RDI Manager by Eurêka C.I

Fiche Technique & Sécurité

1 Introduction

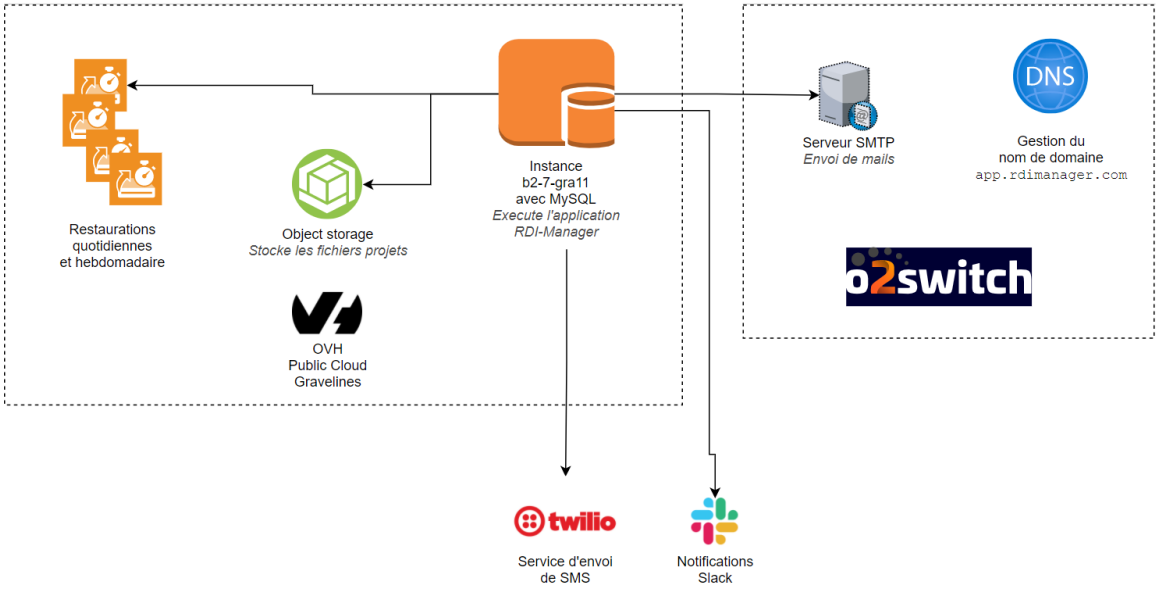
RDI-Manager est une plateforme numérique de management de l'innovation qui se veut simple, intuitive, collaborative, interactive et intelligente. L'objectif de cette plateforme, ainsi que celui de la start-up est d'aider les Grands Groupes, PME et Start-up innovantes à gérer leurs activités de recherche, développement et innovation (RDI) de manière structurée, efficace et simple.

La plateforme est commercialisée sous la forme d'un service web de type SaaS (Software as a Service). Ce document décrit de manière explicite aux utilisateurs, les principaux mécanismes numériques mis en œuvre sous la plateforme pour garantir sa sécurité.

2 Infrastructure Informatique

La palteforme RDI-Manager est hébergée chez OVHcloud, le numéro 1 européen en matière de cloud computing (informatique en nuage). Les principaux serveurs de ce dernier sont situés sur le territoire français. Ceci garanti la souveraineté numérique des données hébergées sur leurs serveurs.

La plateforme RDI-Manager est principalement hébergée sur GRA-11 ; un des datacenter OVHcloud situé à Gravelines (Hauts-de-France). Grâce à la robustesse des systèmes de sécurité OVHcloud, la plateforme RDI-Manager est fortement protégée des attaques informatiques de type *déni de service* ou *déni de service distribué* (**DDoS** : Distributed Denial of Service). Ceci grâce à sa protection anti-DDoS (OVH anti-DDoS) qui permet de garantir une navigation non dégradée aux utilisateurs RDI-Manager. L'architecture de l'infrastructure cloud de la plateforme RDI-Manager peut être illustrée par le schéma ci-dessous.



