

Conditions Particulières – Annexe de sécurité des serveurs – Maintenance Z-INDEX

Version du Lundi 19 février 2024 (Z-INDEX S.A.S. / tiers)

1. Sécurité des données hébergées chez OVH

• Présentation des serveurs

Pour le bon fonctionnement de ses activités, la société Z-INDEX dispose de serveurs Web d'hébergement. Ces serveurs sont dédiés à la seule utilisation de la société Z-INDEX. Il ne s'agit pas ici de systèmes « cloud » ou de serveurs d'hébergement mutualisés. Les ressources physiques et logicielles sont allouées et disponibles uniquement pour les services de la société Z-INDEX. Ci-dessous les configurations possibles des machines qui composent l'infrastructure :

Serveurs de productions Web :

- Système d'exploitation Debian
- Serveur Apache ou Nginx
- Système de gestion des bases de données MariaDB
- PHP

Serveurs de productions Mail

- Système d'exploitation Debian
- Serveur Apache ou Nginx
- Système de gestion des bases de données MariaDB
- PHP
- Plesk

2. Gestion des incidents

Le Client doit s'assurer de la justesse de ses informations de contact détenues par Z-INDEX, afin que Z-INDEX puisse lui notifier les changements, les incidents et les mises à jour ayant potentiellement un impact sur ses solutions. Pour cela, une fiche d'information est transmise annuellement pour assurer le droit d'accès, de modification et de retrait d'informations concernant les informations du Client. Le Client dispose de toutes les coordonnées nécessaires pour exercer un droit de consultation et de modification de ses données personnelles et de contact. Le Client doit avertir la société Z-INDEX par tous les moyens jugés utiles de tout changement de coordonnées.

Lorsqu'un incident est détecté sur un des services fournis par la société Z-INDEX à ses clients (que ce soit via un signalement du client, une alerte du sous-traitant OVH Cloud ou via un outil de monitoring ou tout autre partenaire), la procédure mise en place est la suivante :

- Prévenir le ou les Clients des services impactés ;
- Analyser l'origine de l'incident ;
- Isoler, si nécessaire, le service impacté pour éviter les dégradations en chaîne et les pertes de réputation ;
- Estimer le temps d'intervention avant rétablissement ;
- Résoudre le problème et vérifier le bon fonctionnement ;
- Prévenir le ou les clients du retour à disposition des services ;
- Faire une analyse post-intervention afin d'éviter un nouvel incident du même type ;

L'administrateur système de la société Z-INDEX a, à sa charge, la gestion de ce processus d'intervention avec, en support, si nécessaire, les compétences des techniciens de la société.

3. Gestion des intrusions ou failles de sécurité

Lorsqu'une vulnérabilité est détectée sur un des services fournis par Z-INDEX à ses Clients (que ce soit via un signalement du Client, une alerte du sous-traitant OVH Cloud ou via un outil de monitoring ou via tout autre Partenaire), la procédure mise en place est la suivante :

- Isolement du service concerné afin d'éviter immédiatement toute fuite de données :
 - o Coupure immédiate des accès depuis le web,
 - o Désactivation de l'envoi possible de mails,
 - o Modification des droits d'accès aux fichiers, et permissions de groupes et d'utilisateurs.
- Information au(x) Client(s) des services impactés ;
- Analyse de l'impact de l'intrusion ou de la faille de sécurité,
- Backup des fichiers et base de données pour investigation forensic,
- Estimation du temps d'intervention avant rétablissement,
- Résolution du problème avec application des correctifs de sécurité ou applicatifs,
- Information au(x) client(s) du retour à disposition des services,
- Investigation forensic,

4. Politique de développement des systèmes et applications

• Protocole HTTPS et certificat SSL

Les conceptions livrées par la société Z-INDEX sont obligatoirement faites de manière à être disponibles au travers de noms de domaines au format sécurisé avec une activation forcée du protocole https sur toutes les pages. Les certificats sont générés directement depuis les serveurs d'hébergement à partir de l'autorité de certification « Let's encrypt » : <https://letsencrypt.org/>

• Aide à la navigation et stockage des cookies

Lorsque cela est nécessaire et en fonction de chaque projet, les sites Internet mis en œuvre, créés, développés et/ou gérés par la société Z-INDEX sont livrés avec un module spécifique permettant à l'utilisateur d'accepter, de contrôler ou de refuser l'utilisation des cookies pour la navigation sur le site en question.

