



Sécurité des données informatiques gérées par la société Lucca

30 avril 2021

Table des matières

[Présentation de l'infrastructure de Lucca](#)

[1.1 Contexte](#)

[1.2 Hébergement](#)

[1.3 Infrastructures Lucca](#)

[1.3.1 Le Dedicated Cloud \(Cloud Dédié\)](#)

[1.3.2 Les protocoles de communication](#)

[1.3.3 Surveillance de la disponibilité des serveurs](#)

[1.3.4 Isolation des clients](#)

[1.3.5 Chaîne de sécurité](#)

[1.4 Partenaires et tiers](#)

[2 Evaluation des risques](#)

[2.1 Définitions](#)

[2.2 Les critères de sécurité](#)

[2.3 Description du PCA / PRA](#)

[2.3.1 Coupure réseau ou électrique](#)

[2.3.2 Problème sur un disque](#)

[2.3.3 Problème sur un HOST](#)

[2.3.4 Sinistre majeur sur le DC](#)

[2.3.5 Les garanties Lucca](#)

[2.3.6 Vol de données](#)

[2.3.6.1 Sur le réseau](#)

[2.3.6.2 Sur les serveurs](#)

[2.3.6.3 Vol des données par les salariés Lucca ou les partenaires](#)

[2.3.6.4 Notification en cas d'incident](#)

[2.3.7 Traçabilité et journalisation](#)

[2.3.8 Données personnelles et anonymisation](#)

[2.4 Chiffrement](#)

[2.5 Gestion des sauvegardes](#)

[2.6 Gestion des mises à jour de sécurité](#)

[3 Audit & certification](#)

[3.1 Audit organisationnel](#)

[3.2 Audit de vulnérabilité et tests d'intrusion](#)

[3.3 Rapport d'audit](#)

[4 Roadmap infrastructure](#)

[4.1 Démarche ISO 27001](#)

[4.2 Roadmap sécurité](#)

[4.3 Conteneurisation](#)

Présentation de l'infrastructure de Lucca

1.1 Contexte

La société Lucca (« Lucca » dans la suite de ce document) est un éditeur indépendant de solutions multi-utilisateurs de gestion pour entreprise. Ces solutions sont proposées en mode SaaS.

Le présent document a pour objet la description des procédures permettant à Lucca de garantir la disponibilité, l'intégrité et la confidentialité des données gérées pour le compte de ses clients.

Pour faciliter sa compréhension, voici une liste d'acronyme utilisée dans le document :

PCA : Plan de Continuité d'Activité

PRA : Plan de Reprise d'Activité

SLA : Service Level Agreement (Qualité de service)

TLS : Transport Layer Security (remplaçant de SSL : Secure Sockets Layer)

FTPS : File Transfer Protocol over TLS

SFTP : File Transfer Protocol over SSH

HTTPS : Hyper Text Transfer Protocol over TLS

VM : Machine Virtuelle

SSD : solid-state drive (disque dur sur mémoire flash : extrêmement rapide et sans élément mobile)

DC : Dedicated Cloud (le DC est un produit d'OVH) plateforme de virtualisation basée sur VMware, des HOSTS et un NAS.

NAS : stockage disponible sur le réseau.

DMIA : Durée Maximale d'Interruption Admissible (Recovery Time Objective, RTO)

PDMA : Perte de Données Maximale Admissible (Recovery Point Objective, RPO)

1.2 Hébergement

Lucca a choisi l'hébergeur français OVH sur des critères de sécurité et de support. OVH possède actuellement 27 centres de données dont 4 en France situés à Roubaix, Paris, Strasbourg et Graveline. N°1 en Europe et n°3 mondial. Lucca héberge les données de production sur le datacenter de Roubaix, en France.

Lucca loue également un stockage hors OVH, Microsoft Azure, choisi sur la base de critères d'éloignement géographique et d'indépendance par rapport à l'hébergeur principal OVH. Le centre de données de Azure sélectionné est basé à Paris, en France.

Ces deux sociétés d'hébergement sont les deux plus importantes d'Europe. Leurs datacenters sont certifiées **ISO 27001 : 2013** (OVH depuis le 15 mars 2013 sur le centre d'hébergement du DC). Ces deux sociétés donnent toutes les garanties nécessaires quant à la non-intrusion d'individus dans leurs centres de données.

OVH a été récompensé en 2011 et 2012 du trophée « *vCloud Service Provider of the year* » par VMware et est certifié SOC 1 type II et SOC 2 type II.

La sécurité des centres de données de Azure est détaillée sur leur site sur le [lien suivant](#).

Enfin, pour les clients Suisses, Lucca travaille depuis janvier 2011 (contrat n°153729) avec l'hébergeur Green qui est aussi certifié ISO 27001:2013. L'infrastructure suisse a été améliorée en 2019 et 2020 pour l'amener au niveau de l'infrastructure française.

