Dossier d’Architecture Technique

Les 4 fantastiques / Véolia

[***Consignes sur la documentation technique***](https://sites.google.com/a/veolia.com/ist-efr-archi-perf/infos-pratiques/liste-des-docs-techniques)

**Table des matières**

[**1 Points en suspens & obsolescences**](#_wkdmpe33sosf) **4**

[**2 Présentation de l’application**](#_5f1zwr35u4mw) **5**

[2.1 Contexte](#_w2xzra5hv5e9) 5

[2.2 Descriptif projet / application](#_uuf0owker46j) 6

[2.3 Positionnement SI](#_b90h981ajgy7) 8

[**3 Architecture technique**](#_ex2rk6h35o8t) **8**

[3.1 Schéma](#_6cltv51pwxq2) 9

[3.2 Description des briques (Front, Back, Batch, autres)](#_39vfhfk9hiyp) 11

[3.2.1 Mon Appli](#_7atkpzktan2w) 11

[3.2.2 Appli A](#_83qb5etgpdr3) 11

[3.2.3 Appli B](#_21krz5y55ssk) 11

[3.3 Optimisation(s)](#_832qurkmh6ly) 12

[3.3.1 Performances](#_pdf5jfh41bji) 12

[3.3.2 Financière(s)](#_60mzcd1q23u2) 12

[**4 Architecture Réseau**](#_tp0nrombxymq) **13**

[4.1 Schéma](#_k0mykrrqzjnh) 13

[4.2 Matrice des flux](#_onaqasyuy4ow) 16

[4.3 URL sortantes](#_aoaeycxwzg12) 16

[**5 Infrastructure**](#_4rjunbfnkaub) **17**

[5.1 Production](#_oh78j2yl1xp7) 17

[5.2 Pré production](#_ypq348hy4wa) 18

[5.3 Qualification](#_1c1xe36y4hx) 18

[5.4 Développement](#_9ol9fijhr3r) 18

[5.5 Autres](#_eyri2734k33r) 18

[**6 Sécurité**](#_kkvj1bayzr8z) **19**

[6.1 Coffre fort](#_70g1g2czaiqi) 19

[6.2 Authentification](#_8yynu4srcoy0) 19

[6.2.1 Procédure de gestion des accès](#_cff5jh2gpjzs) 19

[6.2.2 Providers](#_bhgp2eu3ufv9) 19

[6.2.3 Gestion des sessions](#_fokt5cvb38pe) 19

[6.2.4 Traçabilité/Auditabilité](#_mhpq14ygjupt) 19

[6.3 Liste des comptes non nominatifs et justifications](#_tga186sx9z8t) 20

[6.4 Console(s) d’administration](#_s1lyqvq2wxk2) 20

[6.5 Données à caractères personnelles ou sensibles](#_xuo2fjbkfilj) 20

[6.6 Certificat(s)](#_lxql3we7x77) 21

[6.7 Plage de maintenance (patching,service managé ou pas)](#_gf9sd2wdqg0k) 21

[**7 Plan de reprise d'activité**](#_v11oqv3io3v5) **22**

[7.1 Périmètre](#_461avdtvt2sp) 22

[7.2 Processus de bascule](#_tvzmsk3xy0nv) 22

[**8 Chargement & Sauvegarde & Archivage**](#_xw2i05yv62zd) **23**

[8.1 Chargement initial et reprise des données](#_1in55xuyrec2) 23

[8.2 Sauvegarde](#_l2i0lbizgaux) 23

[8.3 Archivage](#_ad9sp7yqpgb5) 23

[8.4 Purge](#_3xmjdqskc9bc) 23

[8.5 Restauration](#_yn09nhefx0ib) 23

# 1 Points en suspens & obsolescences

|  |
| --- |
| Le projet Veolia Cyber Hub (VCH) est une solution déployée dans la Zone Démilitarisée (DMZ) d'un site industriel de Veolia Eau France.  Il assure des services essentiels comme la synchronisation des horloges des équipements, la collecte des journaux d'activité, et la gestion des flux vers le WAN/Internet, tout en garantissant un niveau de sécurité élevé. |

