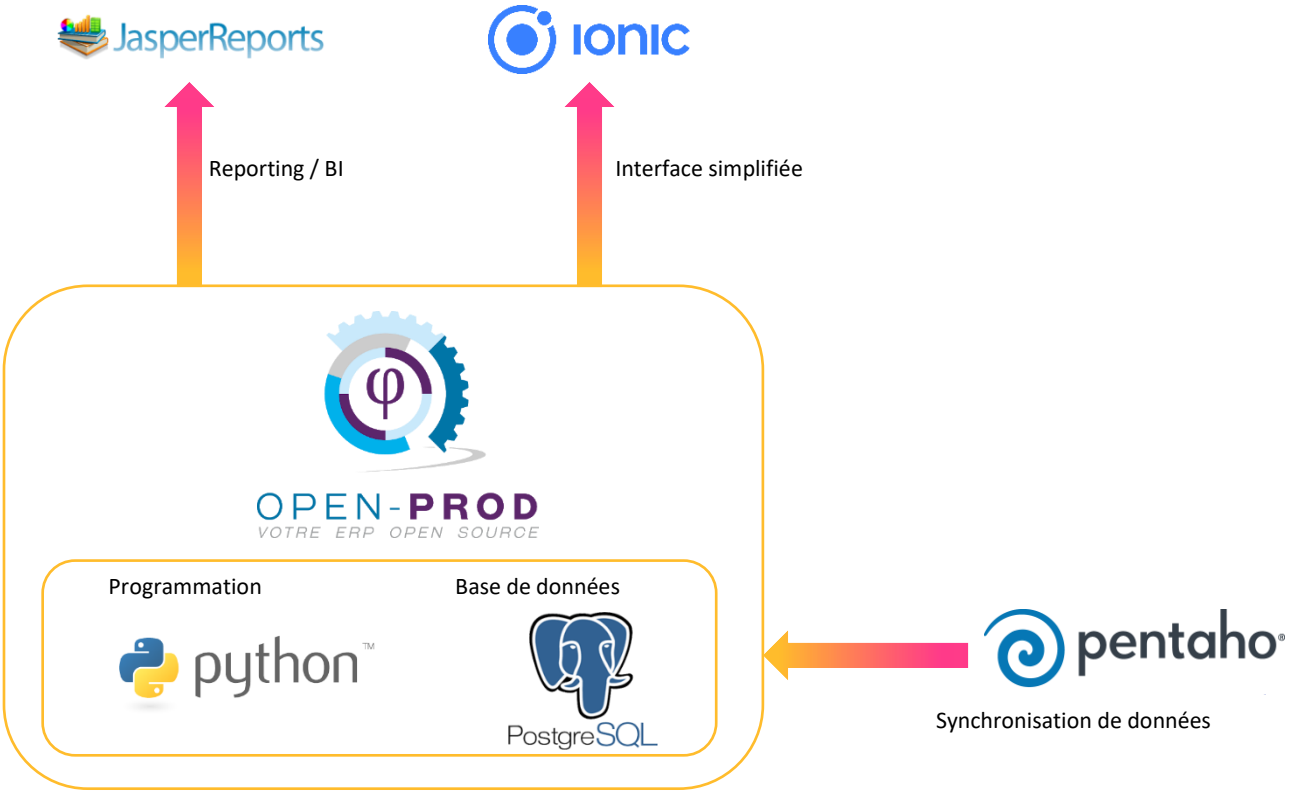
A minima la base de données et les documents de la GED sont à sauvegarder de manière régulière avec rétention sur des supports externes stockés en lieu sûr.

1Life préconise cependant :

- Une sauvegarde totale périodique des différents environnements avec tous les disques sans exception (Système d'exploitation et applicatifs ERP).
- La mise en place d'un Plan de Reprise d'Activité (PRA) cohérent avec le maintien en condition opérationnel d'un système d'information d'entreprise.

Technologie

1. Technologie



Validation des prérequis

Je confirme avoir pris connaissance et compris l'ensemble des prérequis techniques 1Life (28 pages) :

Société :

Date :

Nom et prénom :

Signature :

"Le partenaire unique

De votre système d'information"

26 Rue Benoit Bennier - 69260 CHARBONNIERES-LES-BAINS
Téléphone : +33 (0)4 81 09 07 00
www.1life.fr