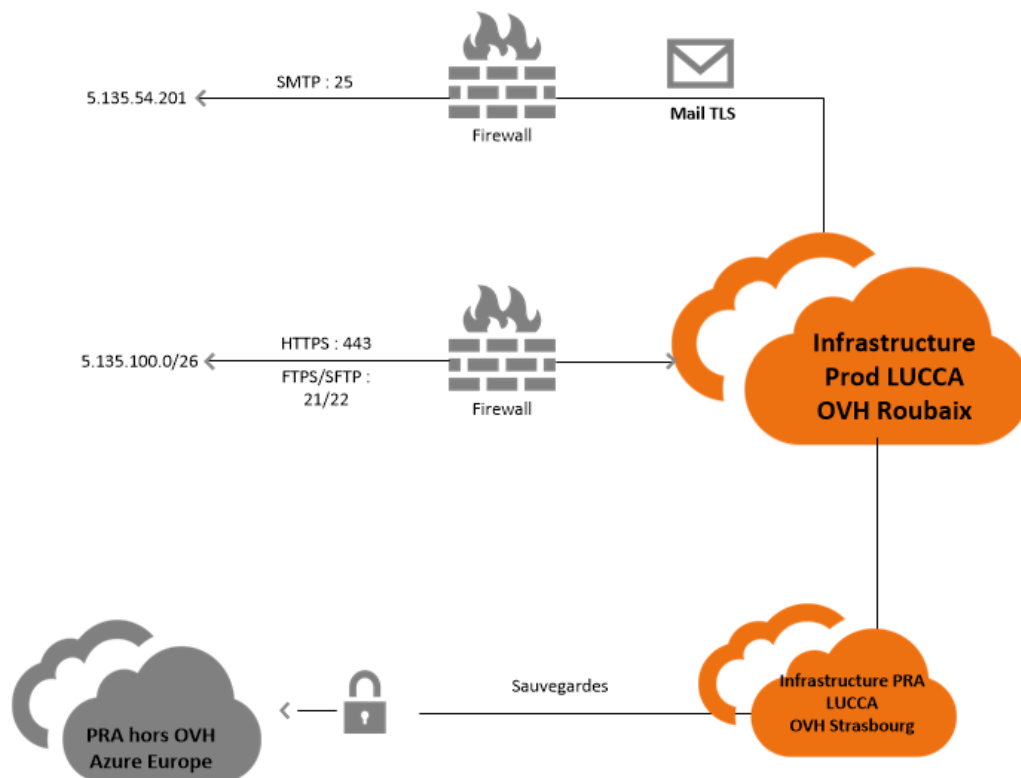
Dans les trois cas, les hébergeurs n'infogèrent pas nos serveurs, ils n'ont donc pas accès à nos données.

Les données de production des clients non suisses sont donc hébergées exclusivement en France, et les sauvegardes chiffrées (AES 256) sont stockées dans un datastore chiffré hébergé dans le centre Azure de Paris en France, en redondance locale.

Les données de production des clients suisse et les sauvegardes 30J chiffrées sont aussi en Suisse.

1.3 Infrastructures Lucca

FRANCE

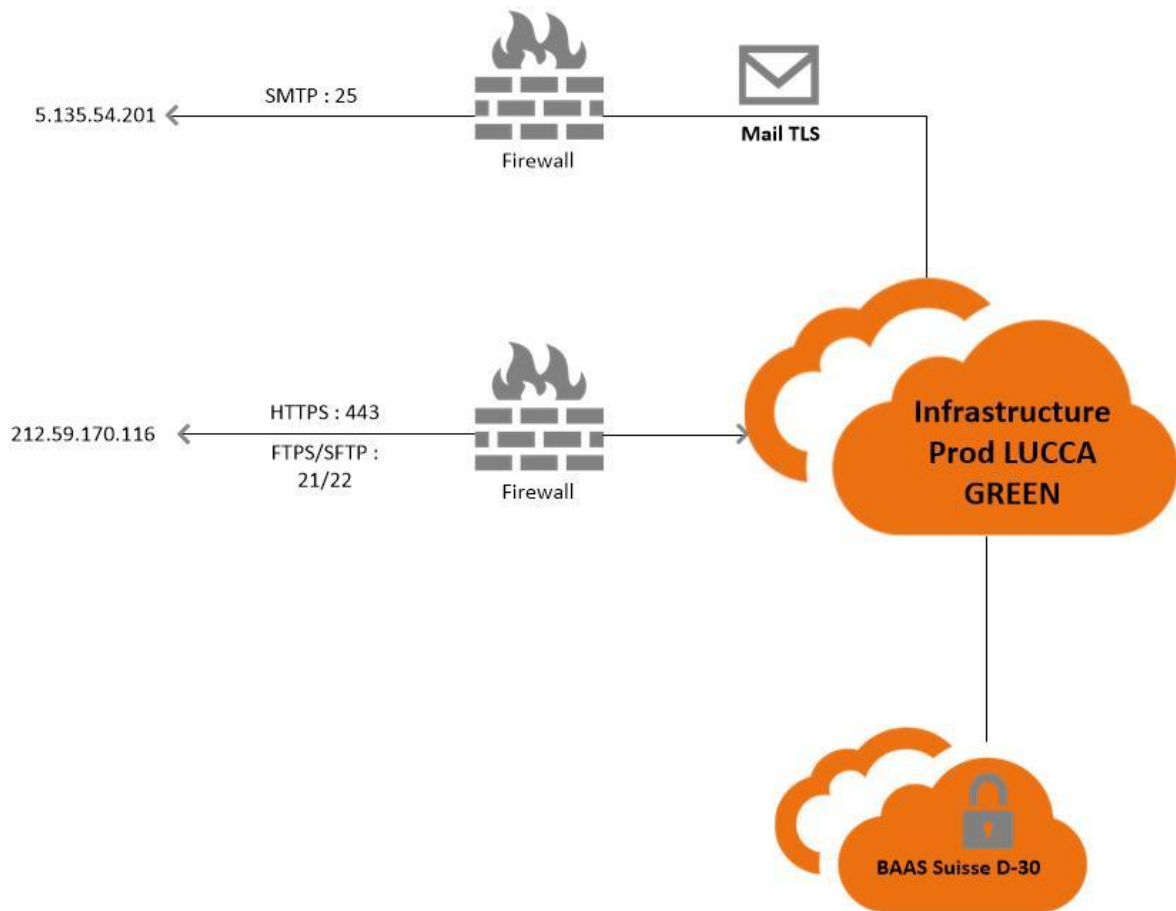


Les blocs RIPE Lucca FR sont :
5.135.100.0/26

5.135.54.192/28

SUISSE

Infrastructure Publique



L'IP Lucca Suisse est 212.59.170.116

1.3.1 Le Dedicated Cloud (Cloud Dédié)

Lucca exploite actuellement deux Dedicated Cloud (DC dans la suite du document) chez OVH :

- Un DC 2018 de production à Roubaix hébergeant les serveurs virtuels de production fonctionnant sous Windows server 2016 et Linux Debian 8.
- Un DC 2014 de PRA à Strasbourg.

Le DC présente toutes les redondances permettant un très grand niveau de service. Le principe de la virtualisation est l'abstraction du matériel et de ses problèmes possibles (cf §2.3). Les composants du DC sont :

- Le **NAS** (stockage)
- Des **HOSTS** : (puissance)

Chez Green (hébergeur Suisse), Lucca possède une infrastructure virtuelle (Azure Pack) disposant de redondances similaires au datacenter d'OVH.

