Dokos
Applications libres de gestion d'entreprise

Dossier d'exploitation

Dokos

Dokos SAS
7B Allée neuve 54520 Laxou
SIREN - 824710776

Votre contact
Charles-Henri Decultot
06.33.47.58.69
chdecultot@dokos.io

Versions du document

Version	Date	Objet	Responsable	Approbateur
v1.0	01.10.2025	Version initiale du document	Charles-Henri Decultot	Charles-Henri Decultot
v1.1	30.03.2026	Retrait notion de VPN	Corentin Forler	Charles-Henri Decultot
v1.2	07.08.2026	Traçabilité fiscale des émissions de justificatifs ; criticité des PDF originaux archivés en sauvegarde, restauration et archivage ; nouveau cas d'incident (original archivé introuvable)	Charles-Henri Decultot	Charles-Henri Decultot

Version du logiciel

Nom	Version
Dodock (Frappe)	5.3.0
Dokos	5.3.0
Certification Caisse	6.0.0

Classification du document

Public sous licence CC-By-SA

SOMMAIRE

Introduction.....7
1. Prérequis et infrastructure.....8
1.1. Exigences matérielles minimales.....9
1.2. Exigences matérielles recommandées selon volumétrie.....9
1.3. Systèmes d'exploitation supportés.....10
1.4. Logiciels tiers requis et versions compatibles.....11
2. Procédures d'installation.....11
2.1. Installation sur environnement Linux.....11
Installation manuelle.....12
Installation de docli.....12
Configuration de MariaDB.....12
Configuration de Redis.....13
Installation de wkhtmltopdf.....13
Installation par conteneurisation Docker.....13
Documentation détaillée.....14
2.2.Configuration initiale du système.....14
Ajout des applications métier.....14
Création d'un site.....14
Basculement en mode production.....15
Configuration DNS et certificat SSL/TLS.....15
2.3. Installation des applications métier.....16
Procédure d'installation.....16
Approche modulaire et évolutive.....16
Précautions.....17
2.4. Vérification post-installation.....17
Contrôle de l'accessibilité du site.....17
Configuration initiale du système.....17
Paramétrage linguistique et organisationnel.....18
3. Configurations et paramétrages système.....18
3.1. Configuration du serveur d'application.....18
Paramétrage des performances.....18
Gestion des ressources système.....19

Dokos SAS
7B Allée neuve 54520 Laxou
SIREN - 824710776

Votre contact
Charles-Henri Decultot
06.33.47.58.69
chdecultot@dokos.io

Méthodes de configuration....19
3.2. Paramétrage de la base de données....19
3.3. Configuration du serveur web et du proxy inverse....20
3.4. Paramétrage des services d'arrière-plan....21
3.5. Gestion des files d'attente et des tâches planifiées....22
Les files d'attente....22
La gestion des tâches planifiées....22
Surveillance de l'état des files d'attente....23
3.6. Configuration de la messagerie électronique....23
Configuration des emails sortants....24
Configuration de plusieurs comptes emails....24
Configuration des emails entrants....24
Validation de la configuration....24
3.7. Paramétrage multisite....25
Configuration....25
Surveillance de la charge....26
4. Gestion des utilisateurs et droits d'accès....26
4.1. Création et administration des comptes utilisateurs....26
Création d'un nouveau compte utilisateur....26
Administration des comptes utilisateurs....27
4.2. Structure des rôles et permissions....28
Les rôles....28
Les permissions....28
Les restrictions utilisateurs....29
4.3. Profils utilisateurs et restrictions d'accès....29
Les restrictions d'accès....30
Les profils utilisateurs....30
4.4. Gestion des sessions et authentification....31
Registre détaillé des sections actives....31
Authentification multi-facteur....32
4.5. Connexion avec annuaires externes (LDAP, OAuth)....32
Connexion LDAP....32
Connexion OAuth....33
5. Sauvegarde et restauration des données....33
5.1. Stratégie de sauvegarde recommandée....33
Redondance multiple....34

Deux sauvegardes complémentaires....34
5.2. Procédures de sauvegarde automatisées....35
Configuration des sauvegardes automatiques....36
Transfert automatique des sauvegardes....36
5.3. Sauvegarde manuelle via l'interface....37
5.4. Procédures de restauration....37
Restauration de la base de données....37
Restauration des fichiers....38
5.5. Tests de restauration et plan de reprise....38
Test de restauration....38
Plan de reprise d'activité....39
5.6 Procédure de restauration pour les sociétés bénéficiant d'un système certifié....40
Restauration pour les clients en auto-hébergement ayant souscrit à l'application certification caisse de Dokos....40
Restauration pour les clients Dokos Cloud....41
6. Administration et supervision du système....42
6.1. Paramètres système et documents de configuration....42
6.2. Surveillance des performances et ressources....43
6.3. Gestion des logs système et applicatifs....44
6.4. Maintenance préventive et mises à jour....45
6.5. Résolution des incidents courants....47
6.6. Outils de diagnostic intégrés....48
7. Sécurité et conformité....49
7.1. Mesures de sécurisation du système....49
7.2. Chiffrement des communications....50
7.3. Gestion des mots de passe et politique de sécurité....52
7.4. Traçabilité et journalisation des actions....53
7.5. Protection contre les menaces courantes....54
Les injections SQL....55
Les attaques par script intersite (XSS - Cross-Site Scripting)....55
Les attaques par falsification de requête intersites (CSRF - Cross-Site Request Forgery). 55
Les attaques par déni de service (DoS - Denial of Service)....56
8. Migration, réversibilité des données et remplacement du système....57
8.1. Export des données et formats supportés....57
L'export via l'interface utilisateur....57

L'export via les outils de sauvegarde....57
L'export via les API REST....58
8.2. Procédure de migration vers nouvelle version....58
Etape 1 : La préparation....58
Etape 2 : Création d'une sauvegarde complète....59
Etape 3 : validation de l'intégrité des sauvegardes....59
Etape 4 : Exécution de la migration....59
Etape 5 : Validation de la migration....60
8.3. Migration depuis ERPNext....60
8.4. Désinstallation complète du système....61
8.5. Archivage des données avant remplacement....62
Durée de conservation....62
Format d'archivage....62
Documentation d'archivage....63

Introduction[1]

Le présent dossier d'exploitation constitue un document de référence essentiel pour l'administration, la maintenance et la supervision du logiciel Dokos. Il s'adresse principalement aux administrateurs système et aux équipes techniques chargées de garantir le bon fonctionnement, la sécurité et la continuité de service de la solution déployée.

Ce document vise à fournir une documentation complète et structurée couvrant les aspects opérationnels du système, depuis les prérequis d'installation jusqu'aux procédures de remplacement, en passant par la configuration, la gestion des utilisateurs et la supervision quotidienne. Il constitue un guide pratique permettant d'assurer une exploitation optimale du système tout en respectant les bonnes pratiques de sécurité et de disponibilité.

L'objectif principal de ce dossier est de centraliser toutes les informations techniques et procédurales nécessaires à l'exploitation du système, facilitant ainsi la prise en charge par les équipes d'administration et garantissant la continuité de service en cas de changement d'intervenants. Il s'inscrit dans une démarche de documentation technique rigoureuse, indispensable à la maintenance d'un niveau de service optimal.

[1] Exigence 1 et 2

1. Prérequis et infrastructure

Dokos peut être déployé selon deux modalités distinctes qui répondent à des besoins différents en termes de compétences techniques et de maîtrise de l'infrastructure.

La première modalité consiste à utiliser la **solution Dokos Cloud**, une offre hébergée entièrement gérée par l'éditeur qui ne nécessite aucune compétence technique particulière de la part de l'organisation utilisatrice.

La seconde modalité repose sur un **auto-hébergement complet** du système, qui demande des compétences approfondies en administration système et en gestion d'infrastructure informatique.

Le choix entre ces deux approches dépend principalement des ressources techniques disponibles au sein de l'organisation, de ses exigences en matière de souveraineté des données et de sa capacité à maintenir une infrastructure informatique dans la durée.

Dans le cas d'un déploiement sur Dokos Cloud, l'organisation bénéficie d'une infrastructure clés en main où toutes les contraintes techniques sont prises en charge par le prestataire. Aucune connaissance en administration de serveurs Linux, en gestion de bases de données ou en configuration réseau n'est requise. Les mises à jour du système, la surveillance de la disponibilité, les sauvegardes automatiques et l'optimisation des performances sont assurées de manière transparente. Cette approche permet aux organisations de se concentrer exclusivement sur l'utilisation métier du logiciel sans avoir à mobiliser des ressources informatiques dédiées à l'exploitation de la plateforme. La seule contrainte technique réside dans la nécessité de disposer d'une connexion internet stable et d'un navigateur web moderne pour accéder à l'application.

L'auto-hébergement impose quant à lui des prérequis techniques qui doivent être soigneusement évalués avant d'engager un déploiement. L'administrateur système doit maîtriser l'environnement Linux, être à l'aise avec l'utilisation de la ligne de commande et posséder des compétences en administration de serveurs web, de bases de données et de services d'arrière-plan. Une connaissance du langage Python est nécessaire pour comprendre l'architecture du système et résoudre d'éventuels problèmes techniques. L'administrateur doit également être capable de gérer les dépendances logicielles, de configurer correctement les services réseau, de mettre en place des stratégies de sauvegarde robustes et d'assurer la

maintenance préventive de l'infrastructure. Cette modalité convient particulièrement aux organisations disposant d'équipes informatiques expérimentées ou souhaitant conserver un contrôle total sur leur infrastructure et leurs données.

1.1. Exigences matérielles minimales

Pour un déploiement sur Dokos Cloud, les exigences matérielles côté utilisateur se limitent au strict minimum nécessaire pour accéder à une application web moderne. Un ordinateur portable ou un poste de travail standard équipé d'un navigateur web à jour suffit amplement pour utiliser l'ensemble des fonctionnalités du système. Les navigateurs basés sur Chromium tels que Google Chrome, Microsoft Edge ou Brave sont recommandés car ils offrent la meilleure compatibilité avec l'interface utilisateur et les fonctionnalités avancées de Dokos. Les navigateurs Firefox et Safari sont également supportés mais peuvent présenter occasionnellement des différences mineures de rendu ou de comportement. Une connexion internet stable est recommandée pour garantir une expérience utilisateur fluide, notamment lors de l'upload de fichiers volumineux ou de l'utilisation de fonctionnalités temps réel.

Dans le cadre d'un auto-hébergement, les exigences matérielles sont nettement plus importantes et constituent un facteur déterminant pour les performances globales du système. La configuration minimale recommandée comprend un serveur disposant d'au moins quatre processeurs virtuels, seize gigaoctets de mémoire vive et quarante gigaoctets d'espace disque disponible. Cette configuration convient pour une utilisation avec un nombre limité d'utilisateurs simultanés, généralement entre cinq et quinze personnes, et pour des volumes de données modérés. Il est fortement recommandé d'utiliser des disques SSD plutôt que des disques mécaniques traditionnels, car les performances en lecture et écriture ont un impact direct sur la réactivité de l'application, notamment lors des opérations de recherche et de génération de rapports. L'espace disque requis augmente progressivement avec l'accumulation de données, de documents attachés et de fichiers générés par le système, nécessitant une planification appropriée de la capacité de stockage.

1.2. Exigences matérielles recommandées selon volumétrie

L'adaptation des ressources matérielles en fonction de la volumétrie d'utilisation constitue un aspect crucial pour maintenir des performances optimales en auto-hébergement. Pour une organisation comptant entre vingt et cinquante utilisateurs actifs, une configuration avec huit processeurs virtuels et trente-deux gigaoctets de mémoire vive est recommandée, accompagnée d'un espace disque d'au moins cent gigaoctets. Au-delà de cinquante utilisateurs

simultanés ou pour des usages intensifs impliquant de nombreuses transactions quotidiennes, des requêtes complexes ou un volume important de documents générés, il convient d'envisager une architecture avec seize processeurs virtuels et soixante-quatre gigaoctets de mémoire vive. L'espace disque doit être dimensionné en tenant compte non seulement des données métier mais également des sauvegardes locales, des fichiers journaux et des fichiers temporaires générés par le système.

La nature des activités métier influence considérablement les besoins en ressources matérielles. Une utilisation intensive de la génération de documents PDF, de l'envoi massif d'emails ou du traitement de grands volumes de données comptables nécessite des capacités de calcul supérieures à celles requises pour une utilisation principalement axée sur la saisie de données. La présence de nombreux utilisateurs consultant simultanément des rapports complexes ou effectuant des recherches dans de larges ensembles de données sollicite particulièrement la mémoire vive et les performances du processeur. Il est recommandé de surveiller régulièrement l'utilisation des ressources pendant les périodes de forte activité afin d'identifier les éventuels goulots d'étranglement et d'ajuster les capacités en conséquence. Une marge de vingt à trente pour cent de ressources disponibles au-delà de l'utilisation moyenne permet d'absorber les pics d'activité sans dégradation notable des performances.

1.3. Systèmes d'exploitation supportés

Dokos en auto-hébergement est conçu pour fonctionner principalement sur des distributions Linux, qui constituent l'environnement d'exploitation recommandé et le mieux supporté. Les distributions basées sur Debian, notamment Ubuntu dans ses versions LTS (Long Term Support), offrent le meilleur niveau de compatibilité et bénéficient d'une documentation complète. Ubuntu 24.04 LTS représente la version la plus récente recommandée au moment de la rédaction de ce document. L'utilisation d'une distribution bénéficiant d'un support à long terme est vivement recommandée pour les environnements de production afin de garantir la disponibilité de mises à jour de sécurité sur une période étendue.

Le système peut également être installé sur macOS pour des environnements de développement ou de test, bien que cette configuration ne soit pas recommandée pour un usage en production. L'installation sur Windows n'est pas supportée nativement, mais il est techniquement possible d'utiliser le sous-système Windows pour Linux (WSL) pour exécuter Dokos dans un environnement Linux virtualisé sous Windows. Cette approche présente toutefois des limitations importantes en termes de performances et de stabilité, et ne doit en aucun cas être envisagée pour un déploiement en production. Les environnements de

conteneurisation tels que Docker peuvent être utilisés pour faciliter le déploiement, mais nécessitent une expertise spécifique en orchestration de conteneurs et en gestion d'infrastructures conteneurisées.

