



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

Présentation technique de l'offre d'hébergement Lizmap Hosting

Excepté la description des offres ci-après, les informations et caractéristiques techniques décrites dans ce document ne sont pas contractuelles, et peuvent évoluer dans le temps. Elles ne sont donc valables qu'à la date de publication de ce document.

Offres

3Liz a des dizaines de clients qui utilisent l'hébergement SAAS de l'application Lizmap Web Client, Lizmap Hosting. Ces clients sont principalement localisés en France, mais aussi aux Antilles, à la Réunion, en Polynésie Française et en Europe.

3Liz propose, au travers de son service Lizmap Hosting, plusieurs offres 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, mémoires, disque dur...). Les mêmes services web, PostgreSQL, QGIS et FTP sont utilisées par plusieurs clients. Par contre, chacun dispose de son propre « Lizmap », de ses propres accès authentifiés, de sa propre base de donnée, 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, mémoires, disque dur...) pour les services tels que serveur web, et FTP. Mais ils disposent chacun de leur propre serveur (logiciel) PostgreSQL et QGIS qui ont chacun des ressources attribuées sur cette machine.
- 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.

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 logiciels.

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 réparties dans plusieurs data-centre OVH en France. Et nous pouvons installer des serveurs dans d'autres data-centre OVH ailleurs dans le monde, en fonction des demandes clients et des contraintes juridiques liées aux données.

Nous avons choisi d'utiliser des **machines 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 coûts, et de proposer à nos clients des prix au plus juste.

Logiciels

Nous utilisons exclusivement des **logiciels libres** qui sont maintenus activement 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.

Pour chaque serveur dédié à un client et chaque serveur mutualisé et semi-dédié, nous avons 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 connecter.

Sécurité des logiciels et de l'infrastructure

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

Les serveurs et conteneurs étant sous des systèmes d'exploitations Linux, et les logiciels installés étant déjà audités au niveau sécurité par les équipes qui développent la distribution Debian ou Proxmox, il n'y a pas d'antivirus installé.

Les systèmes et logiciels sont mis à jour régulièrement, voir automatiquement, afin de colmater les éventuels trous 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. Nous utilisons aussi Fail2ban pour limiter les tentatives d'accès forcés et répétitifs.

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 mettre une machine hors service.

Sécurité des accès

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.

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

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 sponsorisée par OVH, Mozilla, Google, Cisco..), mais aussi par Gandi.net pour certains services. Il est possible pour le client de fournir ses propres certificats (option pour les dédiés), qu'il aura payé auprès d'une autorité de certification reconnue par les navigateurs web.

L'accès aux bases de données et aux services FTP se fait également avec un certificat TLS. L'accès aux bases de données est aussi chiffré en TLS, et peut être limité à certaines IP, si le client en donne la liste.

Chaque utilisateur du client dispose de son propre identifiant et mot de passe pour chaque service (Lizmap, Postgresql, FTP). 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, LemonLdap etc.

Depuis 2013, date d'installation du premier serveur pour notre offre Lizmap Hosting, nous n'avons pas eu à déplorer un seul incident lié à un problème de sécurité.

Données et sauvegardes

Les données d'un client sont automatiquement sauvegardées quotidiennement, chaque nuit, sur des serveurs d'archives. Chaque serveur (dédié ou mutualisé) a son propre accès sécurisé aux serveurs d'archives. Ainsi il n'est pas possible depuis une machine quelconque d'accéder aux données d'une autre machine.

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, comprenant également la liste des utilisateurs, les droits, etc.

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 des clients installés au data-centre de Roubaix, sont envoyées à un serveur d'archive installé en dehors de Roubaix, par exemple dans un data-centre de Graveline.

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 de monitoring 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 support niveau « Business » avec OVH, permettant d'avoir une réactivité accrue de la part d'OVH sur tous les problèmes matériels, qui interviennent 24h/24 et 7j/7.

Nous avons à notre disposition les outils OVH pour avoir des métriques globales d'utilisation des machines (activité des processeurs, de la mémoire, des interfaces réseaux, etc), mais nous avons aussi nos propres outils qui collectent le même type de données et bien plus encore, et qui envoient ces données vers notre tableau de bord central. De la même manière, les outils que nous avons installés surveillent les différents services d'une instance Lizmap Hosting (service web, ftp, PostgreSQL, QGIS, etc.), et nous alertent en cas d'anomalie logicielle, par SMS et/ou par email.

Nous pouvons intervenir rapidement aux heures de bureau (à + 1h ou 2h maximum) pour ces anomalies logicielles. Par contre, nous ne garantissons pas des délais d'intervention courts entre 22h et 8h du matin, heures françaises. Sauf si un contrat d'astreinte pour pouvoir intervenir rapidement 24h/24h est établi, avec les clients ayant des serveurs dédiés.

Quand un incident survient et qu'il cause une dégradation du service de plusieurs minutes, nous alertons le client 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 dû 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 se faire rapidement ou sur devis, en fonction de la complexité des projets), nous proposons des solutions correctives sur les projets et bases de données, ou 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 matériel grave, ou un problème logiciel grave qui demanderait la réinstallation d'un serveur physique complet. Si la durée d'interruption devait durer plus d'une journée (à cause d'un défaut de serveurs en stock chez OVH par exemple), nous essaierons 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.

Déploiements

Chaque client peut demander l'installation d'une ou plusieurs instances Lizmap. Autant la commande d'un d'un serveur dédié peut prendre quelques jours (nous dépendons des délais de livraison d'OVH), autant la création d'une instance Lizmap (sur un serveur mutualisé ou sur un serveur dédié), prend quelques minutes, et cela, grâce à des outils de déploiement et de configuration automatique que nous avons développés et mis en place.

Ces outils ne sont pour le moment pas accessibles à nos clients, mais le seront probablement dans un avenir proche.

Les versions de Lizmap Web Client, de QGIS, et des plugins python QGIS que nous déployons pour nos clients, sont d'abord testées sur notre infrastructure de développement, celle-ci étant une réplique de l'infrastructure de production.

Nous utilisons des outils de tests, d'intégration continue, et de déploiement continu, permettant de livrer rapidement des évolutions et des corrections de bugs. Les instances Lizmap sont ainsi toujours à la dernière version corrective.

Tout ceci nous permet de garantir une qualité de service répondant aux besoins de nos clients. Si des problèmes critiques échappaient à notre vigilance et ne pouvaient se résoudre en quelques minutes après la mise en production, notre système de déploiement nous permet de revenir immédiatement à des versions précédentes.

Et comme pour les autres logiciels systèmes, nous déployons durant des périodes de faible activité, avec une surveillance accrue pendant les premières heures qui suivent la mise à jour.

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 et dans leur intégrité, dans un format 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.