1.3.2 Les protocoles de communication

Les protocoles permettant d'accéder aux serveurs ou aux données des serveurs sont limités à deux :

1. https (port 80, 443), permettant d'accéder à nos applications web à partir d'un navigateur. Seuls les protocoles TLS 1.2 et TLS 1.3 sont actuellement activés et les protocoles SSL sont désactivés. Les protocoles 1.1 et 1.0 sont désactivés depuis le 12 janvier 2018.
2. ftps (port 990 et 989) et sftp (port 22), permettant aux clients de déposer des fichiers sur les serveurs servant aux imports automatiques via un serveur FTP unique.

Tous ces protocoles utilisent un chiffrement pour l'échange des données.

les membres de l'équipe production de Lucca accèdent aux serveurs via un VPN et un compte nominatif.

1.3.3 Surveillance de la disponibilité des serveurs

La disponibilité des serveurs est contrôlée par :

- un ping https effectué par une entreprise extérieure (internetVista) toutes les 30 minutes.
- un ping https effectué en interne, à partir de Strasbourg toutes les 10 minutes.
- une surveillance VMware, la technologie de virtualisation utilisée, réalisée par OVH. Cette surveillance exploite un ensemble de règles qui mesure en permanence l'utilisation des HOSTS (mémoire vive et processeur) et des machines virtuelles.
- un monitoring interne des machines virtuelles et physiques, via PRTG

Ces surveillances déclenchent des alertes par mail ou SMS auprès des responsables de la plateforme Lucca.

Depuis l'année 2012, la disponibilité de nos serveurs de production a été en moyenne de 99,93% (5h 10 min d'indisponibilité par an, principalement hors période ouvrée).

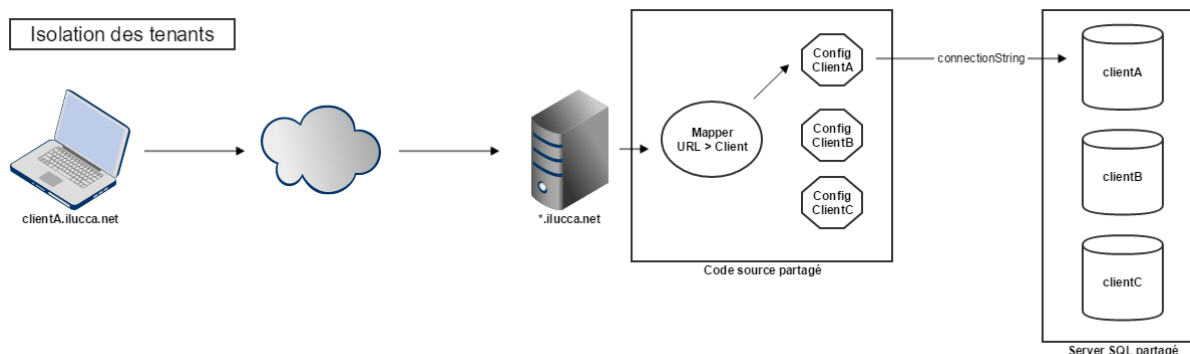
Le statut de notre infrastructure et la performance de nos services sont disponibles sur <https://status.lucca.fr>

Les périodes de maintenance sont des plages horaires planifiées pour les mises à jour des applications Lucca. L'indisponibilité éventuelle qui peut en découler ne rentre pas dans le calcul du pourcentage de disponibilité mensuelle.

Les périodes de maintenance ont lieu chaque jour ouvré de la semaine, entre 22h et 22h10 les lundi, mardi, mercredi et vendredi et entre 22h et 22h30 chaque jeudi (heure de Paris GMT+01).
Des périodes de maintenance d'infrastructure peuvent avoir lieu durant le we, elles sont annoncées sur <https://status.lucca.fr>.

1.3.4 Isolation des clients

Voici un schéma logique qui décrit le mécanisme d'isolation des données entre clients :



Les requêtes web des clients arrivent sur notre infrastructure via un serveur web frontal, qui exécute un code source partagé par tous nos clients.

Pour chaque requête, un module dédié récupère la configuration du client à partir de l'URL.

La configuration contient notamment le connectionString SQL permettant au code de se connecter à la bonne base de données.

Les injections SQL (requêtes trans-bases notamment) sont protégées d'une part par un WAF, et d'autre part par le fait que nous utilisons l'ORM EntityFramework pour construire nos requêtes SQL.

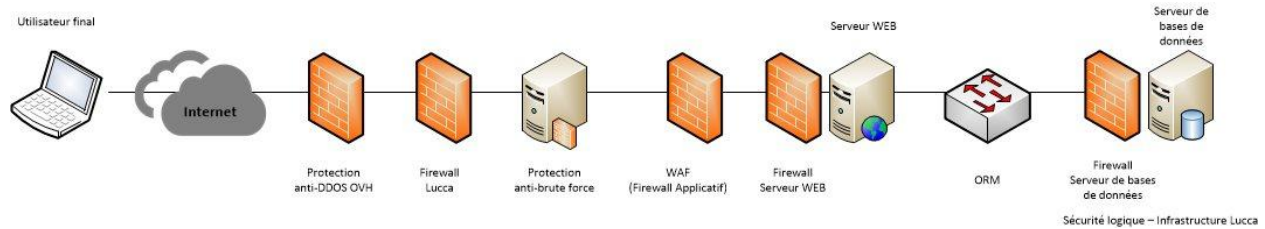
Toutes les requêtes utilisent un compte SQL et une base propre à chaque client.

Notre parc clients est réparti sur plusieurs "cluster" de 1 000 clients. Chaque cluster partage un serveur SQL.

Depuis 2007, date à laquelle Lucca est en mode SaaS uniquement, nous n'avons jamais subi de fuite d'information trans-client.

