Document d’Architecture Technique (DAT)

Veolia Cyber Hub (VCH)

---

1. Points en suspens & obsolescences

- Validation du matériel à utiliser pour l’hébergement de la solution.
- Confirmation des flux réseau précis et de la matrice de flux.
- Besoin d’un agent de collecte pour Linux à développer.
- Conformité aux standards de sécurité ANSSI.

2. Présentation de l’application

2.1 Contexte

Veolia Eau France souhaite renforcer la cybersécurité de ses sites industriels en déployant une solution centralisée, le Veolia Cyber Hub (VCH), positionné dans la DMZ de chaque site. Cette solution doit permettre la synchronisation des horloges, la journalisation des événements, la gestion de la conformité et le transit des flux réseau critiques.

2.2 Descriptif projet / application

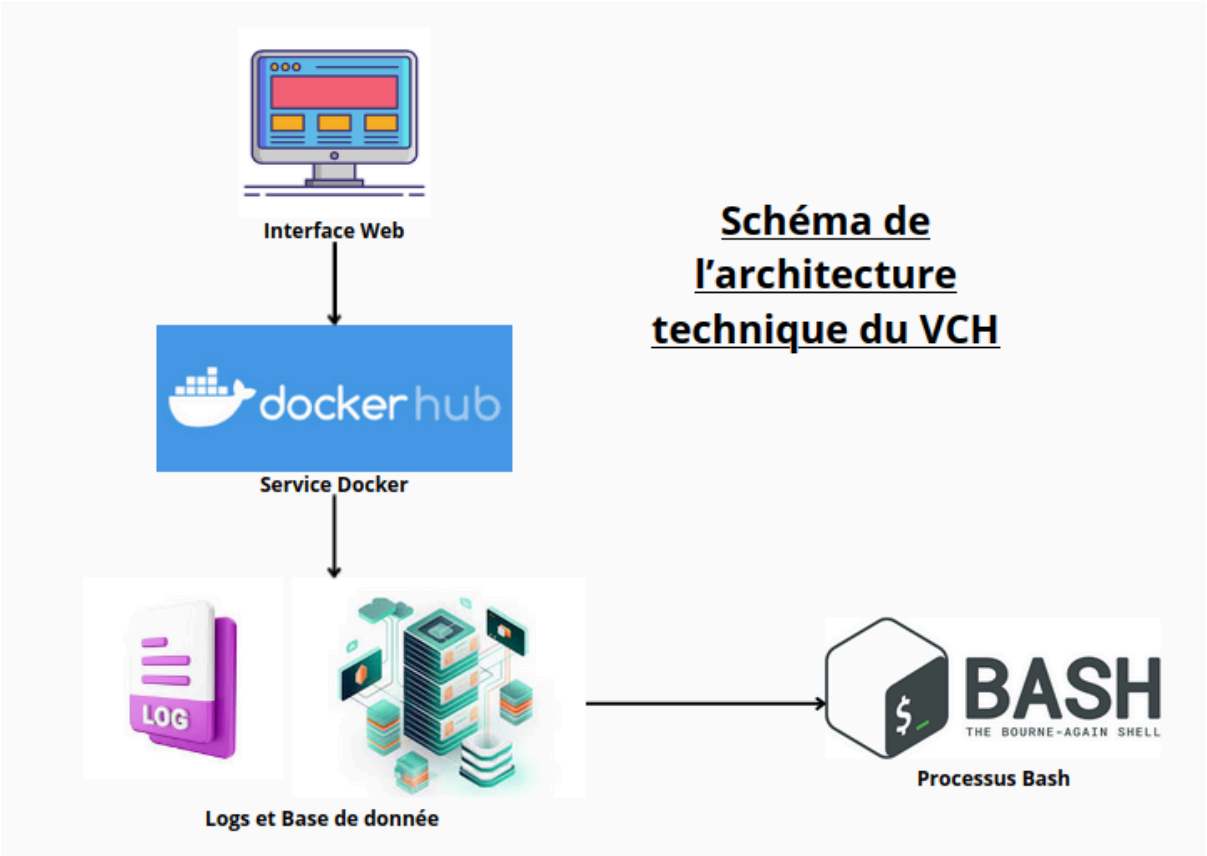
Choix	Explications
Type de solution	IaaS
Internet	Non
Nbre de Users	Internes (Cybersécurité Veolia)
Plages de fonctionnement	24/24 - 7/7
PRA	Oui

2.3 Positionnement SI

Le VCH s'intègre dans le SI de Veolia Eau France en servant de point central pour la cybersécurité des sites industriels.