• Stockage des mots de passe en base de données

Les mots de passe sont stockés dans la base de données selon une méthode sécurisée allant du protocole de cryptage MD5 à SHA1. Les mots de passe ne sont jamais accessibles en clair dans la base de données.

• Informations à caractère personnel

Les formulaires de collecte de données publiques (formulaires de contact par exemple) mis en place sur les sites Internet ou les applications en ligne par la société Z-INDEX disposent tous d'une protection de sécurité et d'analyse de comportement « ReCaptcha » et d'une case à cocher informant l'utilisateur qu'il est sur le point de transmettre des informations personnelles. A ce titre, l'internaute est invité à consulter la politique de confidentialité des données présente sur le site Internet ou l'application pour être informé des traitements possibles des données personnelles du Client. Les formulaires permettant la transmission des données personnelles sont tous soumis à la saisie d'un consentement de l'internaute qui doit, à chaque fois, cocher une case permettant de justifier son information complète et préalable à la transmission des données personnelles.

Il est à noter que tous les documents relatifs aux politiques de confidentialité, politiques cookies, mentions légales, conditions générales sont de la responsabilité du Client, Z-INDEX ne prenant aucunement en charge la rédaction de tels documents juridiques.

• Transfert des données à des tiers

Contractuellement, la société Z-INDEX ne dispose d'aucune autorisation en dehors de celles fournies par les Clients concernés, de fournir des données de ses Clients à des tiers. Les serveurs d'hébergement de la société Z-INDEX sont isolés par défaut de toutes relations commerciales autorisant la vente, le transfert pour quelque raison que ce soit, sauf accord écrit et exprès du Client.

5. Gestion des accès d'administration

Les accès d'administration aux sites web et plateformes de productions sont conservés de manière sécurisée au sein d'un coffre-fort numérique. Pour l'accès aux services d'administration des serveurs, outils de monitoring ou de gestion de bases de données, une authentification à double facteur est mise en place.

6. Sécurité des serveurs Web applicatifs

Les serveurs d'hébergement de la société Z-INDEX sont configurés avec plusieurs outils de protection et d'analyse en temps réel ainsi que diverses procédures de vérification des fichiers.

Ces vérifications et procédures comprennent :

- Des outils anti port-scan configurés pour la surveillance des ports TCP et UDP avec bannissement automatique des adresses IP en cas de détection de scan,
 - Des outils d'analyse de journalisation avec la mise en place de règles personnalisées permettant de bannir les adresses IP de manière temporaire (1 heure) en cas de détection via l'un des patterns configurés,
 - Des outils de scan anti-virus avec mise à jour et analyse hebdomadaire,
 - Des outils de scan anti-malware avec mise à jour et analyse journalière,
 - Des pare-feu configurés et modifiés sur mesure (tous les ports entrants sont fermés sauf ceux strictement nécessaires au bon fonctionnement),
 - Des modifications des ports par défaut des services sensibles et autorisation d'accès par restriction d'adresses IP ;
- Les alertes en cas de problème ou suspicion de problèmes sont faites par email pour les outils :
- De scan anti-virus
 - De scan anti-malware

7. Monitoring des services et des infrastructures

• Engagement pris par Z-INDEX en sa qualité d'hébergeur de solutions

La société Z-INDEX dispose d'outils et de moyens de surveillance de l'état de santé des machines servant à l'hébergement des différentes solutions de ses Clients. Ces moyens de surveillance et de vérification sont purement à usage interne, installés sur les serveurs de la société Z-INDEX. Dans le cas où les clients de la société Z-INDEX souhaitent bénéficier de ses outils pour leur propre compte, ces services feront l'objet d'une facturation distincte.