1.3.5 Chaîne de sécurité

Voici un schéma logique des différents organes de sécurité actuellement en place entre l'utilisateur final et la base de données :



- Protection anti DDOS proposée par OVH : <https://www.ovh.com/fr/anti-ddos/> (non disponible sur Green)
- Firewall Lucca global pour l'ensemble de la plateforme + serveur VPN
- Protection anti brute force configurée au niveau de HAproxy.
 - IP bannie temporairement en cas d'attaque sur certaines URL.
 - Utilisateur bloqué temporairement en cas d'utilisation non appropriée
- WAF : protection applicative basée sur une liste blanche
- Firewall interne, sur chaque serveur
- ORM (Object-Relational Mapping) : protection contre les injections SQL
- Base de données : chaque client a sa propre authentification sur sa base de données

1.4 Partenaires et tiers

Nos applications communiquent avec l'extérieur, voici la liste des partenaires :

Editeur	Nationalité	Localisation	Application	Lien avec Lucca	Stockage	Données personnelles
Datadog	FR/US	Europe	Logs web (30j) Metrics infra (18 mois)	Toutes les applications	oui	non
Sentry	US	USA	Capteur d'erreurs client	Toutes les applications	oui	non
Atatus	US	USA	Capteur d'erreurs client mobile	Cleemy	oui	non
Budget Insight	Français	France	Budget Insight	Cleemy	oui	identifiant du service + données bancaires / factures
Abbyy	Russe	Europe	OCR clients internationaux	Cleemy	non (buffer)	NA
Mindee	Français	(AWS) Irlande	OCR clients français	Cleemy	non (buffer)	NA
Universign	Français	France	Dématisation	Cleemy	non	NA
Anytime	Belgique	Europe	Cartes bancaires. Contrat avec le client final	Cleemy	non	NA

Mail OVH	Francais	France	Email attachment	Cleemy	non (buffer)	NA
Signaturit	Espagnol	(AWS) Irlande	Signature électronique	Poplee Core RH	oui	oui

Pour son fonctionnement interne, la société Lucca travaille avec les sous-traitants suivant :

Editeur	Nationalité	Localisation	Domaine d'activité	Lien avec Lucca	Stockage	Données personnelles
OVH	FR	France	Hebergement iso27001	Hebergement clients FR	oui	oui (utilisateurs)
Microsoft	US	France	Hebergement iso27001	Hebergement sauvegardes chiffrées	oui	oui (utilisateurs)
GREEN	CH	Suisse	Hebergement iso27001	Hebergement clients CH	oui	oui (utilisateurs)
Zendesk	US	Allemagne	Ticketing	Support	oui	oui (administrateurs uniquement)
Salesforce	US	France et Allemagne	CRM	Vente	oui	oui (administrateurs uniquement)
Hubspot	US	US	CRM	Marketing	oui	oui (administrateurs uniquement)
Clearnox	FR	France	Recouvrement	Recouvrement	oui	oui (facturation uniquement)
Teams (Microsoft)	US	France	workspace	Echange de fichiers dans le cadre du lancement du projet	oui sur la phase de lancement du projet	oui
Google workspace	US	Monde	workspace	Echange de fichiers dans le cadre du lancement du projet	oui sur la phase de lancement du projet	oui

2 Evaluation des risques

2.1 Définitions

La sécurité des systèmes d'information (SSI) est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité du système d'information.

2.2 Les critères de sécurité

Les menaces identifiées sur les données gérées par un système d'information sont les suivantes :

1. **Indisponibilité** : masquer les données aux personnes qui doivent y avoir accès
2. **Intégrité** : altération ou destruction des données
3. **Confidentialité** : révéler les données à des tiers qui ne doivent pas en avoir connaissance
4. **Traçabilité** : être capable de retrouver qui a fait quoi et quand

2.3 Description du PCA / PRA

Dans le cadre de la politique de sécurité, les risques envisagés concernant l'indisponibilité et l'intégrité sont les suivants :

- Coupure réseau ou électrique
- Problème sur un disque du NAS
- Problème sur un HOST
- Sinistre majeur sur le DC

Les risques envisagés concernant la confidentialité sont les suivants :

- Vol des données sur le réseau internet
- Vol des données sur le serveur de production
- Vol des données sur le serveur de sauvegarde
- Vol des données sur le serveur de sauvegarde hors OVH
- Vol des données par les salariés Lucca ou les partenaires

2.3.1 Coupure réseau ou électrique

L'installation électrique est redondée et les fournisseurs d'infrastructures (OVH et GREEN) disposent de plusieurs groupes électrogènes et de batteries permettant d'assurer la continuité de l'alimentation électrique. L'installation réseau est aussi redondée et chaque serveur dédié a accès à deux switchs réseau. De plus, ces fournisseurs d'infrastructures possèdent plusieurs contrats d'accès à internet.

OVH et GREEN disposent donc d'un plan de continuité sur les domaines d'alimentation réseau et électrique.

2.3.2 Problème sur un disque

Le datacenter propose un stockage des données dont la redondance Raid 1 permet une disponibilité annoncée à 100% par OVH.

PCA : la continuité de service est assurée par la virtualisation (en cas de défaillance d'un disque composant le stockage chez OVH et GREEN).

2.3.3 Problème sur un HOST

La protection HA (High Availability) est activée. En cas de défaillance d'un HOST, les machines virtuelles sont redémarrées sur un autre host. Le host défaillant est alors remplacé par OVH dans un délai de 15 minutes

PCA : La continuité de service est assurée avec une interruption de moins de 2 minutes sans perte de données.

2.3.4 Sinistre majeur sur le DC

OVH dispose de plusieurs centres de données. Si celui qui héberge le DC principal venait à disparaître (incendie, crash d'un avion, inondation...), la société Lucca dispose de deux PRA.

