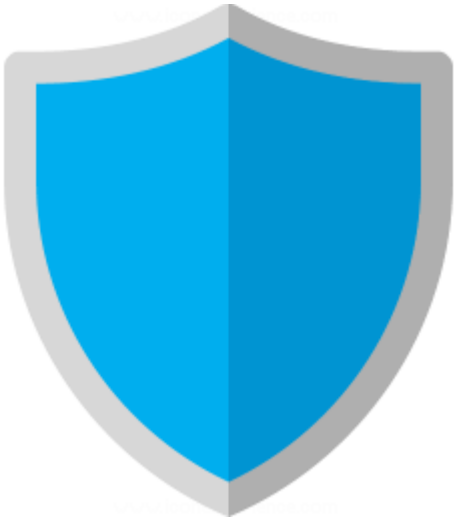
Sécurité/Confidentialité

La sécurité de la solution Gestan Cloud repose sur un ensemble d'éléments complémentaires :



- la sûreté des infrastructures
- la maintenance des serveurs
- la protection des serveurs contre les actions malveillantes de pirates informatiques
- la sûreté des modes de connexion et des transmissions
- la fiabilité des personnels techniques ayant à en connaître.

Sûreté des infrastructures

Les serveurs Gestan Cloud sont infogérés par Netsyst, société lyonnaise de services d'Ingénierie Informatique créée en 2011, constituée d'une équipe de consultants Systèmes, Réseaux & Datacenters.

Cette entreprise garantit la sûreté de ses installations :

- protection anti-intrusion,
- protection anti-incendie,
- contrôles d'accès des personnels
- habilitation des personnels au traitement des données confidentielles.

Les serveurs de production Gestan Cloud sont situés sur dans un datacenter basé à Lyon, tandis que les serveurs de backup appartenant à ICS-Informatique, sont basés dans un autre datacenter Lyonnais, infogérés également par NetSyst.

Maintenance des serveurs

C'est également Netsyst qui garantit la maintenance technique des serveurs physiques, et procède au renouvellement du matériel dès que nécessaire.

Dès que des machines présentent un rapport coût / efficacité intéressant, ICS peut entreprendre la migration d'une machine vers une autre.

Actuellement, le profil standard des serveurs Cloud Gestan est :

Core-4-S-SSD 2 x Intel® Xeon E5 2620v4 128 Go 3 x 500 Go SSD 1Gbit/sec 500 Mbit/sec RPNv2

Chaque serveur héberge environ une centaine de clients.

Protection des serveurs

Le monitoring sécurité des serveurs assuré par Netsyst permet d'assurer un niveau élevé de protection vis à vis des attaques malveillantes. Dans cette optique, NetSyst réalise :

- virtualisation des machines
- snapshots système à chaque mise à jour logicielle
- sauvegarde supplémentaire des données
- monitoring technique (CPU, espace disque, etc)
- application de la stratégie de sécurité (réglages firewall, réglages proxy, etc)
- monitoring des alertes anti-virus

Protection brute-force

Tous les serveurs Gestan Cloud sont équipés d'un logiciel de protection brute force.

Protection DDOS

La protection DDOS est assurée par NetSyst.

Nous avons déjà essuyé plusieurs attaques DDOS, perturbant le trafic pendant une durée limitée, attaques jugulées dans un délai de quelques heures.

Sûreté des transmissions

Les communications entre votre ordinateur et les serveurs Gestan cloud utilisent le protocole HTTPS, le même que celui utilisé par votre banque, par exemple.

Ce protocole de communication, devenu une norme mondiale, assure le plus haut degré de confidentialité de la communication.

Procédures internes de sûreté

A l'intérieur d'ICS-Informatique, seules les personnels de support technique Cloud peuvent connaître vos identifiants de connexion. Tous ont signé un engagement de confidentialité.

Les identifiants que nous vous communiquons sont générés aléatoirement, afin d'offrir un niveau

correct de résistance aux attaques.