# 2 Présentation de l’application

## 2.1 Contexte

***Description***

|  |
| --- |
| **Rédacteurs** : groupe  **Lecteurs**  : Tous  **Valideurs**  : Chapter  *Description succincte du projet :*  Positionnement métier : Le VCH est une solution visant à garantir la sécurité et la performance des services industriels de Veolia Eau France.  Positionnement SI : Il s'intègre dans un SI très sécurisé, avec des contrôles rigoureux des flux et de la gestion des accès.  Solution: Solution Web utilisée pour le contrôle et la gestion des flux industriels. Elle est intégrée à l’infrastructure cloud de Veolia et déployée dans une DMZ pour garantir la sécurité des échanges.  Entité: Veolia Eau France Service: IS&T EFR Responsables : Chapter Lead, Tech Lead / Plateforme |

***Entité, service et contacts***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Entité** | **Domaine** | **Code imputation** | **Prénom** | **Nom** |
| IS&T EFR |  |  |  |  |

***Interlocuteur(s) à privilégier***

|  |  |  |  |
| --- | --- | --- | --- |
| **Entité** | **Prénom** | **Nom** | **Responsabilité** |
| IS&T EFR |  |  | Chapter Lead |
| IS&T EFR |  |  | Tech lead / Plateforme |
| IS&T EFR |  |  | Tech Lead / Chapter |

***Identification du projet***

|  |  |  |  |
| --- | --- | --- | --- |
| **Entité** | **Domaine** | **Chapter** | **Application** |
| IS&T EFR |  |  |  |

## 2.2 Descriptif projet / application

|  |
| --- |
| **Rédacteurs** : Chapter / Squad  **Lecteurs**  : Tous  **Valideurs**  : Chapter  *Cette fiche permet d'avoir une idée rapide du projet.* |

|  |  |  |
| --- | --- | --- |
|  | **Choix** | **Explications** |
| **Modules** | * WEB * Mobile * Service * Batch * Application locale |  |
| **Type de solution** | * SaaS * PaaS * CaaS * IaaS |  |
| **Internet** | * OUI * NON | déployé dans un environnement fermé. |
| **Nbre de Users** | * Mobile : * WEB : * Interne : * Externe : | Utilisateurs internes de Veolia Eau France, personnel de maintenance et administrateurs système. |
| **Types utilisateurs** | * Interne * Indus * Partenaires * Internautes * Clients finaux * autres | système interne uniquement. |
| **Plages de fonctionnement**  **IHM** | 24/24 -- 7/7 | IHM : 24/24 – 7/7 |
| **Plages de fonctionnement**  **BATCH** | 24/24 -- 7/7 | BATCH : 24/24 – 7/7 |
| **Astreinte** | * Oui * non | Oui, les équipes IT sont en astreinte 24/7 pour la gestion des alertes et la sécurité. |
| **Plages de maintenance** |  | Liste des modules (services) qui sont indispo pour cause de maintenance + plages |
| **PRA ou**  **Dispositif failover** | * Oui * non |  |
| **Proxy sortant** | * Oui * Non * Pas concerné | les équipes IT sont en astreinte 24/7 pour la gestion des alertes et la sécurité. |

|  |  |  |  |
| --- | --- | --- | --- |
| Domaine applicatif | Criticité | Liste des référentiels impactés ou pas ? | Remplace l’application ? |
|  | Critique Majeur  Normal |  |  |
|  |  |  |  |

Pour la criticité se référer au tableau suivant : [Criticités Métiers des Applications](https://docs.google.com/spreadsheets/d/1jPpgDrxa154yvHYJlWH6fsMBHbCfjdHfkf8nJs0ApP0)

## 2.3 Positionnement SI (cartographie)

|  |
| --- |
| **Rédacteurs** : Chapter / Squad  **Lecteurs**  : Tous  **Valideurs**  : Chapter + Archi + sécu  *Le Veolia Cyber Hub (VCH) est intégré au réseau industriel de Veolia Eau France dans un environnement sécurisé en DMZ, garantissant ainsi l’isolement et la sécurité des flux industriels.* |

# 

# 

# 3 Architecture technique

|  |
| --- |
| *Ce chapitre doit décrire l'architecture technique : listes des composants applicatifs de la solution.* |

