



www.3liz.com
info@3liz.com

Plan Assurance Sécurité de l'hébergement Lizmap Hosting

Historique des modifications

- 4 octobre 2023 : Les mots de passes dans Lizmap ont une longueur minimal de 12 caractères, et la qualité des mots de passes est vérifiée lors de leurs créations par les utilisateurs, en calculant l'entropie et en vérifiant si ils ne contiennent pas un des mots de passes les plus utilisés.

Prestations

3Liz propose, au travers de son offre SAAS Lizmap Hosting, plusieurs prestations d'hébergement, qui peuvent se regrouper en trois catégories :

- offre d'**hébergement mutualisé** (BASIC) : les instances Lizmap de plusieurs clients et leurs données sont sur une même machine physique. Ils partagent donc les ressources de ce serveur (processeurs, mémoire, disques durs...). Les mêmes services web, PostgreSQL, QGIS et FTP sont utilisés par plusieurs clients. En revanche, chacun dispose de son propre « Lizmap », de ses propres accès authentifiés, de sa propre base de données, etc.
- offre d'**hébergement semi-dédié** (STANDARD) : les instances Lizmap de plusieurs clients et leurs données sont sur une même machine physique. Ils partagent donc les ressources de ce serveur (processeurs, mémoire, disques durs...) pour les services tels que serveur web et FTP. Ils disposent chacun de leurs propres serveurs (logiciel) PostgreSQL et QGIS, et des ressources pré-attribuées.
- offre d'**hébergement dédié** (ADVANCED) : le client est seul sur une machine physique. Sur celle-ci, il n'y a que ses propres instances Lizmap, ses propres données, et il profite de toutes les ressources que peut offrir le serveur en matière de puissance de calcul, de mémoire disponible etc.

Une instance Lizmap est une installation d'une application « Lizmap Web Client », avec une base de données sur un serveur PostgreSQL. Elle comprend aussi un accès FTP dédié à l'application Lizmap Web Client.

À ce jour, 3Liz héberge plusieurs dizaines de clients, principalement localisés en France, mais aussi aux Antilles, à la Réunion, en Polynésie Française et en Europe.

Organisation mise en place

L'offre d'hébergement est gérée par une équipe de 4 personnes, dont :

- Un responsable commercial

- Un responsable technique
- Un administrateur système
- Un développeur pour nos outils de gestion de l'offre et des instances applicatives

Le responsable technique et l'administrateur systèmes se partagent l'activité de support client, les astreintes, le développement et la gestion de l'infrastructure.

Responsabilités liées au PAS

3Liz est responsable du maintien en conditions opérationnel des plateformes, de la supervision, des mises à jour de sécurité, des sauvegardes des données des clients.

Le client est quant à lui responsable de la gestion de ses données métiers et personnelles dans ses bases de données et ses espaces de stockage, ainsi que de l'utilisation responsable des ressources mises à sa disposition (ex : le FTP n'est pas un espace de partage, respect des quotas sur les volumes de stockage...).

Procédure d'évolution du PAS

Le Plan d'Assurance Sécurité est mis à jour régulièrement, en fonction des évolutions de l'infrastructure et de l'organisation du service d'hébergement.

Tout incident de sécurité sur notre infrastructure ou alerte CVE concernant l'un de ses composants donne également lieu à une analyse de risques et à une éventuelle actualisation de nos procédures internes.

Mesures de sécurité

Matériel

Nos serveurs sont des machines que nous louons chez OVH, le leader de l'hébergement en Europe. Il s'agit de serveurs physiques dédiés, sur lesquels nous avons la totale maîtrise au niveau système d'exploitation et logiciel.

Nous avons deux infrastructures, une pour nos développements et tests, une pour la production. Elles ne sont pas reliées entre elles, de manière à ce que les problèmes survenant sur l'une (surtout en développement), n'affectent pas l'autre.

Les serveurs d'une même infrastructure sont reliés ensemble via un réseau privé virtuel (technologie appelée VRACK chez OVH), pour que nos outils de déploiement et d'administration système puissent communiquer en toute sécurité, sans passer par « l'extérieur ».

Les machines sont principalement réparties dans plusieurs data-centres OVH en France, et nous pouvons louer des serveurs dans d'autres data-centres OVH ailleurs dans le monde, en fonction des demandes clients et des contraintes juridiques liées aux données.

Nous avons choisi d'utiliser des serveurs **physiques**, et non des offres « cloud » (machines virtuelles ou conteneurs) pour avoir des garanties quant à la localisation physique des données, et maîtriser la façon dont elles sont stockées. Cela nous permet de respecter au mieux les contraintes du **RGPD** (le Règlement Général sur la Protection des données). De plus cela permet de maîtriser les ressources systèmes et les coûts, et de proposer à nos clients des prix au plus juste.