1.4. Logiciels tiers requis et versions compatibles

L'installation de Dokos en auto-hébergement nécessite la présence de plusieurs composants logiciels tiers dont les versions doivent être soigneusement respectées pour garantir le bon fonctionnement du système. Python constitue le socle technique principal sur lequel repose l'application et doit être présent dans une version comprise entre 3.10 et 3.12. NodeJS dans sa version 20 ou supérieure est indispensable pour la compilation des ressources front-end et l'exécution de certains outils de développement. Git version 2.43 ou ultérieure permet la gestion du versionnement du code et facilite les procédures de mise à jour du système.

Redis en version 7 ou supérieure assure la gestion du cache applicatif et des sessions utilisateurs, contribuant significativement aux performances globales du système. MariaDB version 10.8 ou ultérieure constitue le système de gestion de base de données recommandé. La bibliothèque wkhtmltopdf en version 0.12.6.1 avec correctifs Qt (patched qt) est requise pour la génération de documents PDF à partir de contenus HTML. Cette version spécifique est importante car elle corrige des problèmes de rendu présents dans les versions standard. L'ensemble de ces dépendances doit être maintenu à jour avec les correctifs de sécurité publiés par leurs éditeurs respectifs, tout en veillant à la compatibilité avec Dokos avant d'effectuer des mises à jour majeures de version. Un serveur web tel que Nginx ou Apache configuré en proxy inverse est également nécessaire pour exposer l'application de manière sécurisée et performante.

2. Procédures d'installation

2.1. Installation sur environnement Linux

L'installation de Dokos sur un environnement Linux peut s'effectuer selon deux approches principales qui répondent à des besoins différents en termes de maîtrise technique et de flexibilité.

Installation manuelle

La méthode d'installation manuelle offre un contrôle complet sur chaque composant du système et permet une compréhension approfondie de l'architecture logicielle. Cette approche commence par la préparation du système d'exploitation qui doit disposer de tous les prérequis logiciels mentionnés précédemment. L'administrateur doit créer un utilisateur dédié distinct de l'utilisateur root pour des raisons de sécurité (généralement nommé frappe ou dokos). Cet utilisateur non privilégié exécutera l'ensemble des processus applicatifs et détiendra les droits sur les répertoires de l'application.

Installation de docli

La première étape consiste à installer l'outil *docli* qui constitue l'utilitaire central de gestion du système Dokos. Cet outil en ligne de commande permet d'orchestrer l'ensemble des opérations d'installation, de configuration et de maintenance. L'installation de *docli* s'effectue via pip, le gestionnaire de paquets Python, en créant préalablement un environnement virtuel Python isolé pour éviter les conflits de dépendances avec d'autres applications présentes sur le serveur.

Une fois *docli* installé, l'administrateur initialise un nouveau répertoire bench qui contiendra l'ensemble des composants du système. Cette initialisation télécharge automatiquement le cadriciel Dodock qui constitue la base technique sur laquelle Dokos est construit. Le processus d'initialisation configure également la structure de répertoires nécessaire, installe les dépendances Python requises et prépare l'environnement pour l'ajout d'applications métier.

Configuration de MariaDB

La configuration de la base de données MariaDB nécessite une attention particulière car elle stockera l'ensemble des données de l'application. L'administrateur doit créer un utilisateur de base de données dédié disposant des privilèges suffisants pour créer et gérer des bases de données.

La configuration du fichier my.cnf de MariaDB doit inclure des paramètres spécifiques recommandés pour Doko:

- jeu de caractères utf8mb4 (permettant le stockage de tous les caractères Unicode incluant les emoji.
- paramètres de mémoire tampon (buffer pool size) ajustés en fonction de la mémoire vive disponible sur le serveur, généralement entre cinquante et soixante-dix pour cent de la RAM totale pour un serveur dédié exclusivement à Dokos.

Configuration de Redis

Redis gère le cache applicatif et les files d'attente de tâches asynchrones. Il doit être configuré pour démarrer automatiquement au démarrage du système et être accessible via socket Unix ou port réseau local uniquement. La configuration par défaut de Redis convient généralement pour une installation standard, mais des ajustements peuvent être nécessaires pour des environnements à forte charge.

Installation de wkhtmltopdf

Cette étape est cruciale pour la génération de documents PDF. Il est impératif d'utiliser la version compilée avec les correctifs Qt (patched qt) disponible sur le site officiel du projet, car les versions fournies par les dépôts Linux standard ne disposent pas de ces correctifs et produiront des PDF avec des problèmes de rendu. Le binaire téléchargé doit être installé dans un répertoire système standard et rendu exécutable pour l'utilisateur qui exécute les processus Dokos.

Installation par conteneurisation Docker

L'approche par conteneurisation Docker offre une alternative à l'installation manuelle en encapsulant l'ensemble des dépendances dans des images de conteneurs isolées. Cette méthode présente l'avantage de garantir un environnement d'exécution cohérent indépendamment du système d'exploitation hôte et facilite les déploiements sur plusieurs serveurs.

Cependant, l'utilisation de Docker pour Dokos nécessite une expertise approfondie en orchestration de conteneurs et en configuration d'infrastructures conteneurisées. Les images Docker doivent être configurées en amont pour inclure tous les composants nécessaires, les applications métier souhaitées et les paramètres spécifiques à l'environnement cible. La documentation officielle fournit des exemples de fichiers Docker Compose permettant d'orchestrer les différents services requis, notamment les conteneurs pour l'application Dokos, la base de données MariaDB, Redis et Nginx.

Cette méthode convient particulièrement aux organisations disposant déjà d'une infrastructure conteneurisée ou souhaitant déployer Dokos dans des environnements cloud natifs.

Documentation détaillée

Les étapes d'installation sont décrites et détaillées sur le site de documentation public: https://doc.dokos.io/dodock/installation

2.2.Configuration initiale du système

Une fois l'environnement bench correctement installé et initialisé, la configuration du système débute par l'ajout des applications métier dans l'environnement virtuel.

Ajout des applications métier

Cette opération s'effectue via la commande *bench get-app* qui télécharge les dépôts Git des applications souhaitées et installe leurs dépendances.

L'application principale Dokos doit être ajoutée en premier car elle fournit l'ensemble des fonctionnalités de gestion d'entreprise. Pour les organisations nécessitant une conformité avec la certification LNE, l'application Certification Caisse doit également être ajoutée à l'environnement avant la création du site. Cette application spécifique apporte les fonctionnalités permettant de garantir la conformité à la réglementation fiscale française et aux exigences de certification.

D'autres applications optionnelles peuvent être ajoutées selon les besoins métier, telles que des modules spécialisés pour des secteurs d'activité particuliers ou des extensions développées par la communauté.

Création d'un site

La création d'un site représente une instance complète de Dokos avec sa propre base de données et sa configuration dédiée. La commande *bench new-site* permet de créer un nouveau site en spécifiant le nom de domaine qui sera utilisé pour y accéder.

Durant ce processus, le système

- crée automatiquement une nouvelle base de données MariaDB
- initialise les tables nécessaires
- configure un utilisateur administrateur avec un mot de passe défini lors de la création

Un même environnement bench peut héberger plusieurs sites distincts, chacun disposant de sa propre base de données et de ses propres utilisateurs, ce qui permet de consolider plusieurs instances sur une même infrastructure matérielle. Cette architecture multisite s'avère particulièrement utile pour les prestataires de services hébergeant plusieurs clients ou pour les organisations gérant plusieurs filiales de manière indépendante.

Basculement en mode production

Le basculement en mode production nécessite une configuration spécifique de l'environnement pour optimiser les performances et la sécurité. La commande *bench setup production* orchestre automatiquement l'ensemble des opérations requises :

- la configuration de Nginx comme serveur web et proxy inverse
- la création des fichiers de configuration systemctl pour gérer les services en tant que démons système
- l'activation du mode superviseur qui surveille et redémarre automatiquement les processus en cas d'arrêt inopiné
- la compression des ressources statiques
- la mise en cache des fichiers CSS et JavaScript
- configuration des en-têtes HTTP appropriés pour la sécurité

Les services d'arrière-plan (background workers) sont configurés pour s'exécuter en tant que processus permanents gérés par systemd, permettant leur démarrage automatique au redémarrage du serveur et facilitant leur supervision.

Configuration DNS et certificat SSL/TLS

Parallèlement à la configuration technique du serveur, la mise en place de la configuration DNS constitue une étape indispensable pour rendre le site accessible via son nom de domaine. L'administrateur doit créer un enregistrement DNS de type A pointant le nom de domaine ou sous-domaine choisi vers l'adresse IP publique du serveur hébergeant Dokos. Pour les déploiements nécessitant une haute disponibilité ou une répartition de charge, des enregistrements DNS supplémentaires peuvent être configurés.

Il est fortement recommandé de configurer un certificat SSL/TLS pour sécuriser les communications via HTTPS. L'outil certbot peut être utilisé pour obtenir gratuitement un certificat Let's Encrypt et l'intégrer automatiquement dans la configuration Nginx. La commande *bench setup lets-encrypt* automatise ce processus en générant le certificat, en configurant Nginx pour l'utiliser et en mettant en place le renouvellement automatique avant expiration.

Sans cette sécurisation, les données transitant entre les navigateurs des utilisateurs et le serveur seraient transmises en clair, exposant les informations sensibles à d'éventuelles interceptions.

2.3. Installation des applications métier

Une fois le site créé et configuré, l'installation des applications métier s'effectue individuellement pour chaque site selon les besoins fonctionnels de l'organisation.

Procédure d'installation

La commande *bench install-app* permet d'installer une application préalablement ajoutée à l'environnement bench sur un site spécifique. Cette opération déploie les modules de l'application, crée les tables de base de données nécessaires, installe les types de documents (doctypes) et configure les paramètres par défaut.

L'installation de l'application Dokos en premier est obligatoire car elle fournit l'ensemble des fonctionnalités de base du système de gestion d'entreprise. L'application Certification Caisse doit être installée après pour les organisations nécessitant la conformité LNE, avant toute utilisation du système de caisse.

Approche modulaire et évolutive

La flexibilité de l'architecture permet d'installer des applications supplémentaires à tout moment après le déploiement initial, sans nécessiter de reconstruction complète du site ou de migration complexe des données existantes. Cette approche modulaire permet aux organisations de commencer avec un périmètre fonctionnel restreint et d'étendre progressivement les capacités du système en fonction de l'évolution de leurs besoins.

L'ajout ultérieur d'applications s'effectue selon le même processus en deux temps :

1. ajout de l'application à l'environnement bench via get-app
2. installation sur le site concerné via install-app

Précautions

Il convient toutefois de vérifier la compatibilité entre les versions des différentes applications avant d'en installer de nouvelles, car certaines dépendances ou incompatibilités peuvent exister. La désinstallation d'une application installée est également possible via la commande *bench uninstall-app*, mais cette opération supprime définitivement toutes les données associées à l'application et doit être effectuée avec précaution.

2.4. Vérification post-installation

La vérification post-installation constitue une étape critique pour s'assurer du bon fonctionnement du système avant sa mise en service.

Contrôle de l'accessibilité du site

L'administrateur doit d'abord vérifier que le site est accessible via l'URL configurée en ouvrant un navigateur web et en naviguant vers le nom de domaine défini. La page de connexion de Dokos doit s'afficher correctement avec tous les éléments visuels chargés, notamment le logo, les feuilles de style et les scripts JavaScript. Si le certificat SSL a été configuré, le navigateur doit indiquer que la connexion est sécurisée avec un cadenas dans la barre d'adresse. Toute erreur à ce stade, telle qu'une page blanche, une erreur 502 Bad Gateway ou un avertissement de sécurité, indique un problème de configuration nécessitant une investigation des fichiers journaux Nginx et des processus Dokos.

Configuration initiale du système

Après confirmation de l'accès au site, l'administrateur doit se connecter avec les identifiants créés lors de l'initialisation du site pour accéder à l'interface d'administration. Au premier accès, Dokos présente un flux d'accueil (onboarding wizard) guidant l'utilisateur à travers la configuration initiale du système. Ce processus interactif permet de définir les paramètres fondamentaux nécessaires au fonctionnement du système.

La première étape consiste à configurer le responsable système, c'est-à-dire l'utilisateur administrateur fonctionnel qui supervisera l'utilisation quotidienne du logiciel et pourra créer d'autres comptes utilisateurs. Le flux demande ensuite de sélectionner le pays d'exploitation et le fuseau horaire correspondant, paramètres essentiels pour le bon fonctionnement des fonctionnalités liées aux dates et aux réglementations locales.

Paramétrage linguistique et organisationnel

La configuration de la langue par défaut du système influence l'interface utilisateur, les modèles de documents et les traductions affichées. Pour une exploitation sur le territoire français, la langue française doit être sélectionnée, bien que le système supporte le multilinguisme et permette aux utilisateurs de choisir individuellement leur langue d'interface.

L'étape suivante concerne la création de la société principale qui utilisera le système, incluant son nom légal, son siège social et ses informations d'identification fiscale. Le flux d'accueil propose ensuite de sélectionner le plan comptable approprié, avec des modèles prédéfinis pour différents pays et types d'organisations. Pour une société française, le plan comptable général français est proposé par défaut et peut être installé automatiquement avec l'ensemble des comptes standards.

Une fois ce flux d'accueil complété, le système est opérationnel et l'administrateur peut procéder aux configurations métier plus détaillées selon les besoins spécifiques de l'organisation.

3. Configurations et paramétrages système

3.1. Configuration du serveur d'application

Le serveur d'application Dokos repose sur le framework Dodock qui utilise Gunicorn comme serveur WSGI pour traiter les requêtes HTTP entrantes.

Paramétrage des performances

La configuration de ce serveur s'effectue principalement via le fichier de configuration du site situé dans le répertoire de l'environnement bench. Les paramètres de performance tels que le nombre de processus worker peuvent être ajustés en fonction de la charge attendue et des ressources disponibles. Par défaut, le système calcule automatiquement le nombre optimal de workers en fonction des processeurs disponibles, mais ce paramètre peut être modifié manuellement via la commande bench set-config pour des besoins spécifiques.