Architecture de l'infrastructure cloud de la plateforme

3 Logiciels Utilisés

Outre les langages tels que **php**, **html**, **java**, **css** et **SQL** ; la plateforme RDI-Manager est principalement développée à base du **framework Symfony 5.2**. Symfony est un framework open source, très utilisé de nos jours et doté d'une grande communauté de développeurs. Il jouit d'une bonne réputation pour l'évolution de ses librairies de développement, ainsi que pour son approche de sécurité des systèmes d'information.

La version 5.2 de **Symfony** date de novembre 2020 et intègre au framework de nombreuses fonctionnalités récentes et très utiles en termes de sécurité. La maintenance et les évolutions Symfony sont assurées par Symfony SAS, ainsi que par de nombreux contributeurs parmi lesquels des développeurs de SensioLabs

Les requêtes à la base de données sont exécutées à l'aide de l'**ORM**[1] **Doctrine**. Cette librairie contribue à prévenir les risques d'attaques par injection de code **SQL** directement dans la base de données. Ceci permet de sécuriser toutes les requêtes vers la base de données avant leurs exécutions.

4 Sauvegarde et Stockage des données

La sauvegarde et le stockage des données informatiques sous RDI-Manager respectent les standards de bonnes pratiques en la matière pour les plateformes numériques : **- Sauvegarde** régulière, planifiée, protégée et testée **- Support de stockage** adapté, vérifié et déconnectés de la plateforme de production.

4.1 Infrastructure de stockage

Les données de la plateforme RDI-Manager sont stockées dans un espace scalable et résilient d'**OVHcloud**. Plus précisément, les données liées aux sociétés, projets et utilisateurs sont en base de données dans une instance ; tandis que les fichiers associés aux projets sont stockés dans un **Object Storage**. Ceux-ci ont la particularité de pouvoir moduler automatiquement leur capacité de stockage en fonction de l'augmentation des données stockées. Ils bénéficient également d'une triple réplication des données sur des disques physiques et des serveurs différents. Ceci suivant le standard d'excellence et de sécurité d'OVHcloud, Object Storage.

4.2 Politique de sauvegarde

La politique de sauvegarde des données déployées par l'équipe RDI-Manager se base sur une approche de sauvegardes automatiques journalières et hebdomadaires des données en production sous la plateforme (*DAILY BACKUPS* et *WEEKLY BACKUPS*). Suivant le script de déploiement des sauvegardes,

- **DAILY BACKUPS** : tous les jours une sauvegarde des données en instance sous la plateforme est réalisée dans un espace dédié à la sauvegarde journalière. Ces sauvegardes sont progressivement remplacées par les nouvelles sauvegardes ; et à chaque fois **sont conservées les données à J -1 et J - 2**.

- **WEEKLY BACKUPS** : de même, toutes les semaines, une sauvegarde des données en instance sous la plateforme est réalisée dans un espace dédié à la sauvegarde hebdomadaire ; et à chaque fois seules **les données à S -1 et S - 2 sont conservées**.

[1] ORM : Object-Relationnal Mapper. Dans le cas de RDI-Manager, **Doctrine** est l'**ORM** qui sert à offrir une couche d'abstraction de connexion à la base de données

Cette approche standardisée de la sauvegarde des données de la plateforme, permet en cas de besoin, de pouvoir récupérer des données saines et intègres à l'échelle de temps *J -1*, *J -2*, *S -1* et *S -2*.

5 Les 6 piliers de sécurité de la plateforme

- **L'authentification**

Les mots de passe sont hachés avec la librairie **Libsodium**, qui utilise l'algorithme **argon2**. La page de connexion est chargée en *https*, et la requête POST de connexion l'est également. Ceci permet d'envoyer le mot de passe de manière chiffrée depuis l'ordinateur client jusqu'au serveur.