Logiciels

Nous utilisons exclusivement des **logiciels libres** qui sont activement maintenus par leurs équipes de développement respectives.

Tous nos serveurs ont pour système d'exploitation **Proxmox**, une distribution basée sur Debian. **Debian** est une distribution Linux connue pour sa robustesse et son support long terme. Nous utilisons Proxmox pour gérer facilement les conteneurs LXC dans lesquels sont installés les divers logiciels d'une offre Lizmap Hosting. Certains services sont déployés avec Docker dans les conteneurs LXC.

Chaque serveur comprends au moins 4 conteneurs sous Debian 11 Bullseye, installés sur Proxmox 7 (basé sur Debian 11). Les serveurs récents sont équipés des logiciels suivants :

- **Service web** : Nginx + PHP 8.1 + Redis + des applications Lizmap Web Client
- **Base de données** Postgresql 14 + Postgis 3
- **Service cartographique** QGIS 3.22 ou 3.28 (versions maintenues sur le long terme)
- **Service FTP**, avec PureFTPd, serveur ftp le plus robuste en terme de sécurité à l'heure actuelle

Bien que les services peuvent être partagés ou non en fonction du type d'hébergement choisi, chaque client dispose toujours de sa propre application Lizmap. Elle n'est pas partagée avec d'autres clients. Elle dispose de sa propre adresse web, et seuls les utilisateurs du client peuvent s'y authentifier.

Sécurité des logiciels et de l'infrastructure

Bien que l'hébergement Lizmap Hosting n'ait pas encore de qualification de sécurité officielle (normes ISO, etc), l'infrastructure est développée et gérée par des administrateurs systèmes et développeurs qui ont de 10 à 20 ans d'expérience, avec une connaissance avancée sur la sécurisation des systèmes et services, ainsi que sur les bonnes pratiques dans ce domaine.

Nous utilisons exclusivement des versions de Linux maintenues, dont les équipes de sécurité assurent un audit permanent. De plus, les applications constituant l'environnement Lizmap ne permettent pas l'exécution de fichiers déposés par les clients ; des pistes d'améliorations sont par ailleurs en cours de réflexion, pour ajouter des vérifications supplémentaires en amont de leur intégration au sein des projets (analyse anti-virale, par exemple).

Les systèmes et logiciels sont mis à jour régulièrement, voir automatiquement, afin de colmater les éventuelles failles de sécurité, et corriger des bugs. Ces mises à jours sont en général réalisées la nuit, afin de limiter les indisponibilités de service.

Nous migrons chaque serveur vers des systèmes plus récents, à la demande du client ou quand cela s'avère nécessaire (lorsque la version d'un système n'est plus maintenue par exemple). Dans ce cas, nous convenons avec le client d'une procédure de migration et d'une date, afin de limiter l'impact sur l'activité du client.

Chaque serveur a un pare-feu qui permet de filtrer les accès aux conteneurs et aux services. Nous utilisons aussi Fail2ban pour limiter les tentatives d'accès forcés et répétitifs sur les outils d'administration exposés sur Internet.

De plus, chaque serveur profite du système anti-DDOS d'OVH, présent en amont sur le réseau d'OVH, permettant d'éviter les attaques de masse qui pourraient compromettre la disponibilité du service.

Sécurité des accès

Accès aux serveurs et réseaux

Les accès SSH aux machines sont restreints aux seuls employés de 3Liz qui ont le droit d'administrer les machines. L'authentification se fait uniquement par clé SSH, l'accès par mot de passe étant désactivé, et de manière nominative, chaque utilisateur ayant son propre identifiant.

Il en va de même pour l'accès au réseau privé, par lequel nous utilisons nos applications d'administration.

Accès au service Lizmap

L'accès web aux instances Lizmap et à nos applications d'administration se fait exclusivement via le protocole HTTPS. Les certificats TLS sont générés pour la plupart via le service gratuit Let's Encrypt (organisation soutenue par OVH, Mozilla, Google, Cisco et bien d'autres..) ou par notre fournisseur Gandi. Il est possible pour le client de fournir ses propres certificats (option pour les dédiés), qu'il aura payés auprès d'une autorité de certification reconnue par les navigateurs web.

Chaque utilisateur d'une instance Lizmap peut disposer de son propre identifiant et mot de passe. La gestion des comptes utilisateurs et leur finalité reste à la discrétion du client, et la gestion se fait directement dans Lizmap.