Le timeout des requêtes constitue un autre paramètre important qui détermine la durée maximale d'exécution d'une requête avant son interruption, généralement fixé à trois cents secondes pour permettre le traitement de rapports complexes ou d'imports massifs de données.

Gestion des ressources système

La gestion de la mémoire du serveur d'application nécessite une attention particulière pour éviter les problèmes de performance ou les plantages dus à une consommation excessive de ressources. La limite de taille maximale des requêtes HTTP peut être augmentée via le paramètre http_timeout pour permettre l'upload de fichiers volumineux.

Le mode de débogage peut être activé temporairement pour diagnostiquer des problèmes mais doit impérativement rester désactivé en production car il expose des informations sensibles et dégrade significativement les performances.

Méthodes de configuration

L'ensemble de ces paramètres est accessible via le fichier site_config.json situé dans le répertoire du site concerné ou via les commandes *bench set-config* et *bench config* qui permettent une modification sécurisée sans édition manuelle des fichiers de configuration.

3.2. Paramétrage de la base de données

La configuration de MariaDB pour une utilisation optimale avec Dokos nécessite l'ajustement de plusieurs paramètres dans le fichier de configuration my.cnf ou mariadb.conf.d selon la distribution Linux utilisée.

Le paramètre innodb_buffer_pool_size représente le réglage le plus critique car il détermine la quantité de mémoire allouée au cache des données et des index InnoDB. Pour un serveur dédié exclusivement à Dokos, ce paramètre devrait être configuré entre cinquante et soixante-dix pour cent de la mémoire vive totale disponible, permettant ainsi de maintenir en mémoire les données les plus fréquemment consultées et réduisant drastiquement les accès disque.

Le jeu de caractères doit être défini sur utf8mb4 avec le classement utf8mb4_unicode_ci pour garantir le support complet de tous les caractères Unicode incluant les emojis et les caractères spéciaux de diverses langues.

Les paramètres de journalisation binaire (binary logging) peuvent être configurés selon les besoins de sauvegarde et de réplication, bien qu'ils ne soient pas strictement nécessaires pour une installation autonome. La taille maximale des paquets réseau (max_allowed_packet) doit être augmentée à au moins soixante-quatre mégaoctets pour permettre l'importation de données volumineuses et l'insertion de documents avec de nombreuses pièces jointes.

Les paramètres de connexion tels que max_connections doivent être dimensionnés en fonction du nombre d'utilisateurs simultanés attendus, avec une marge de sécurité pour absorber les pics de charge. Une valeur typique se situe entre cent cinquante et trois cents connexions pour une installation moyenne.

L'analyse des requêtes lentes via le journal slow_query_log aide à identifier les opérations nécessitant une optimisation, généralement par l'ajout d'index ou la réécriture de requêtes. La surveillance de la taille de la base de données et de ses fichiers journaux permet d'anticiper les besoins en espace disque et d'éviter les interruptions de service dues à une saturation du stockage.

Dokos intègre des outils de maintenance accessibles via l'interface d'administration permettant de visualiser les statistiques de la base de données et d'exécuter certaines opérations d'optimisation sans nécessiter un accès direct au serveur MariaDB.

3.3. Configuration du serveur web et du proxy inverse

Nginx agit comme serveur web et proxy inverse pour Dokos, gérant les connexions entrantes, servant les fichiers statiques et transmettant les requêtes dynamiques au serveur d'application.

La configuration générée automatiquement par la commande *bench setup production* crée un fichier de configuration dans le répertoire de configuration de Nginx qui définit l'ensemble des paramètres nécessaires au bon fonctionnement du système.

Ce fichier configure un ou plusieurs blocs serveurs correspondant aux différents sites hébergés sur l'instance, chacun écoutant sur les ports standard HTTP (80) et HTTPS (443). La directive server_name spécifie le nom de domaine associé au site tandis que les directives location définissent le routage des différents types de requêtes vers les composants appropriés.

Les fichiers statiques tels que les images, feuilles de style, scripts JavaScript et documents téléchargeables sont servis directement par Nginx sans solliciter le serveur d'application, améliorant considérablement les performances et réduisant la charge sur les processus Python.

Les directives de mise en cache avec des en-têtes Expires et Cache-Control appropriés permettent aux navigateurs de conserver localement ces ressources et de réduire le trafic réseau. La compression gzip est activée pour les fichiers texte afin de minimiser la bande passante utilisée, particulièrement bénéfique pour les connexions à débit limité.

Les paramètres *client_max_body_size* et *proxy_read_timeout* doivent être ajustés pour permettre l'upload de fichiers volumineux et le traitement de requêtes longues, avec des valeurs typiques de cent mégaoctets et trois cents secondes respectivement.

3.4. Paramétrage des services d'arrière-plan

Les services d'arrière-plan (background services) de Dokos assurent le traitement asynchrone des tâches qui ne peuvent ou ne doivent pas être exécutées de manière synchrone lors d'une requête utilisateur.

Ces services comprennent le gestionnaire de files d'attente (queue manager), le planificateur de tâches (scheduler) et les processus workers qui exécutent effectivement les tâches en attente.

En mode production, ces services sont gérés par systemctl qui garantit leur démarrage automatique au boot du serveur et leur redémarrage en cas d'arrêt inopiné. La commande *bench setup production* crée automatiquement les fichiers de service systemctl nécessaires dans le répertoire système approprié avec des noms préfixés par le nom de l'environnement bench.

Le service principal *frappe-bench-web* gère les processus Gunicorn qui traitent les requêtes HTTP, tandis que *frappe-bench-{type}-worker* lance les processus workers responsables de l'exécution des tâches d'arrière-plan.

Le nombre de workers peut être configuré en fonction de la charge de travail attendue, un nombre trop faible entraînant des files d'attente saturées et des délais de traitement importants, tandis qu'un nombre excessif consomme inutilement des ressources système. Une configuration typique utilise entre quatre et huit workers pour une installation moyenne, mais ce nombre peut être augmenté significativement pour des environnements à forte charge. Chaque worker traite séquentiellement les tâches de sa file d'attente, et la distribution des tâches entre workers s'effectue automatiquement selon leur disponibilité et leur charge respective.

La supervision et le redémarrage automatique des services s'effectuent via les mécanismes standard de systemctl. Les commandes systemctl status, start, stop et restart permettent de contrôler l'état des services individuellement.

La configuration des services inclut des paramètres de redémarrage automatique qui garantissent qu'un processus défaillant sera relancé après un court délai, évitant ainsi une interruption prolongée du service.

Les fichiers journaux des services sont gérés par journald et peuvent être consultés via la commande journalctl pour diagnostiquer d'éventuels problèmes. Il est recommandé de surveiller régulièrement les journaux pour détecter les erreurs récurrentes ou les signes de dysfonctionnement avant qu'ils n'impactent significativement le service.

La commande bench restart permet de redémarrer l'ensemble des services Dokos de manière coordonnée, opération nécessaire après certaines modifications de configuration ou mises à jour du système.

3.5. Gestion des files d'attente et des tâches planifiées

Les files d'attente

Le système de files d'attente de Dokos repose sur Redis qui stocke temporairement les tâches en attente de traitement et coordonne leur distribution aux workers disponibles.

Plusieurs files d'attente distinctes permettent de prioriser et d'organiser les différents types de tâches selon leur nature et leur urgence.

- **la file par défaut (default)** traite les tâches génériques de priorité normale
- **la file courte (short)** est réservée aux tâches rapides nécessitant un traitement quasi immédiat comme l'envoi d'emails transactionnels ou les notifications
- **la file longue (long)** accueille les opérations potentiellement très longues telles que la génération de rapports complexes, les imports massifs de données ou les traitements batch qui peuvent s'exécuter sur plusieurs minutes voire heures.

La gestion des tâches planifiées

Les tâches planifiées (scheduled tasks) constituent un mécanisme complémentaire permettant l'exécution automatique de traitements récurrents à des intervalles définis. Le planificateur de

Dokos vérifie périodiquement les tâches devant être exécutées et les ajoute automatiquement dans les files d'attente appropriées.

Ces tâches incluent notamment les synchronisations automatiques avec des systèmes externes, les envois d'emails programmés, les calculs de statistiques périodiques, les archivages automatiques et les opérations de maintenance système.

La configuration des tâches planifiées s'effectue via des fichiers *hooks.py* dans les applications installées ou directement dans l'interface d'administration pour certaines fonctionnalités. Chaque tâche spécifie sa fréquence d'exécution selon différentes options : toutes les X minutes, quotidiennement à une heure précise, hebdomadairement un jour particulier ou mensuellement selon un calendrier défini.

Surveillance de l'état des files d'attente

La surveillance de l'état des files d'attente permet d'identifier rapidement les problèmes de performance ou de saturation.

L'interface d'administration de Dokos propose un tableau de bord affichant le nombre de tâches en attente dans chaque file, le nombre de tâches échouées nécessitant une intervention et les statistiques d'exécution des workers.

Une accumulation anormale de tâches en attente indique généralement un nombre insuffisant de workers ou des tâches individuelles anormalement longues qui monopolisent les ressources.

Les tâches échouées peuvent être consultées individuellement pour analyser la cause de l'échec, et peuvent être relancées manuellement après correction du problème.

La commande *bench doctor* fournit un diagnostic de l'état du système incluant la vérification du bon fonctionnement des services d'arrière-plan et l'identification d'éventuelles anomalies dans les files d'attente.

3.6. Configuration de la messagerie électronique

La configuration de la messagerie électronique dans Dokos permet au système d'envoyer et de recevoir des emails automatiquement pour diverses fonctionnalités métier telles que les notifications, les relances clients, les confirmations de commande ou la gestion des tickets de support.

Configuration des emails sortants

La configuration s'effectue via l'interface d'administration dans la section Paramètres Email où l'administrateur définit les serveurs SMTP sortant et IMAP ou POP3 entrant.

Pour le serveur SMTP, il convient de renseigner l'adresse du serveur, le port utilisé (généralement 587 pour SMTP avec STARTTLS ou 465 pour SMTPS), ainsi que les identifiants d'authentification nécessaires. La plupart des fournisseurs de messagerie modernes exigent l'utilisation d'une connexion chiffrée, paramètre qui doit être activé pour garantir la sécurité des échanges.

Configuration de plusieurs comptes emails

Dokos permet de configurer plusieurs comptes email pour différents usages, chacun pouvant être associé à des fonctionnalités spécifiques. Un compte peut être défini comme compte par défaut pour l'envoi de tous les mails générés automatiquement par le système, tandis que d'autres comptes peuvent être dédiés à des services particuliers comme le support client ou la comptabilité.

La configuration de chaque compte inclut la possibilité de définir un nom d'expéditeur lisible, une signature automatique et des paramètres de réponse automatique.

Configuration des emails entrants

Pour la réception d'emails, la configuration du serveur IMAP permet à Dokos de récupérer périodiquement les messages entrants et de les traiter automatiquement selon des règles définies, par exemple en créant automatiquement des tickets de support à partir d'emails reçus sur une adresse dédiée.

Validation de la configuration

La validation de la configuration email s'effectue via des fonctions de test intégrées permettant d'envoyer un email de vérification pour confirmer le bon fonctionnement des paramètres SMTP.

Il est recommandé de configurer les enregistrements DNS SPF, DKIM et DMARC du domaine utilisé pour l'envoi d'emails afin d'améliorer la délivrabilité et éviter que les messages soient classés comme spam par les serveurs destinataires.

La surveillance des emails échoués via la *file d'attente d'envoi des emails* permet d'identifier rapidement les problèmes de configuration ou les adresses invalides. Le système conserve un historique complet de tous les emails envoyés et reçus, incluant le contenu, les destinataires, les horodatages et les statuts de livraison, facilitant ainsi le suivi et l'audit des communications électroniques.

Le détail des éléments de configuration à mettre en place est décrit dans la documentation publique: *https://doc.dokos.io/dodock/administration/emails*

3.7. Paramétrage multisite

L'architecture multisite de Dokos permet d'héberger plusieurs instances complètement indépendantes sur une même infrastructure matérielle et un même environnement bench.

Chaque site dispose de sa propre base de données, de ses propres utilisateurs, de sa configuration spécifique et peut avoir un ensemble différent d'applications installées.

Cette approche s'avère particulièrement pertinente pour les prestataires de services hébergeant plusieurs clients sur une infrastructure mutualisée, pour les groupes d'entreprises gérant plusieurs entités juridiques distinctes sans partage des données de référentiel, ou pour les organisations maintenant séparément des environnements de production, de test et de développement.

Configuration

La création d'un nouveau site dans un environnement bench existant s'effectue simplement via la commande *bench new-site* suivie du nom de domaine souhaité, processus qui crée automatiquement la base de données associée et initialise la structure de données.

La configuration du routage entre les différents sites hébergés repose sur le mécanisme de virtual hosts de Nginx qui dirige chaque requête entrante vers le site approprié en fonction du nom de domaine utilisé dans la requête HTTP.

Lors de l'ajout d'un nouveau site à un environnement configuré en mode production, il est nécessaire de régénérer la configuration Nginx via la commande *bench setup nginx* pour que le nouveau site soit correctement pris en compte dans le routage. Chaque site doit disposer d'un enregistrement DNS pointant vers l'adresse IP du serveur, et peut bénéficier de son propre certificat SSL/TLS configuré individuellement via *bench setup lets-encrypt.* Les sites partagent

les mêmes processus workers et les mêmes files d'attente Redis, mais le système garantit l'isolation complète des données et des traitements entre sites.

Surveillance de la charge

La gestion des ressources dans un environnement multisite nécessite une attention particulière pour éviter qu'un site particulièrement actif ne monopolise les ressources au détriment des autres. La surveillance de la charge de chaque site permet d'identifier les éventuels déséquilibres et d'ajuster la configuration en conséquence.

Pour des besoins spécifiques, il est possible de dédier des workers particuliers à certains sites ou de configurer des files d'attente séparées, bien que la configuration par défaut partage équitablement les ressources entre tous les sites.

Les sauvegardes doivent être configurées individuellement pour chaque site car chacun dispose de sa propre base de données, et les procédures de mise à jour peuvent être appliquées sélectivement site par site ou globalement à l'ensemble des sites d'un environnement bench.

La commande *bench migrate* permet de mettre à jour la structure de base de données d'un site spécifique après une mise à jour des applications, tandis que bench migrate-all applique les migrations à l'ensemble des sites hébergés.