Nous disposons de 4 sites :

- OVH Roubaix : production + Sauvegarde locale RPO 10 minutes RTO 2h
- GREEN : production + PRA 24h (clients suisses)
- OVH Strasbourg : PRA chez OVH (pour les clients hébergés en France) - RPO 30 minutes RTO 72h
- AZURE Paris : PRA hors OVH - RPO 30 minutes - RTO 1 semaine

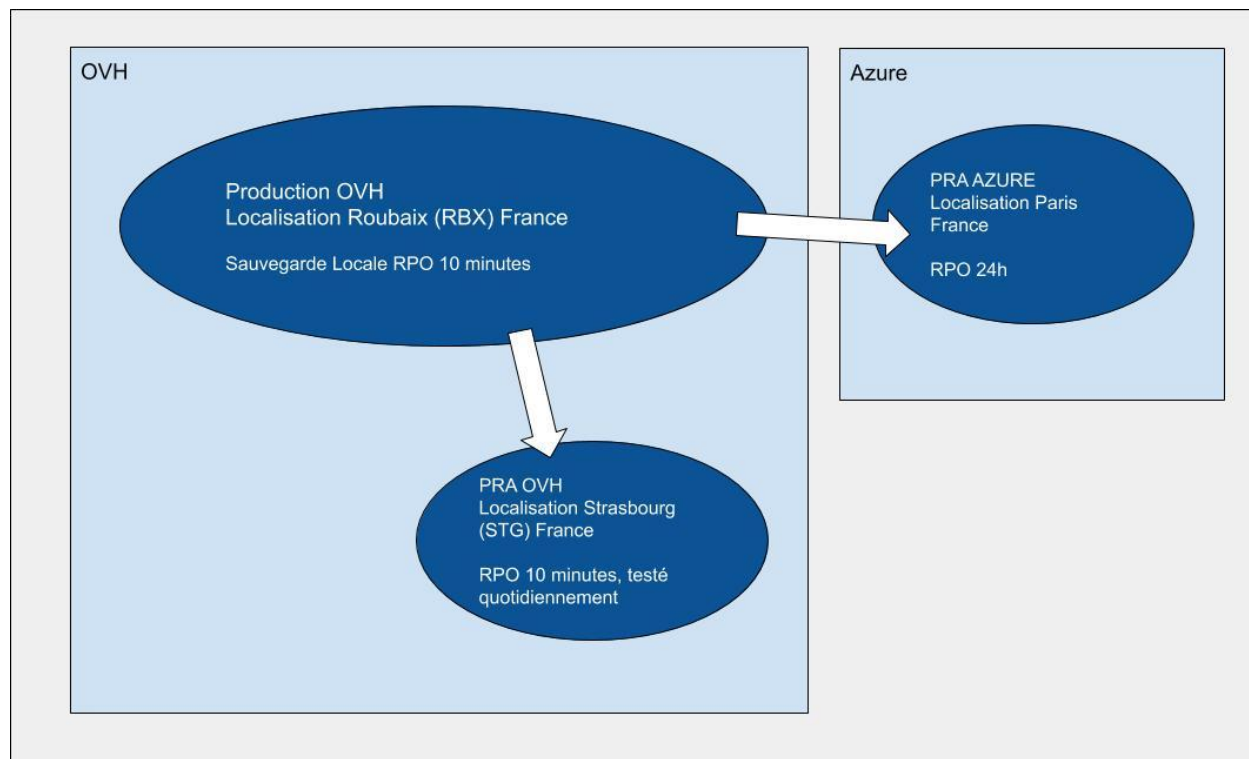
Nous distinguons deux PRA :

Un premier chez OVH, à Strasbourg, testé chaque jour automatiquement :

- L'ensemble des bases des clients sont restaurées, leur intégrité est vérifiée.
- L'ensemble des fichiers (justificatifs, documents...) sont synchronisés.
- Les artefacts du code sont disponibles
- L'infrastructure n'est pas prête

Un deuxième hors OVH, sur Azure.

- L'ensemble des bases et fichiers sont disponibles de façon chiffrés
- Ces archives sont transférées sur Azure quotidiennement.



2.3.5 Les garanties Lucca

	Incident	Garantie Lucca
Panne disque	Obsolescence entraînant une panne matérielle Probabilité : 0,1 % (1 panne tous les 3 ans)	Continuité d'activité totale grâce à une redondance des disques • Pas d'interruption de service • Pas de perte de donnée
Panne serveur (host)	- Obsolescence entraînant une panne matérielle - Coupure réseau Probabilité : une panne par host tous les 5 ans.	Continuité d'activité • Indisponibilité max : 2 min • Redémarrage des machines concernées (perte des sessions) • Pas de perte de données
Panne centre de données	Sinistre majeur sur l'ensemble du data center Exemple : Incendie d'un datacenter Probabilité : rare	Plan de reprise d'activité • Prise en charge de l'incident par un technicien dans les 2h ouvrées • Rétablissement du service : une semaine • Perte de données max : 1h
Panne système d'exploitation	Problème de mise à jour système d'exploitation sur une machine virtuelle Probabilité : inconnue	Continuité d'activité : 95% des briques de l'infra sont redondées Plan de reprise d'activité : • Prise en charge de l'incident par un technicien dans les 2h ouvrées • 4h pour une machine virtuelle affectée • Perte de données max : 1h (pas de perte de donnée en cas de correction)
Panne Logiciel Lucca	Anomalie logicielle bloquant l'utilisation de l'application NB : tout développement est suivi de tests techniques et fonctionnels	Plan de reprise d'activité : • Prise en charge de l'incident par un technicien dans les 2h ouvrées • Mise à jour sous 24h ouvrés max • Pas de perte de données

2.3.6 Vol de données

2.3.6.1 Sur le réseau

Les données transitent sur le réseau dans plusieurs contextes :

- entre les postes clients et le serveur (https)
- entre nos serveurs mail et le serveur mail du client (smtp sur TLS)
- entre les postes des administrateurs des serveurs et le serveur (ftps, TS sur TLS)
- entre le serveur et le serveur de sauvegarde (ftps et IP privée)
- entre le serveur OVH PRA et Azure (https)
- dans l'infrastructure d'OVH et de Azure
- dans les locaux de Lucca

Dans les cinq premiers cas, les données sont exploitées par un protocole sécurisé basé sur TLS et chiffrant les données, ce qui signifie que si les données venaient à être interceptées, elles seraient difficilement déchiffrables. L'identité des domaines est certifiée par la société GeoTrust Inc. via des certificats de sécurité Wildcard de classe 3 (chiffrement des données via une clé de 128 bits minimum). Le chiffrement SSL utilisé chez Lucca est comparable à celui utilisé pour les transferts bancaires.

