29-31 mai 2024

Sécurité augmentée en mode SAAS

Forum OASIS-OKAPI – Session 9

OASIS-OKAPI

Vendredi 31 mai 2024

Les SAAS

- OVH Gravelines, Strasbourg
- 8 cœurs, 16 Go RAM,
- Disque 160→640 Go, Réseau 2 Gbits/s
- Debian 12
- Postgresql 15 / Oracle 23c

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 du Geoserver dans le répertoire DATA
- Backup journalier de la base de données

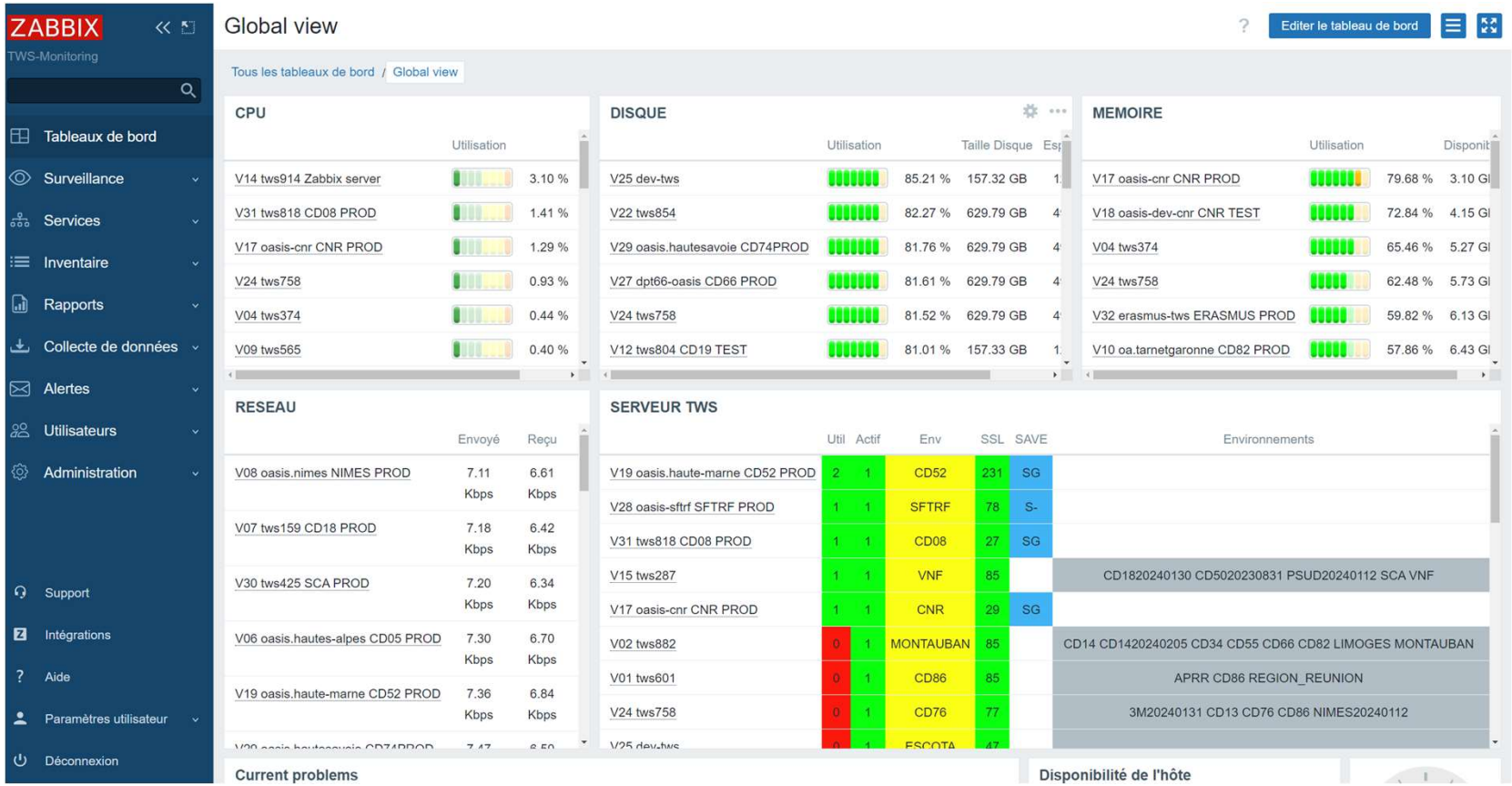
Sauvegarde des données

- 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 (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)



Mode SAAS – Sécurité augmentée

Maintien en fonctionnement et performance du service (3)

- Attaques massives → Mitigation OVH (Protection contre attaques DOS et DDOS)
- Tentatives d'intrusion: Mise en quarantaine

Maintien en fonctionnement et performance du service (4)

- Mise à jour du système d'exploitation

  Debian10 → Debian 12 et du SGBD

  Postgresql 11 → Postgresql 15

- Mise à jour en 2024 de l'ensemble des composants logiciel: Java, Wildfly, Geoserver, OpenLayers

Contrôle de l'utilisation

- Règles des mots de passe : âge, taille, non réutilisation, verrouillage de compte, complexité, périmètre, …
- Interfaçage avec Azure AD et Keycloak

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

- Clients riches :
  - OpenJDK 20 (2023-03-21)
- Serveur :
  - OpenJDK 21.0.2+13-58
  - Wildfly 31.0.1
  - Geoserver 2.24.2
  - OpenLayers 9.1.0

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 des clients riches (revue selon bonnes pratiques) :
  - Sous TLS, passage du mot de passe en clair au lieu de son emprunte chiffrée
- Authentification des requêtes des clients riches par jeton à durée limitée
- Renforcement du chiffrage 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