- **Le contrôle d'accès**

Sous la plateforme RDI-Manager, les rôles à l'échelle de la société (*Administrateur*, *Chef de projet* et *Utilisateur*) ; ainsi que les rôles à l'échelle d'un projet projet (*chef de projet*, *contributeur*, *observateur*), sont définis en base de données, et automatiquement vérifiés sur chaque page sur laquelle un rôle est requis. Plusieurs tests de non-régression automatisés sont effectués sur des pages précises, à chaque modification du code source (évolution ou re-factorisation). Ceci afin de vérifier que la modification ne permette pas aux utilisateurs d'accéder aux pages pour lesquelles ils n'ont en principe pas de droit d'accès.

- **L'intégrité des données**

Les fichiers joints aux différents projets sous la plateforme, sont stockés dans un **object storage** OVHcloud. Les informations relatives aux projets (*descriptifs projets*, *faits marquants*, ...) sont stockées dans une base **MySQL**, sur une *instance* (serveur) OVHcloud. Les sauvegardes planifiées de l'*instance OVHcloud* sont réalisées de manière périodique comme présenté plus haut. Ces sauvegardes permettent de démarrer (en cas de besoin) un nouveau serveur en moins de 2 minutes à l'état de récupération désiré pour les données (- *24 Heures*, *-48 Heures*, - *1 Semaine* et - *2 Semaines*).

- **La confidentialité des données**

Les infrastructures physiques OVHcloud sont situés en France. Ils sont sécurisés, mieux contrôlés et facilement contrôlables en termes de neutralité vis-à-vis des données et d'infogérance. Ceci en comparaison aux principaux acteurs mondiaux du marché du cloud computing. De plus RDI-MANAGER SAS engage sa neutralité, ainsi que celle de son partenaire OVHcloud SAS, vis-à-vis des données clients, gérées sous sa plateforme.

- **La non-répudiation (protection contre l'analyse du trafic)**

La plateforme RDI-Manager est fournie par un serveur web qui implémente le protocole *https*, avec un certificat de tierce partie *Let's encrypt*. Ceci permet au client-serveur d'échanger des données chiffrées avec le serveur. *Let's encrypt* permet ainsi de vérifier que le client communique au bon serveur, sans que les données ne soient compromises lors de leur acheminement.

- **CNIL & RGPD**

Conformément au règlement général sur la protection des données (RGPD[2]) ; les données personnelles des utilisateurs stockées sous la plateforme leurs appartiennent. Il est ainsi possible de demander l'accès, la modification ou la suppression de ceux-ci en contactant le service client RDI-Manager à l'adresse mail contact@rdimanager.com.

- Liste des données personnelles stockées et utilisation

Donnée	Utilisation
Nom et prénom	Permet d'identifier l'utilisateur dans la gestion opérationnelle de la plateforme Sert dans la génération de feuille de temps Sert dans la génération du contenu des mails et SMS
Email et numéro de téléphone	Sert d'identifiant de connexion Sert pour l'envoi de mails de sécurité (mot de passe oublié) Sert pour l'envoi de notifications liées à la gestion opérationnelle sous la plateforme Mentionné sur les feuilles de temps générées pour l'email
Photo de profil	Affichable à côté du prénom/nom sur certaines pages de RDI-Manager

- Services tiers

RDI-Manager utilise des services externes, par lesquels certaines des données personnelles peuvent transiter :

Service tiers	Utilisation
Twilio	Service d'envoi de SMS ; utilise votre numéro de téléphone, ainsi que votre prénom et nom dans certains SMS envoyés seulement par l'application RDI-Manager.
O2Switch	Hébergeur web dont le serveur SMTP est utilisé pour l'envoie des mails RDI-Manager ; votre email, votre nom et votre prénom y sont utilisés pour l'envoie des notifications mails RDI-Manager.
Slack	Si votre administrateur a connecté RDI-Manager à Slack, des notifications sont envoyées sur un canal précis, mais aucune de vos données personnelles ne sont utilisées.

En outre, l'ensemble des données des Utilisateurs (clients / entreprises / structures morales) collectées, stockées et gérées sous la plateforme RDI-Manager, sont la propriété exclusive de ces derniers. RDI-MANAGER SAS garantit sa neutralité, ainsi que celle de ses partenaires de développement vis-à-vis de ces données.

[2]Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).