Les mots de passe des comptes de Lizmap sont stockés en base de données sous une forme rendue illisible et irréversible, avec une méthode de hachage utilisant l'algorithme « bcrypt » avec un « sel » aléatoire, et la comparaison avec un mot de passe donnée est sécurisée contre les attaques liées au temps d'exécution.

Le mot de passe du premier utilisateur créé lors de l'installation de l'instance est un mot de passe généré aléatoirement entre 12 et 20 caractères (minuscules, majuscules, chiffres). Lors de la création d'un compte via Lizmap, ou lors du changement d'un mot de passe, l'utilisateur peut choisir un mot de passe entre 12 et 120 caractères, avec n'importe quel caractère, sans contrainte sur la typologie de caractère. Depuis Lizmap 3.6.6, la qualité du mot de passe est vérifiée, en calculant l'entropie et en vérifiant si ils ne contiennent pas un des mots de passes d'une liste des mots de passes les plus utilisés. L'utilisateur ne peut pas ainsi pas choisir un mot de passe jugé trop faible par le mécanisme de vérification.

Il n'y a pas de mécanisme de fréquence de renouvellement de mots de passe, de non réutilisation de mot de passe, ni de blocage automatique au bout d'un certain nombre d'essai. Cependant ces mécanismes sont envisagés dans de futures versions de Lizmap.

Une authentification de type SSO est proposée en option pour Lizmap, utilisant le protocole SAML, et pouvant s'interfacer avec des services d'identité comme Active Directory, Azure, LemonLdap etc. Cela permet en outre de profiter de techniques d'authentification plus forte (2FA, mot de passe fort, blocage de compte etc) quand elles sont activées chez le fournisseur d'identité.

Accès aux services FTP et PostgreSQL

L'accès aux services FTP et PostgreSQL se fait avec un certificat TLS. Les connexions sont enregistrées dans les journaux du système.

L'accès à PostgreSQL peut être restreint à certaines IP si le client en fait la demande.

Chaque utilisateur dispose de son propre identifiant et mot de passe pour accéder aux services FTP et PostgreSQL. La gestion des comptes utilisateurs et leur finalité reste à la discrétion du client même si pour le

moment, il doit passer par le support technique de Lizmap Hosting pour cette gestion. Une application permettant aux clients de gérer eux-même les comptes FTP et PostgreSQL, est en cours de développement.

Les mots de passes peuvent être différents de ceux pour Lizmap. Ils sont générés aléatoirement par les outils d'administration de Lizmap Hosting, de ce fait il n'y a pas de politique de non réutilisation de mot de passe. Ils comportent entre 12 et 20 caractères (minuscules, majuscules, chiffres). Il n'y a pas de fréquence de renouvellement, mais les mots de passe peuvent être renouvelé en le demandant au support, sachant que le renouvellement d'un mot de passe PostgreSQL peut être très contraignant, si il est utilisé dans plusieurs projets QGIS. Il n'y a pas non plus de blocage de comptes au bout d'un certain nombre de tentatives.

Sécurité des données

Sur les hébergements mutualisés, les données des clients sont isolées d'un client à l'autre, que ce soit par des mécanismes d'isolation au niveau des espaces FTP ou par le biais de restrictions d'accès fortes au niveau des bases de données.

Sur les hébergements semi-dédiés, les mêmes mécanismes sont mis en œuvre au niveau des espaces FTP, et chaque client dispose de son propre serveur de bases de données indépendant.

Enfin, sur les hébergements dédiés chaque client est complètement isolé par l'utilisation de serveurs physiques distincts d'un client à l'autre.

Sauvegardes

Les données d'un client sont automatiquement sauvegardées quotidiennement, toutes les nuits, sur des serveurs d'archives. Chaque serveur dispose de son propre accès sécurisé aux serveurs d'archives, permettant ainsi de cloisonner les connexions et d'éviter tout accès indésirable aux données d'un autre client.

Sur les machines d'archives, les données sont répliquées incrémentalement, sur 6 jours glissants, et une copie hebdomadaire est conservée pendant 2 semaines.

Les données sauvegardées concernent :

- le contenu des bases de données
- les fichiers QGIS et autres que le client aura déposé via FTP
- les configurations des instances Lizmap.

Les machines d'archives sont situées dans des data-centres d'OVH différents de ceux où sont installés les serveurs de nos clients. Par exemple, les sauvegardes des serveurs installés au data-centre de Roubaix sont envoyées à un serveur d'archives installé en dehors de Roubaix, par exemple dans un data-centre de Graveline. Et vice-versa.

