ANNEXE 3 – CHARTE QUALITÉ

Les conditions de la charte qualité sont reprises en détail en « Annexe 4 – OVHCloud – Conditions particulières du service public Cloud ».

Le Prestataire s'engage à respecter la Charte Qualité et notamment les points suivants qui sont le gage de la qualité de sa prestation, à savoir :

DISPONIBILITÉ

Le Prestataire s'engage à mettre en place des contrôles efficaces de nature à procurer une assurance raisonnable que le Client peut accéder et utiliser les Solutions concernées aux heures déterminées au Contrat.

Pénalités

En cas de non respect au cours d'un mois des engagements de disponibilité, les pénalités seront appliquées selon l' « Annexe 4 – OVHCLOUD – Conditions particulières du service public Cloud ».

SÉCURITÉ ET CONFIDENTIALITÉ

Le Prestataire s'emploie à sécuriser l'accès et l'utilisation des Solutions, en tenant compte des protocoles, conformément aux usages en la matière.

PRÉCISIONS SUR LA SÉCURITÉ DES SERVEURS SAAS HÉBERGÉS PAR OVH ET GÉRÉS PAR TWS

Les serveurs SAAS

- Serveurs OVH sur les sites de Gravelines et Strasbourg
    - Serveurs localisés en France et soumis au Droit Français
- 8 cœurs, 16 Go RAM,
- Disque 160 → 640 Go, Réseau 2 Gbits/s
- Debian 12
- Postgres 15 / Oracle 23c

Sécurité des données

- Empêcher tout accès ou utilisation frauduleuse des données
- Prévenir toute perte, altération ou destruction des données
- Intégration de la configuration du Geoserver dans le répertoire DATA
- Backup journalier de la base de données

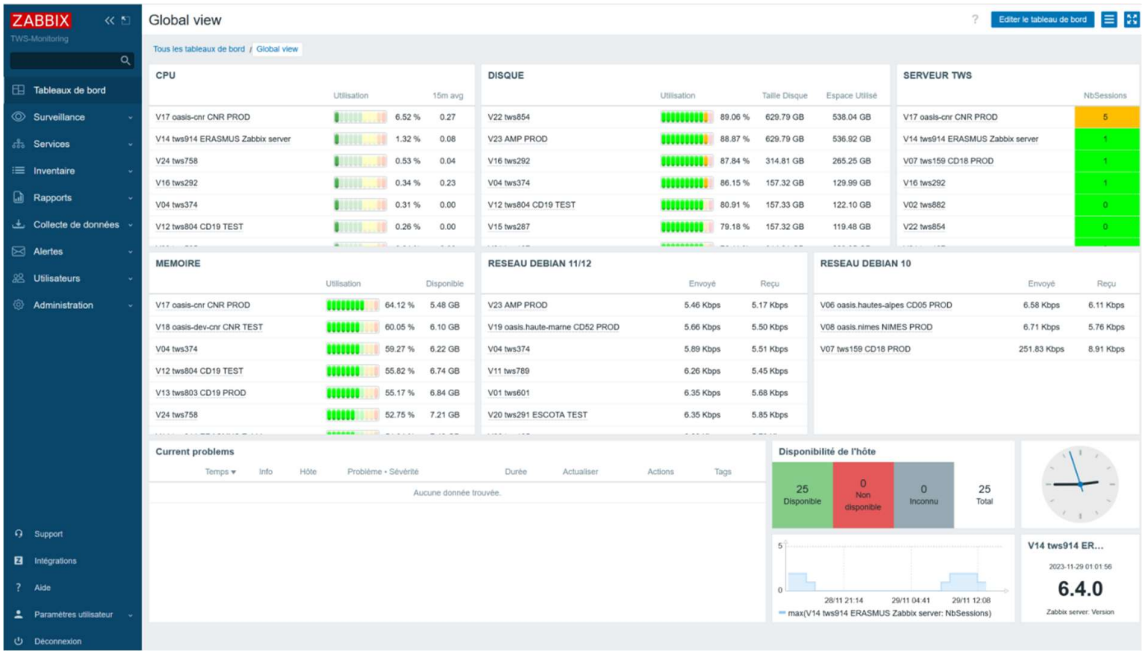
Sauvegarde des données

- Instance Backup : Sauvegarde machine
- Sauvegarde journalière de l'ensemble des données (Dump, Data, Documents), sur deux sites physiques différents
- Possibilité de mise à disposition de l'ensemble des données via un serveur SFTP

Maintien en fonctionnement et performance du service

- Supervision de la mémoire
- Supervision de l'espace disque
- Supervision de l'utilisation de la CPU
- Supervision de la bande passante
- Détection et gestion des anomalies logicielles

- Utilisation de ZABBIX :



- Attaques massives → Mitigation OVH (Protection contre attaques DOS et DDOS)
- Tentatives d'intrusion : Mise en quarantaine
- Mise à jour « système » réalisées par TWS :
    - Mise à jour du système d'exploitation :
        - Debian10 → Debian 12 et du SGBD
        - Postgres 11 → Postgres 15
    - Mise à jour en 2024 de l'ensemble des composants logiciel : Java, Wildfly, Geoserver

Contrôle de l'utilisation

- Règles des mots de passe : âge, taille, non réutilisation, verrouillage de compte, complexité, périmètre, …
- Interfaçage avec Azure Ad
- Audit de sécurité :
    - Un audit de sécurité a été réalisé en avril 2023 par la société Elysium Security sur un environnement client.
    - La politique de sécurité a été approuvée.

Autres mesures

- TWS a contracté une assurance professionnelle « Services numériques »

INTÉGRITÉ

Le Prestataire s'engage à mettre en place des contrôles efficaces de nature à procurer une assurance raisonnable que les applications mises à dispositions des Clients traitent les Données qui lui sont confiées sans risques d'omission, altération, déformation ou toutes autres formes d'anomalie susceptibles de nuire à l'intégrité des résultats issus de ces applications et que les traitements sont en conformité avec la réglementation légale qui leur sont applicables, et que les Données et traitements sont accessibles pour les contrôles et audits extérieurs qui pourraient être diligentés.

L'intégrité du traitement s'étend à toute composante du système et à toutes les phases du traitement (entrée de données, transmission, traitement, stockage et sortie des données). Ces contrôles consistent en des contrôles de cohérence des traitements, la détection et la gestion des anomalies ainsi que l'information des Utilisateurs relativement à tout risque de non-conformité associée.

PERFORMANCE

La performance correspond au temps de réponse des applications. Les temps de réponses peuvent être primordiaux pour les entreprises dans la mesure où ils peuvent avoir un impact économique significatif pour des applications critiques. Il est donc nécessaire de définir des métriques de performances, les niveaux de performances minimum attendus ainsi que d'anticiper et de corriger d'éventuelles défaillances. Il n'est pas inutile de mettre à disposition des futurs utilisateurs un profil de performances de l'application par heure, par jour, par semaine, par mois.

Autres éléments à examiner : les capacités réseau et bande passante garanties, les consignes de test de l'application et les dispositifs d'assistance. Dans le cas où le prestataire ne fournit pas la connexion (c'est-à-dire hors cloud privé), il conviendra d'exclure les réseaux du calcul.

Lorsque le prestataire fournit la connexion, il est recommandé qu'il dispose de plusieurs connexions réseau avec l'application SaaS, pour garantir l'absence de ralentissement ainsi que des temps de réponse minimum réduits.