Tous les accès aux serveurs sont enregistrés et peuvent être vérifiés.

Plan de reprise de l'activité (PRA)

L'incendie survenu dans les datacenters d'OVH (mars 2021) démontre que si la fréquence des incidents majeurs est rare, elle n'est cependant pas nulle.

L'ensemble des serveurs Gestan Cloud sont virtualisées sous VMWare, ce qui permet d'envisager une remise en route rapide.

Dans le cas d'un incident de type OVH sur le datacenter de production, et hors cas d'autre incident majeur concomitant impactant la disponibilité de Netsyst, la reprise d'activité suivra ces étapes :

- ouverture d'un nouveau serveur dans un autre site NetSyst : environ 15 minutes,
- remontage de la machine virtuelle : environ 15 minutes
- remontage des données : environ 10 minutes par client, soit 17 heures pour 100 clients, norme habituel de charge par serveur.

A noter que les données sont en permanence à disposition des clients, pour tout backup local éventuel, via un programme de compression intégré à Gestan, qui génère une archive ZIP, d'usage immédiat en local.



Contexte légal

La solution Gestan Cloud est 100% française : le programme est développé par ICS-Informatique, SARL de droit français, et les serveurs sont infogérés par NetSyst, SAS de droit français également, dans des datacenters situés sur le territoire métropolitain.

Les entreprises Françaises sont soumises à des obligations légales souvent méconnues, dont les suivantes :

- le dépôt des documents comptables à l'extérieur de l'union européenne est interdit
- le stockage de vos factures électroniques à l'extérieur du territoire national fait l'objet d'une déclaration obligatoire à l'administration fiscale
- le traitement des données personnelles doit être conforme avec la législation française, spécialement la loi "Informatique et Libertés" n°78-17 du 6 janvier 1978 ainsi qu'au RGPD.

France : Les "boites noires" de la loi renseignement

Une disposition de la loi renseignement de 2015, au prétexte de lutter contre le terrorisme, permet à l'Etat d'installer des “boites noires” sur les structures des hébergeurs, exploitées par la DGSI et par la DGSE.

Le fonctionnement de ces “boites noires” n'est pas connu actuellement : si l'Etat espionne légalement les transmissions par Internet, on ne sait pas quelles sont les données transmises à la DGSI et la DGSE, et encore moins la manière dont elles sont

exploitées.

USA : Le Patriot Act

Il faut signaler que les fournisseurs de service situés sur les territoire des États-Unis ne peuvent garantir de confidentialité à vos données.

En effet, depuis l'instauration en 2001 du Patriot Act, la législation américaine permet à ses services de sécurité d'accéder à toutes les données à caractère personnel.



Cela concerne les données :

- des sociétés américaines, même si les données sont stockées physiquement sur le territoire européen
- de leurs filiales, même si elles sont implantées dans un autre pays du monde
- des serveurs qui sont hébergés aux Etats-Unis, y compris si la société qui possède les serveurs est d'une autre nationalité

Cette intrusion dans vos données n'a pas besoin d'être effectuée sous le contrôle d'un juge, ni même d'être rendue publique : vos informations peuvent être lues, dupliquées, conservées et divulguées à des tiers sans que vous en soyez informé.

Autres articles "Cloud"

Astuces pour Gestan Cloud
Bureau à distance Gestan Cloud
Connexion Gestan Cloud via RDP Windows
Double connexion
Etat des serveurs Gestan Cloud
Etat des serveurs Gestan Cloud (archives)
Imprimer avec Gestan Cloud
Problème de connexion à Gestan Cloud
Se connecter à Gestan Cloud
Sécurité/Confidentialité
Transférer vos données dans le Cloud
Vademecum Gestan Cloud
Vérifier votre votre connexion Internet

Despuis :
https://wiki.gestan.fr/ - **Le wiki de Gestan**

Lien permanent:
https://wiki.gestan.fr/doku.php?id=wiki:cloud:securite

Derni?re mise ? jour : **2024/09/23 14:14**