Il est de votre responsabilité de vérifier qu'un espace de stockage suffisant est disponible pour le bon fonctionnement du logiciel. Une alerte est affichée dans l'interface utilisateur si l'espace disponible passe en dessous de 5 Go.

4. Gestion des utilisateurs et droits d'accès

4.1. Création et administration des comptes utilisateurs

La gestion des utilisateurs dans Dokos s'effectue principalement via l'interface d'administration accessible aux utilisateurs disposant des privilèges appropriés.

Création d'un nouveau compte utilisateur

La création d'un nouveau compte utilisateur nécessite au minimum la saisie d'une adresse email qui servira d'identifiant de connexion unique dans le système.

Lors de la création, l'administrateur peut choisir d'envoyer automatiquement un email de bienvenue contenant un lien permettant au nouvel utilisateur de définir son mot de passe initial, ou de définir manuellement un mot de passe temporaire qui devra être modifié lors de la première connexion.

Chaque utilisateur dispose d'une fiche complète permettant de renseigner des informations complémentaires telles que le nom complet, le numéro de téléphone, le service d'appartenance, la fonction occupée et une photo de profil. Ces informations facilitent l'identification des utilisateurs dans l'interface et enrichissent les métadonnées associées aux documents créés ou modifiés.

Administration des comptes utilisateurs

L'administrateur système dispose d'outils complets pour gérer le cycle de vie des comptes utilisateurs.

La désactivation temporaire d'un compte s'effectue en décochant simplement la case d'activation dans la fiche utilisateur, empêchant ainsi toute connexion sans supprimer les données associées.

Cette fonctionnalité s'avère particulièrement utile pour gérer les absences prolongées, les départs temporaires ou les comptes suspendus suite à des incidents de sécurité.

La suppression définitive d'un utilisateur est également possible mais doit être effectuée avec précaution car elle peut impacter l'intégrité référentielle des données si l'utilisateur a créé ou modifié de nombreux documents.

Le système conserve une trace de toutes les actions effectuées par un utilisateur via les journaux d'audit, permettant ainsi de maintenir la traçabilité même après la suppression du compte.

La gestion des mots de passe suit des règles de sécurité configurables permettant d'imposer une complexité minimale, une longueur minimale et une expiration périodique.

L'administrateur peut forcer la réinitialisation du mot de passe d'un utilisateur ayant oublié ses identifiants ou dont le compte a été compromis. Le système intègre un mécanisme de réinitialisation autonome permettant aux utilisateurs de récupérer l'accès à leur compte via un lien envoyé à leur adresse email enregistrée.

Les tentatives de connexion échouées sont enregistrées et peuvent déclencher un verrouillage temporaire du compte après un nombre configurable d'échecs consécutifs, protégeant ainsi contre les attaques par force brute.

L'interface d'administration affiche les statistiques de connexion de chaque utilisateur, incluant la date de dernière connexion et la fréquence d'utilisation, informations utiles pour identifier les comptes inactifs pouvant être désactivés.

4.2. Structure des rôles et permissions

Le système de permissions de Dokos repose sur une architecture flexible de rôles qui peuvent être attribués individuellement aux utilisateurs pour définir leurs droits d'accès aux différentes fonctionnalités et données du système.

Les rôles

Un rôle représente un ensemble cohérent de permissions correspondant généralement à une fonction métier ou à un niveau de responsabilité au sein de l'organisation.

Le système propose de nombreux rôles prédéfinis correspondant aux fonctions courantes telles que commercial, comptable, responsable des achats, gestionnaire de stock ou responsable des ressources humaines. Ces rôles standard sont configurés avec des permissions par défaut appropriées qui peuvent être ajustées selon les besoins spécifiques de l'organisation.

L'administrateur peut également créer des rôles personnalisés pour répondre à des besoins particuliers non couverts par les rôles standards.

Les permissions

Les permissions sont définies au niveau de chaque type de document (doctype) et déterminent les actions qu'un rôle peut effectuer sur ce type de document.

Les actions possibles incluent :

- la **lecture** qui permet simplement de consulter les documents existants
- l'**écriture** qui autorise la modification de documents existants
- la **création** qui permet de générer de nouveaux documents

- la **suppression** qui autorise l'effacement définitif de documents
- la **soumission** qui concerne les documents nécessitant une validation formelle

Des permissions plus spécifiques peuvent également être définies comme l'impression, l'export, l'import ou l'annulation de documents soumis.

Cette granularité permet de construire des profils de permissions très précis adaptés aux responsabilités exactes de chaque fonction.

Les restrictions utilisateurs

Le système de permissions supporte également des règles avancées permettant de restreindre l'accès aux documents en fonction de critères dynamiques.

Les règles de restrictions utilisateur permettent de limiter la visibilité des documents selon des attributs spécifiques comme la société, le département, le territoire de vente ou tout autre champ de liaison.

Par exemple, un commercial peut être restreint à ne voir que les clients et opportunités de son territoire géographique, tandis qu'un comptable n'accède qu'aux données financières de sa filiale.

Les permissions peuvent également être conditionnées par l'état du document, permettant par exemple à un utilisateur de modifier un document en brouillon mais pas après sa validation.

Cette approche par règles métier garantit que chaque utilisateur accède uniquement aux informations pertinentes pour son activité, renforçant ainsi la sécurité et la confidentialité des données sensibles.

4.3. Profils utilisateurs et restrictions d'accès

Au-delà des rôles et permissions, Dokos propose un système de profils utilisateurs permettant d'appliquer des restrictions globales affectant l'expérience et les capacités d'un utilisateur dans le système.

Ces profils constituent une couche supplémentaire de contrôle d'accès qui complète le système de permissions basé sur les rôles.

Les restrictions d'accès

Un profil utilisateur peut restreindre l'accès à **certains modules de l'application** indépendamment des permissions sur les documents individuels, masquant ainsi des sections entières de l'interface pour certains utilisateurs.

Cette approche simplifie l'interface pour les utilisateurs n'ayant besoin que d'un sous-ensemble limité de fonctionnalités, réduisant la complexité apparente du système et facilitant l'adoption.

Les restrictions d'adresse IP constituent un mécanisme de sécurité permettant de limiter les connexions à partir de plages d'adresses réseau autorisées.

Cette fonctionnalité s'avère particulièrement pertinente pour les comptes disposant de privilèges élevés ou pour les organisations souhaitant restreindre l'accès au système depuis le réseau de l'entreprise uniquement.

Les restrictions horaires peuvent également être configurées pour définir des plages horaires pendant lesquelles un utilisateur est autorisé à se connecter, utile pour contrôler l'accès des prestataires externes ou des employés à temps partiel.

Le système permet de définir des **limitations sur les actions simultanées** qu'un utilisateur peut effectuer, comme le nombre de sessions actives simultanées, prévenant ainsi le partage de comptes entre plusieurs personnes.

Les profils utilisateurs

Les profils permettent également de configurer des préférences d'interface par défaut pour certains groupes d'utilisateurs, comme :

- la page d'accueil affichée après connexion
- le thème de couleurs utilisé
- la densité d'affichage des informations

Ces paramètres peuvent être définis au niveau du profil pour standardiser l'expérience d'un groupe d'utilisateurs partageant des caractéristiques communes, tout en laissant la possibilité à chaque utilisateur de personnaliser individuellement son interface selon ses préférences.

La gestion centralisée de ces paramètres via les profils facilite l'administration de grandes populations d'utilisateurs en évitant la configuration individuelle de chaque compte. Les modifications apportées à un profil s'appliquent automatiquement à tous les utilisateurs

associés, permettant des ajustements rapides de configuration en réponse à des évolutions organisationnelles ou réglementaires.

4.4. Gestion des sessions et authentification

Le mécanisme d'authentification de Dokos repose sur un système de sessions sécurisées établies lors de la connexion réussie d'un utilisateur.

Lorsqu'un utilisateur saisit correctement son email et son mot de passe, le système génère un jeton de session unique stocké de manière sécurisée côté serveur et transmis au navigateur via un cookie HTTP. Ce jeton identifie de manière unique la session de l'utilisateur et permet au système de maintenir l'état de connexion à travers les différentes requêtes HTTP sans nécessiter de ressaisie des identifiants.

La durée de validité des sessions peut être configurée selon les exigences de sécurité de l'organisation.

Une durée de session courte renforce la sécurité en limitant la fenêtre d'exploitation d'un jeton volé, mais nécessite des reconnexions fréquentes qui peuvent impacter négativement l'expérience utilisateur.

Une durée prolongée améliore le confort d'utilisation mais augmente le risque associé à un vol de session.

Le système propose un compromis via un *mécanisme d'expiration d'inactivité* qui déconnecte automatiquement les sessions restées inactives au-delà d'un délai configurable (7 jours par défaut). Cette approche protège contre les sessions abandonnées sur des postes partagés ou non surveillés. L'utilisateur peut également se déconnecter manuellement à tout moment, action qui invalide immédiatement le jeton de session et empêche toute utilisation ultérieure.

Registre détaillé des sections actives

Le système maintient un registre détaillé de toutes les sessions actives et historiques pour chaque utilisateur, accessible via l'interface d'administration.

Ces informations incluent l'adresse IP d'origine de la connexion, le navigateur et le système d'exploitation utilisés, l'horodatage de connexion et la durée de la session. L'administrateur peut

visualiser toutes les sessions actives d'un utilisateur particulier et forcer la déconnexion de sessions suspectes ou compromises.

Les utilisateurs peuvent également consulter leurs propres sessions actives et déconnecter à distance des sessions qu'ils ne reconnaissent pas, fonctionnalité importante pour maintenir la sécurité du compte en cas d'accès non autorisé.

Authentification multi-facteur

L'authentification multifacteur peut être activée pour ajouter une couche de sécurité supplémentaire en exigeant un second facteur de vérification lors de la connexion, typiquement un code temporaire généré par une application d'authentification sur smartphone.

Il est également possible d'activer un mécanisme de connexion via lien envoyé par email.

4.5. Connexion avec annuaires externes (LDAP, OAuth)

L'intégration avec des annuaires externes permet de centraliser la gestion des identités et d'unifier l'authentification à travers les différents systèmes d'information de l'organisation.

Connexion LDAP

La connexion LDAP (Lightweight Directory Access Protocol) permet à Dokos de s'authentifier contre un annuaire d'entreprise tel que Microsoft Active Directory ou OpenLDAP.

Cette intégration évite la duplication des comptes utilisateurs et permet aux employés d'utiliser leurs identifiants habituels pour accéder à Dokos. La configuration LDAP nécessite de renseigner l'adresse du serveur d'annuaire, le port de connexion, le DN de base pour la recherche des utilisateurs et les attributs de correspondance entre l'annuaire et les champs utilisateurs de Dokos.

Lors de la première connexion d'un utilisateur via LDAP, le système crée automatiquement un compte local correspondant en important les informations disponibles dans l'annuaire telles que le nom complet et l'adresse email.

Les connexions ultérieures utilisent ce compte local mais l'authentification continue de s'effectuer contre l'annuaire LDAP, garantissant que les changements de mot de passe dans l'annuaire sont immédiatement effectifs pour l'accès à Dokos.

Cette approche hybride permet de maintenir localement les informations de rôles et permissions spécifiques à Dokos tout en déléguant l'authentification à l'infrastructure centralisée.

La synchronisation périodique peut être configurée pour mettre à jour automatiquement les informations utilisateurs locales lorsque des modifications sont apportées dans l'annuaire.

Connexion OAuth

L'intégration OAuth permet l'authentification via des fournisseurs d'identité externes tels que Google, Microsoft, GitHub ou tout autre fournisseur compatible avec le protocole OAuth 2.0/OpenID Connect.

Cette méthode d'authentification fédérée simplifie l'accès pour les utilisateurs qui peuvent se connecter à Dokos en utilisant leurs comptes existants sur ces plateformes, sans créer ni mémoriser de nouveaux identifiants.

La configuration OAuth nécessite l'enregistrement de l'application Dokos auprès du fournisseur d'identité pour obtenir un identifiant client et un secret partagé.

Le flux d'authentification OAuth redirige l'utilisateur vers le site du fournisseur pour la saisie des identifiants, puis renvoie un jeton d'authentification à Dokos une fois l'utilisateur vérifié.

Cette approche présente l'avantage de ne jamais exposer les mots de passe des utilisateurs à Dokos, renforçant la sécurité globale du système. Les organisations peuvent configurer plusieurs méthodes d'authentification simultanément, permettant aux utilisateurs de choisir leur méthode préférée parmi l'authentification locale, LDAP ou OAuth selon leurs préférences et contraintes.

5. Sauvegarde et restauration des données

5.1. Stratégie de sauvegarde recommandée[2]

La mise en place d'une stratégie de sauvegarde robuste constitue un élément fondamental de l'exploitation d'un système Dokos, garantissant la capacité à restaurer les données en cas de défaillance matérielle, d'erreur humaine, de corruption de données ou d'incident de sécurité.

[2] Exigences 10, 11, 16

Redondance multiple

Une stratégie efficace repose sur le principe de redondance multiple avec des sauvegardes conservées à différents emplacements et sur différents supports pour minimiser le risque de perte totale.

La règle communément admise du **3-2-1** constitue une base solide : maintenir trois copies des données sur deux supports différents avec une copie stockée hors site.

Pour Dokos, cela se traduit typiquement par :

- des sauvegardes quotidiennes stockées sur le serveur de production
- des copies hebdomadaires transférées sur un serveur de sauvegarde distant
- des archives mensuelles conservées dans un espace de stockage cloud ou sur support physique externe

La fréquence des sauvegardes doit être déterminée en fonction du volume de transactions quotidiennes et de la criticité des données pour l'activité de l'organisation.

Pour une utilisation intensive avec de nombreuses modifications quotidiennes, des sauvegardes plusieurs fois par jour peuvent être nécessaires pour limiter la perte de données en cas d'incident.

Une organisation avec une activité plus modérée peut se contenter d'une sauvegarde quotidienne effectuée pendant les heures creuses pour minimiser l'impact sur les performances.

La durée de rétention des sauvegardes doit également être définie selon les exigences réglementaires et opérationnelles, avec généralement une conservation des sauvegardes quotidiennes pendant une semaine, des sauvegardes hebdomadaires pendant un mois et des sauvegardes mensuelles pendant une année ou plus selon les obligations légales applicables au secteur d'activité.