3. Architecture technique

3.1 Schéma



3.2 Description des briques

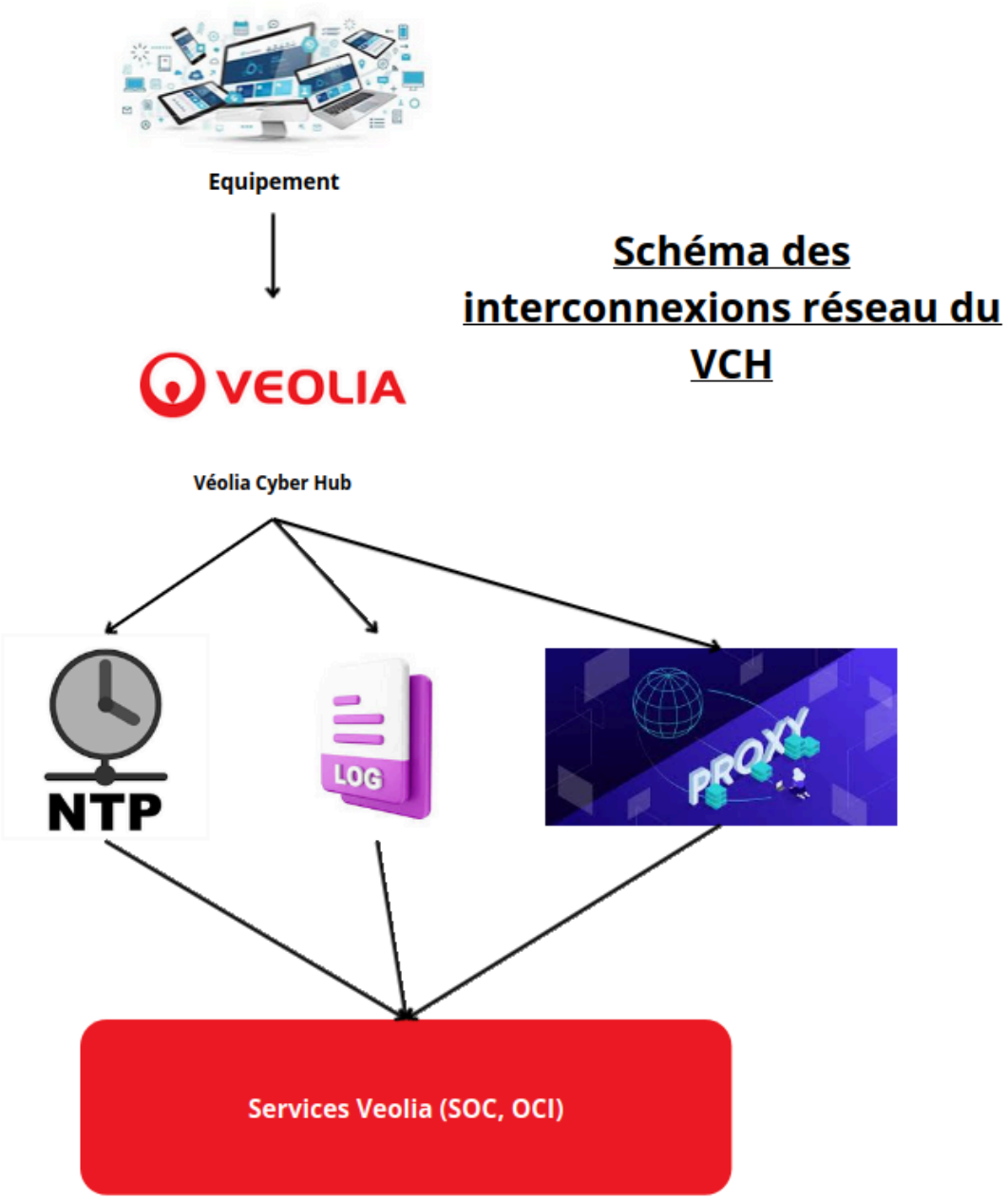
- Front : Interface Web pour la gestion et la consultation des logs et de la conformité.
- Back : Services Docker déployés sous Debian 12.9.
- Base de données : Stockage des logs et des configurations.
- Batch : Processus de synchronisation et d'analyse des journaux.

3.3 Optimisations

- Performances : Architecture modulaire avec Docker.
- Financières : Minimisation des besoins en ressources.

4. Architecture Réseau

4.1 Schéma



4.2 Matrice des flux

Service	IP Source	IP Destination	Port
NTP	VCH	Serveur NTP Veolia	123
Journalisation	Équipements	VCH	514
Journalisation	VCH	SOC Veolia	6514
Conformité	Équipements	VCH	443
Conformité	VCH	OCI Veolia	443
Proxy WSUS	VCH	Serveur WSUS Veolia	8530
Proxy DN	VCH	Serveur DNS Veolia	53

4.3 URL sortantes

Non applicable (la solution ne doit pas se connecter à Internet).

5. Infrastructure

- Production : Hébergement sur DMZ industrielle.
- OS : Debian 12.9.
- Services : Docker, NTP, Syslog, Proxy.

6. Sécurité

- Authentification : Conforme aux standards ANSSI.
- Traçabilité : Journalisation des accès.
- Chiffrement : Communications chiffrées.

7. Plan de reprise d'activité

- Bascule : Redéploiement automatisé sur un autre VCH.
- RPO/RTO : 24h max.

8. Chargement & Sauvegarde

- Rétention logs : 1 mois ou 196 Go.
- Sauvegarde : Stockage local + transfert SOC.

Ce document constitue une première ébauche du DAT pour le projet Veolia Cyber Hub. Dis-moi si tu veux des ajustements ou des ajouts !