## 3.1 Schéma

|  |
| --- |
| Schéma d'architecture technique : Faire apparaître les briques applicatives et leurs interactions, Client (device), Module web, Module APP, Module Batch,  ***Attention, il faut adopter un vocabulaire commun sur tout le document (ma brique A s'appelle A sur tout le document)*** |

|  |
| --- |
| L'exemple de schéma ci-dessus doit faire apparaître les petits noms de vos modules (pas de version, pas de port, pas de protocole ⇒ des patates).  Mettre des gommettes sur le schéma avec un explication succincte :   1. Utilisateurs internes (exploitants Usines) , utilisent leurs ordinateurs fixes sous Chrome 2. Flux entre mon application et l'application B : échange d'information sur ... |

## 3.2 Description des briques (Front, Back, Batch, autres)

|  |
| --- |
| *Liste des composants logiciels avec version et date de fin de support* |

### 3.2.1 Mon Appli

|  |
| --- |
| 1. Acteurs :  * Les exploitants usines, qui utilisent des ordinateurs fixes avec un navigateur Chrome. * Briques : * Front :   + Fonction : Interface utilisateur pour l’administration et la gestion des flux.   + Technologie : HTML5, CSS, JavaScript (React ou similaire). * Back :   + Fonction : Gestion des demandes utilisateurs, traitement des données, interactions avec la base de données et services externes.   + Technologie : Node.js, Express, API REST. * Batch :   + Fonction : Collecte des logs et gestion des événements en arrière-plan.   + Technologie : Cron jobs, scripts Python. |

### 3.2.2 Appli A

|  |
| --- |
| Échange d'informations sécurisées avec d'autres services industriels pour assurer la synchronisation des données. |

### 3.2.3 Appli B

|  |
| --- |
| Utilisation pour la gestion des flux externes ou des API d'autres systèmes. |

## 3.3 Optimisation(s)

### 3.3.1 Performances

|  |
| --- |
| *Optimisation des performances :*   * *Cache : Mise en cache des données fréquemment utilisées pour réduire les latences.* * *Scalabilité : Utilisation d'infrastructure cloud pour pouvoir augmenter les ressources en fonction des besoins.* |

### 3.3.2 Financière(s)

|  |
| --- |
| *Optimisation des coûts :*   * *Cloud : Utilisation d’instances réservées pour réduire les coûts à long terme.* * *Automatisation : Mise en place de processus automatiques pour optimiser l’utilisation des ressources.* * *Relation : Utilisation d’un arduino pour la relation véolia france et les petites infrastructures.* |

# 

# 4 Architecture Réseau

|  |
| --- |
| *Ce chapitre décrit tous les aspects liés au réseau. L'objectif est de référencer l'ensemble des ressources réseaux utilisées.* |

## 4.1 Schéma

|  |
| --- |
| *Ce schéma doit faire apparaître :*   * *Les entités (partenaires, aws, gcp, SI …)* * *Les hosted zones* * *Les VPC, les urls, ports, protocols* * *Les couches réseaux (Public, Private admin, Private app)* * *Security group, network ACLs* |

|  |
| --- |
| Ceci est une template que vous pouvez copier.  L'exemple ci-dessous fait apparaître les ports et les protocoles, en fonction de la complexité de vos architectures, vous pouvez avoir plusieurs schémas (soit en zoomant, soit par typologie à afficher …) |

## 4.2 Matrice des flux

***Utiliser le modèle Google sheet ⇒*** [***Modèle “Matrice des flux”***](https://sites.google.com/a/veolia.com/ist-efr-archi-perf/infos-pratiques/liste-des-docs-techniques)

## 4.3 URL sortantes

|  |
| --- |
| *Faire apparaître la liste des url sortantes dans le tableau suivant.* |

## 

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Composant  Impacté** | **Service Description** | **Service URL** | **Authentification Compte / clé / token** | **Commentaires** |
|  |  |  |  |  |

# 

# 5 Infrastructure

|  |
| --- |
| Ressources AWS **:**  *Application : VCH*  *Domaine : Veolia Eau France*  *Chapter : IS&T EFR* |

|  |
| --- |
| **INFRA GCP**  *Pour les projets de type GCP, veuillez renseigner les informations suivantes :*  *Compte Google :*  *ID projet :*  *Lien sur le projet :* |

## 

## **5.1 Production**

|  |
| --- |
| Ressource AWS, Tags :   * Application : * Domaine : * Chapter :   Liens AWS "Groupes de ressources" |

## 5.2 Pré production

|  |
| --- |
| Ressource AWS, Tags :   * Application : * Domaine : * Chapter :   Liens AWS "Groupes de ressources" |

