

12-14 juin 2024



Sécurité augmentée en mode SAAS

Forum ERASMUS – Session 8



Les SAAS

- OVH Gravelines
- 8 cœurs, 16 Go RAM,
- Disque 160 Go, Réseau 2 Gbits/s
- Debian 12
- Postgresql 15



Les mesures de sécurité

- Sécurité des données
- Sauvegarde des données
- Maintien en fonctionnement et performance du service
- Contrôle de l'utilisation
- Autres mesures



Sécurité des données (1)

- Empêcher tout accès ou utilisation frauduleuse des données
- Prévenir toute perte, altération ou destruction des données



Sécurité des données (2)

- Intégration de la configuration d'Etools dans le répertoire DATA
- Backup journalier de la base de données



Sauvegarde des données

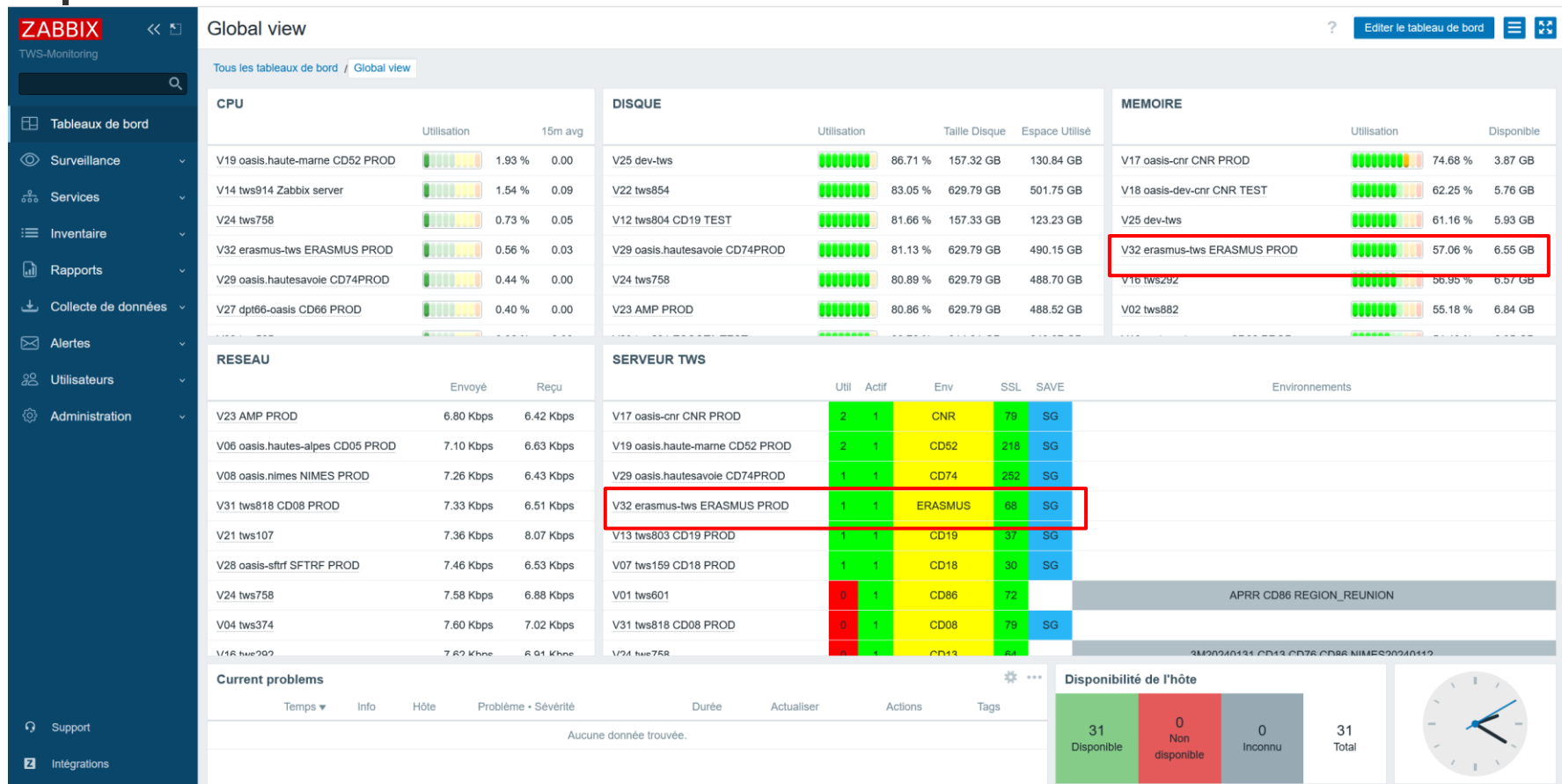
- Instance Backup : Sauvegarde machine
- Sauvegarde journalière de l'ensemble des données (Dump, Data, Documents), sur deux sites physiques différents