• En ce qui concerne la partie logicielle « Software » :

- Vérification du statut du service Apache à intervalle de 5 minutes avec alerte mail en cas de coupure ;
- Vérification du statut du service MySQL à intervalle de 5 minutes avec alerte mail en cas de coupure ;
- Alerte par mail en cas de tentative d'envoi de mail en masse ;

En ce qui concerne la partie physique et matérielle des machines « hardware » :

- Vérification du statut des disques et du raid avec alerte par mail lorsque le taux d'utilisation dépasse les 80% d'utilisation et de charge ;
- Vérification du statut de l'utilisation de la RAM avec alerte par mail lorsque le taux d'utilisation dépasse les 80% d'utilisation et de charge ;
- Vérification du statut de l'utilisation des CPU avec alerte par mail lorsque le taux d'utilisation dépasse les 80% d'utilisation et de charge ;

• **Procédure de sauvegarde des données**

Pour toutes les données stockées au sein de l'infrastructure d'hébergement, sur les serveurs disponibles dans les Data Center de la société OVH Cloud, la société Z-INDEX a mis en place ses propres processus et systèmes de sauvegardes aussi bien pour les données brutes, que les conteneurs de données, les bases de données, les médias, les fichiers de paramètres et les fichiers de configuration. Les fichiers de sauvegardes sont alors tous externalisés vers un espace de stockage dédié, fourni par la société OVH Cloud et accessible uniquement via les serveurs dédiés associés.

8. Précisions sur l'espace de stockage OVH Cloud pour les sauvegardes internes

• **Espace de stockage illimité et scalable**

La société Z-INDEX n'a plus à anticiper le provisionnement de l'espace de stockage nécessaire à ses besoins. Le système « Object Storage » et « Cloud Archive » fournit un espace illimité pour toutes les applications. La société peut stocker tous types de fichiers sans se retrouver contrainte par un éventuel manque d'espace disque.

• **Espace de stockage résilient**

Les données sauvegardées sont distribuées au sein de clusters profitant d'une triple réplication pour chaque objet. Ces répliquions sont placées à la fois sur des disques et sur des serveurs différents afin d'en assurer la longévité.

9. Gestion de la continuité d'activité

• **Garantie de temps d'intervention : GTI**

Dès lors que la société Z-INDEX a communication d'une demande d'intervention de quelque nature que ce soit, la société Z-INDEX fournira tous les efforts nécessaires pour avoir un temps d'intervention inférieur :

- A 48h les jours ouvrés pour une demande de niveau 1 :

Intervention entrant dans le cadre du contrat de maintenance ou nécessitant moins d'une heure de travail et impactant un seul client.

- A 24h les jours ouvrés pour une demande de niveau 2 :

Intervention impactant plusieurs clients suite à une mise à jour des outils web ou des softwares.

- A 6h les jours ouvrés pour une demande de niveau 3 :

Intervention en lien avec un problème hardware lié à l'infrastructure d'hébergement

Ces délais courent à partir du moment où la société Z-INDEX confirme avoir bien reçu et pris en compte la demande, au travers de moyens de communication actuels à savoir :

- Téléphone : 04 71 48 42 02
- Email : contact@zindex.fr

10. Garantie de temps de rétablissement

Pour toute intervention en cours, la société Z-INDEX fournira tous les efforts nécessaires pour avoir un temps de rétablissement des services :

- Inférieur à 7h les jours ouvrés pour une demande de niveau 1 :

Intervention entrant dans le cadre du contrat de maintenance ou nécessitant moins d'une heure de travail et impactant un seul Client.

- Inférieur à 14h les jours ouvrés pour une demande de niveau 2 :

Intervention impactant plusieurs Clients suite à une mise à jour des outils web ou des softwares.

- Inférieur à 21h les jours ouvrés pour une demande de niveau 3 :

Intervention en lien avec un problème hardware.

Ces délais sont valables et pris en compte uniquement à partir du moment où la société Z-INDEX confirme avoir démarré l'intervention.

11. Journalisation

Pour garantir le bon fonctionnement de son infrastructure de serveurs d'hébergement, la société Z-INDEX dispose sur ces machines de journaux d'enregistrement des principales actions effectuées.

Les données récoltées et tracées dans ces journaux sont :

- Les données de Sécurité (analyse des tentatives d'intrusion) ;
- Les données de surveillance et de Monitoring (vérifications régulières des statuts des services) ;
- Les données de Statistiques et de Performances (nombre de processus ou éléments chargés) ;
- Les données de Débogage (analyse des erreurs, d'exécution de scripts) ;

La journalisation des serveurs stocke uniquement l'adresse IP publique des utilisateurs afin d'assurer le fonctionnement des différents outils précédemment cités. Aucune donnée personnelle autre que l'adresse IP n'est stockée et ne peut être utilisée ni consultée.