Deux sauvegardes complémentaires

La stratégie doit distinguer deux types de sauvegardes complémentaires :

1. les sauvegardes complètes de la base de données qui contiennent l'intégralité des données structurées du système
2. les sauvegardes des fichiers qui incluent les documents téléversés, les images, les pièces jointes et les fichiers générés.

La base de données constitue le cœur du système et nécessite une attention particulière avec des procédures de sauvegarde fréquentes et une vérification systématique de l'intégrité des archives créées.

Les fichiers occupent généralement un volume plus important et évoluent moins rapidement, permettant d'envisager des stratégies de sauvegarde incrémentielle où seuls les fichiers modifiés depuis la dernière sauvegarde sont copiés.

Cette approche optimise l'utilisation de l'espace de stockage et réduit la durée des opérations de sauvegarde tout en maintenant un niveau de protection adéquat.

Cas particulier des systèmes certifiés. Sur un système disposant du module Certification Caisse, les fichiers privés du site contiennent les PDF originaux archivés des justificatifs émis. Ces fichiers sont créés à chaque émission, ne sont jamais modifiés ensuite, et conditionnent la capacité du système à réémettre un justificatif : leur perte rend le justificatif définitivement inémettable, sans possibilité de reconstitution. Ils doivent donc être sauvegardés à la même fréquence que la base de données, et non selon un cycle plus lâche. Une sauvegarde incrémentielle reste appropriée (ces fichiers ne sont jamais réécrits) à condition que sa fréquence suive celle de la base et que sa rétention couvre au moins la même fenêtre.

Dokos permet également l'export du fichier *site_config.json,* contenant les variables d'environnement. Il est conseillé de l'inclure dans la stratégie de sauvegarde pour permettre une restauration complète et rapide en cas de besoin.

5.2. Procédures de sauvegarde automatisées

L'automatisation des sauvegardes élimine le risque d'oubli lié aux procédures manuelles et garantit une exécution régulière selon la fréquence définie dans la stratégie.

Dokos intègre un **mécanisme de sauvegarde automatiqu**e de la base de données configurable via l'interface d'administration ou directement via les paramètres du site.

Cette fonctionnalité utilise le planificateur de tâches intégré pour déclencher automatiquement une sauvegarde complète de la base de données, par défaut toutes les 8 heures. Les archives générées sont stockées dans un répertoire dédié (/private/backups) sur le serveur avec une nomenclature incluant la date et l'heure de création, facilitant l'identification et la gestion des différentes versions.

Configuration des sauvegardes automatiques[3]

Elle permet de définir le nombre de sauvegardes à conserver localement, le système supprimant automatiquement les archives les plus anciennes une fois ce quota atteint pour éviter la saturation de l'espace disque.

Il est recommandé de conserver localement au minimum les 3 dernières sauvegardes quotidiennes pour disposer d'une fenêtre de récupération raisonnable en cas de détection tardive d'une corruption de données.

La commande *bench set-config* la durée pendant laquelle sont conservées les sauvegardes (*keep_backups_for_hours*). Le nombre de sauvegardes à conserver avant suppression, ainsi que le chiffrement des sauvegardes sont configurables dans les paramètres système.

Les sauvegardes automatiques génèrent des fichiers compressés au format SQL contenant l'intégralité du schéma et des données de la base MariaDB.

Transfert automatique des sauvegardes

Le transfert automatique des sauvegardes vers un emplacement distant constitue une étape critique souvent négligée mais essentielle pour protéger contre les défaillances affectant l'infrastructure de production.

Des scripts personnalisés utilisant rsync, scp ou des outils de synchronisation cloud peuvent être configurés via cron pour copier automatiquement les archives de sauvegarde vers un serveur distant, un espace de stockage réseau ou un service cloud tel que Amazon S3, Google Cloud Storage ou Backblaze B2.

Ces scripts doivent inclure une vérification de l'intégrité des fichiers transférés et une notification par email en cas d'échec pour alerter immédiatement les administrateurs.

L'utilisation de connexions chiffrées et le chiffrement des archives avant leur transfert protègent la confidentialité des données pendant leur transit et leur stockage sur des infrastructures tierces.
Cette fonctionnalité n'est pas native dans Dokos, et relève de la responsabilité de l'hébergeur de la solution. L'application Offsite Backup permet de bénéficier de certaines fonctionnalités d'externalisation de sauvegardes.

[3] Exigence 11

Pour les clients Dokos Cloud, les sauvegardes externalisées sont incluses dans le service proposé, pour tous les sites hébergés, selon les termes prévus dans les termes et conditions.

5.3. Sauvegarde manuelle via l'interface

Il n'est pas possible de déclencher une procédure de sauvegarde manuelle via l'interface de Dokos.

Le déclenchement est uniquement possible depuis la ligne de commande ou les interfaces des plateformes d'hébergement (Press, Dokos Cloud,...)
L'installation d'applications dédiées comme Offsite Backup permet d'avoir accès à un interface de déclenchement de sauvegardes externes depuis l'interface utilisateur.

5.4. Procédures de restauration

Restauration de la base de données

La procédure de restauration d'une sauvegarde de base de données s'effectue exclusivement via la commande *bench restore* qui accepte le chemin vers le fichier d'archive SQL à restaurer. Cette commande arrête automatiquement les services nécessaires, supprime la base de données existante, crée une nouvelle base vierge et importe l'intégralité du contenu de l'archive de sauvegarde.

L'opération peut prendre plusieurs minutes pour des bases volumineuses et nécessite que l'espace disque disponible soit suffisant pour contenir simultanément l'archive compressée, les fichiers temporaires d'import et la base de données restaurée.

Avant d'effectuer une restauration sur un environnement de production, il est impératif de créer une sauvegarde préventive de l'état actuel du système pour pouvoir revenir en arrière si la restauration ne produit pas le résultat attendu.

La restauration doit idéalement être testée d'abord sur un environnement de test ou de développement pour vérifier l'intégrité de l'archive et s'assurer que la version restaurée correspond aux attentes.

Lors de la restauration d'archives anciennes, il est nécessaire de vérifier la compatibilité entre la version de Dokos utilisée lors de la sauvegarde et celle présente sur le système cible. Des différences de version peuvent nécessiter l'exécution de migrations de schéma via la commande *bench migrate* après la restauration pour mettre à jour la structure de la base de données.

Cohérence base / fichiers sur un système certifié. La restauration de la seule base de données place le système dans un état incohérent au regard du module Certification Caisse : le Journal SAS restauré référence des fichiers originaux archivés qui peuvent être absents du système de fichiers, ou inversement. Les justificatifs concernés deviennent alors inémettables (voir §6.5). Sur un système certifié, la restauration de la base et celle des fichiers privés doivent porter sur le même point de reprise et être effectuées conjointement.

Restauration des fichiers

La restauration des fichiers s'effectue en parallèle de la restauration de la base de données et consiste à copier les répertoires *public* et privée (*private)* depuis l'archive de sauvegarde vers l'emplacement approprié dans le répertoire du site.

La commande *bench restore* permet d'indiquer les liens absolus vers les archives de documents générés par le système de sauvegarde de Dokos, afin d'effectuer cette copie.

Après une restauration complète, il est recommandé d'exécuter la commande *bench update* pour s'assurer que tous les composants prennent en compte les données restaurées. Une vérification approfondie de l'état du système doit ensuite être effectuée incluant la connexion à l'interface, la consultation de plusieurs types de documents, la vérification du bon fonctionnement des recherches et la consultation des journaux système pour détecter d'éventuelles erreurs ou incohérences.

5.5. Tests de restauration et plan de reprise

Test de restauration[4]

La réalisation régulière de tests de restauration constitue un élément souvent négligé mais absolument essentiel d'une stratégie de sauvegarde efficace.

[4] Exigence 12

Une sauvegarde non testée ne peut être considérée comme fiable car de nombreux problèmes peuvent affecter silencieusement l'intégrité des archives :

- corruption progressive des fichiers de sauvegarde
- modifications de configuration rendant la restauration impossible
- incompatibilités de versions
- erreurs dans les scripts d'automatisation

Un test de restauration complet doit être effectué régulièrement, avec des tests plus fréquents recommandés pour les environnements critiques. Ces tests s'effectuent sur un environnement isolé distinct de la production pour éviter tout impact sur le système en service et consistent à restaurer une sauvegarde récente puis à vérifier méthodiquement l'intégrité et la cohérence des données restaurées.

Le processus de test doit suivre une procédure documentée détaillant chaque étape de la restauration depuis la récupération des archives jusqu'à la validation fonctionnelle du système restauré.

Cette documentation sert également de guide opérationnel en situation d'urgence réelle où le stress et la pression temporelle peuvent compromettre la qualité de l'exécution. Les tests doivent inclure la mesure du temps nécessaire à chaque étape de la restauration pour estimer l'objectif de temps de récupération (RTO - Recovery Time Objective) réaliste que l'organisation peut garantir. Cette métrique permet d'évaluer si la stratégie de sauvegarde actuelle répond aux exigences de continuité d'activité ou si des améliorations sont nécessaires, comme l'augmentation de la fréquence des sauvegardes ou l'optimisation des procédures de restauration.

Plan de reprise d'activité

Le plan de reprise d'activité (PRA) doit décrire précisément les scénarios d'incident possibles et les procédures de réponse appropriées pour chaque situation.

Un incident mineur tel que la suppression accidentelle d'un document nécessite simplement la restauration ciblée de l'élément depuis une sauvegarde récente, tandis qu'une défaillance complète du serveur de production nécessite la restauration intégrale sur un nouveau serveur avec reconfiguration complète de l'infrastructure.

Le plan doit identifier clairement les responsabilités de chaque intervenant dans le processus de reprise, les coordonnées des personnes à contacter en cas d'urgence et les critères de décision pour choisir la procédure de restauration appropriée. Les objectifs de point de récupération

(RPO - Recovery Point Objective) doivent être définis pour quantifier la perte de données acceptable, guidant ainsi la fréquence nécessaire des sauvegardes pour respecter cet engagement.

Un RPO de quatre heures implique par exemple des sauvegardes au minimum toutes les quatre heures pour garantir que la perte de données en cas d'incident n'excède pas cette durée.

5.6 Procédure de restauration pour les sociétés bénéficiant d'un système certifié[5]

Les organisations utilisant Dokos avec l'application Certification Caisse pour une conformité à la certification LNE sont soumises à des obligations particulières concernant les opérations exceptionnelles de restauration de données.

Ces exigences réglementaires visent à garantir la traçabilité complète des modifications apportées aux données de caisse et à prévenir toute manipulation frauduleuse du système certifié. En outre, la perte partielle des Enregistrements SAS implique que les signatures déjà consignées par le système externe de journalisation soient notées comme étant obsolètes.

Restauration pour les clients en auto-hébergement ayant souscrit à l'application certification caisse de Dokos

Toute opération de restauration doit faire l'objet d'une déclaration formelle auprès de Dokos SAS qui assure le rôle de tiers de confiance dans le cadre de la certification.

Cette déclaration permet de maintenir un registre exhaustif des interventions sur le système certifié et constitue un élément de l'audit de conformité réalisé par l'organisme certificateur.

Le client doit informer Dokos SAS de toute opération de restauration planifiée ou effectuée en fournissant un ensemble d'informations précises permettant la traçabilité complète de l'intervention.

Ces informations comprennent :

- la date exacte de l'opération de restauration

[5] Exigences 10, 12

- l'identité et la fonction de la personne responsable ayant décidé et supervisé la restauration
- la justification détaillée motivant cette restauration telle qu'une défaillance matérielle, une corruption de données ou une erreur grave lors d'une maintenance
- la date/heure du fichier de sauvegarde utilisé pour la restauration

Dokos SAS consigne l'ensemble de ces éléments dans un registre dédié qui peut être consulté lors des audits de conformité effectués par tout organisme de contrôle. Cette traçabilité garantit qu'aucune restauration ne peut être effectuée de manière dissimulée dans le but de modifier rétroactivement des données fiscales ou comptables.

Restauration pour les clients Dokos Cloud

Pour les clients bénéficiant de l'offre Dokos Cloud, la procédure de restauration présente des spécificités supplémentaires liées à l'architecture hébergée.

Dans cette configuration, le client ne dispose pas d'un accès direct à l'infrastructure technique et ne peut donc pas effectuer lui-même les opérations de restauration au niveau système.

Toute demande de restauration doit être transmise au service support de Dokos SAS via les canaux de support officiels. La demande doit inclure les mêmes informations que pour un système auto-hébergé, complétées par une description précise de la situation nécessitant la restauration et la période approximative vers laquelle le système doit être ramené.

L'équipe support de Dokos SAS analyse la demande, valide sa légitimité et procède à la restauration selon les procédures internes garantissant la sécurité et l'intégrité des données.

Le délai d'intervention pour une restauration Cloud dépend de la criticité de la situation et du niveau de support souscrit, les contrats de service définissant des engagements de temps de réponse adaptés aux besoins de continuité d'activité de chaque organisation. Il est recommandé aux organisations soumises à la certification LNE de documenter dans leurs procédures internes le processus de demande de restauration et de conserver une copie de toutes les communications avec Dokos SAS relatives aux opérations de restauration effectuées.

6. Administration et supervision du système

6.1. Paramètres système et documents de configuration

Le module Administration de Dokos centralise l'ensemble des fonctionnalités de paramétrage technique et fonctionnel du système, offrant aux administrateurs un point d'accès unique pour configurer et personnaliser le comportement de la plateforme selon les besoins spécifiques de l'organisation.

Ce module regroupe non seulement les documents de configuration des différents modules métier, mais également les outils de gestion des utilisateurs, l'accès aux journaux et logs système ainsi que les utilitaires transverses tels que les notifications, les workflows (flux de travail), les tâches à faire (todo), les calendriers et les règles d'attribution automatique.

Les paramètres système accessibles via le document *Paramètres Système* définissent les comportements globaux de l'application indépendamment des configurations spécifiques à chaque module.

Ces paramètres incluent :

- la désactivation ou l'activation de fonctionnalités transverses comme la possibilité pour les utilisateurs de modifier leurs profils
- l'autorisation de création de comptes utilisateurs par auto-inscription
- la configuration du nombre maximum de tentatives de connexion échouées avant verrouillage d'un compte
- la durée de conservation des documents supprimés avant purge définitive.