Chez OVH, l'infrastructure Lucca est en Cloud Privé, non infogéré par OVH. Les données transitent sur un réseau local (Vlan)

Dans les locaux de Lucca, nous avons une politique de sécurité physique qui permet d'éviter les vols de données :

- ordinateurs sécurisés, mis à jour régulièrement
- gestion des visites extérieures
- interdiction d'utiliser des clés USB pour le transport de données
- politique de mot de passe forte
- chiffrement des postes clients

L'infrastructure d'Azure n'est utilisée que pour stocker des données qui ont été chiffrées sur OVH.

L'identité de l'entreprise Lucca est également certifiée de classe 2 par l'organisme de certification GeoTrust Inc.

2.3.6.2 Sur les serveurs

Les données des clients sont localisées dans des serveurs de base de données non accessibles à l'extérieur du serveur. Les données sont exposées à l'extérieur uniquement par le serveur web (IIS). Chaque client a une base de données propre.

Les seuls protocoles autorisés sur les serveurs sont les suivants :

- https
- ftps et sftp
- smtp sur TLS

Un accès technique est possible en terminal server via tunnel VPN pour l'équipe infrastructure de Lucca.

La politique des mots de passe est sévère :

- Les mots de passe sont différents par serveur et par service.
- Chaque mot de passe est fort (plus de 8 caractères composés de chiffres, de lettres et de caractères spéciaux)
- Ils sont régulièrement modifiés

Sur chaque serveur, les connexions sont loguées et dans le cadre de la connexion au terminal server, les logs de connexion sont externalisés.

Dans les trois cas, les hébergeurs n'infogèrent pas nos serveurs, ils n'ont donc pas accès à nos données.

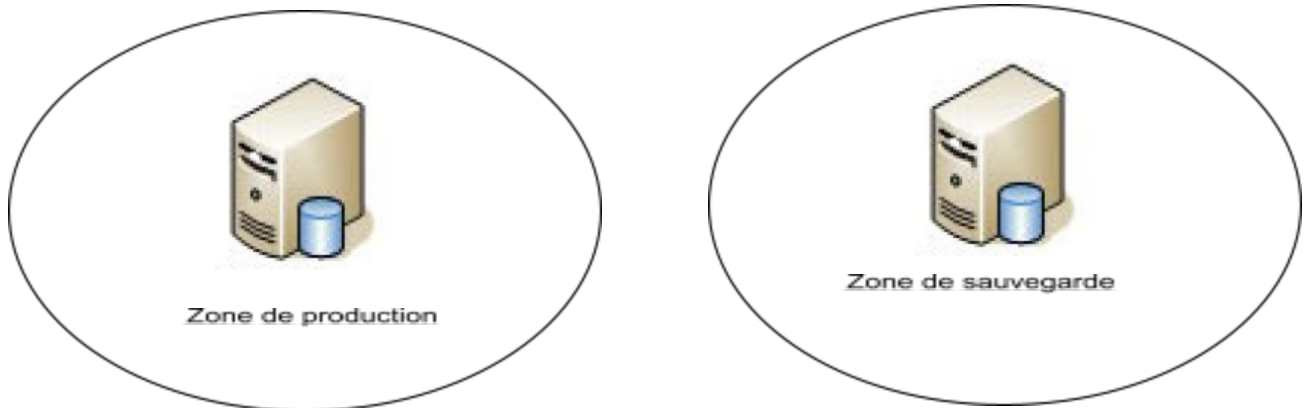
La traçabilité applicative a été mise en place, ainsi que sur notre plateforme de support. Chaque connexion des consultants "support" sont horodatés.

2.3.6.3 Vol des données par les salariés Lucca ou les partenaires

Les contrats de travail des salariés contiennent une clause de confidentialité vis-à-vis des données qu'ils manipulent.

De plus, après la phase de mise en place de l'instance d'un client, les données permettant cette mise en place ne sont pas conservées sur les postes clients des salariés, ils sont systématiquement supprimés.

Récapitulatif des zones de confidentialité :



Zone de production :

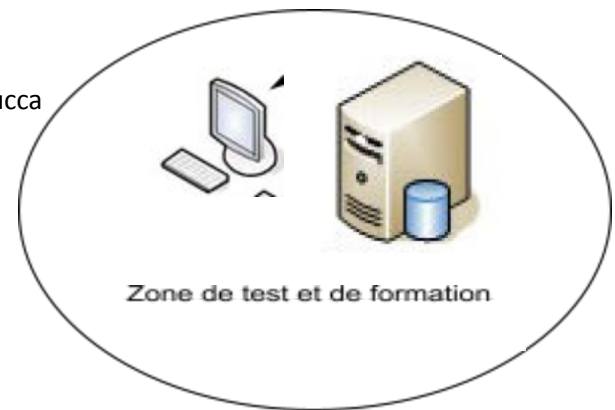
Serveurs accessibles uniquement par le service infrastructure de Lucca
Données client accessibles via les applications Lucca
par les utilisateurs et le support

Zone de sauvegarde :

Accessibles uniquement par le service infrastructure de Lucca
Données chiffrées non accessibles de l'extérieur

Zone de test et de formation

Les données sensibles et critiques des clients sont anonymisées selon des règles irréversibles mais respectueuses du type de données.

**2.3.6.4 Notification en cas d'incident**

Conformément à la réglementation européenne, en cas d'atteinte avérée aux Données Personnelles, Lucca s'engage à communiquer cette violation au client afin que ce dernier puisse la communiquer à l'autorité de contrôle compétente et, lorsque cela est exigé par la réglementation, aux personnes concernées (de manière individuelle ou générale selon les cas). En cas de violation de données, Lucca notifiera au plus tôt le responsable de traitement au plus tard 24 heures après en avoir eu connaissance et s'engage à coopérer pleinement avec le client pour identifier les causes de la violation de données.

Dans ce cadre, les informations communiquées au client seront les suivantes :

- Description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- Communication du nom et des coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- Description des conséquences probables de la violation de données à caractère personnel ;
- Description des mesures prises ou que le responsable de traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

2.3.7 Traçabilité et journalisation

Lucca a mis en place plusieurs systèmes permettant la traçabilité.

Traçabilité applicative :

Dans nos différentes solutions, une notion d'historique est implémentée pour les actions et données importantes

D'autre part, nous travaillons avec la société Datadog, qui nous permet d'analyser les traces de méta-data (pas de données personnelles) sur les 30 derniers jours.