Maintien en fonctionnement et performance du service (1)

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

Maintien en fonctionnement et performance du service (2)



Maintien en fonctionnement et performance du service (3)

- Attaques massives → Mitigation OVH
(Protection contre attaques DOS et DDOS)

Chère cliente, cher client,

Notre système de surveillance du réseau a détecté des modèles de trafic inhabituels qui peuvent indiquer une attaque ciblant vos services sur [REDACTED].
Pour protéger votre entreprise et supprimer toute activité malveillante, nous dirigeons dès à présent votre trafic vers nos centres de nettoyage réseau.

Veuillez noter que ces attaques visent généralement à rendre les services indisponibles et ne devraient pas présenter de risque pour la sécurité de vos données.

En général, aucune action de votre part n'est requise.

Pour plus de détails, rendez-vous dans votre espace client, partie « Bare Metal Cloud », « Network », puis cliquez sur le tableau de bord Anti-DDoS. Vous pouvez également y accéder en cliquant sur le lien suivant :
<https://www.ovh.com/manager/#/dedicated/network-security/scrubbing-center>

En tant que client-e OVHcloud, vous bénéficiez d'un service de protection anti-DDoS de pointe qui isole et filtre le trafic malveillant. Plus d'informations ici : <https://www.ovhcloud.com/fr/security/anti-ddos/>

Nous vous remercions pour la confiance que vous nous accordez.

L'équipe OVHcloud

- Tentatives d'intrusion: Mise en quarantaine



Maintien en fonctionnement et performance du service (4)

- Mise à jour du système d'exploitation
Debian10 → Debian 12
- Mise à jour du SGBD
Postgresql 11 → Postgresql 15
- Mise à jour en 2024 de l'ensemble des composants logiciel: Java, Wildfly, Geoserver



Audit de sécurité

- Audit de sécurité réalisé en avril 2023 par la société Elysium Security sur un environnement client
- Audit de sécurité réalisé en avril 2024 par la société Advens sur un environnement client



Autres mesures

- Assurance professionnelle « Services numériques »
- Serveurs localisés en France et soumis au Droit Français

Mises à jour des composants logiciels



- Client :
 - OpenJDK 20 (2023-03-21)
- Serveur :
 - OpenJDK 21.0.2+13-58
 - Wildfly 31.0.1
 - Geoserver 2.24.2



Sécurisation des services d'administration

- Passage du service d'administration Wildfly en localhost
- Passage du service d'administration du Geoserver en localhost
- Le service SSH est restreint aux IP des administrateurs TWS



Sécurisation de l'authentification

- Authentification des utilisateurs du client (revue selon bonnes pratiques) :
 - Sous TLS, passage du mot de passe en clair au lieu de son empreinte chiffrée
- Authentification des requêtes du client par jeton à durée limitée
- Renforcement du chiffrement des mots de passe stockés (SHA256)



Échanges client/serveur HTTP

- Support de TLSv1.3 avec cipher-suite=
TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS
_AES_128_GCM_SHA256
- Entête "HttpOnly"
- Entête "Secure"
- Précision de la définition du CSP
- Entête HSTS
- Utilisation de jetons CSRF pour les
requêtes au geoserver