Le document permet également de définir des préférences d'affichage globales telles que le format de date et d'heure par défaut, le premier jour de la semaine pour les calendriers ou le fuseau horaire du système.

Les valeurs par défaut globales sont une extension des paramètres système, s'appliquant uniquement à l'application Dokos (les paramètres système sont liés au cadriciel Dodock) et permettent de configurer des éléments plus métiers, comme la société par défaut ou la devise.

Chaque module fonctionnel de Dokos dispose de ses propres documents de paramétrage spécifiques regroupés dans le module Administration sous des sections dédiées.

Le module Comptabilité propose des paramètres comptables permettant de configurer les règles régissant les écritures comptables, la TVA ou les règles associées à la clôture.

Le module Ventes et le module Achats comportent des paramètres configurant les règles de nommage des clients/fournisseurs, les listes de prix par défaut et les paramètres applicables aux transactions de vente et d'achat.

Les paramètres des stocks permettent de définir les règles applicables aux articles stockés, les règles de valorisation, de réservation de stock, de numéros de lots et numéros de série, ainsi que les éléments liés à la planification et clôture des stocks.

Les modules de ressources humaines, de **gestion de projet**, de **support client,** de **production** et **CRM** disposent également de leurs documents de configuration spécifiques accessibles depuis le module Administration.

Cette structuration modulaire des paramètres permet aux responsables fonctionnels de chaque domaine d'accéder facilement aux configurations relevant de leur périmètre sans être exposés à la complexité des paramètres d'autres modules qu'ils n'utilisent pas.

Le module Administration regroupe également les outils de gestion des utilisateurs permettant de créer, modifier et désactiver les comptes, d'attribuer les rôles et permissions appropriés et de configurer les restrictions d'accès.

L'accès aux journaux système et applicatifs facilite le diagnostic des problèmes en permettant la consultation des traces d'erreurs, des avertissements et des événements significatifs survenus dans le système. Les outils transverses disponibles incluent le gestionnaire de notifications permettant de configurer des alertes automatiques sur événements spécifiques, le concepteur de workflows pour la mise en place de processus d'approbation, le gestionnaire de tâches à faire pour suivre les actions en attente et le configurateur de calendriers pour gérer les différents calendriers utilisés par l'organisation.

6.2. Surveillance des performances et ressources

La surveillance continue des performances du système Dokos permet d'identifier proactivement les problèmes potentiels avant qu'ils n'impactent significativement les utilisateurs et de dimensionner correctement l'infrastructure en fonction de la charge réelle.

L'interface d'administration intègre un tableau de bord : *Analyse de la santé du système*, affichant les métriques essentielles en temps réel ou quasi-réel, incluant le nombre d'utilisateurs actifs, l'état des tâches de fond et l'occupation de l'espace disque. Ces indicateurs permettent de détecter rapidement une saturation des ressources qui pourrait dégrader les performances ou provoquer des dysfonctionnements.

Les performances de la base de données constituent un facteur déterminant de la réactivité globale du système et méritent une attention particulière.

Les requêtes lentes représentent souvent le principal goulot d'étranglement et peuvent être identifiées via l'analyse des journaux de MariaDB ou via l'outil **Enregistreur (Recorder)** intégré à Dokos qui tracent les temps d'exécution des opérations. L'examen régulier de ces requêtes lentes permet d'identifier les opportunités d'optimisation par l'ajout d'index, la réécriture de requêtes ou l'ajustement de la structure des données. La taille de la base de données et sa croissance au fil du temps doivent être surveillées pour planifier l'extension du stockage avant saturation.

Les opérations de maintenance telles que l'optimisation des tables et l'analyse des statistiques améliorent les performances en maintenant les structures de données dans un état optimal.

La surveillance des processus d'arrière-plan et des files d'attente fournit des informations cruciales sur la capacité du système à traiter la charge de travail asynchrone. Un nombre croissant de tâches en attente dans les files signale généralement un déséquilibre entre la charge de travail et les ressources allouées aux workers.

Le tableau de bord des **Tâche RQ** affiche le nombre de tâches dans chaque file, le nombre de tâches en cours de traitement et le nombre de tâches échouées nécessitant une intervention. Pour les environnements hautement sollicités, des outils de monitoring externes tels que Prometheus combiné avec Kibana peuvent être déployés pour collecter et visualiser des métriques détaillées avec des capacités d'alerting automatique lorsque des seuils prédéfinis sont dépassés. Ce système est mis en place sur le service Dokos Cloud.

6.3. Gestion des logs système et applicatifs

Les fichiers journaux (logs) constituent une source d'information essentielle pour comprendre le comportement du système, diagnostiquer les problèmes et assurer la traçabilité des opérations effectuées. Dokos génère plusieurs types de journaux répartis dans différents emplacements selon leur nature et leur origine. Les journaux applicatifs produits par le cadriciel Dodock et les

applications Dokos se trouvent dans le répertoire logs de chaque site et contiennent les traces d'exécution des processus, les erreurs rencontrées, les avertissements et les informations de débogage selon le niveau de verbosité configuré. Ces fichiers sont organisés par type de service avec des journaux distincts pour le serveur web, les workers d'arrière-plan et le planificateur de tâches.

Les journaux système gérés par systemd pour les services Dokos en mode production sont accessibles via la commande *journalctl* qui permet de filtrer les messages par service, par période temporelle ou par niveau de sévérité. Cette commande offre une interface puissante pour naviguer dans les volumes importants de journaux générés quotidiennement et extraire les informations pertinentes pour une investigation. Les journaux du serveur web Nginx situés dans le répertoire standard de journalisation système contiennent les traces de toutes les requêtes HTTP reçues avec leurs codes de statut, les adresses IP sources et les temps de traitement. L'analyse de ces journaux d'accès révèle les patterns d'utilisation, les pages les plus consultées et les éventuelles tentatives d'accès non autorisé ou d'exploitation de vulnérabilités.

La rotation automatique[6] de ces fichiers est effectuée par le cadriciel Dodock, selon des règles indiquées dans le dossier de maintenance.

L'indexation et la centralisation des journaux via des solutions telles que la pile ELK (Elasticsearch, Logstash, Kibana) ou des alternatives comme Loki facilitent la recherche et l'analyse des événements à travers l'ensemble des composants du système, particulièrement utile pour les installations distribuées ou multiserveurs où la corrélation des événements entre différentes sources devient complexe. Ce système est mis en place sur le service Dokos Cloud.

6.4. Maintenance préventive et mises à jour

La maintenance préventive régulière du système Dokos garantit sa stabilité à long terme et prévient l'accumulation de problèmes mineurs pouvant conduire à des dysfonctionnements majeurs.

Cette maintenance comprend plusieurs activités récurrentes à planifier selon un calendrier défini.

L'optimisation périodique de la base de données via la commande OPTIMIZE TABLE ou via les outils intégrés de Dokos (Actions > Optimiser dans le rapport **Utilisation de la base de**

[6] Exigence 13

données par table) défragmente les tables, récupère l'espace inutilisé et met à jour les statistiques d'index utilisées par l'optimiseur de requêtes. Cette opération améliore les performances des requêtes et réduit l'espace disque occupé, particulièrement bénéfique après des suppressions massives de données ou des imports importants. La vérification de l'intégrité des fichiers du système via des sommes de contrôle ou des outils de détection d'anomalies permet d'identifier précocement les corruptions pouvant résulter de défaillances matérielles. Sur un système certifié, cette vérification prend un caractère préventif particulier pour les PDF originaux archivés : chacun est nommé d'après son empreinte SHA-256, ce qui permet de recalculer et de comparer l'empreinte de chaque fichier sans recourir à un référentiel externe. Une divergence signale une corruption à traiter avant qu'elle ne soit découverte au moment d'une réémission, c'est-à-dire face au client.

Les mises à jour du système Dokos suivent un processus structuré visant à appliquer les corrections de bugs, les améliorations de sécurité et les nouvelles fonctionnalités tout en minimisant les risques de régression ou d'interruption de service.

Dokos suit un cycle de publication avec des versions majeures introduisant des changements structurels significatifs et des versions mineures apportant des corrections et améliorations incrémentales. La procédure de mise à jour commence par la consultation des notes de version (release notes) qui détaillent les modifications apportées, les éventuelles incompatibilités introduites et les actions requises avant ou après la mise à jour. Une sauvegarde complète du système doit impérativement être effectuée avant toute opération de mise à jour pour permettre un retour en arrière en cas de problème.

L'exécution technique de la mise à jour s'effectue via les commandes bench qui orchestrent les différentes étapes du processus. La commande *bench update* télécharge les dernières versions des applications installées depuis leurs dépôts Git, installe les dépendances Python et Node mises à jour, compile les ressources front-end et exécute les migrations de base de données nécessaires pour adapter le schéma aux nouvelles versions. Cette opération peut nécessiter plusieurs minutes et impose généralement une interruption temporaire du service, d'où l'importance de planifier les mises à jour pendant les fenêtres de maintenance convenues avec les utilisateurs. Après la mise à jour, des tests de validation doivent vérifier le bon fonctionnement des fonctionnalités critiques avant de remettre le système en service normal.

Pour les environnements Dokos Cloud, les mises à jour sont gérées par Dokos SAS selon un calendrier planifié détaillé dans le dossier de maintenance, garantissant ainsi l'application uniforme des correctifs de sécurité et l'homogénéité des versions. L'architecture de Nuage, l'outil d'hébergement sous-jacent à Dokos basé sur Press, garantit une interruption de service minimale voire nulle et une gestion automatisée des erreurs lors de la migration.

6.5. Résolution des incidents courants

La résolution efficace des incidents repose sur une méthodologie systématique combinant l'analyse des symptômes, la consultation des journaux et l'application de solutions éprouvées. Les incidents les plus fréquemment rencontrés dans un système Dokos incluent les problèmes de performance se manifestant par une lenteur généralisée de l'interface, les erreurs d'authentification empêchant les utilisateurs de se connecter, les échecs d'envoi d'emails bloquant les communications automatiques, et les erreurs lors de la génération de documents PDF. Pour chaque catégorie d'incident, des procédures de diagnostic et de résolution standardisées permettent d'accélérer le rétablissement du service normal et de limiter l'impact sur l'activité des utilisateurs.

Les problèmes de performance nécessitent généralement une investigation en plusieurs étapes commençant par la vérification des ressources système pour identifier d'éventuelles saturations.

Une charge processeur constamment élevée peut indiquer des requêtes inefficaces, des boucles infinies dans du code personnalisé ou un nombre insuffisant de workers pour traiter la charge. Une consommation excessive de mémoire suggère des fuites mémoire dans des processus ou une charge de travail dépassant les capacités de l'infrastructure. L'analyse des requêtes lentes en base de données révèle fréquemment des opérations mal optimisées nécessitant l'ajout d'index ou la réécriture de rapports complexes.

Le redémarrage des services via *bench restart* résout temporairement certains problèmes de performance liés à l'accumulation de ressources non libérées, mais ne constitue pas une solution pérenne si le problème sous-jacent n'est pas identifié et corrigé.

Les erreurs de génération de documents PDF proviennent souvent d'une installation incorrecte de wkhtmltopdf ou de l'utilisation d'une version non compatible. La vérification de la présence et de l'exécutabilité du binaire wkhtmltopdf via la commande which wkhtmltopdf constitue le premier diagnostic. Les problèmes de rendu peuvent résulter de l'utilisation d'une version standard plutôt que de la version avec correctifs Qt, nécessitant le remplacement du binaire par la version appropriée.

Une seconde catégorie d'erreur, propre aux systèmes disposant du module Certification Caisse, concerne les justificatifs devenus inémettables. Toute réémission d'un justificatif déjà émis (réimpression, renvoi par courriel, duplicata explicite) est dérivée du fichier PDF original archivé dans l'espace de fichiers privé du site, et non d'un nouveau rendu du document. Si ce fichier est absent ou si son empreinte ne correspond plus à celle consignée au Journal SAS, le justificatif

ne peut plus être émis : le système refuse l'opération et affiche un message explicite indiquant que le fichier original archivé est introuvable et que le duplicata ne peut pas être généré. Ce comportement est délibéré: reconstituer le document à partir des données actuelles produirait un justificatif différent de celui remis au client.

Un original manquant empêche toute réémission du justificatif concerné. Le diagnostic consiste à vérifier la présence du fichier dans le répertoire des fichiers privés du site, sous un nom dérivé de l'empreinte SHA-256 consignée dans l'enregistrement SD_ImpressionOriginal correspondant. La cause la plus fréquente est une restauration de la base de données sans restauration concomitante des fichiers, ou une sauvegarde des fichiers moins fréquente que celle de la base (voir §5.1 et §5.4).

La résolution consiste à restaurer le fichier depuis une sauvegarde des fichiers. Aucune reconstitution n'est possible : le Journal SAS est une chaîne signée à ajout seul, et y insérer un enregistrement correspondant à un fichier reconstruit constituerait une falsification. Il n'existe pas à ce jour d'outil de diagnostic recensant les originaux archivés manquants ; la vérification se fait au cas par cas.

Les échecs d'envoi d'emails nécessitent la vérification de la configuration SMTP dans les paramètres système, le test de connectivité au serveur de messagerie et l'examen des journaux pour identifier les messages d'erreur spécifiques retournés par le serveur SMTP.

Les problèmes d'authentification peuvent résulter de cookies corrompus, de sessions expirées ou de modifications de configuration, et se résolvent généralement par la suppression des cookies du navigateur ou la réinitialisation du mot de passe utilisateur.

Le forum communautaire est une base d'information importante pour aider à résoudre les problèmes les plus couramment rencontrés: *https://community.dokos.io/*

6.6. Outils de diagnostic intégrés

Dokos intègre plusieurs outils de diagnostic facilitant l'identification et la résolution des problèmes cités dans les paragraphes précédents:

- La page **Analyse de la santé du système**
- Le rapport **Utilisation de la base de données par table**

- La page **Enregistreur**
- La **Console Système** pour exécuter des commandes en Python et accéder à l'API Frappe.