Chaque sauvegarde se termine par l'envoi d'un rapport par mail, nous permettant d'être averti d'éventuels échecs d'archivage.

Des restaurations sont régulièrement faites, sur demande de clients ou pour tester qu'une restauration se passe bien.

Surveillance des services

Les machines et services sont surveillés en permanence par divers outils afin de détecter les problèmes qui conduisent à des interruptions de services.

En cas de défaillance matérielle, OVH intervient automatiquement dans l'heure, et remplace les éventuelles pièces défectueuses. Nous avons un contrat de support niveau « Business », permettant d'avoir une réactivité accrue de la part d'OVH sur tous les problèmes matériels, qui intervient 24h/24 et 7j/7.

Chaque serveur est configuré à l'aide de différents outils de métrologie et de supervision, qui collectent des informations sur l'état des services, du matériel et des ressources utilisées, et qui envoient ces données vers notre tableau de bord central. Toute anomalie quand à la disponibilité d'un service (web, FTP, PostgreSQL, QGIS, etc) donne lieu à une alerte par mail ou SMS, ainsi qu'à certaines actions de remédiation automatique dans la mesure du possible.

Nous pouvons intervenir rapidement en heures ouvrées (à + 1h ou 2h maximum) pour ces anomalies logicielles. En revanche, nous ne garantissons aucun délai d'intervention entre 22h et 8h du matin, heures françaises, sauf si un contrat d'astreinte 24h/24h est établi (option réservée aux clients de l'offre dédiée).

Quand un incident survient et qu'il cause une dégradation du service de plusieurs minutes, nous alertons nos clients par mail sur la prise en charge de la résolution de l'incident.

Une des causes d'une interruption de service ou d'une forte dégradation du service, peut être due à des projets Qgis peu optimisés ou très lourds, ou des bases de données mal structurées. Dans ce cas, après audit des projets (qui peut soit directement, soit sur devis, en fonction de la complexité des projets), nous proposons des solutions correctives sur les projets et bases de données, une évolution des capacités de l'hébergement, ou un changement d'offre d'hébergement.

Continuité de service

Nous nous efforçons de fournir un service qui fonctionne 24h sur 24h. Cependant, il peut arriver une défaillance matérielle ou un problème logiciel grave qui nécessiterait la réinstallation d'un serveur physique complet. Si la durée d'interruption devait durer plus d'une journée (à cause d'un défaut de stock chez OVH par exemple), nous essaierions de trouver une solution temporaire, comme la réinstallation des instances sur d'autres serveurs mutualisés par exemple, à partir des dernières sauvegardes à notre disposition.

Nous ne proposons pour le moment pas de solutions de haute disponibilité, avec redondance des services sur plusieurs serveurs.

Enfin, nos clients étant hébergés au sein de plateformes différentes (mutualisées, semi-dédiées et dédiées), chacune rend compte d'un taux de disponibilité distinct, sur lequel nous n'avons pas d'engagement. En effet ce taux est en partie lié à la manière dont le client utilise nos services (par exemple, il peut arriver qu'un client déploie un projet qui fait des requêtes non optimisées, qui peuvent mettre à mal les ressources de la plateforme).

Réversibilité

Lorsque le contrat d'hébergement arrive à échéance, ou que le client nous en fait la demande, nous nous engageons à rendre les données hébergées dans leur intégralité, dans un format intègre et exploitable. Ces données sont les suivantes :

- archive ZIP contenant les fichiers posés sur le FTP (projets QGIS, données spatiales, médias, documents, etc.),
- sauvegarde de l'intégralité de la ou des base(s) de données PostgreSQL au format SQL zippé,
- utilisateurs et groupes d'utilisateurs créés pour la gestion des accès à l'instance Lizmap, au format SQL zippé,
- logs de connexion visibles dans l'interface d'administration de l'application Lizmap Web Client, au format SQL zippé.

Ces données sont transmises au client au maximum un mois après la date d'arrêt de la prestation d'hébergement. Elles sont récupérables pendant une durée maximum de 3 mois après l'arrêt de la prestation.

Les logiciels QGIS Server, Lizmap Web Client et PostgreSQL sont des logiciels libres, qui pourront être utilisés par le client pour exploiter ces données après la prestation d'hébergement. Cela assure une pleine réversibilité qui permet au client de recouvrir la jouissance de son capital informationnel.

Après le délai de 3 mois suite à l'arrêt de la prestation, 3liz s'engage à supprimer de manière irréversible toutes les données du client sur ses serveurs et ses supports de sauvegarde.