Traçabilité des accès :

L'ensemble des accès internes aux instances des clients à des fins de support ou de configuration est géré par une solution interne nommée CC. Cette application contient un système de journalisation très fin.

De même, sur notre plateforme, l'ensemble des accès aux serveurs sont logués sur notre contrôleur de domaine.

2.3.8 Données personnelles et anonymisation

Nous sommes très sensibles aux données personnelles de nos clients que nous manipulons. Lors de l'accueil d'un nouveau collaborateur, une session de sensibilisation à la sécurité et à la manipulation des données personnelles est faite.

L'infrastructure de Lucca comprend des zones (cf 2.3.6.3). Les données personnelles sont anonymisées dès qu'elles sortent de la zone de production. Toutes ces actions sont journalisées.

Suite à une résiliation, l'ensemble des données de production sont détruites. Le mécanisme 30 jours glissants des sauvegardes fait que 30 jours après la résiliation, l'ensemble des données sauvegardées sont détruites.

Une page spécifique a été réalisée pour rentrer dans les détails du RGPD : <https://www.lucca.fr/rgpd/>

Nos applications utilisent des cookies pour servir deux objectifs :

- maintenir une session utilisateur ouverte entre le navigateur et le serveur
- se souvenir de certaines préférences de l'utilisateur

Cette politique d'utilisation des cookies est différente sur notre site web commercial www.lucca.fr

2.4 Chiffrement

Les données critiques sont actuellement chiffrées au niveau applicatif :

- les mots de passes de nos utilisateurs sont hashés en PBKDF2
- les données chiffrées de façon réversible (mots de FTP passes externes / oauth tokens externes, etc) le sont en AES 256 CBC
- Les clés de chiffrement sont uniques par application, révocables manuellement, et stockées uniquement sur nos propres serveurs.

Le chiffrement des bases de données est sur la roadmap 2020/2021.

2.5 Gestion des sauvegardes

Pour la France

Sauvegarde locale

- Une sauvegarde intégrale des bases et fichiers de OVH & GREEN est faite chaque nuit.
- Un système de sauvegarde différentielle des bases de données a été mis en place toutes les 10 minutes.

Les sauvegardes sont réalisées vers un support de stockage local sur Roubaix, puis sont remontées à la fois sur un réplica sur Roubaix, et sur un autre réplica localisé à Strasbourg en France, donc distant géographiquement du serveur sauvegardé (+ de 500km).

Sauvegardes distantes (hors OVH)

Les sauvegardes sont externalisées quotidiennement sur Azure, à Paris. Les sauvegardes sont chiffrées et conservées 30 jours. Passée cette période, les données sont détruites. Les clés de chiffrement ne sont pas stockées sur Azure

Chaque instance logicielle hébergée en France **est restaurée quotidiennement** sur le serveur de reprise d'activité (hébergé chez OVH à Strasbourg). Les éléments suivants sont validés :

- La date de la bases de données
- L'intégrité de la base (CHECKSUM)
- Les fichiers des clients

La restauration des sauvegardes des bases de données des clients hébergés en France est réalisée en continu sur l'infrastructure OVH à la fois sur le site de Roubaix et le site de Strasbourg. L'intégrité est testée de façon systématique.

La PDMA (ou RPO) est de 10 minutes pour les bases de données et de 24h pour les fichiers. L'ensemble des contextes clients sont testés automatiquement chaque jour.

Pour la Suisse

- les sauvegardes sur 30 jours sont gérées sur un [service BAAS \(Backup As A Service\) de Acronis, localisé en Suisse](#).



RTO/DMIA détaillé dans le paragraphe 2.3.5.

2.6 Gestion des mises à jour de sécurité

L'infrastructure est hybride. Nous avons mis en place un système d'alertes permettant d'être informé des différentes mises à jour de sécurité.

- OVH gère la partie VMware. dernière mise à jour de sécurité : <https://www.ovh.com/fr/blog/vulnerabilites-meltdown-spectre-cpu-x86-64-ovh-pleinement-mobilise/>
- Mises à jour Windows automatiques
- Alertes sur les failles Linux et FreeBSD : mises à jour régulière en fonction de la sévérité
- Mise à jour du WAF periodique
- Analyse des bibliothèques Front par GitHub
- Outils interne pour l'analyse des bibliothèques Back

>	 angular / angular.js angular	1.5.5
>	 lgalfaso / angular-dynamic-locale	0.1.32
>	 angular / bower-angular-mocks angular-mocks	1.5.8
	 angular / bower-angular-route angular-route	1.5.8
	 angular / bower-angular-sanitize angular-sanitize	1.5.5
>	 angular-translate / angular-translate	2.12.1
>	 angular-ui / bootstrap angular-ui-bootstrap	2.1.4
>	 griffithlab / angular-ui-router-civic angular-ui-router	0.3.1
>	 s-panferov / awesome-typescript-loader	3.1.3
>	 babel / babel babel-core	6.18.2

Vue partielle de l'analyse des sources externes de GitHub

3 Audit & certification

3.1 Audit organisationnel

La société Lucca a été auditée par un de ses clients bancaire sur une base ISO27001 en janvier 2019.