7. Sécurité et conformité

7.1. Mesures de sécurisation du système

La sécurisation d'un système Dokos repose sur une approche de défense en profondeur combinant plusieurs couches de protection complémentaires pour minimiser les risques d'intrusion, de compromission ou de perte de données.

Au niveau de l'infrastructure**,** le **durcissement du système d'exploitation** constitue la première ligne de défense et comprend la désactivation des services inutiles, la configuration d'un pare-feu restrictif n'autorisant que les ports strictement nécessaires et l'application systématique des correctifs de sécurité publiés par l'éditeur de la distribution Linux. Le pare-feu doit être configuré pour n'autoriser que les connexions HTTPS sur le port 443 depuis l'extérieur, tout en bloquant l'accès direct aux ports de la base de données MariaDB et de Redis qui ne doivent être accessibles que localement ou depuis des adresses IP spécifiquement autorisées pour l'administration système.

Politique par défaut :

- Entrées : DENY (tout bloqué par défaut)
- Sorties : ALLOW (autorisé)

Ports ouverts :

- Port 80/tcp (HTTP) : Ouvert uniquement pour redirection HTTPS
- Port 443/tcp (HTTPS) : Ouvert pour le trafic applicatif chiffré
- Port 22/tcp (SSH) : Ouvert via authentification par clé Ed25519 ou RSA 4096 bits
- Ports internes : Communication entre serveurs sur ports spécifiques (bases de données, réplication) avec restriction par IP source

L'isolation des composants via **des comptes utilisateurs système distincts** renforce la sécurité en limitant l'impact potentiel d'une compromission. Les processus Dokos s'exécutent

sous un compte non privilégié distinct du compte root, empêchant ainsi un attaquant ayant compromis l'application d'obtenir immédiatement un contrôle total du serveur.

Les permissions sur les fichiers et répertoires doivent être configurées selon le principe du moindre privilège, chaque composant n'ayant accès qu'aux ressources strictement nécessaires à son fonctionnement.

Les **fichiers téléversés** par les utilisateurs sont stockés dans des répertoires dédiés avec des permissions empêchant leur exécution comme scripts ou programmes, prévenant ainsi l'injection de code malveillant via l'upload de fichiers.

La sécurisation de la base de données MariaDB nécessite plusieurs mesures complémentaires incluant :

- la modification du mot de passe root par défaut
- la suppression des comptes anonymes et de test créés lors de l'installation
- la restriction des connexions pour n'autoriser que les adresses IP du serveur Dokos
- L'activation de l'audit des connexions et des requêtes sensibles permet de détecter les tentatives d'accès non autorisé ou les comportements anormaux.

La mise en place d'une **supervision de sécurité active** permet de détecter rapidement les incidents et d'y répondre avant qu'ils ne causent des dommages significatifs. Les systèmes de détection d'intrusion tels que Fail2ban peuvent être configurés pour analyser les journaux d'accès et bloquer automatiquement les adresses IP manifestant des comportements suspects comme des tentatives répétées de connexion échouées ou des scans de vulnérabilités.

Les alertes automatiques doivent être configurées pour notifier les administrateurs en cas d'événements critiques tels que des modifications de configuration sensibles, des accès privilégiés inhabituels ou des volumes de trafic anormaux.

La réalisation périodique d'audits de sécurité via des outils automatisés ou par des experts externes permet d'identifier les vulnérabilités émergentes et de vérifier l'efficacité des mesures de protection déployées.

7.2. Chiffrement des communications

Le chiffrement des communications constitue une protection indispensable pour garantir la confidentialité et l'intégrité des données échangées entre les utilisateurs et le système Dokos.

L'utilisation du protocole HTTPS avec TLS version 1.3 ou supérieure doit être systématiquement imposée pour toutes les connexions au système, empêchant ainsi l'interception des identifiants, des données métier sensibles et des cookies de session par des attaquants positionnés sur le réseau.

La configuration du serveur web Nginx doit forcer la redirection automatique de toutes les tentatives de connexion HTTP vers HTTPS, garantissant qu'aucune communication en clair ne puisse survenir même si un utilisateur omet de spécifier le protocole sécurisé dans l'URL.

L'en-tête HTTP Strict Transport Security (HSTS) doit être activé pour instruire les navigateurs de n'utiliser que HTTPS pour toutes les connexions futures au domaine, même si l'utilisateur tente explicitement d'accéder en HTTP.

Les certificats SSL/TLS utilisés pour le chiffrement doivent être émis par une autorité de certification reconnue pour garantir leur acceptation par les navigateurs sans avertissement de sécurité. Les certificats Let's Encrypt constituent une solution gratuite et largement acceptée, avec renouvellement automatique via l'outil certbot évitant les expirations inopinées qui bloquerait l'accès au système. La configuration du serveur doit privilégier les suites de chiffrement fortes en désactivant les algorithmes obsolètes ou présentant des vulnérabilités connues. Les recommandations de l'ANSSI fournissent des configurations de référence adaptées selon le niveau de sécurité souhaité et les contraintes de compatibilité avec les navigateurs anciens.

Le chiffrement s'applique également aux communications sortantes du système Dokos, notamment pour l'envoi d'emails via SMTP et l'interrogation de services externes. Les connexions aux serveurs SMTP doivent utiliser **STARTTLS ou SMTPS** pour chiffrer le transit des messages électroniques contenant potentiellement des informations sensibles. Les webhooks et les intégrations avec des API tierces doivent privilégier les connexions HTTPS pour protéger les données échangées et les jetons d'authentification utilisés. Pour les communications entre serveurs dans une architecture distribuée ou entre environnements de production et de sauvegarde, l'établissement de tunnels VPN ou l'utilisation de protocoles sécurisés comme SSH garantit la confidentialité des transferts même à travers des réseaux non fiables.

7.3. Gestion des mots de passe et politique de sécurité

La robustesse de la gestion des mots de passe constitue un pilier fondamental de la sécurité globale du système Dokos car les identifiants représentent souvent le vecteur d'attaque le plus exploité.

Les paramètres système permettent de définir une politique de mots de passe imposant des exigences de complexité minimale incluant une longueur minimale recommandée d'au moins douze caractères, l'obligation de combiner majuscules, minuscules, chiffres et caractères spéciaux, et l'interdiction de réutiliser les mots de passe précédents.

Ces contraintes techniques doivent être complétées par une sensibilisation des utilisateurs aux bonnes pratiques de création et de gestion de mots de passe, notamment l'utilisation de phrases de passe longues mais mémorables plutôt que des combinaisons aléatoires difficiles à retenir qui encouragent les pratiques dangereuses comme la réutilisation ou la notation sur support physique.

L'expiration périodique des mots de passe peut être configurée pour forcer les utilisateurs à renouveler régulièrement leurs identifiants, bien que cette pratique fasse l'objet de débats dans la communauté de la sécurité car elle peut conduire à des comportements contre-productifs comme l'utilisation de variations mineures prévisibles ou l'affaiblissement progressif de la complexité. Une approche alternative consiste à imposer le changement de mot de passe uniquement en cas d'indication de compromission plutôt que de manière systématique, tout en maintenant des exigences de complexité élevées.

Les mots de passe sont stockés dans la base de données sous forme de hachages cryptographiques utilisant l'algorithme Argon2, rendant extrêmement difficile leur récupération même en cas d'accès non autorisé à la base de données. Le système ajoute automatiquement un sel aléatoire unique pour chaque mot de passe avant hachage, empêchant les attaques par tables arc-en-ciel précalculées.

L'authentification multifacteur (MFA) ajoute une couche de sécurité significative en exigeant un second facteur de vérification en complément du mot de passe lors de la connexion. Dokos supporte l'authentification à deux facteurs basée sur des codes temporaires générés par des applications comme Google Authenticator, Microsoft Authenticator ou Authy installées sur le smartphone de l'utilisateur. L'activation de cette fonctionnalité peut être rendue obligatoire pour les comptes disposant de privilèges élevés comme les responsables système ou pour tous les

utilisateurs. Le processus d'enrôlement guide l'utilisateur à travers la configuration initiale incluant le scan d'un code QR et la validation du premier code généré.

La gestion des tentatives de connexion échouées constitue une protection essentielle contre les attaques par force brute visant à deviner les mots de passe.

Le système enregistre chaque tentative infructueuse et peut être configuré pour verrouiller temporairement un compte après un nombre défini d'échecs consécutifs, par défaut 10 tentatives par minute. Des options de configuration sont disponibles dans les paramètres système.

Le système de réinitialisation de mot de passe oublié utilise un mécanisme sécurisé envoyant un lien à usage unique avec expiration temporelle à l'adresse email enregistrée, empêchant son utilisation pour prendre le contrôle d'un compte sans accès à la boîte email associée. Le nombre maximum de mails de récupération de mots de passe envoyés par heure est paramétrable également dans les paramètres système.

7.4. Traçabilité et journalisation des actions[7]

La traçabilité des actions effectuées dans le système Dokos remplit plusieurs objectifs complémentaires incluant la sécurité, la conformité réglementaire et la résolution de problèmes.

Le système enregistre automatiquement un ensemble d'informations pour chaque modification de document incluant l'identité de l'utilisateur ayant effectué l'action, la date et l'heure précise de l'opération, la nature de la modification effectuée et éventuellement les valeurs avant et après modification pour les champs significatifs.

Ces informations sont stockées de manière persistante dans des tables dédiées de la base de données et ne peuvent être modifiées ou supprimées par les utilisateurs standard, garantissant ainsi l'intégrité de la piste d'audit. L'accès à ces journaux d'audit est restreint aux utilisateurs disposant de privilèges d'administration appropriés.

L'interface de consultation de l'historique des documents permet de visualiser chronologiquement toutes les modifications apportées à un enregistrement particulier depuis sa création. La section **Activité** remplit ce rôle dans tous les types de documents de Dokos, en affichant toutes les informations de versions enregistrées dans la table **Version** ou dans la table **Commentaire**.

[7] Exigence 15

La journalisation des événements système[8] complète la traçabilité applicative en enregistrant les actions techniques d'administration et les événements de sécurité significatifs. Les connexions et déconnexions d'utilisateurs sont systématiquement consignées dans le document type : **Journal d'activité** avec l'horodatage, l'adresse IP source et l'utilisateur du navigateur, permettant de détecter des connexions anormales depuis des localisations inhabituelles.

Les modifications de configuration sensibles comme les changements de permissions, la création ou suppression de comptes utilisateurs, les modifications de paramètres système ou l'installation d'applications génèrent des entrées détaillées dans les journaux d'audit système correspondants à condition que le suivi des modifications soit activé.

Traçabilité fiscale des émissions de justificatifs. Sur un système disposant du module Certification Caisse, la traçabilité des justificatifs remis relève d'un mécanisme distinct des journaux décrits ci-dessus : le Journal SAS, chaîne d'enregistrements signés cryptographiquement et chaînés entre eux. Chaque émission d'un justificatif y donne lieu à un enregistrement: SD_ImpressionOriginal pour la première remise, SD_ImpressionDuplicata pour chacune des suivantes, avec son numéro d'ordre et son canal. La consultation d'un justificatif à l'écran n'y produit aucun enregistrement. Ces enregistrements sont décrits au dossier de spécifications fonctionnelles, §5.10 et §7.3, et au dossier d'architecture technique, §10.3.

La conservation à long terme des journaux est configurable via les **Paramètres de journaux**. Les responsables système peuvent ajuster les durées de rétention de chaque journal selon les besoins de l'entreprise ou la réglementation locale. Dokos ne dispose pas de système d'archivage progressif pour les journaux d'audit, le stockage est intégralement effectué en base de données.

Ce paramétrage de rétention ne s'applique pas au Journal SAS : celui-ci est une chaîne signée à ajout seul, dont aucun enregistrement ne peut être supprimé ni modifié, y compris par un responsable système. Le système ne dispose d'aucune fonctionnalité de purge, totale ou partielle, des données d'encaissement.

7.5. Protection contre les menaces courantes

La protection contre les menaces courantes visant les applications web nécessite la mise en œuvre de mécanismes de défense spécifiques pour chaque catégorie d'attaque.

[8] Exigence 15

Les injections SQL

Elles représentent l'une des vulnérabilités les plus critiques et consistent à insérer du code SQL malveillant dans les entrées utilisateur pour manipuler les requêtes exécutées par l'application.

Dokos utilise systématiquement des requêtes paramétrées et des mécanismes d'échappement fournis par le cadriciel Dodock pour neutraliser automatiquement toute tentative d'injection, rendant cette attaque inefficace dans les conditions normales d'utilisation. Les développeurs de personnalisations ou d'applications tierces doivent impérativement respecter ces bonnes pratiques et éviter la construction de requêtes SQL par concaténation directe de chaînes incluant des données utilisateur.

Les attaques par script intersite (XSS - Cross-Site Scripting)

Les attaques par script intersite (XSS - Cross-Site Scripting) visent à injecter du code JavaScript malveillant qui sera exécuté dans le navigateur d'autres utilisateurs, permettant le vol de cookies de session, la modification de l'interface ou l'exécution d'actions non autorisées.

La protection contre cette menace repose sur l'échappement systématique des données utilisateur avant leur affichage dans les pages HTML, transformant les caractères spéciaux en entités HTML inoffensives.

Le cadriciel Dodock applique automatiquement cet échappement dans la majorité des contextes d'affichage, mais les développeurs doivent rester vigilants lors de l'utilisation de fonctions permettant l'injection de HTML brut. La politique de sécurité du contenu (CSP - Content Security Policy) configurée via les en-têtes HTTP renforce la protection en restreignant les sources autorisées pour le chargement de scripts, feuilles de style et autres ressources. Il est à ajuster dans la configuration Nginx en fonction des usages et des bonnes pratiques de chaque organisation utilisatrice de Dokos.

Les attaques par falsification de requête intersites (CSRF - Cross-Site Request Forgery)

Les attaques par falsification de requête intersites (CSRF - Cross-Site Request Forgery) exploitent la confiance qu'un site accorde à un utilisateur authentifié en lui faisant exécuter involontairement des actions via des requêtes forgées depuis un site tiers malveillant.

Dokos implémente une protection CSRF via l'utilisation de jetons uniques générés pour chaque session et validés lors de chaque requête modifiant des données. Ces jetons sont transmis dans les formulaires et vérifiés côté serveur avant l'exécution de l'action demandée, garantissant que la requête provient légitimement de l'interface Dokos et non d'un site externe. Les requêtes dépourvues de jeton valide sont systématiquement rejetées.