## 5.3 Qualification

|  |
| --- |
| Idem. |

## 5.4 Développement

|  |
| --- |
| idem. |

## 5.5 Autres

|  |
| --- |
| Idem. |

# 

# 

# 6 Sécurité

## 6.1 Coffre fort

|  |
| --- |
| *Est ce que vous utilisez un coffre fort ?*   * *Utilisation d'un coffre-fort pour la gestion des secrets et des clés SSH.* * *Coffre-fort : HashiCorp Vault* * *Accès : Restreint aux administrateurs système.* |

## 6.2 Authentification

### 6.2.1 Procédure de gestion des accès

|  |
| --- |
| *Mécanisme d'authentification :*   * *Provider : LDAP / Active Directory* * *Politique de mot de passe : Complexité requise, expiration tous les 90 jours.* * *Double authentification : Oui, pour l'accès administrateur.* |

### 6.2.2 Providers

|  |
| --- |
| *Liste des types de provider d'authentification.*  *Pour chaque provider, il faut décrire le mécanisme de réinitialisation des mots de passe : existe il une API ?* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Module | Provider | Protocole | Politique de mot de passe | Double authentication |
| WEB ? | Cloudpages / AD / Autres | SAML / Oauth / ... | Oui / non | Oui / non |
|  |  |  |  |  |
|  |  |  |  |  |

### 6.2.3 Gestion des sessions

### 6.2.4 Traçabilité/Auditabilité

## 6.3 Liste des comptes non nominatifs et justifications

### 

|  |
| --- |
| *Pour chaque, il faut décrire le mécanisme de réinitialisation des mots de passe : existe il une API ? préciser si c'est un compte générique.* |

|  |  |  |  |
| --- | --- | --- | --- |
| Module / serveur / service | Compte | Type de droit | Justificatif |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 6.4 Console(s) d’administration

### 

|  |
| --- |
| *Préciser ci-dessous l'existence de console d'administration autres que fonctionnelles qui permettent d'administrer et sur quel environnement la console est activée.* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Module / serveur / service | Console | URL | Fonction | Env. activée ? |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## 6.5 Données à caractères personnelles ou sensibles

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type de stockage | Format des données (fichier, binaire, sql, autre) | Chiffré ? | Nature des données  (contrat, commerciale, client, bancaire,...) | Besoin d’anonymisation sur les autres env. |
|  |  | Oui / non |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## **6.6 Certificat(s)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Usage | Type de certificat | Fournisseur | Date de création | Date de validité | Rotation auto ? |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## 6.7 Plage de maintenance (patching,service managé ou pas)

|  |
| --- |
| Prévoir de préciser également la façon dont l'application doit être arrêtée/redémarrée. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Module | Managé / vm | Plage de maintenance | Indisponibilité |  |  |
|  |  |  | Total / partielle |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# 

# **7 Plan de reprise d'activité**

|  |
| --- |
| **Rédacteurs** : Chapter / Squad & Plateforme  **Lecteurs**  : Tous  **Valideurs**  : Plateforme  *Le PRA repose sur les services cloud d’AWS, avec des mécanismes de bascule automatiques en cas de panne.* |

## 7.1 Périmètre

|  |
| --- |
| Décrire le périmètre de reprise (technique et fonctionnel) |

## 7.2 Processus de bascule

|  |
| --- |
| Décrire le mécanisme de bascule :   * Élément déclencheur * Mécanisme de synchro * Mécanisme de reprise * Mécanisme de retour à l'état initial   Décrire aussi :   * Les fonctions qui ne sont plus couvertes (mode dégradé ?) * Le RPO et le RTO |

## 

# 

# 

# **8 Chargement & Sauvegarde & Archivage**

|  |
| --- |
| **Rédacteurs** : Chapter / Squad & Plateforme  **Lecteurs**  : Tous  **Valideurs**  : Plateforme & Chapter  *Sauvegarde : Mise en place de sauvegardes régulières des configurations et journaux d’activité.*  *Archivage : Archivage des logs et des données critiques pour répondre aux exigences de conformité.* |

## 

## 8.1 Chargement initial et reprise des données

## 8.2 Sauvegarde

## 8.3 Archivage

## **8.4 Purge**

## 8.5 Restauration