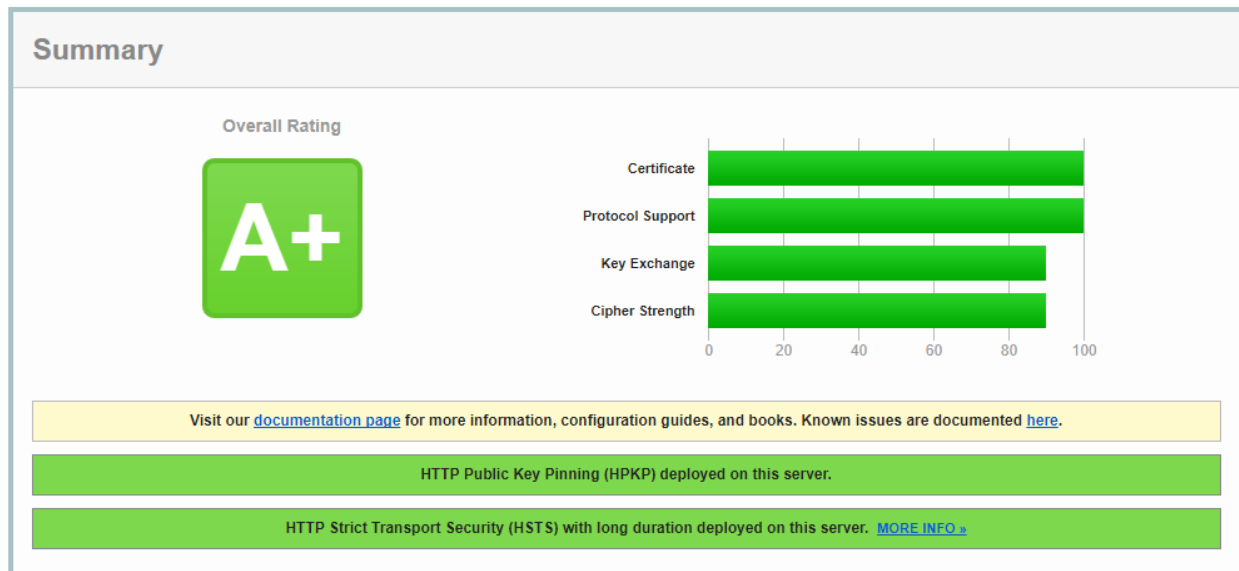
3.2 Audit de vulnérabilité et tests d'intrusion

Plusieurs audits de vulnérabilité sont effectués chaque année. Les sociétés Qualys, DenyAll, Olféo et Advens ont testé notre plateforme (environ 5 audits externes par an).

Un test d'intrusion est réalisé en interne tous les 3 mois, permettant de faire émerger des faiblesses et de les corriger dans un délai qui dépend de la gravité. Ils sont menés par une équipe de développeurs et animés par l'équipe sécurité.

Un audit Qualys de notre plateforme a été mis en place et automatisé. Chaque semaine, un bilan est disponible.

La note A+ a été obtenue pour l'ensemble des serveurs sur le test de la configuration SSL (notamment SSLv2 et 40 bit ciphers)



Protocols

TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

For TLS 1.3 tests, we only support RFC 8446.

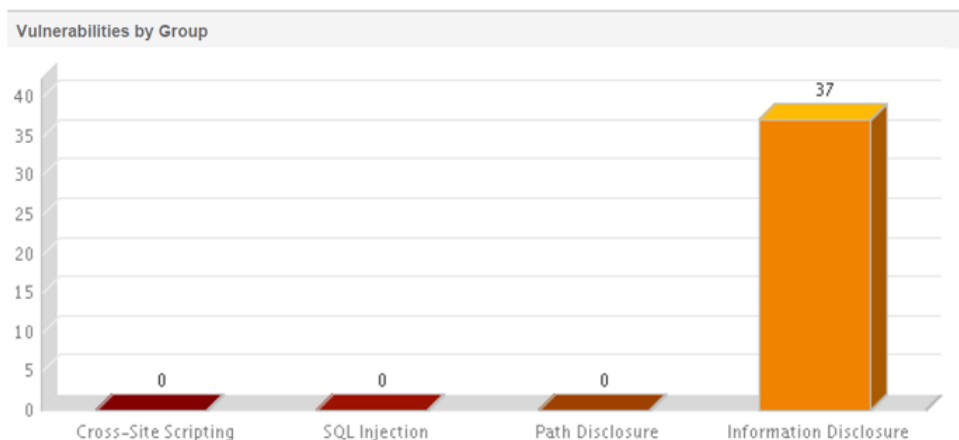
Les protocoles 1.0 et 1.1 ont été désactivés en 12 janvier 2018.

Le chiffrement utilisé est **RSA 2048 bits (SHA256withRSA)**

3.3 Rapport d'audit

Nos rapports d'audit sont confidentiels.

Voici cependant un graphique représentant le type de failles trouvées :



Les “divulgations d’informations” signalées sont des alertes :

- information sur le chemin de répertoire sur une url d’api rest : /api/roles : faux positifs
- le mot “admin” a été détecté dans une url : faux positifs
- attribut “secure” non présent sur les cookies : corrigé le 3 mars 2016
- attribut “httponly” non présent sur les cookies : corrigé le 3 mars 2016
- CSRF ou Clickjacking possible, X-Frame-Options non implémenté : corrigé le 3 mars 2016

Plus de détails sur ces 3 derniers points dans l’[article dédié](#).

3.4 Certification iso 27001

Nous allons étudier la certification iso 27001 en 2020. Nous avons commencé par une analyse des risques basées sur la méthode **Framework EBIOS Risk Manager** au premier semestre 2019.

4 Roadmap infrastructure

4.1 Démarche ISO 27001

Nous sommes actuellement dans une démarche de certification iso 27001.

Nous avons mené mi-2019 une analyse de risque basée sur la méthode EBIOS (<https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/>).

Actuellement, nous reformulons notre PSSI.

Nous visons une certification sur l’année 2021

4.2 Roadmap sécurité

Abandon du TLS 1.0 et 1.1 sur la partie WEB : **fait depuis début 2018.**

Abandon du TLS 1.0 et 1.1 sur la partie FTPS : **fait depuis le 15 janvier 2019.**

Chiffrement partiel ou total des bases de données ou des machines :

- chiffrement des VM : en pause
- chiffrement des bases de données au niveau SQL Server 2019 : **mise en production 15 avril 2021**

Primitives de chiffrement :

- Fonction de dérivation de clé pour les mots de passe : systématisation de Argon2id (Q1 2021)
- Fonction de chiffrement symétrique : systématisation de XChaCha20+Poly1305 (Q1 2021)

4.3 Conteneurisation

Pour améliorer l'agilité sur l'infrastructure, nous procédons actuellement à un effort de R&D sur la conteneurisation.

Début 2020, nous adhérons au concept d'infrastructure as code que nous allons déployer par lots sur la production, avec une garantie de disponibilité pour nos clients.

Paris, le 30 avril 2021

Bruno Catteau

Responsable infrastructure & sécurité