Les attaques par déni de service (DoS - Denial of Service)

Les attaques par déni de service (DoS - Denial of Service) visent à rendre le système indisponible en saturant ses ressources via un volume excessif de requêtes ou via des requêtes spécialement conçues pour consommer un maximum de ressources.

La limitation du taux de requêtes (rate limiting) configurée dans Nginx restreint le nombre de requêtes qu'une adresse IP peut effectuer dans un intervalle de temps donné, bloquant automatiquement les sources générant un trafic anormal. Il peut être accompagné de l'utilisation de Fail2Ban pour bannir les adresses IP identifiées comme malveillantes.

Les timeouts configurés sur les requêtes longues empêchent qu'une opération mal optimisée ou malveillante ne monopolise indéfiniment un worker.

Pour les attaques distribuées (DDoS) orchestrées depuis de nombreuses adresses IP différentes, l'utilisation de services de protection spécialisés comme Cloudflare ou des solutions de filtrage au niveau réseau devient nécessaire pour absorber le volume d'attaque avant qu'il n'atteigne l'infrastructure de production.

La configuration de ces services est extérieure au logiciel Dokos.

8. Migration, réversibilité des données et remplacement du système

8.1. Export des données et formats supportés[9]

L'export des données depuis Dokos constitue une fonctionnalité essentielle permettant de récupérer les informations stockées dans le système pour archivage, analyse externe, migration vers une autre plateforme ou conformité réglementaire.

Le système propose plusieurs mécanismes d'export adaptés à différents besoins et niveaux de granularité.

L'export via l'interface utilisateur

Il permet de télécharger les données affichées dans n'importe quelle liste de documents au format tableur, offrant une méthode simple et accessible pour extraire des ensembles de données ciblés.

Cette fonctionnalité génère des fichiers au format Excel (XLSX) ou CSV (valeurs séparées par virgules) incluant les colonnes visibles dans la vue liste avec possibilité de personnaliser les champs exportés via la configuration des filtres et des colonnes affichées. Cette fonctionnalité est disponible dans le module **d'Administration** via les modules d'**Import et d'Export de données.**

L'export via les outils de sauvegarde

L'export complet de la base de données via les outils de sauvegarde intégrés génère un fichier SQL contenant l'intégralité du schéma et des données dans un format restaurable directement dans une instance MariaDB.

Ce format technique convient particulièrement pour les migrations complètes, les archivages réglementaires ou les transferts entre environnements Dokos.

Le fichier SQL préserve toutes les relations entre tables, les contraintes d'intégrité et les index, garantissant une reproduction fidèle de la structure de données. Pour les migrations vers des systèmes non basés sur Dodock, des outils de transformation peuvent être nécessaires pour

[9] Exigence 19

convertir le schéma SQL et adapter les structures de données aux conventions du système cible. L'export des fichiers attachés et documents générés nécessite une extraction séparée du répertoire de fichiers du site, ces éléments n'étant pas inclus dans la sauvegarde SQL.

L'export via les API REST

Les API REST de Dokos offrent une méthode programmatique d'extraction de données permettant l'automatisation d'exports réguliers ou l'intégration avec des systèmes externes.

Ces interfaces acceptent des requêtes structurées spécifiant les types de documents à extraire, les filtres à appliquer et les champs à inclure dans la réponse, retournant les données au format JSON facilement traitable par des scripts ou des applications tierces.

Cette approche s'avère particulièrement adaptée pour les synchronisations incrémentales où seules les données modifiées depuis le dernier export doivent être extraites. Les webhooks configurables permettent également de pousser automatiquement certaines données vers des systèmes externes lors d'événements spécifiques, inversant le modèle traditionnel d'extraction par interrogation.

Pour les organisations nécessitant des formats d'export spécifiques répondant à des normes sectorielles ou réglementaires, des développements personnalisés peuvent implémenter des exportateurs dédiés générant les fichiers dans les formats requis.

8.2. Procédure de migration vers nouvelle version

La migration vers une nouvelle version de Dokos suit un processus structuré visant à intégrer les améliorations, corrections et nouvelles fonctionnalités tout en préservant l'intégrité des données existantes et la continuité de service.

Etape 1 : La préparation

La préparation constitue l'étape initiale critique déterminant largement le succès de l'opération.

Cette phase comprend la consultation détaillée des notes de version (release notes) publiées par Dokos qui documentent exhaustivement les changements apportés, les éventuelles incompatibilités introduites, les fonctionnalités obsolètes retirées et les prérequis techniques modifiés.

Une attention particulière doit être portée aux changements majeurs (breaking changes) susceptibles d'affecter les personnalisations existantes, les intégrations avec des systèmes tiers ou les workflows métier établis.

Etape 2 : Création d'une sauvegarde complète

La création d'une sauvegarde complète précédant immédiatement la migration constitue une obligation absolue permettant le retour à l'état antérieur en cas de problème. Cette sauvegarde doit inclure non seulement la base de données via *bench backup* mais également l'intégralité du répertoire bench incluant les fichiers de configuration, les personnalisations et les fichiers téléversés.

Etape 3 : validation de l'intégrité des sauvegardes

La validation de l'intégrité de ces sauvegardes et leur transfert vers un emplacement distinct du serveur de production garantissent leur disponibilité même en cas de défaillance majeure du système.

Pour les environnements critiques, la migration devrait d'abord être testée sur un environnement de préproduction ou de développement cloné depuis la production, permettant d'identifier et de résoudre les problèmes potentiels avant d'affecter le système en service.

Etape 4 : Exécution de la migration

L'exécution technique de la migration s'effectue principalement via la commande *bench update* qui orchestre automatiquement les multiples étapes du processus.

Cette commande télécharge les dernières versions des applications depuis leurs dépôts Git, met à jour les dépendances Python et Node nécessaires, recompile les ressources front-end et déclenche les scripts de migration de base de données qui adaptent progressivement le schéma et les données aux exigences de la nouvelle version.

Les migrations de base de données (database migrations) constituent des opérations délicates pouvant inclure la création de nouvelles tables, l'ajout ou la suppression de colonnes, la transformation de données existantes ou la restructuration de relations. Ces opérations s'exécutent de manière séquentielle et idempotente, garantissant qu'une migration interrompue peut être relancée sans corruption de données.

La durée de l'opération de migration varie considérablement selon le volume de données à traiter, la complexité des transformations requises et les performances de l'infrastructure. Les migrations mineures sur des bases de données modestes s'effectuent généralement en quelques minutes, tandis que les migrations majeures sur des systèmes volumineux peuvent nécessiter plusieurs dizaines de minutes.

Durant cette période, le système est placé en mode maintenance pour empêcher les utilisateurs d'accéder et de modifier des données pendant les transformations, prévenant ainsi les incohérences ou corruptions.

Etape 5 : Validation de la migration

Après l'exécution réussie de la migration, une phase de validation approfondie doit vérifier le bon fonctionnement des fonctionnalités critiques, la cohérence des données transformées et l'absence de régressions avant de rouvrir l'accès aux utilisateurs.

Pour les environnements Dokos Cloud, les migrations sont orchestrées par l'équipe technique de Dokos SAS selon un calendrier planifié décrit dans le dossier de maintenance, minimisant ainsi les risques et garantissant un support immédiat en cas de difficulté.

8.3. Migration depuis ERPNext

La migration depuis ERPNext vers Dokos présente des particularités spécifiques liées à l'historique de développement de Dokos en tant que fork (adaptation) du projet ERPNext.

Cette filiation commune signifie que les deux systèmes partagent une architecture technique similaire basée sur le cadriciel Frappe et une structure de données largement compatible, facilitant considérablement le processus de migration comparativement à une migration entre systèmes complètement distincts.

Les versions récentes de Dokos maintiennent une compatibilité structurelle avec ERPNext permettant dans de nombreux cas une migration relativement directe des données et configurations. Cette compatibilité ne garantit cependant pas une équivalence fonctionnelle totale car Dokos a progressivement divergé d'ERPNext en introduisant des fonctionnalités spécifiques, en modifiant certains comportements et en adaptant l'interface aux besoins du marché francophone.

Toute opération de migration depuis ERPNext nécessite une analyse approfondie des divergences et des tests extensifs. Dokos SAS ne garantit pas la compatibilité complète entre les deux applications.

La procédure de migration technique commence par l'évaluation de la version ERPNext actuellement utilisée et l'identification de la version Dokos cible compatible. La migration peut souvent s'effectuer par la création d'un nouvel environnement bench basé sur Dodock/Dokos, suivi d'une réinstallation avec import de données des données de l'ancien environnement. Après réinstallation, l'opération bench update va lancer la migration des données de la base de données et l'exécution des patches de migration.

Les scripts personnalisés, les rapports développés spécifiquement et les intégrations avec des systèmes tiers nécessitent une révision et potentiellement une adaptation pour assurer leur compatibilité avec les spécificités de Dokos. Cette phase de vérification et d'adaptation justifie une planification minutieuse avec identification anticipée des dépendances critiques.

Les organisations envisageant une migration depuis ERPNext vers Dokos sont fortement encouragées à solliciter l'accompagnement de Dokos SAS ou de partenaires certifiés disposant de l'expertise spécifique à ce type d'opération. Cette assistance professionnelle permet d'identifier les risques potentiels, de planifier une stratégie de migration adaptée au contexte particulier de l'organisation, d'exécuter les opérations techniques dans les conditions optimales et de résoudre rapidement les difficultés éventuelles.

Pour les clients souhaitant bénéficier de la certification LNE après migration, des étapes supplémentaires incluant l'installation de l'application Certification Caisse et la mise en conformité des processus selon les exigences du référentiel doivent être planifiées. La migration représente également une opportunité de réviser les configurations, de nettoyer les données obsolètes et d'optimiser les processus métier pour tirer pleinement parti des capacités spécifiques de Dokos.

8.4. Désinstallation complète du système

Dokos SAS recommande l'installation du système sur un ou plusieurs serveurs dédiés, ce qui simplifie grandement les opérations d'un système Dokos en auto-hébergement.

Avant toute opération de désinstallation, une sauvegarde finale complète et vérifiée doit impérativement être créée et stockée dans un emplacement sûr distinct du serveur, constituant

la dernière opportunité de récupération des données en cas de besoin ultérieur. Cette sauvegarde doit inclure la base de données via bench backup, l'intégralité du répertoire bench avec tous les fichiers de configuration et personnalisations, les fichiers contenant les variables d'environnement et idéalement un export structuré des données métier dans des formats standards facilitant une éventuelle réutilisation future.

L'opération suivante consiste à étendre le serveur applicatif, le serveur de base de données (le cas échéant) et à modifier le paramétrage DNS associé.

8.5. Archivage des données avant remplacement

L'archivage des données avant le remplacement d'un système Dokos par une solution alternative constitue une étape cruciale répondant simultanément à des obligations légales de conservation, des besoins opérationnels potentiels et des exigences de continuité de l'information.

Durée de conservation[10]

La stratégie d'archivage doit être planifiée en fonction des durées de conservation réglementaires applicables selon les juridictions et secteurs d'activité concernés.

- Les données comptables et fiscales sont généralement soumises à des obligations de conservation s'étendant sur six à dix années, imposant le maintien d'archives consultables et auditables pendant ces périodes.
- Les données relatives aux ressources humaines, aux contrats commerciaux ou à certaines transactions spécifiques peuvent être soumises à des durées de conservation distinctes nécessitant une analyse détaillée des obligations applicables.

Format d'archivage[11]

Le format d'archivage doit privilégier des standards ouverts et largement supportés garantissant la capacité de lecture des archives sur le long terme indépendamment de l'évolution des technologies.

[10] Exigence 17
[11] Exigences 10, 17

L'export des données transactionnelles au format CSV ou Excel offre une lisibilité immédiate et une compatibilité universelle, bien que ces formats ne préservent pas la richesse des relations entre documents ni les métadonnées complètes.

Pour une préservation plus fidèle de la structure et des relations, l'archivage de la base de données complète au format SQL accompagné d'une documentation du schéma permet une restauration intégrale dans un environnement MariaDB si nécessaire. Cette approche technique nécessite cependant le maintien d'une expertise et d'une infrastructure capables d'exploiter ces archives, contrainte qui peut devenir problématique sur des durées très longues.

L'archivage des documents générés et des fichiers téléversés constitue un complément indispensable à l'archivage des données structurées.

Ces fichiers incluent les factures PDF, les bons de livraison, les contrats scannés, les pièces justificatives comptables et tous les documents attachés aux transactions. L'organisation de ces fichiers dans une arborescence structurée par type de document et par période facilite leur consultation ultérieure.

Sur un système certifié, ils incluent en outre les PDF originaux archivés des justificatifs émis, conservés dans l'espace de fichiers privé du site et nommés d'après leur empreinte SHA-256. Leur archivage est indispensable : ce sont les exemplaires effectivement remis aux clients, et ils constituent la seule source à partir de laquelle un duplicata conforme peut être reproduit. Leur nom de fichier permet par ailleurs de les rapprocher directement des enregistrements du Journal SAS présents dans l'archive fiscale, qui, elle, ne les contient pas.

L'inclusion de fichiers index au format texte ou tableur référençant les documents archivés avec leurs métadonnées principales permet une recherche efficace même sans système de gestion électronique de documents. Pour les volumes importants, la création d'images disque ou d'archives compressées facilite le stockage et le transfert tout en préservant l'intégrité de l'ensemble.

Documentation d'archivage

La documentation accompagnant les archives constitue un élément essentiel pour garantir leur exploitabilité future. Cette documentation doit décrire la structure des données archivées, expliquer la signification des champs et codes utilisés, documenter les processus métier en vigueur lors de la génération des données et fournir les informations contextuelles nécessaires à leur interprétation correcte. L'inclusion d'un guide de consultation expliquant comment accéder et exploiter les archives permet à des personnes n'ayant pas participé à l'archivage initial de comprendre et utiliser les données.

Le stockage des archives sur supports multiples dans des localisations distinctes protège contre les sinistres physiques ou les défaillances techniques, tandis que la vérification périodique de leur intégrité et lisibilité prévient les dégradations progressives pouvant rendre les données inaccessibles.